МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ по дисциплине
«Технологии построения защищенных компьютерных сетей»
для студентов направления подготовки
10.04.01 Информационная безопасность

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Ставрополь

СОДЕРЖАНИЕ

Методические указания к лабораторным работам

РАЗДЕЛ 1. ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Лабораторная работа №1 Аудит безопасности (4 часа)

Содержание:

1. Аудит безопасности протокола SNMP
2. Аудит безопасности протокола STP

Цель работы:

Изучение способов мониторинга и управления сетью на основе протокола SNMP с использованием собственных механизмов безопасности. Изучение уязвимостей алгоритма Spanning Tree и Rapid Spanning Tree.

Теоретические сведения:

Протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью) является протоколом Прикладного уровня, разработанный для выполнения двух задач: мониторинг сетевых устройств и сети в целом; управление сетевыми устройствами. Протокол SNMP предоставляет возможность станциям управления считывать и изменять настройки шлюзов, маршрутизаторов, коммутаторов и прочих сетевых устройств.

1.2. Версии протокола SNMP Опишем различия между версиями протокола SNMP и документы, определяющие эти версии. По состоянию на 2006 год единственной не устаревшей версией SNMP является SNMPv3, определённая в RFC 3411-3418.

SNMPv1 Первые RFC, описывающие стандарты SNMP, появились в 1988 году. Версия 1 подверглась критике за её посредственную модель безопасности на основе сообществ. В то время безопасность в Интернете не входила в круг первоочередных задач рабочих групп IETF.

SNMPv2 Версия 2, известная так же, как Party-based SNMPv2, или SNMPv2p, не получила широкого распространения из-за серьёзных разногласий по поводу инфраструктуры безопасности в стандарте. SNMPv2 улучшал версию 1 в области быстродействия, безопасности, конфиденциальности и взаимодействий «менеджер-менеджер». Он представил новый тип PDU Get-Bulk-Request, альтернативу Get-Next-Request для получения больших объёмов информации при помощи одного запроса. Тем не менее, новая система безопасности на основе сторон выглядела для многих как чересчур сложная и не была широко признана.

SNMPv2c Community-based SNMPv2, или SNMPv2c, представил SNMPv2 без новой модели безопасности версии 2. Вместо неё предлагалось использовать старую модель безопасности версии 1 на основе сообществ. Соответствующее предложение RFC было принято только как черновик стандарта, однако стало де факто стандартом SNMPv2. Безопасность SNMP снова оказалась нерешённым вопросом.

SNMPv2u User-based SNMPv2, или SNMPv2u, является компромиссом между незащищённостью SNMPv1 и чрезмерной сложностью SNMPv2p. Предложенная модель безопасности на основе пользователей была положена в основу SNMPv3.

Виртуальная ЛВС (VLAN, Virtual LAN) – логическая группа компьютеров в пределах одной реальной ЛВС, за пределы которой не выходит любой тип трафика (широковещательный [broadcast], многоадресный [multicast] и одноадресный [unicast]). За счет использования VLAN администратор сети может организовать пользователей в логические группы независимо от физического расположения рабочих станций этих пользователей.

Основные цели введения виртуальных сетей в коммутируемую среду: повышение полезной пропускной способности сети за счет локализации широковещательного

(broadcast) трафика в пределах виртуальной сети; повышения уровня безопасности сети за счет локализации одноадресного (unicast) трафика в пределах виртуальной сети; формирование виртуальных рабочих групп из некомпактно (в плане подключения) расположенных узлов; улучшение соотношения цены/производительности по сравнению с применением маршрутизаторов.

Устройства связываются в виртуальные сети на основе портов коммутатора, к которым они физически подключены. То есть каждой порт коммутатора включается в одну или более виртуальных сетей. К достоинствам данного типа виртуальных сетей можно отнести высокий уровень безопасности и простоту в настройке. К недостаткам можно отнести статичность данного типа виртуальных сетей. То есть при подключении компьютера к другому порту коммутатора необходимо каждый раз изменять настройки VLAN.

Сеть на базе маркированных кадров (IEEE 802.1Q VLANs) В отличие от двух предыдущих типов виртуальных сетей VLAN на основе маркированных кадров могут быть реализованы на двух и более коммутаторах. В заголовок каждого кадра Ethernet вставляется маркер, который идентифицирует членство компьютера в определенной VLAN.

Задание для выполнения работы:

Аудит безопасности протокола SNMP

1. Постройте топологию сети, показанную на рисунке 1.

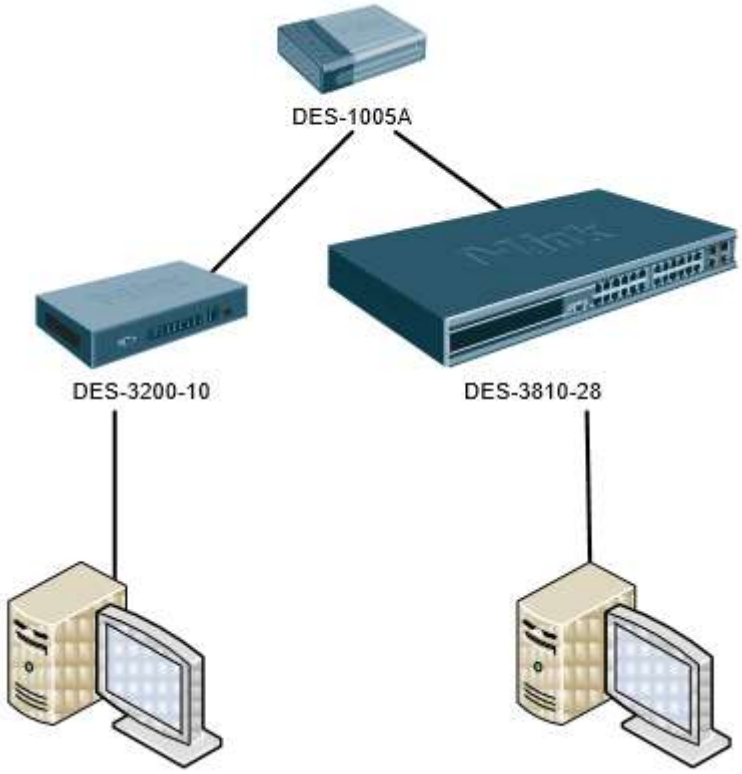


Рис.1.

2. Изучите раздел «Протокол SNMP» теоретического пособия.

3. Настройте SNMP-протокол на коммутаторах.

4. Изучите раздел «Утилиты управления сетью по протоколу SNMP» в пособие по операционной системе Linux.

5. Запустите утилиту iReasoning MIB Browser.

6. Загрузите базу MIB RFC-1213.

7. На обоих коммутаторах (DES-3200-10 и DES-3810-28) выясните следующие параметры:

- название устройства, время работы устройства, службы, запущенные на устройстве (ветвь system);

- количество интерфейсов на устройстве, содержимое таблицы интерфейсов, назначение двух дополнительных виртуальных портов (ветвь interfaces);

- IP-адрес устройства, содержимое таблицы маршрутизации (ветвь ip);
- TCP-соединения, установленные устройством (ветвь tcp).

8. Загрузите базы MIB Time, DES-3200-10-L2MGMT с официального сайта компании DLink.

9. Определите текущее системное время коммутатора.

10. Определите состояния портов коммутатора (база DES-3200-10-L2MGMT, ветвь swL2PortInfoTable, таблица swL2PortMgmt).

Аудит безопасности протокола STP

1. Изучите раздел «Аудит безопасности протокола связующего дерева STP» теоретического пособия и раздел «L2 Features»/«Spanning Tree» коммутатора 320010 в пособие по управлению стендом.

2. Соберите сеть с топологией, представленной на рисунке 2.

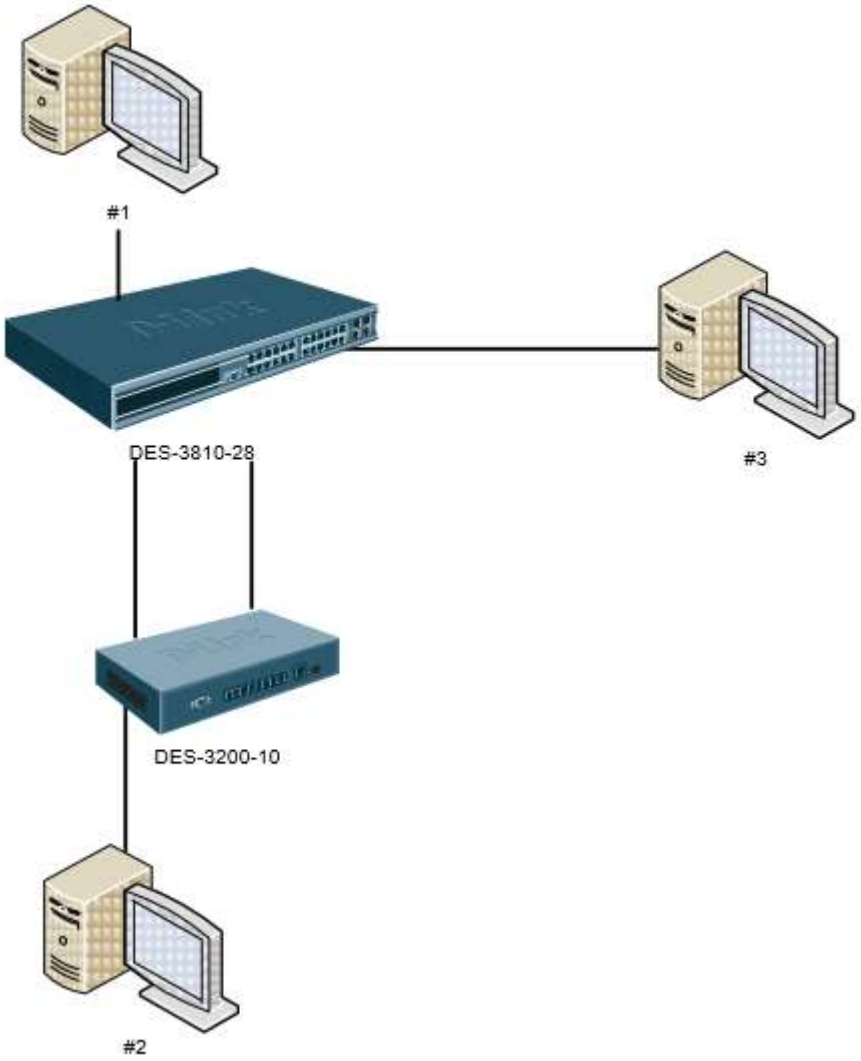


Рис.2.

