Г.М. Михайлов, М.А. Жижченко,
А.М. Чернецов

Повышение безопасности локальной сети учреждения путем внедрения аутентификации устройств

Рекомендуемая форма библиографической ссылки

Михайлов Г.М., Жижченко М.А., Чернецов А.М. Повышение безопасности локальной сети учреждения путем внедрения аутентификации устройств // Научный сервис в сети Интернет: труды XXI Всероссийской научной конференции (23-28 сентября 2019 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2019. — С. 501-510. — URL: http://keldysh.ru/abrau/2019/theses/51.pdf doi:10.20948/abrau-2019-51

Размещена также презентация к докладу

Повышение безопасности локальной сети учреждения путем внедрения аутентификации устройств

Г.М. Михайлов, М.А. Жижченко, А.М. Чернецов

Вычислительный центр им. А.А. Дородницына ФИЦ ИУ РАН

Аннотация. Работа посвящена проблемам реализации безопасности в локальных сетях (ЛВС) научного учреждения в рамках выполнения проекта развертывания новых сегментов, включая беспроводную Wi-Fi–сеть. В представленной работе отражены основные результаты, полученные авторами при решении проблем безопасности при развертывании ЛВС ВЦ ФИЦ ИУ РАН. Из огромного списка накопленных к настоящему времени стандартов, методов и протоколов по обеспечению сетевой безопасности технологий в работе представлено одно из решений проблем по аутентификации устройств с учетом привязки новых подключаемых сегментов и элементов к существующей ЛВС учреждения. В основу решения задачи положен стандарт IEEE 802.1x. Основными средствами этой технологии являются протоколы EAP (Extendable Authentication Protocol - расширенный протокол аутентификации) и сервер RADIUS (Remote Authentication in Dial-In User Service) - протокол для аутентификации, авторизации и сбора сведений об использованных ресурсах между центральной платформой и оборудованием.

Ключевые слова: информационные системы, локальные сети, беспроводные сети, информационная безопасность, ключи защиты, сетевые стандарты защиты информации, аутентификация, авторизация, сетевые протоколы.

Increase the security of the local network of the institution by implementing device authentication

G.M. Mikhailov, M.A. Zhizhchenko, A.M. Chernetsov

Dorodnicyn Computing Center FRC CSC of RAS

Abstract. The work is devoted to the problems of security implementation in local area networks (LAN) of the scientific institution within the framework of the project of deployment of new segments, including wireless Wi–Fi network. The presented work reflects the main results obtained by the authors in solving security

problems in the deployment of LAN of Dorodnicyn Computing Center FRC CSC of RAS. From a huge list accumulated to date standards, methods and protocols to ensure network security technologies, the paper presents one of the solutions to the problems on the authentication of devices, including binding new plug-in segments and elements to an existing LAN companies. The solution is based on the IEEE 802.1x standard. The main means of this technology are EAP (Extendable Authentication Protocol) and RADIUS server (Remote Authentication in Dial-In User Service) - a Protocol for authentication, authorization and collection of information about the used resources between the Central platform and the equipment.

Keywords: information systems, local area networks, wireless networks, information security, security keys, network information security standards, authentication, authorization, network protocols.

Введение

Представленная работа является продолжением серии публикаций по проблемам развития и совершенствования корпоративных локальных сетей, внедрению новых современных аппаратно-программных средств, созданию сегмента беспроводной сети, решению вопросов безопасности и защиты информации [1-4]. При разработке и реализации проекта по развертыванию Wi-Fi - сегмента локальной сети решался комплекс задач, в том числе по выбору топологии сегмента с учетом ее масштабируемости, по выбору производителя сетевого оборудования, по обеспечению контроля доступа к ресурсам сети в соответствии с классами QoS, а также по обеспечению безопасности беспроводной сети на базе протокола WPA2 (Wireless Protected Access ver.2) [1]. В этой же работе дано обоснование развертывания трех Wi-Fi-сегментов сети с разными идентификаторами SSID (Service Set Identifier) и уровнями доступа: сеть CCAS_GUEST (гостевая), сеть CCAS_EMP (корпоративная) и сеть CCAS_SER (управления). Протокол WPA2 обеспечивает самый высокий уровень защиты данных и контроль доступа в беспроводную сеть для корпоративных (WPA2-Enterprise) и индивидуальных пользователей (WPA2-Personal). Заметим, что WPA2- это вторая версия набора алгоритмов и протоколов, обеспечивающих защиту данных в беспроводных сетях Wi-Fi. В нем предусмотрено, в частности, обязательное использование более мощного алгоритма шифрования AES (Advanced Encryption Standard) и аутентификации 802.1x. В данной работе будет представлено описание технологии обеспечения безопасности сети при подключении к ней пользовательских устройств, а также контроля соответствия их конфигураций правилам доступа к корпоративным ресурсам. Эта задача здесь решается применительно к проводному сегменту корпоративной сети учреждения.