3. Настройте и активизируйте на коммутаторах протокол Spanning Tree (замечание: по причине недоработки компанией D-Link программного обеспечения коммутатора DES-3810-28 приоритет коммутатора на данной модели выставить невозможно. Поэтому приоритет коммутатора DES-3810-28 постоянен и равен 32768, что не мешает выполнению лабораторной работы).

4. Параллельно с шагом 3 запустите на машине #3 утилиту tcpdump и выясните MACадреса коммутаторов, анализируя содержимое пактов BPDU.

5. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Контрольные вопросы:

Базовый уровень:

1. Назначение протокола SNMP
2. Базовые утилиты управления сетью.

Повышенный уровень:

3. Особенности SNMPv2
4. Уязвимости протокола STP.

Лабораторная работа №2 Виртуальные локальные сети IEEE 802.1q (4 часа)

Содержание:

1. Виртуальные локальные сети IEEE 802.1q

Цель работы:

Изучение технологий виртуальных сетей. Получение навыков настройки VLAN на основе тэгов IEEE 802.1q в сети, построенной на коммутаторах D-Link.

Теоретические сведения:

Сети VLAN на основе маркированных кадров могут быть реализованы на двух и более коммутаторах. В заголовок каждого кад-ра Ethernet вставляется маркер, который идентифицирует членство компьютера в опре-деленной VLAN. На рисунке 3 показан пример такой VLAN.

Механизмы добавления идентифицирующего маркера в заголовок кадра Ethernet

Маркеры с номером VLAN в виртуальных сетях 802.1Q могут быть добавлены:

- явно, если сетевые карты поддерживают стандарт IEEE 802.1Q, и на этих картах включены соответствующие опции, то исходящие кадры Ethernet от этих карт бу-дут содержать маркеры идентификации;
- неявно, если сетевые адаптеры, подключенные к этой сети, не поддерживают стандарт IEEE 802.1Q, то добавление маркеров выполняется на коммутаторе на основе группировки по портам.

Предположим, что некоторые порты коммутатора сгруппированы в VLAN. Коммутатор с поддержкой IEEE 802.1Q будет добавлять маркер к входящим на этот порт кадрам Ethernet с соответствующим ID VLAN. Но эти маркеры будут удаленны коммутатором из исходящих с этих же портов кадров, чтобы конечные компьютеры могли разобрать заго-ловок кадра Ethernet. 42

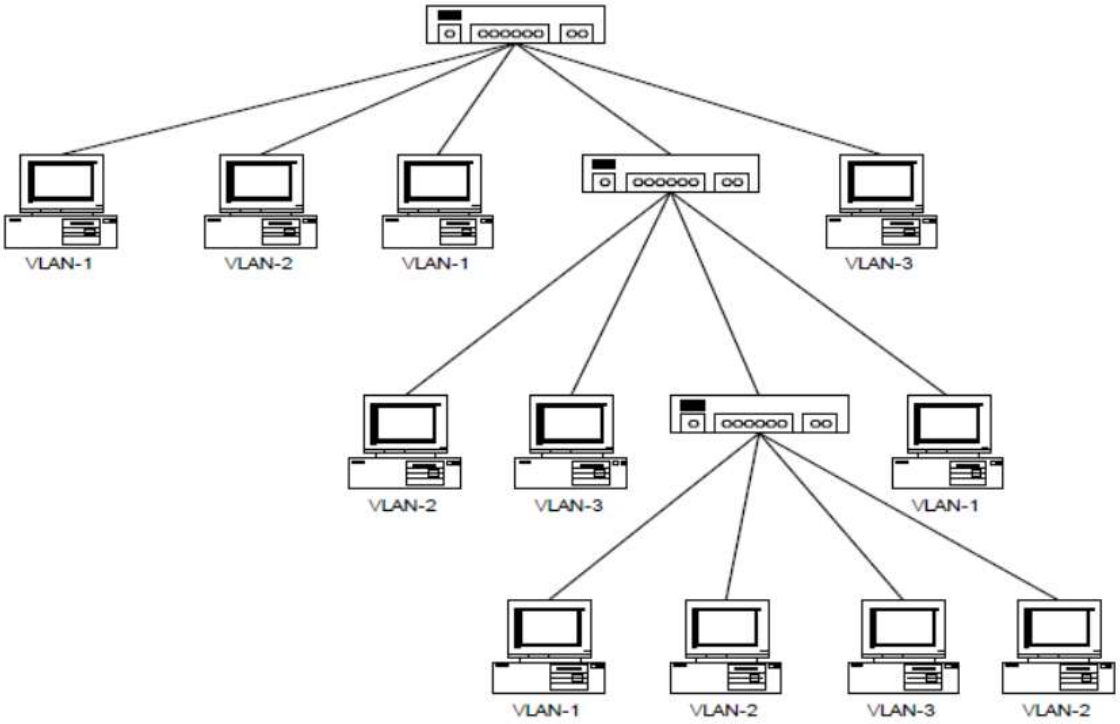


Рис.3 Виртуальная сеть на основе нескольких коммутаторов с использованием стандарта IEEE 802.1Q.

Если идентификация VLAN маркерами протокола 802.1Q была осуществлена обоими способами – явно и неявно, входящие кадры к портам коммутатора могут состоять из обоих типов кадров (с маркерами и без). В этой ситуации к неотмеченным входящим кадрам будут добавляться маркеры. В то время как маркированные кадры уже поддерживают членство в явно определенной виртуальной сети. Способность VLAN 802.1Q извлечения маркеров из заголовков кадров Ethernet позволяет VLAN работать с существующими коммутаторами и сетевыми адаптерами, которые не распознают маркеры. Способ-ность добавления маркеров позволяет VLAN распространяться через множество 802.1Q-совместимых коммутаторов.

Компоненты конфигурации виртуальной сети на основе тэгов

Необходимо понять суть двух ключевых переменных для настройки VLAN 802.1Q:

- Port VLAN ID (PVID, идентификатор номера порта);
- VLAN ID (VID, идентификатор номера VLAN).

Обе переменные назначаются для одного и того же порта коммутатора, но между ними имеется существенная разница.

Пользователь может назначить ТОЛЬКО ОДИН номер PVID для каждого порта. Номер PVID определяет, к какой VLAN принадлежит данный порт. Когда ИЗ СЕТИ на порт ком-мутатора поступает НЕМАРКЕРОВАННЫЙ пакет, то принадлежность данного пакета к определенной VLAN осуществляется как раз на основе номера PVID порта. Номер PVID вставляется в заголовок кадра Ethernet и идентифицирует членство пакета в одной опре-деленной VLAN. Необходимо отметить важный момент: если пакет уже содержит маркер (заданный явно сетевой картой компьютера или заданный неявно на другом коммутато-ре), то повторная маркировка пакета, поступающего из вне на какой-либо порт коммута-тора, НЕ производится. 43

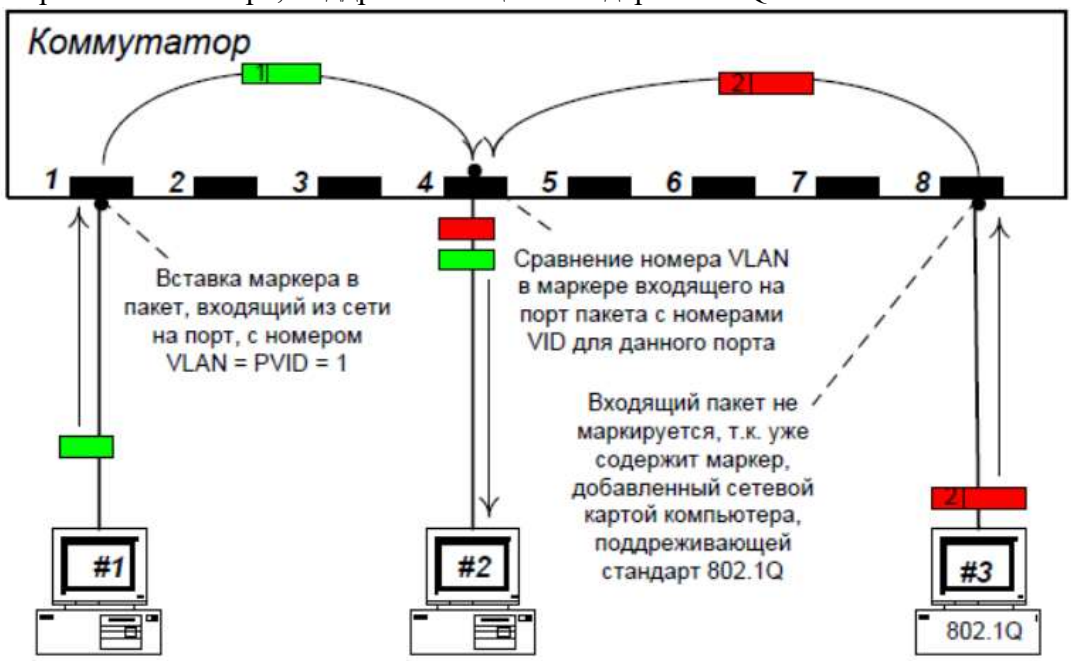
С другой стороны, можно задать МНОЖЕСТВО идентификаторов VID для одного и того же порта. Данные идентификаторы определяют, пакеты каких виртуальных сетей

может принимать данный порт. Данная проверка осуществляется, когда пакет УЖЕ ПОЛУЧЕН ИЗ СЕТИ и МАРКИРОВАН, во время процедуры перенаправления пакета с порта на порт ВНУТРИ коммутатора.

Построение виртуальных сетей 802.1Q на одном коммутаторе

Рассмотрим следующую модель (рисунок 4), которая помогает понять принцип работы виртуальных сетей 802.1Q. В данном примере порт #1 является членом VLAN #1, а порты #4 и #8 являются членами VLAN #2. При этом порт #1 может принимать входящие пакеты только из своей VLAN, то есть только из первой VLAN. Порт #4 может принимать входя- щие пакеты из обоих VLAN (первой и второй). Порт #8, также как первый порт, может принимать входящие пакеты только из своей VLAN (второй). В результате полноценно функционировать в данной сети смогут только машины #2 и #3. Машины #1 и #2 не смогут обмениваться информацией, так как порт #4 может принимать пакеты с порта #1, но не наоборот.

Коммутатор 1 2 3 4 5 6 7 8 PVID Номер порта 122 148 VID Номера портов 12 1,4 4,8 #1 #2 #3 802.1Q 2 2 1 Вставка маркера в пакет, входящий из сети на порт, с номером VLAN = PVID = 1 Сравнение номера VLAN в маркере входящего на порт пакета с номерами VID для данного порта Входящий пакет не маркируется, т.к. уже содержит маркер, добавленный сетевой картой компьютера, поддреживающей стандарт 802.1Q



PVID	Номер порта
1	1
2	4
2	8

VID	Номера портов
1	1,4
2	4,8

Рис. 4 Модель функционирования виртуальной сети 802.1Q на одном коммутаторе

Построение виртуальных сетей 802.1Q на нескольких коммутаторах

Как уже отмечалось, виртуальные сети 802.1Q могут быть построены на нескольких ком- мутаторах и охватывать всю локальную сеть. При этом все коммутаторы сети должны поддерживать стандарт 802.1Q. Необходимо понять следующие важные термины:

- Маркировка (Tagging) – процесс вставки информации о виртуальной сети 802.1Q в заголовок кадра Ethernet. Порт, для которого включен режим маркировки, будет оставлять без изменения заголовок ИСХОДЯЩЕГО С КОММУТАТОРА В СЕТЬ па- кета

Ethernet, то есть будет оставлять в нем маркер 802.1Q. Подобная возмож- ность необходима для связи двух устройств, поддерживающих стандарт 802.1Q.

- Демаркировка (Untagging) – процесс удаления информации о виртуальной сети 802.1Q из заголовка кадра Ethernet. Порт, для которого включен режим демаркировки, будет удалять маркер из заголовка пакета, ИСХОДЯЩЕГО С КОММУТАТО-РА В СЕТЬ. Подобная возможность необходима для связи коммутатора и устрой-ства, не поддерживающего стандарт 802.1Q.
- Входящий порт (Ingress Port) – порт коммутатора, на который поступают пакеты из сети. Для каждого порта можно настроить фильтр Ingress Filter. Если этот фильтр отключен (состояние Disabled) то порт функционирует в обычном режиме, то есть проверка пакета на принадлежность какой-либо VLAN (сравнение номера VLAN пакета с номерами VID порта) производится при поступлении пакета на данный порт с другого порта ВНУТРИ коммутатора (как это показано на рисунке 4). При включении фильтра (состояние Enabled) данная проверка ДОПОЛНИТЕЛЬНО про-изводится для любого маркированного пакета, входящего на данный порт ИЗ СЕ-ТИ.

Исходящий порт (Egress Port) – порт коммутатора, с которого пакеты выходят в сеть и при этом необходимо принять решение о маркировке/демаркировке пакета.

С учетом всего ниже приведена расширенная модель функционирования виртуальной сети 802.1Q на основе нескольких коммутаторов (рисунок 5).

Преимущества виртуальных сетей 802.1Q

Дополнительное преимущество VLAN 802.1Q заключается в том, что можно изменять то-пологию сети без физического перемещения станций или изменения кабельных соедине-ний. Станции можно назначить другую VLAN и, соответственно, общаться и совместно использовать ресурсы с членами в новой VLAN просто изменив настройки порта с одной VLAN (например, VLAN отдела продаж) на другую (VLAN отдела маркетинга). Таким об-разом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании се-ти. Следует отметить, что в современных коммутаторах поддерживается единственный тип VLAN – тэгированные виртуальные сети. 45

Коммутатор 1 2 3 4 5 6 7 8 Вставка маркера в пакет, входящий из сети на порт, с номером VLAN = PVID = 1 Сравнение номера VLAN в маркере входящего на порт пакета с номерами VID для данного порта Входящий пакет не маркируется, т.к. уже содержит маркер, добавленный другим коммутатором 1 Коммутатор 1 2 3 4 5 6 7 8 Сравнение номера VLAN в маркере входящего на порт пакета с номерами VID для данного порта 1 Ingress Filter is Enabled Дополнительное сравнение номера VLAN в маркере входящего на порт пакета с номерами VID для данного порта 1 Tagging Для порта включен режим маркировки, поэтому маркер не удаляется из исходящего пакета Untagging Для порта включен режим демаркировки, поэтому маркер удаляется из исходящего пакета

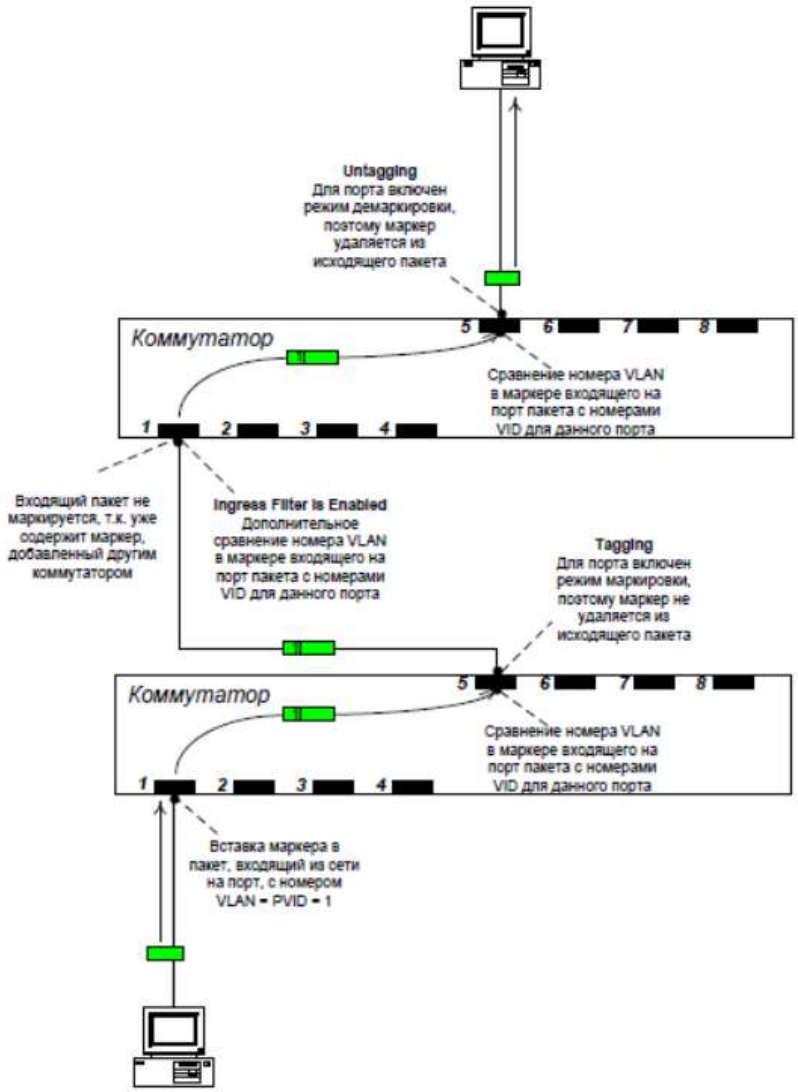


Рис. 5 Модель функционирования VLAN 802.1Q на нескольких коммутаторах.

Задание для выполнения работы:

1. Изучите раздел «Виртуальные сети. Сети на базе маркированных кадров» теоретического пособия и раздел «L2 Features»/«802.1Q Static VLAN» коммутатора 3200-10 в пособие по управлению стендом.
2. Постройте топологию сети, представленную на рисунке 6.

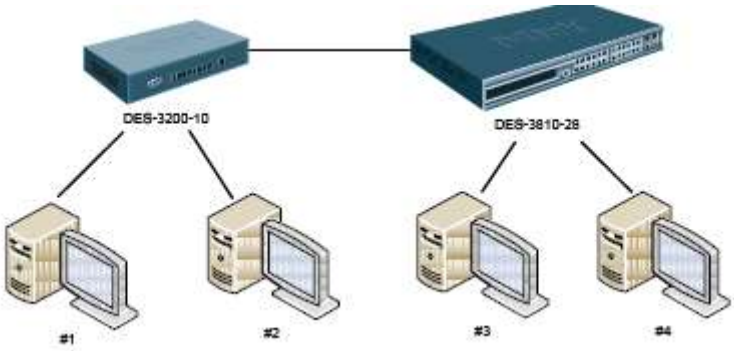


Рисунок 6. Коммутируемая топология для настройки виртуальных сетей VLAN.

3. Сконфигурируйте VLAN на основе тегов таким образом, чтобы рабочие станции 1 и 4 принадлежали виртуальной сети №1, станция 2 принадлежала виртуальной сети №2, а станция №3 – виртуальной сети №3 и при этом являлась общедоступным ресурсом. То есть машины в виртуальных сетях №1 и №2 не должны взаимодействовать между собой, но должны взаимодействовать с машиной №3.

4. Проверьте правильность конфигурации сети. Результаты мониторинга покажите и поясните преподавателю.

5. Сбросьте настройки коммутаторов в фабричные и перезагрузите его.

Контрольные вопросы:

Базовый уровень:

1. Механизмы добавления идентифицирующего маркера в заголовок кадра Ethernet
2. Компоненты конфигурации виртуальной сети на основе тэгов
3. Сети на базе MAC-адресов (MAC-based VLANs)
4. Сети на базе портов (Port-based VLANs

Повышенный уровень:

3. Построение виртуальных сетей 802.1Q на нескольких коммутаторах
4. Преимущества виртуальных сетей 802.1Q

Лабораторная работа №3 Безопасность коммутаторов (4 часа)

Содержание:

1. Базовые механизмы безопасности коммутаторов.
2. Безопасность на основе протокола IEEE 802.1x.

Цель работы:

Изучение технологий Trusted Hosts, IP-MAC Binding и Port Security. Изучение механизма сегментации трафика.

Теоретические сведения:

Ограничение количества управляющих компьютеров Современные коммутаторы позволяют задать конкретные компьютеры (IP-адреса), с которых будет происходить настройка данных коммутаторов по Web- или Telnet- инерфейсам или через протокол SNMP. Попытка прочих компьютеров подключиться к коммутаторам для управления ими будет отклонена.

Настройка безопасности индивидуального порта. Данная функция позволяет:

заблокировать дальнейшее обновление таблицы коммутатора – если конфигурирование Вашей сети больше не изменятся, Вы блокируете таблицу коммутации, и коммутатор будет просто отбрасывать все пакеты, которые поступают с неизвестных адресов. Причём данное действие можно выбрать для конкретных портов. При этом записи в таблице коммутации не будут удаляться по тайм-ауту;

задать максимальное количество MAC-адресов для привязки к конкретному порту.