Основная часть

802.1x, - стандарт, который работает совместно с EAP (Extendable Authentication Protocol - расширенный протокол аутентификации) и описывает,

как взаимодействуют пользователь и сервер аутентификации в сети передачи данных [5]. Благодаря стандарту 802.1x можно предоставить пользователям права доступа к корпоративной сети и ее сервисам в зависимости от группы политики безопасности, выделяемой сервером RADIUS, к которой привязана учетная запись пользователя или рабочей станции. Рекомендуемые схемы развертывания корпоративных и частных сетей VPN, реализующих технологию NAC (Network Admission Control), в данное время представлены в печати достаточно широко. Большинство из них – это учебно-методические материалы, аналитика, отдельные работы по загрузке и настройке 802.1x на оборудованиях различных производителей. В нашей работе мы представляем решение этой проблемы применительно к корпоративной сети научного учреждения, включающей в себя порядка 400 и более пользователей, имеющих разрешенный доступ к ресурсам разного уровня сети с 600 и более компьютеров разного класса. Важнейшим фактором при этом является прохождение аудита всей инфраструктуры сети в части проводного сегмента, проведенного с привлечением внешней организации. Основные результаты, полученные в процессе аудита, изложены в работе [3]. Последующее вслед за аудитом внедрение NAT-технологии проводилось с соблюдением сохранности всей полноты функциональности локальной сети, а также средств обеспечения ее защиты и безопасности. Сеть защищена межсетевым экраном (firewalls), выполняющим все предусмотренные правила фильтрации исходящих и входящих пакетов и действий над ними.

Следующим этапом функционального и структурного расширения сети стало создание беспроводного Wi-Fi – сегмента [1]. В этом сегменте обеспечивается поддержка стандартов аутентификации, авторизации и учета пользователей на базе 802.1x, RFC 2865 RADIUS Authentication, RFC 2866 Accounting, RFC 2867 Tunnel Accounting, Web-based Authentication. Так как проект Wi-Fi – сегмента разрабатывался с «чистого листа», при его исполнении не было проблем, затрагивающих изменений в структуре проводного сегмента, за исключением завершающего этапа стыковки обоих сегментов в единую сеть. Одним из важнейших свойств сети, выполненных на перечисленных выше стандартах, является возможность реализации групповой политики, которая позволяет строить алгоритмы и процедуры предоставления прав доступа пользователям сети к ее сервисам и ресурсам зависимости от принадлежности пользователя к той или иной группе. В рамках беспроводного сегмента сети Wi-Fi эта проблема решена созданием трех подсетей: GUEST (гостевая), _EMP (корпоративная) и _SER (управления).

Применительно к корпоративной сети в целом все подключаемые к ней пользовательские устройства должны удовлетворять требованиям безопасности, а конфигурации этих устройств должны соответствовать принятым правилам доступа к ресурсам сети. В работе [6] представлен обзор современных технологий, которые отражены в решениях Cisco Network Admission Control (Cisco NAC), Symantec NAC (Symantec Access Control) и

Microsoft NAP (Microsoft Network Protection) и Juniper Networks Unified Access Control. Как указано в этой работе, ни одно из перечисленных выше решений не может реализовано без привлечения Microsoft NAP. Таким образом, в реализации любое решение – это гибрид. Пример практической реализации модели технологии NAP представлен в статье [7]. В настоящее время на рынке данного профиля появились более современные решения. Пример одного из таких решений представлен в работе [8], где изложен вариант реализации виртуальной модели на новой технологии Cisco – Identity Services Engine (ISE) взамен известной технологии Cisco ACS (Access Control Server). При всей убедительности перечисленных выше решений, эти технологии должны закладываться на стадии проектирования корпоративных сетей. Решения же по внедрению дополнительных средств обеспечения безопасности доступа к ресурсам уже функционирующих распределенных сетей учреждений с учетом их конфигураций, оборудования, установленных в сетях групповых политик имеют свои особенности, но в любом исполнении они базируются на общепринятых концепциях стандарта 802.1x.