Технология фильтрации IP-MAC Binding Основное назначение данной технологии – это ограничить доступ к коммутатору определённого количества компьютеров. Для этого индивидуально для каждого желаемого порта создаётся таблица соответствия IP- и MAC-адресов. Далее коммутатор будет пропускать только пакеты с указанными MAC-адресами и только в том случае, если истинно соответствие IP- и MAC-адреса. Существенные отличия данной технологии от технологии фильтрации MAC-адресов:

фильтрация работает на всех портах, а в данной технологии можно настраивать каждый порт в отдельности;

фильтрация содержит «чёрный» список, то есть работает по принципу: не пропускать те пакеты, MAC-адреса которых содержатся в таблице фильтрации. Данная технология, наоборот, содержит «белый» список, то есть пропускает только те пакеты, MAC-адреса которых содержатся в созданных списках;

в отличие от фильтрации технология IP-MAC Binding проверяет не только MACадрес источника пакета, но и его IP-адрес.

Сегментация трафика (Traffic Segmentation) Сегментация трафика служит для разграничения портов на Канальном уровне. Данная функция позволяет настраивать порты или группу портов таким образом, чтобы они были изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети провайдера. Очень важной является возможность одновременного использования данной функции с виртуальными сетями (VLAN), что позволяет производить дальнейшее разграничение прав.

Данная технология схожа с технологией VLAN, но является более ограниченной по функциональности. К преимуществам технологии можно отнести:

простота настройки;

более низкая загрузка процессора коммутатора по сравнению с VLAN

Задание:

Базовые механизмы безопасности коммутаторов

1. Соберите топологию сети, представленную на рисунке 7.

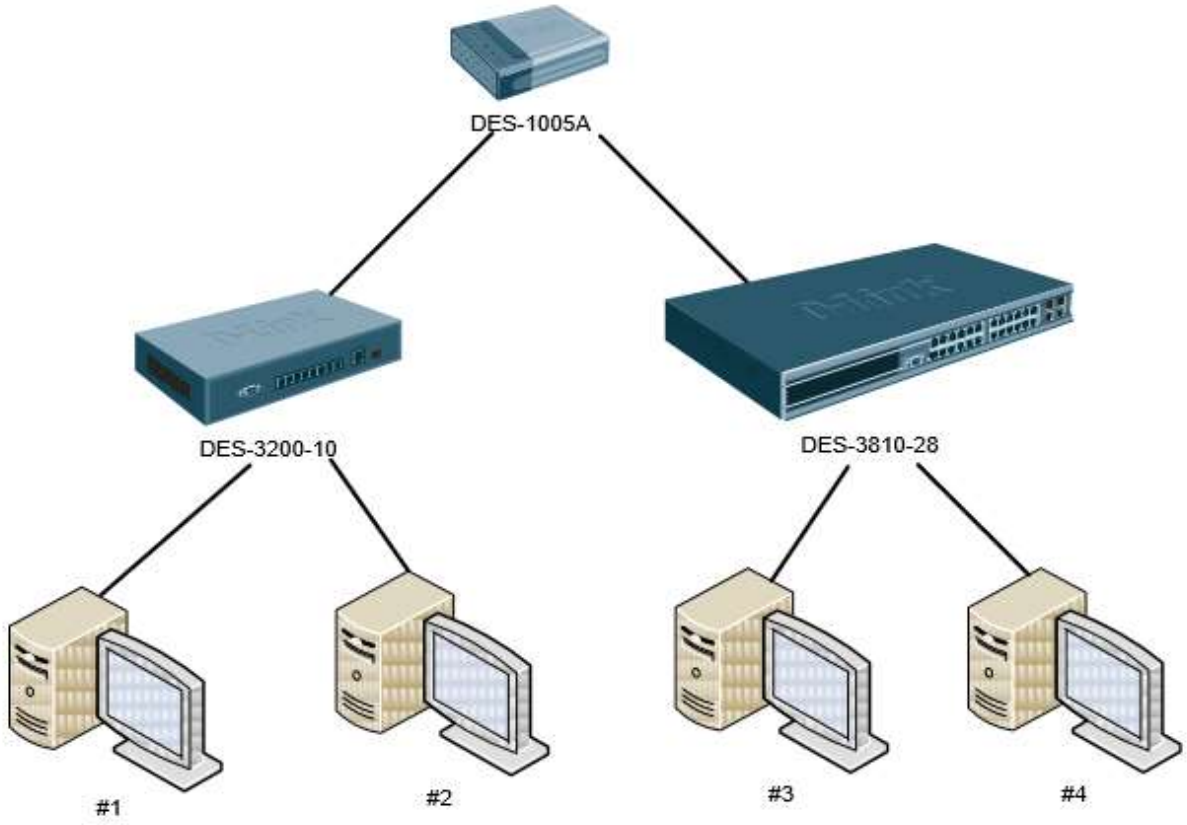


Рис.7.

2. Изучите следующие разделы теоретического пособия: «Ограничение количества управляющих компьютеров», «Настройка безопасности индивидуального порта» и «Технология фильтрации IP-MAC Binding».

3. Изучите раздел «Security»/«Trusted Hosts» коммутатора 3200-10 в пособие по управлению стендом.

4. Настройте коммутаторы таким образом, чтобы ими могли управлять только машины #1 и #3.

5. Проверьте выполненные настройки.

6. Изучите раздел «Security»/«Port Security» коммутатора 3200-10 в пособие по управлению стендом.

7. Очистите таблицы коммутации на всех коммутаторах.

8. С машин #1 и #2 «пропингуйте» машину #3

9. Убедитесь, что в таблицах коммутации не присутствует аппаратного адреса машины #4. 10. Заблокируйте на обоих коммутаторах таблицу коммутации в режиме Permanent. 11. Попытайтесь осуществить взаимодействие с 4-ым компьютером с любого компьютера. Объясните полученный результат.

12. Изучите раздел «Security»/«IP-MAC-Port Binding» коммутатора 3200-10 в пособие по управлению стендом. 13. Сбросьте блокировку таблиц коммутации. 14. Используя технологию IP-MAC Binding, настройте на коммутаторах фильтры таким образом, чтобы в сети могли работать только машины #1 и #3.

15. Сбросьте настройки коммутаторов в фабричные и перезагрузите его.

Безопасность на основе сегментации трафика

1. Соберите топологию сети, представленную на рисунке 8.

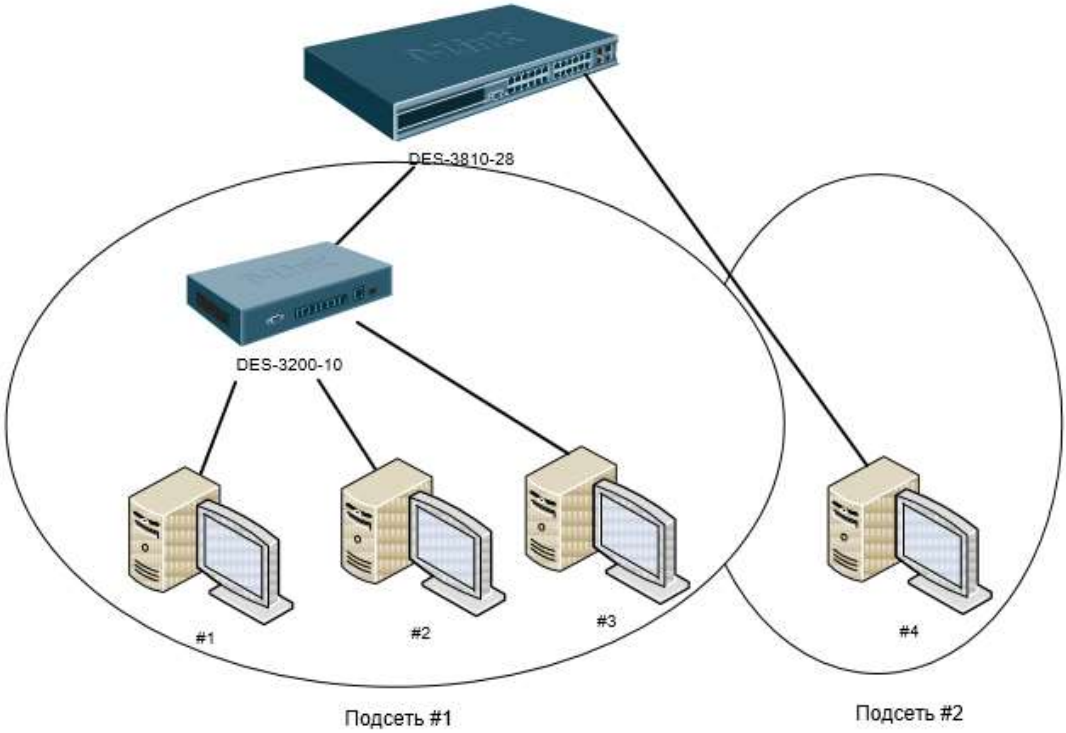


Рис.8.

2. Изучите раздел «L3 Features»/«IPv4 Static/Default Route Settings» коммутатора 381028 в пособие по управлению стендом.

3. Создайте IP-подсети, как это показано на рисунке 8. Назначьте каждому компьютеру IP-адрес из собственной подсети.

4. Изучите раздел «Сегментация трафика» теоретического пособия и раздел «L2 Features»/«Traffic Segmentation» коммутатора 3200-10 в пособие по управлению стендом.

5. Организуйте на коммутаторе DES-3200-10 принцип «расчески» – каждый компьютер, подключенный к коммутатору, может обмениваться информацией только с внешним миром, но не с другими компьютерами, подключенными к этому же коммутатору.

6. Проверьте правильность сделанных настроек.

7. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Задание

Контрольные вопросы:

Базовый уровень:

1. Для чего применяется настройка безопасности индивидуально порта.
2. Сегментация трафика.

Повышенный уровень:

3. Что такое адрес подсети?
4. Фильтрация на основе Mac-адресов.

РАЗДЕЛ 2. БЕЗОПАСНОСТЬ СЕТЕЙ Wi-Fi

Лабораторная работа №4 Шифрование канала беспроводной связи (4 часа)

Содержание:

1. Шифрование канала с использованием протокола WEP
2. Шифрование канала с использованием протокола WPA

Цель работы: Получение навыков построения сетей Wi-Fi с использованием механизма шифрования WEP и WPA.

Теоретические сведения:

Шифрование WEP (Wired Equivalent Privacy - секретность на уровне проводной связи) основано на алгоритме RC4 (Rivest's Cipher v.4 – код Ривеста), который представляет собой симметричное потоковое шифрование. Как было отмечено ранее, для нормального обмена пользовательскими данными ключи шифрования у абонента и точки радиодоступа должны быть идентичными.

Ядро алгоритма состоит из функции генерации ключевого потока. Эта функция генерирует последовательность битов, которая затем объединяется с открытым текстом посредством суммирования по модулю два. Дешифрация состоит из регенерации этого ключевого потока и суммирования его с шифрограммой по модулю два для восстановления исходного текста. Другая главная часть алгоритма - функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока.

RC4 – фактически класс алгоритмов, определяемых размером его блока. Этот параметр n является размером слова для алгоритма. Обычно, n = 8, но в целях анализа можно уменьшить его. Однако для повышения уровня безопасности необходимо задать большее значение этой величины. Внутреннее состояние RC4 состоит из массива размером 2n слов и двух счетчиков, каждый размером в одно слово. Массив известен как S-бокс, и далее он будет обозначаться как S. Он всегда содержит перестановку 2n возможных значений слова. Два счетчика обозначены через i и j. Алгоритм инициализации RC4 приведен ниже. Этот алгоритм использует ключ, сохраненный в Key и имеющий длину l байт. Инициализация начинается с заполнения массива S, далее этот массив перемешивается путем перестановок, определяемых ключом.

До мая 2001г. стандартизация средств информационной безопасности для беспроводных сетей 802.11 относилась к ведению рабочей группы IEEE 802.11e, но затем эта проблематика была выделена в самостоятельное подразделение. Разработанный стандарт 802.11i призван расширить возможности протокола 802.11, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные производители Wi-Fi оборудования в лице организации WECA (Wireless Ethernet Compatibility Alliance), иначе именуемой Wi-Fi Alliance, устав ждать ратификации стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию W-Fi Protected Access (WPA), соответствие которой обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности WPA обеспечивает уровень безопасности куда больший, чем может предложить WEP Он перебрасывает мостик между стандартами WEP и 802.11i и имеет немаловажное преимущество, которое заключается в том, что микропрограммное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

Задание для выполнения работы:

Шифрование канала с использованием протокола WEP

1. Постройте сеть, содержащую 1 роутер и 2 ПК.
2. Изучите раздел «Механизмы шифрования в беспроводных сетях» теоретического пособия.

3. Включите точку доступа, настройте канал и имя сети. Включите внутренний DHCPсервер. Включите шифрование WEP, используя 40-битный ключ.

4. Ассоциируйте два компьютера с этой точкой доступа.

5. Запустите на третьем компьютере утилиту «Airodump-ng» для перехвата пакетов.

6. Выполните взаимодействие между компьютерами 1 и 2.

7. Убедитесь (по экрану airodump-ng), что несколько пакетов с данными было перехвачено.

8. Сгенерируйте файл словаря, содержащий несколько произвольных ключей и добавьте в конец файла заданный ключ. Длина словаря должна быть не меньше 10000 записей. Скрипт для генерации находится на диске в каталоге /root/Desktop/Scripts/wep

9. Используя полученный словарь и перехваченные пакеты выполните атаку на файл с перехваченными пакетами с помощью утилиты «WepAttack».

10. Выполните эти же действия, изменяя длину ключа и используя в качестве перехватчика Kismet вместо airodump. Варьируйте размер файла словаря, добавляя или удаляя записи. Сделайте вывод о влиянии длины ключа и размера словаря на скорость атаки.

Шифрование канала с использованием протокола WPA

1. Постройте сеть, содержащую 1 роутер и 2 ПК.

2. Используя утилиту wpa_supplicant, настройте защищенную сеть с использованием аутентификации WPA и системой шифрования TKIP. 3. Используя ssh, сравните полезную пропускную способность канала до и после использования WPA

Для проверки скорости соединения воспользуйтесь SSH 1. На первом компьютере задайте пароль пользователю root: passwd. 2. На втором компьютере для копирования файла выполните команду: scp ip_адрес_компьютера_1:путь_к_файлу /dev/null Эта команда скопирует указанный файл с первого компьютера на второй, причём файл не будет сохранён на диске, что позволит оценить реальную пропускную способность сети. Скорость передачи данных будет указана в выводе команды scp.

4. Используя утилиту tcpdump осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения WPA.

5. Используя утилиту wpa_supplican, настройте защищенную сеть с использованием аутентификации WPA2/PSK и системой шифрования TKIP. 6. Используя ssh, сравните полезную пропускную способность канала до и после использования WPA2/PSK.

7. Используя утилиту wpa_supplican, настройте защищенную сеть с использованием аутентификации WPA2/PSK и системой шифрования AES. 8. Используя ssh, сравните полезную пропускную способность канала с использованием системы шифрования TKIP с системой шифрования AES.

Контрольные вопросы:

Базовый уровень:

1. Способы проверки скорости соеденнеия.

2. Дайте характеристику RC4.

Повышенный уровень:

3.Основные типы угроз безопасности беспроводных сетей.

4.Алгоритм шифрования AES.

Лабораторная работа №5 Аутентификация беспроводных клиентов (4 часа)

Содержание:

1. Аутентификация беспроводных клиентов на основе учётных записей пользователей и аппаратных адресов компьютеров.

2. Обнаружение атак диссоциации с использованием ОС Linux.

Цель работы: Получение навыков построения защищённых wi-fi сетей с использованием RADIUScервера и фильтрации по MAC-адресам. Изучение работы и возможностей утилиты Kismet.

Теоретические сведения:

Беспроводные точки доступа часто являются головной болью администраторов корпоративных сетей. В основном речь идет о безопасности и удобстве; пользователям придётся запоминать пароли от точек (и кто им запретит сообщить пароль знакомому?). И чем больше точек, тем больше проблем. Но и заставлять пользователей сидеть с воткнутой в ноутбук витой парой — тоже неправильно. Поскольку в сети используется Active Directory и у каждого пользователя есть учетная запись, уместно будет для аутентификации эти учетные записи и использовать.

Сегодня я хочу рассказать об использовании стандарта 802.1x и RADIUS сервера для настройки аутентификации клиентов по доменным учетным записям.

Важно знать, что в процессе участвуют 3 сущности:

Supplicant — это клиентский ноутбук, который связывается с точкой. В терминологии NPS сабж фигурирует как Access Client, что порождает некоторую путаницу

Client или Authenticator — это наша точка доступа или, в случае с проводной сетью, управляемый коммутатор

AAA Server — собственно, сервер аутентификации. У нас это будет Network Policy Server (NPS)

В процессе аутентификации supplicant связывается с клиентом по протоколу EAP (в это время разрешен только EAP трафик), после чего клиент связывается с сервером AAA по протоколу RADIUS, сначала проходит аутентификацию сам, как клиент (при помощи заранее заданного на клиенте и сервере пароля), после чего передает данные саппликанта, получает ответ и, соответственно, пускает или не пускает клиента в сеть. На самом деле там ещё используется challenge и информация шифруется, но это мы сейчас подробно рассматривать не будем. Важно то, что саппликант и сервер не общаются напрямую, а только через клиента.

Соответственно, основная настройка будет производиться на сервере. На точке (клиенте) надо всего лишь выбрать вид аутентификации (802.1x), IP адрес и порт сервера, и пароль (shared secret). Саппликантов разных много и особой сложности в настройке нет, скажу только, что в используемых у нас Win XP и 7 вполне нормально работают встроенные саппликанты.

AAA серверю Вот мы вбили нужные настройки на беспроводной точке, подняли сервер (у нас это Win 2008 R2), на нём роль NPS. Но для начала надо выписать сертификат нашему RADIUS серверу. Дело в том, что иначе PEAP аутентификация не будет работать. Если в вашей сети еще нет сервера служб сертификатов AD, процесс его настройки и выдачи сертификата описан на technet.

Собственно, настраиваем RADIUS

Открываем консоль NPS, заходим во вкладку Clients, создаем клиента. Здесь всё интуитивно понятно — IP адрес беспроводной точки, имя клиента, пароль (такой же, как и на точке).

Далее нас интересует вкладка Policies и два её пункта:

Connection Request Policies

Здесь настраиваются действия NPS, когда к нему обращаются с данными о саппликанте. Опций немного — саппликанта, попадающего под выбранные нами условия можно или пропускать без дальнейшей проверки, или перенаправлять на другой AAA сервер, или же аутентифицировать на нашем сервере, в последнем случае происходит переход к политикам вкладки Network Policies.

Задание:

Аутентификация беспроводных клиентов на основе учётных записей пользователей и аппаратных адресов компьютеров.

1. Используя утилиту freeradius, настройте RADIUS-сервер и создайте двух произвольных пользователей.

2. Настройте маршрутизатор DIR-300 на использованием IEEE 802.1x.

3. Настройте клиентов, используя утилиту wpa_supplicant.

4. Проверьте работоспособность сети.

5. Соберите топологию.

6. К точке доступа 1 разрешить подключение компьютеров 1 и 2 с помощью разрешенных списков MAC-адресов. К точке доступа 2 запретить подключение с компьютера А с помощью запрещенных списков MAC-адресов.

7. Проверьте правильность выполненных настроек.

Обнаружение атак диссоциации с использованием ОС Linux.

1. Включите и настройте 2 точки доступа на разные каналы и имена сетей. Включите внутренний DHCP-сервер точки доступа.

2. Подключите 2 компьютера к разным сетям.

3. Запустите Kismet на 3 компьютере. Просмотрите обнаруженные сети.

4. Определите каналы, на которых располагаются точки доступа.

5. Посмотрите, какие типы пакетов перехватываются, когда компьютеры ассоциированы, но не активны. Наблюдайте за графиком количества перехваченных пакетов в секунду

6. Выполните взаимодействие между 2 компьютерами, находящимися в одной сети (например, скопируйте файл с одного компьютера на другой с помощью scp). Какие типы пакетов появились в эфире? Как изменился график?

7. Определите клиентов обнаруженных сетей.

8. Запустите на одном из 2 компьютеров, подключенных к одной сети, непрерывную атаку диссоциации на вторую сеть (с помощью MDK или с помощью aireplay).

9. Посмотрите на реакцию Kismet.

Контрольные вопросы:

Базовый уровень:

1. Опишите утилиту Kismet.

2. Как работает RADIUS-сервер.

Повышенный уровень:

3.дайте характеристика протоколу IEEE 802.1x..

4. Атака диссоциации.