В стандарте 802.1x определены три основных элемента:

- supplicant – пользователь (аппликант), который нуждается в сетевой аутентификации;
- authentication server – обычно RADIUS- сервер, который производит фактическую аутентификацию;
- authenticator – сетевое устройство, находящееся между аппликантом и сервером аутентификации и предоставляющее доступ в сеть, например, точка доступа AP или Ethernet- коммутатор

Ключевым элементом в этом решении является RADIUS-сервер. Он позволяет аутентификаторам оперировать большим количеством устройств (пользователей) которые нуждаются в аутентификации и выдаче им ресурсов в соответствии с политиками, установленными в организации. Данные по политикам RADIUS-сервер может брать из любого хранилища информации (файл, LDAP, MS AD, MySQL и т. д.). В действующей сети ВЦ РАН используется MS Active Directory (AD). В нашей работе для построения и реализации предлагаемой модели, базирующейся на оборудовании Cisco Systems, используются следующие компоненты сетевых элементов:

- коммутаторы, выполняющие функции аутентификатора (Cisco Systems);
- freeRadius [9];
- DHCP - сервер;
- аппликант (клиент) 802.1x на рабочей станции пользователя.

Настройка IEEE 802.1x аутентификации – процедура сложная, кропотливая и требует профессионального подхода к решению ряда задач. Она включает в себя следующие составляющие:

- настройку коммутаторов;

- настройку сервера RADIUS;
- настройку клиента.

Каждое из перечисленных составляющих – это пошаговое выполнение ряда процедур в режиме создания конфигурации, настройки связи с сервером RADIUS, настройки отдельного порта, настройки VLAN, выполнение общекомандного блока интерфейса Gigabit Ethernet и др. В рамках ограничений печатных объемов статьи описание всего процесса пошаговой настройки по перечисленным выше разделам не представляется. К тому же это описание не может быть универсальным в принципе, так как каждая схема привязана к реальной конфигурации сети и выбора решения, описанного выше.

Только после успешного проведения указанных выше операций можно приступить к авторизации пользователя по его учетным данным в AD или в другой базе данных, например, MySQL или в других файлах. При отсутствии авторизации порт на коммутаторе переходит либо в гостевой VLAN, либо порт блокируется до момента успешной авторизации. При авторизации возможно несколько сценариев в зависимости от ответа RADIUS - сервера:

- включить порт в VLAN, который настроен на порту;
- прописать VLAN, который пришлет RADIUS – сервер;
- прописать пользовательский список доступа ACL, который также выдает RADIUS - сервер.

Для запуска этой системы необходимо на коммутаторах включить аутентификацию и учет (accounting). После чего следует включить dot1x и настроить доступ к RADIUS - серверу на портах, предназначенных для пользователей сети и иных служб.

Проведение работ подобного масштаба на действующей корпоративной сети, требующих внесения значительных дополнений и ее реконфигурации в соответствии с теми стандартами и протоколами, которые изложенными выше, практически невозможно без разработки соответствующих моделей или виртуальной машины. В рамках создания и тестироаания такой модели применительно к действующей сети в нашем решении создается тестовый сегмент-модель. Для этого сегмента на этапе проведения отладочных работ не будут использоваться данные Active Directory действующей сети. Авторизация пользователей в этом сегменте будет происходить с использованием данных из текстового файла. Фрагменты текстового сегмента представлены ниже.

Выдача VLAN от freeRadius
в секции post-auth файла /sites-enabled/default
update reply {
Tunnel-Type :=”VLAN”
Tunnel-Medium-Type :=”IEEE-802”
Tunnel-Private-Group-ID:1=”100”
}

файл users

```
user1 Cleartext-Password := "test8021x1"
Tunnel-Type:1 = VLAN
Tunnel-Medium-Type:1 = IEEE-802
Tunnel-Private-Group-ID:1 = "100"

/eap.conf
peap {
  ...
  use_tunneled_reply = yes
  ...
}
```