РАЗДЕЛ 3. МЕХАНИЗМЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ БРАНДМАУЭРОВ

Лабораторная работа №6 Технологии и методы работы брандмауеров (4 часа)

Содержание:

1. Протокол PPPoE

2. Технология Network Address Translation.

Цель работы: Изучение технологии NAT и способов её настройки на брандмауэре Cisco ASA 5505. Изучение протокола PPPoE и способов его настройки и использования в ОС Linux и брандмауэре Cisco ASA 5505.

Теоретические сведения:

Обзор протокола PPPoE Point-to-Point Protocol over Ethernet (PPPoE) – способ установления сеанса и инкапсуляции PPP-пакетов при передаче их по Ethernet. Применяется как протокол туннелирования, используемый для подключения нескольких пользователей в одной Ethernet-подсети к Интернету через общий последовательный интерфейс, например, DSL-линия, беспроводной канал, или кабельный модем. Все

пользователи сети делят одно подключение, однако контроль доступа может быть выполнен для каждого пользователя. PPPoE даёт провайдеру следующие преимущества:

аутентификация по логину/паролю;

автоматическое выделение IP-адресов пользователям (похоже на DHCP);

автоматическое определение PPPoE-сервера.

Так как физически устанавливается PPP-сеанс, то PPPoE-соединение обладает всеми свойствами PPP-соединения.

Процесс установления PPPoE-соединения состоит из 2 этапов:

поиск сервера (Discovery);

установление PPP-соединения.

На этапе поиска клиент производит поиск PPPoE-сервера. Если в сети используется несколько серверов, то происходит выбор нужного. Так как PPPoE-соединение организуется на канальном уровне, то для его установления участникам достаточно знать MAC-адреса друг друга. Этап поиска происходит в 4 шага: 1. Клиент передаёт инициирующее сообщение (Initiation) по широковещательному адресу канального уровня (FF:FF:FF:FF:FF:FF). 2. Один или несколько серверов передают сообщение-предложение (Offer) на аренду MAC-адрес клиента. 3. Клиент передаёт сообщение о запросе сеанса (Session Request) по MAC-адресу выбранного сервера. 4. Выбранный сервер передаёт сообщение о подтверждении (Confirmation) установлении сеанса.

Существует 5 видов PPPoE-сообщений:

1. Active Discovery Initiation (PADI) – начало поиска клиентом сервера.

2. Active Discovery Offer (PADO) – оповещение клиента о наличии сервера.

3. Active Discovery Request (PADR) – запрос клиента на установление соединения.

4. Active Discovery Session-confirmation (PADS) – подтверждение установления сеанса связи сервером.

5. Active Discovery Terminate (PADT) – завершение соединения.

На этом шаге заканчивается первый этап. Второй этап представляет из себя PPP-сеанс. Отличие PPPoE от PPP заключается в том, что блоки данных передаются не по выделенной линии, а по сети Ethernet. Заголовок PPPoE занимает 8 байт, что необходимо учитывать при расчёте MTU (1500-8=1492).

Point-to-Point Protocol (PPP) — протокол для связи между двумя компьютерами, например, для соединения абонентской станции с провайдером через коммутируемое соединение.

Функциями PPP являются:

1. Управление адресами протокола сетевого уровня (IP).

2. Асинхронное и синхронное формирование пакета данных.

3. Мультиплексирование протоколов сетевого уровня.

4. Конфигурирование канала связи. 5. Проверка качества канала связи. 6. Обнаружение ошибок при передаче данных. 7. Согласование параметров сжатия информации.

Задание:

Протокол PPPoE

1.Соберите топологию сети на риснке 9.

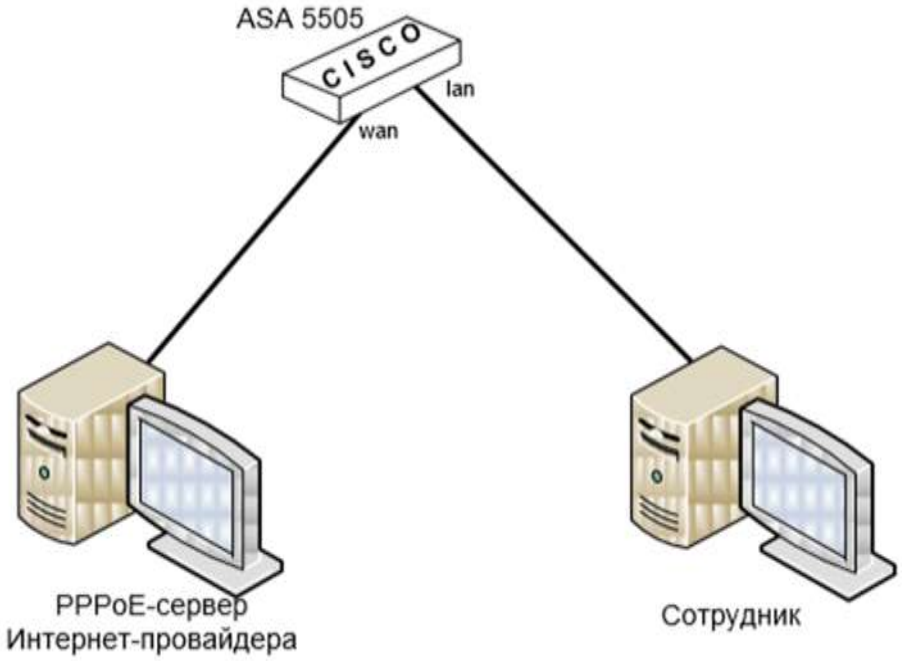


Рис.9.

2. Настройте рабочие станции и брандмауэр таким образом, чтобы условный интерфейс wan Cisco ASA 5505 и PPPoE-сервер принадлежали одной IP-подсети, а условный интерфейс lan Cisco ASA 5505 и машина сотрудника – другой.

3. Изучите главу «Протокол PPPoE» теоретического пособия и раздел «Протокол PPPoE» в пособие по настройке ОС Linux.

4. Используя утилиту rp-pppoe, настройте PPPoE-сервер на машине Интернетпровайдера.

5. Настройте ASA 5505 в качестве PPPoE-клиента (используя созданную в п.5 учетную запись пользователя). Установите PPPoE-туннель.

6. Осуществите доступ с машины сотрудника в сеть Интернет, то есть к машине провайдера.

Технология Network Address Translation

1. Соберите топологию сети, представленную на рисунке 10.

2. Настройте рабочие станции и брандмауэр таким образом, чтобы условный WANинтерфейс ASA 5505 и маршрутизатор провайдера принадлежали одной IP-подсети, а условный LAN-интерфейс ASA 5505 и машины #1 и #2 – другой.

3. Изучите главу «Веб-сервер Apache» в пособие по настройке ОС Linux.

4. Настройте и запустите на маршрутизаторе провайдера веб-сервер.

5. Изучите главу «Транслятор адресов» теоретического пособия, а также раздел «NAT» для ASA 5505 в пособие по управлению стендом.

6. Настройте NAT на ASA 5505.

7. Одновременно осуществите обращение с машин #1 и #2 к веб-серверу провайдера.

8. Если попытка успешна (получена стартовая страница Apache), то запустите на машине провайдера утилиту tcpdump и снова осуществите запрос к веб-серверу с машин локальной сети.

9. Проанализируйте результаты, выдаваемые утилитой tcpdump и ответьте на вопрос: какой IP-адрес и номер порта стоит в адресе отправителя запросов, получаемых вебсервером.

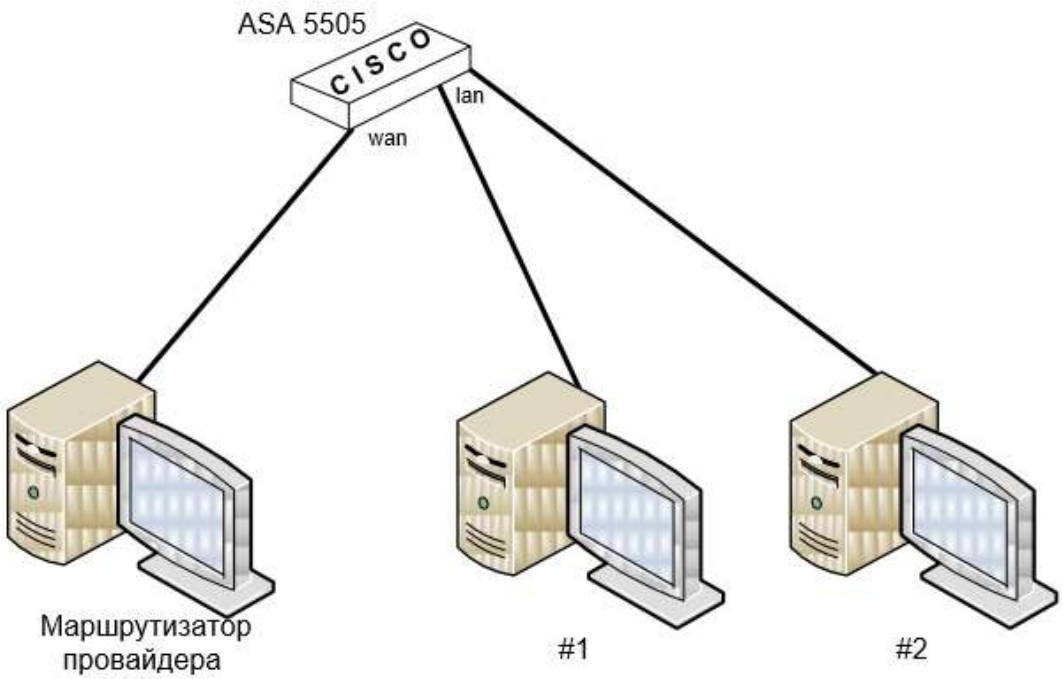


Рис 10

Контрольные вопросы:

Базовый уровень:

1. Технология NAT.
2. Преимущества PPPoE.

Повышенный уровень:

3.Виды PPPoE-сообщений
4. Функции PPP.

Лабораторная работа №7 Виртуальные частные сети (4 часа)

Содержание:

1 Виртуальные частные сети

Цель работы:

Изучение протокола IPSec и способа его настройки в ОС Linux и на брандмауэре Cisco ASA 5505.

Теоретические сведения:

Несмотря на то, что протокол IP стал наиболее используемым протоколом связи во всем мире и базовой технологией Интернета, он имеет множество существенных недостатков. Среди них необходимо отметить ограниченность адресного пространства и недостатки внутренней безопасности. Главной причиной этих недостатков является то, что IP-протокол изначально не был предназначен для массового использования.

В качестве развития IP-протокола была разработана его новая версия IPv6 (IP-протокол версии 6), в которой пытались решить проблемы предшествующих версий. Поскольку принятие новой версии IP-протокола затруднительно, что вызвано постоянным ростом Интернета и громадным разнообразием установленной аппаратуры и программного обеспечения, то меры безопасности, включенные в IPv6, были перенесены в текущую версию IPv4 в виде дополнительного комплекта протоколов. Этот набор протоколов назвали комплектом протоколов IPSec (IPSec Protocol Suite).

Подключение по протоколу IPSec имеет два основных режима: транспортный (transport) и туннельный (tunnel). Транспортный режим — это форма связи типа узел-узел, где применяется шифрование только содержательной части пакета. Из-за двухточечного характера связи соответствующее программное обеспечение необходимо загрузить

(установить) на все связывающиеся между собой узлы сети, что представляет собой достаточно серьез-ную проблему. Этот режим VPN удобно использовать для зашифрованной связи между узлами одной сети.

Режим туннелирования применяется при создании большинства VPN; потому что он шифрует весь оригинальный пакет. Режим туннелирования может применяться для организации связи типа узел-узел, узел-шлюз или шлюз-шлюз. При организации связи типа шлюз-шлюз значительно упрощается связь между сетями, не требуется установка специального ПО на узлах сети.

Первая цель семейства протоколов IPSec состоит в обеспечении конфиденциальности, целостности и аутентификации информации, передаваемой посредством IP-протокола. Это достигается с помощью протокола обмена интернет-ключами (Internet Key Exchange, IKE), протокола ESP и протокола AH. Комбинация этих трех протоколов обеспечивает безопасный обмен информацией.

Второй целью семейства протоколов IPSec является предоставление разработчикам ПО набора стандартов. Установление безопасного соединения начинается с формирования ассоциации обеспечения безопасности (Security Association, SA) между двумя сообщающимися сторонами. 107 НПП «Учтех-Профи» – Сетевая безопасность – Теория

Основа ассоциации обеспечения безопасности заключается в соглашении двух сторон о том, как они могут безопасно передавать свою информацию. В процессе соглашения сто-роны оговаривают детали защищенного обмена. Результатом такого соглашения и явля-ется ассоциация обеспечения безопасности. Каждому сеансу связи сопоставляются две ассоциации — по одной на каждого партнера связи.

Положительными чертами протокола IPSec являются открытость его стандарта для под-держки множества протоколов и режимов связи, а также поддержка различных алгорит-мов шифрования и различных хэш-функций. Прежде чем договариваться об ассоциации обеспечения безопасности, необходимо локальное конфигурирование элементов прото-кола IPSec, которые данный партнер собирается поддерживать. Эти параметры настрой-ки хранятся в базе данных политики безопасности (Security Policy Database, SPD).

После согласования ассоциация обеспечения безопасности содержится в базе данных ассоциации обеспечения безопасности (Security Association Database, SAD). Это необхо-димо, поскольку узел сети может инициализировать несколько сеансов, каждому из кото-рых может соответствовать своя SA.

Поскольку для каждого сетевого устройства доступно множество сеансов протокола IPSec, для правильного функционирования процесса необходимо, чтобы каждый сеанс согласования SA имел свой собственный уникальный идентификатор. Этот иден-тификатор составляется из уникального индекса параметра обеспечения безопасности (Security Parameter Index, SPI), который определяет, какая запись БД SA соответствует рассматриваемому подключению. Кроме того, учитывается адрес назначения и идентификатор используемого протокола (ESP или AH).

Протокол обмена интернет-ключами предназначен для аутентификации и согласования параметров обмена протокола IPSec. Протокол IKE представляет собой комбинацию двух протоколов: протокола управления ассоциациями и протокола управления ключами обес-печения безопасности в сети Интернет (Internet Security Association and Key Management Protocol, ISAKMP), называемых фазами установления. Управление ключами можно вы-полнять вручную или используя альтернативы протокола IKE, такие как безопасная служ-ба доменных имен (Secure DNS), Photuris или простой протокол обмена интернет-ключами (Simple Key Internet Protocol, SKIP).

Первая фаза протокола IKE. На первой фазе протокола IKE удаленный пользователь на-чинает сеанс со шлюзовым устройством VPN. Первая фаза выполняет две функции: аутентификацию удаленного пользователя и обмен информацией об открытых ключах, которые будут использоваться во второй фазе.

Аутентификацию можно выполнить несколькими различными способами. Наиболее часто используются технология предварительно распространяемых ключей (pre-shared keys) и технология цифровых сертификатов. Термин «предварительно распространяемые клю-чи» означает, что значения ключей предварительно задаются на всех компьютерах, кото-рые собираются устанавливать соединения через VPN (что является существенным не-достатком). При втором способе используются цифровые удостоверения (цифровые сер-тификаты, digital certificates), которые могут назначаться отдельно для каждого объекта, который соединяется с VPN. Цифровыми сертификатами можно удаленно управлять и администрировать из уполномоченного центра сертификации (Certificate Authority, CA).

Сертификационная служба является центральным элементом структуры, называемой инфраструктурой с открытым ключом (Public Key Infrastructure, PKI). За инфраструктурой PKI стоит концепция публично доступной структуры, распределяющей информацию об открытых (публичных) ключах.

В первой фазе при обмене аутентификационной информацией и параметрами безопас-ности могут использоваться два режима: основной (main mode) и агрессивный (aggressive mode). Различия между ними заключаются в количестве сетевых пакетов, которыми об-мениваются стороны, и во времени, за которое генерируется открытый ключ. Агрессив-ный режим использует дополнительный заголовок меньшего размера, но основной режим обладает большей безопасностью и используется чаще всего.

Вторая фаза протокола IKE. Во второй фазе протокола IKE согласовываются конкретные параметры ассоциации обеспечения безопасности IPSec. Данное согласование подобно агрессивному режиму обмена информацией первой фазы. После завершения второй фа-зы формируется SA и пользователь получает подключение к VPN.

Во второй фазе возможен единственный режим согласования – быстрый режим (quick mode). Быстрый режим представляет собой короткий обмен, использующий три пакета. Все обмены второй фазы зашифрованы с помощью согласованных во время первой фа-зы протоколов и типов кодирования. При этом используется только защита, основанная на использовании хэш-функции и нонсе (nonce), включаемых в сетевые пакеты для под-тверждения их оригинальности (нонсе является подтверждением того факта, что инфор-мация о ключе исходит из ожидаемого источника. Нонсе – это случайное число, генери-руемое инициатором связи, которое заверяется респондентом цифровой подписью и по-сылается обратно).

Данная реализация включает в себя также идентификатор поставщика (vendor ID, VID), позволяющий участникам межплатформенных взаимодействий делать предположения о возможностях и конфигурации их партнеров, которые могут иметь различных изготовите-лей. После создания ассоциации обеспечения безопасности, используемой протоколом IKE, можно применять протоколы обеспечения безопасности. При построении VPN, осно-ванной на протоколе IPSec, можно выбрать использование одного из протоколов (AH или ESP) или использовать их одновременно.

Управление ключами. Применяемый по умолчанию для IPSec протокол автоматизиро-ванного управления ключами называется ISAKMP/Oakley и состоит из следующих эле-ментов:

- протокол определения ключей Oakley – протокол на основе алгоритма Диффи-Хеллмана, но обеспечивающий дополнительную защиту. Протокол Oakley называет-ся общим, так как он не диктует использования каких-либо конкретных форматов;
- протокол защищенных связей и управления ключами в Интернете – обеспечивает ос-нову схемы управления ключами и поддержку специального протокола и необходи-мых форматов процедуры согласования атрибутов защиты.

ISAKMP не заставляет использовать какой-то конкретный алгоритм обмена ключами, а предлагает использовать любой подобный алгоритм. 109 НПП «Учтех-Профи» – Сетевая безопасность – Теория

Протокол Oakley разработан в целях сохранения преимуществ алгоритма Диффи-Хеллмана и устранения его недостатков. Алгоритм Oakley характеризуется следующими особенностями:

- использование механизмов рецептов (cookies) для защиты от атак засорения;
- соглашение двух сторон о группе, которая определяет параметры алгоритма обмена ключами Диффи-Хеллмана;
- использование оказий для противостояния атакам повтора сообщений;
- обмен открытыми ключами Диффи-Хеллмана;
- аутентификация обмена для противостояния атакам «человек посередине».

Задание:

1. Соберите топологию сети, представленную на рисунке 11.

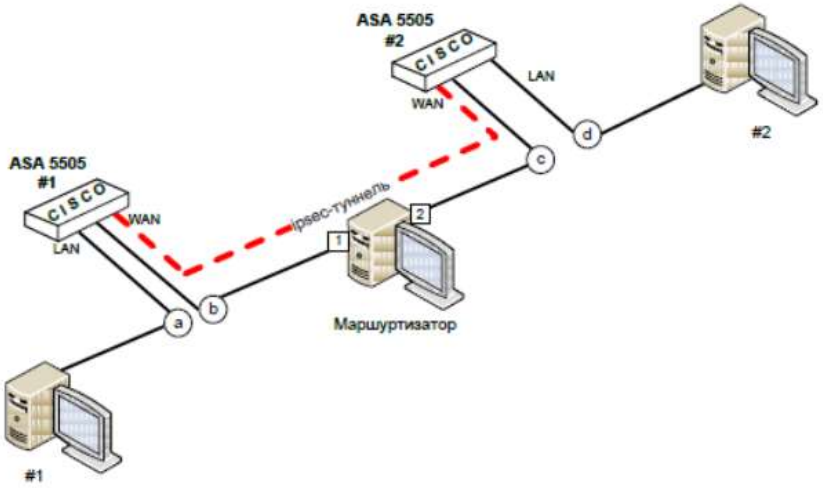


Рисунок 11.

2. Настройте рабочие станции и брандмауэры таким образом, чтобы создать четыре различных IP-подсети: a, b, c и d (в соответствие с рисунком 11).

3. Изучите главу «Протокол IPSec» теоретического пособия, а также главы «Настройка туннеля IPSec ASA 5505» в пособие по управлению стендом и «Протокол IPSec» в пособие по настройке ОС Linux.

4. Настройте ipsec-туннель, как это показано на рисунке 11

5. Проверьте работоспособность сети, обратившись с машины #1 на машину #2.