Далее представлено наше решение для тестового участка с авторизацией по 802.1x.

```
Cisco40-4(config)#vlan 22
Cisco40-4(config-vlan)#name SERVER
Cisco40-4(config-vlan)#vlan23
Cisco40-4(config-vlan)#name GROUP 1
Cisco40-4(config-vlan)#vlan 24
Cisco40-4(config-vlan)#name GROUP 2
Cisco40-4(config-vlan)#vlan 25
Cisco40-4(config-vlan)#name GUEST_and_AUTHFAIL
Cisco40-4(config-vlan)#exit
Cisco40-4(config)#interface vlan 22
Cisco40-4(config-if)#ip address 172.16.2.1 255.255.255.0
Cisco40-4(config-if)#no shut
 Адрес шлюза для RADIUS-сервера.
Cisco40-4(config-if)#interface vlan 23
Cisco40-4(config-if)#ip address 172.16.3.1 255.255.255.0
Cisco40-4(config-if)#no shut
 Адрес шлюза для клиентов VLAN 23.
Cisco40-4(config-if)#interface vlan 24
Cisco40-4(config-if)#ip address 172.16.4.1 255.255.255.0
Cisco40-4(config-if)#no shut
 Адрес шлюза для клиентов PC в VLAN 24.
Cisco40-4(config-if)#interface vlan 25
Cisco40-4(config-if)#ip address 172.16.5.1 255.255.255.0
Cisco40-4(config-if)#no shut
 Адрес шлюза для клиентов PC в VLAN 25.
Cisco40-4(config-if)#exit Cisco40-4(config)#ip routing
 Активация IP-маршрутизации между VLAN.
Cisco40-4(config)#interface fastEthernet 0/24
Cisco40-4(config-if)#switchport mode access
```

Cisco40-4(config-if)#switchport access vlan 22
!Выделенная VLAN для RADIUS-сервера.
Cisco40-4(config)#interface range fastEthernet 0/1 , fastEthernet 0/4
Cisco40-4(config-if-range)#switchport mode access
Cisco40-4(config-if-range)#dot1x port-control auto
Активирование аутентификации IEEE 802.1x на порте.
Cisco40-4(config-if-range)#dot1x host-mode multi-domain
Разрешение для хоста ! режима аутентификации на порте, авторизованном
в соответствии с IEEE 802.1x.
Cisco40-4(config-if-range)#dot1x guest-vlan 25
Cisco40-4(config-if-range)#dot1x auth-fail vlan 25
Функции гостевой VLAN и ограниченной VLAN применимы только
на порте, для которого активирована аутентификация MDA.
Cisco40-4(config-if-range)#dot1x reauthentication
Активация периодической повторной аутентификации клиента.
Cisco40-4(config-if-range)#dot1x timeout reauth-period 60
! Установка количества секунд между попытками повторной аутентификации.
Cisco40-4(config-if-range)#dot1x auth-fail max-attempts 2
Указание количества разрешенных попыток аутентификации перед тем, как порт переходит в ограниченную VLAN.
Cisco40-4(config-if-range)#exit
Cisco40-4(config)#interface range fastEthernet 0/2 - 3
Cisco40-4(config-if-range)#switchport mode access
Cisco40-4(config-if-range)#dot1x port-control auto
По умолчанию порт, авторизованный в соответствии с 802.1x, позволяет
функционировать только с одним клиентом.
Cisco40-4(config-if-range)#dot1x guest-vlan 25
Cisco40-4(config-if-range)#dot1x auth-fail vlan 25
Cisco40-4(config-if-range)#dot1x reauthentication
Cisco40-4(config-if-range)#dot1x timeout reauth-period 60
Cisco40-4(config-if-range)#dot1x auth-fail max-attempts 2
Cisco40-4(config-if-range)#spanning-tree portfast
Cisco40-4(dhcp-config)#ip dhcp pool GROUP_1
Cisco40-4(dhcp-config)#network 172.16.4.0 255.255.255.0
Cisco40-4(dhcp-config)#default-router 172.16.4.1
С помощью этого пула назначается IP-адрес для клиентов PC в GROUP_1.
Cisco40-4(dhcp-config)#ip dhcp pool GROUP_2
Cisco40-4(dhcp-config)#network 172.16.5.0 255.255.255.0
Cisco40-4(dhcp-config)#default-router 172.16.5.1

С помощью этого пула назначается IP-адрес для клиентов PC в GROUP_2.

Cisco40-4(dhcp-config)#exit
Cisco40-4(config)#ip dhcp excluded-address 172.16.3.1
Cisco40-4(config)#ip dhcp excluded-address 172.16.4.1
Cisco40-4(config)#ip dhcp excluded-address 172.16.5.1
Cisco40-4(config)#aaa new-model
Cisco40-4(config)#aaa authentication dot1x default group radius

Должен использоваться стандартный список методов.

В противном случае dot1x не работает.

Cisco40-4(config)#aaa authorization network default group radius

Чтобы работать с RADIUS, необходима авторизация для назначения динамической VLAN.

Cisco40-4(config)#radius-server host 172.16.2.201 key CisCo123

Ключ должен соответствовать ключу, используемому на сервере RADIUS. Cisco40-4(config)#dot1x system-auth-control

Пример настройки клиентов ПК для использования аутентификации по стандарту 802.1x представлен ниже. Этот пример относится исключительно к клиенту Расширяемого Протокола Аутентификации (EAP) Microsoft Windows XP через LAN (EAPOL):

1. Выбрать Start > Control Panel > Network Connections, а затем нажать правой кнопкой мыши Local Area Connection и выберите Properties.
2. Убедиться, что на вкладке General установлен параметр Show icon in notification area when connected (при подключении показывать значок в области уведомлений).
3. На вкладке Authentication установить Enable IEEE 802.1x authentication for this network (включить аутентификацию IEEE 802.1x для этой сети).
4. Установить тип EAP: MD5-Challenge.

Для настройки клиентов на получение IP-адреса с сервера DHCP, выполните следующие действия:

1. Выбрать Start > Control Panel > Network Connections, а затем нажать правой кнопкой мыши Local Area Connection и выберите Properties.
2. На вкладке General нажать Internet Protocol (TCP/IP), а затем – Properties.
3. Выбрать Obtain an IP address automatically (получить IP-адрес автоматически).

Заключение

В настоящей работе представлены основные результаты внедрения стандартов безопасности 802.1x применительно к проводному сегменту ЛВС Центра. В основу реализации проекта положена AAA-технология, которая базируется на стандартах аутентификации IEEE 802.1x, а также на множестве

протоколов, в том числе EAP (EAPOL) и RADIUS. Отличительной особенностью представленной работы является то обстоятельство, что указанные выше стандарты и протоколы были реализованы при развертывании Wi-Fi-сегмента локальной сети [1], который успешно и надежно функционирует в составе сети в целом. Однако сетевая инфраструктура и аутентификация проводного сегмента ЛВС - это отдельная самостоятельная работа, требующая строгого и продуманного подхода к внедрению новых разработок, в том числе и в частности AAA - технологии. Одним из главных требований при этом является принцип сохранения и обеспечения режима полного сервиса для пользователей сети, а также его непрерывности в условиях постоянной эксплуатации всего телекоммуникационного комплекса учреждения. С учетом этих условий наиболее оптимальным решением представляется поэтапное выполнение всей совокупности работ по данной теме. Первый этап – это создание тестовой модели сетевой аутентификации и авторизации пользователей с использованием RADIUS. Тестовая модель создается для ограниченного круга пользователей-клиентов, включая административный персонал – Default Device Admin и группу пользователей – Default Network Access. Данная модель является основой для полной схемы аутентификации, авторизации и учета через RADIUS. После успешной апробации тестовой модели будет продолжен этап практической реализации внедрения разработанной технологии по отношению ко всему проводному сегменту ЛВС. Полученные к настоящему времени результаты относятся только к экспериментальной группе пользователей модельной структуры. Содержание представленной работы будет скорректировано и дополнено по результатам, полученным после внедрения модели в общую схему локальной сети.

Литература и источники

1. Михайлов Г.М., Жижченко М.А., Чернецов А.М. Опыт организации единой беспроводной сети научного учреждения // Научный сервис в сети Интернет: труды XX Всероссийской научной конференции (17-22 сентября 2018 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2018. —528 с. ISBN 978-5-98354-046-0. С.387-394 https://doi.org/10.20948/abrau-2018-5.
2. Михайлов Г.М., Жижченко М.А., Чернецов А.М. Обеспечение плавной перенумерации сети при смене провайдера // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18-23 сентября 2017 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2017. —С. 351-355. — URL: http://keldysh.ru/abrau/2017/44.pdf.
3. Михайлов Г.М., Рогов Ю.П., Чернецов А.М. Организация почтового IMAP сервера в научной организации // Труды XVIII Всероссийской научной конференции "Научный сервис в сети интернет", Новороссийск,19 по 24 сентября 2016 г. ИПМ им. М.В. Келдыша РАН. (РИНЦ) С. 271-273. ISBN 978-5-98354-027-9.

4. Рогов Ю.П., Чернецов А.М. Аппаратно-программные средства и развитие инфраструктуры ИВС ВЦ РАН. — М,: ВЦ РАН, 2010. 120 с.
С. 271-273. — URL: http://keldysh.ru/abrau/2016/2.pdf.
5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: 2012. – С. 960
6. https://www.anti-malware. ru/node/1043
7. https://www.osp.ru/winitpro/2008/04/5291530/
8. https://www. easyit.com/2017/08/
9. https://freeradius.org/