Контрольные вопросы:

Базовый уровень:

1. Протокол обмена интернет-ключами.
2. Протокол определения ключей Oakley.

Повышенный уровень:

3. Протокол аутентификации заголовка
4. Протокол безопасной инкапсуляции содержимого пакета.
5. Совместное использование протоколов ESP и AH

РАЗДЕЛ 4. МЕХАНИЗМЫ ПОСТРОЕНИЯ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ОС LINUX

Лабораторная работа №8 Программные межсетевые экраны (4 часа)

Содержание:

1. Утилита iptables.

2. Цифровые сертификаты.

Цель работы:

Получение навыков построения программного межсетевого экрана на базе ОС Linux с использованием утилиты iptables. Изучение технологии цифровых сертификатов и получение навыков построения зашифрованной сети на базе этой технологии и ОС Linux.

Теоретические сведения:

Системы трансляции адресов (Network Address Translation, NAT) обычно являются компонентой МЭ. Службы межсетевой безопасности обычно устанавливаются и работают на маршрутизаторах. Дополнительно к этому межсетевые экраны (МЭ) и системы обнаружения атак (СОАВ) желательно устанавливать и на компьютеры, находящиеся во внешнем периметре сети.

Межсетевой экран (брандмауэр, файерволл) – это комплекс программных или аппаратных средств, который позволяет реализовать набор правил, определяющих условия прохождения пакетов между сетями. Межсетевой экран включает следующие средства (рисунок 12):

- фильтр пакетов;
- фильтр состояний;
- транслятор адресов;
- транспортный шлюз;
- шлюз приложений (прокси-сервер).

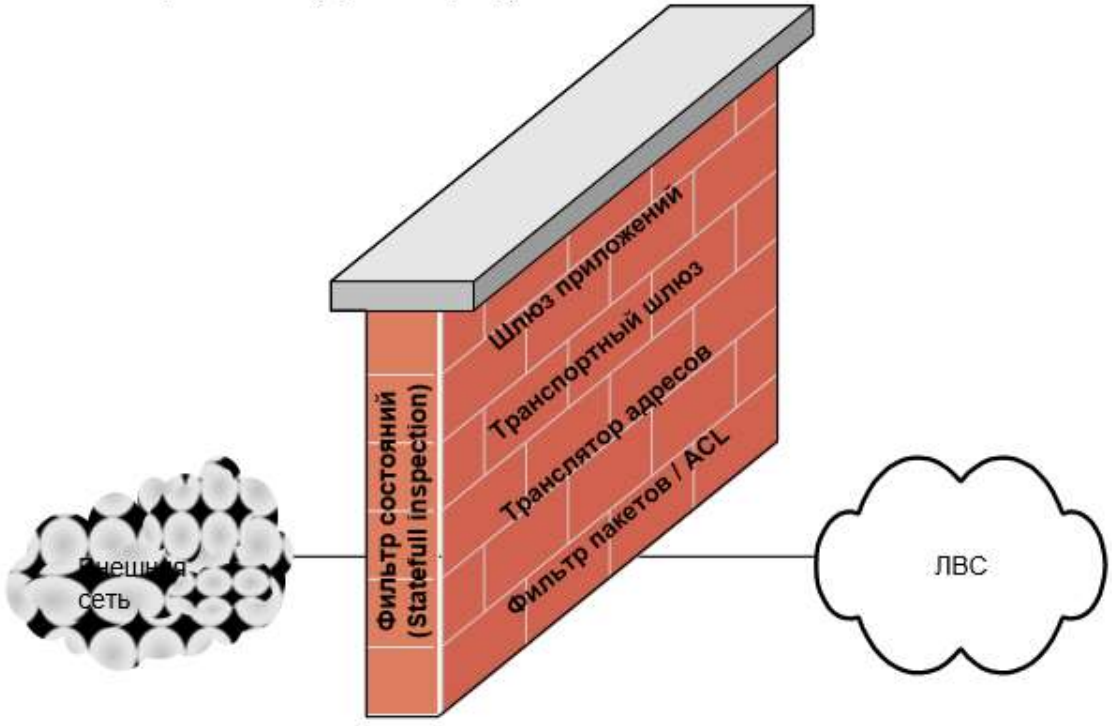


Рисунок 12. Упрощенная архитектура межсетевого экрана.

ФП разрешает или запрещает прохождение пакета в соответствии с заданными администратором правилами. Эти правила опираются на информацию, имеющуюся в заголовке каждого пакета и в сетевой системе:

- IP-адрес источника и назначения;
- протокол Транспортного уровня;
- порт источника и назначения;
- Флаги;
- Тип сообщения ICMP;
- Входящий и исходящий сетевой интерфейс.

Таким образом, для описания правил прохождения пакетов составляются таблицы

типа:

Дейст-вие	Тип паке-та	Адрес источника	Порт источ-ника	Адрес назначе-ния	Порт назначе-ния	Фла-ги	Входя-щий интер-фейс	Исходя-щий интер-фейс
DROP	TCP	194.186.1.2	80	-	-	-	-	
ACCEPT	UDP	83.142.162.49	53	-	-	-	-	
ACCEPT	ICMP	-	-	-	-	-	-	
DROP	-	-	-	-	-	-	eth1	eth0

Фильтры работают быстро, поскольку они просто просматривают информацию о пакете при принятии решения. Но фильтры пакетов имеют один существенных недостаток – они не в состоянии отслеживать конкретный сетевой сеанс и не в состоянии анализировать содержимое сообщения конкретного приложения, которое в свою очередь может содержать зловредный код

Технология инспекции состояний (statefull inspection) используется многими разработчиками, но, поскольку наименование запатентовано компанией Check Point, они вынуждены присваивать ему различные наименования (expert inspection, smart filtering, adaptive screening, multilevel inspection и др.). Данная технология является дальнейшим развитием фильтра пакетов и включает следующую дополнительную функцию – поддержка таблицы состояний TCP-соединений и контроль сессий на её основе.

Жизненый цикл TCP-соединения имеет несколько фаз. Таблица состояний (netstat) содержит информацию о соединение и состояние, в котором находится данное соединение. На основе этой информации происходит фильтрация пакетов. Например, если не был произведен запрос, то пакет-ответа не будет пропущен в локальную сеть.

Трансляция адресов – технология, позволяющая изменять такие параметры IP-пакета, как адрес и порт источника пакета, адрес и порт назначения. При этом ведётся таблица измененных данных, и при получении обратного пакета происходит обратная трансляция адреса, если она нужна. Существуют 2 причины, по которым имеет смысл осуществлять трансляцию адресов:

предоставление компьютерам локальной сети полноценного доступа в Интернет при условии, что имеющееся число внешних адресов или подключений к провайдеру меньше, чем число компьютеров, которым необходим доступ в Интернет. Стоит учесть, что некоторые протоколы не поддерживают трансляцию адресов (например, PPTP), либо использование трансляции накладывает ограничения на использование служб (например, пассивный режим FTP был разработан для решения проблемы NAT). Для обхода таких проблем маршрутизатор должен иметь возможность разбирать пакеты, вносить изменения и собирать их снова;

скрытие внутренней структуры локальной сети. За счёт выполнения трансляции адресов запросы компьютеров локальной сети выглядят так, будто выполняются с одного и того же компьютера. Однако на самом деле это могут быть запросы от разных машин. Также можно с помощью трансляции адреса совместно с портом осуществлять скрытие серверной инфраструктуры.

Существуют 2 способа трансляции адресов:

- Network Address Translation (NAT) – замена адрес источника на адрес маршрутизатора. При этом порт остаётся неизменным;
- Static Address Translation (SAT) – замена адрес источника или приёмника на некоторый адрес. Возможна одновременная замена порта. SAT подразделяется на 2 типа:Source SAT – трансляция адреса источника, Destination SAT – трансляция адреса назначения.

Задание:

Утилита iptables.

1. Соберите топологию сети, представленную на рисунке 12.

2. Настройте рабочие станции таким образом, чтобы создать две различных IP-подсети: a и b (в соответствие с рисунком 13).

3. Настройте и запустите на сервере веб и файловый сервисы.

4. Изучите главу «Утилита iptables» в пособие по настройке ОС Linux.

5. Используя утилиту iptables, настройте на маршрутизаторе транслятор сетевых адресов и создайте два правила межсетевого экрана, согласно которым:

клиент может обращаться к веб-серверу;

клиент не может обращаться к файловому серверу.

6. Проверьте правильность сделанных настроек (в том числе используя утилиту tcpdump).

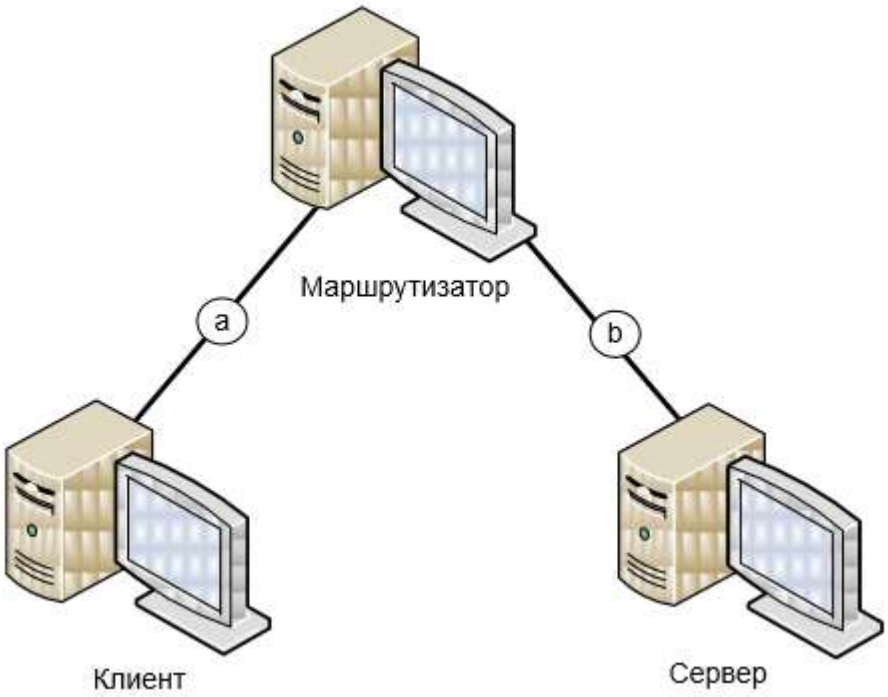


Рис.13.

Цифровые сертификаты.

1. Соберите топологию сети, представленную на рисунке 14.

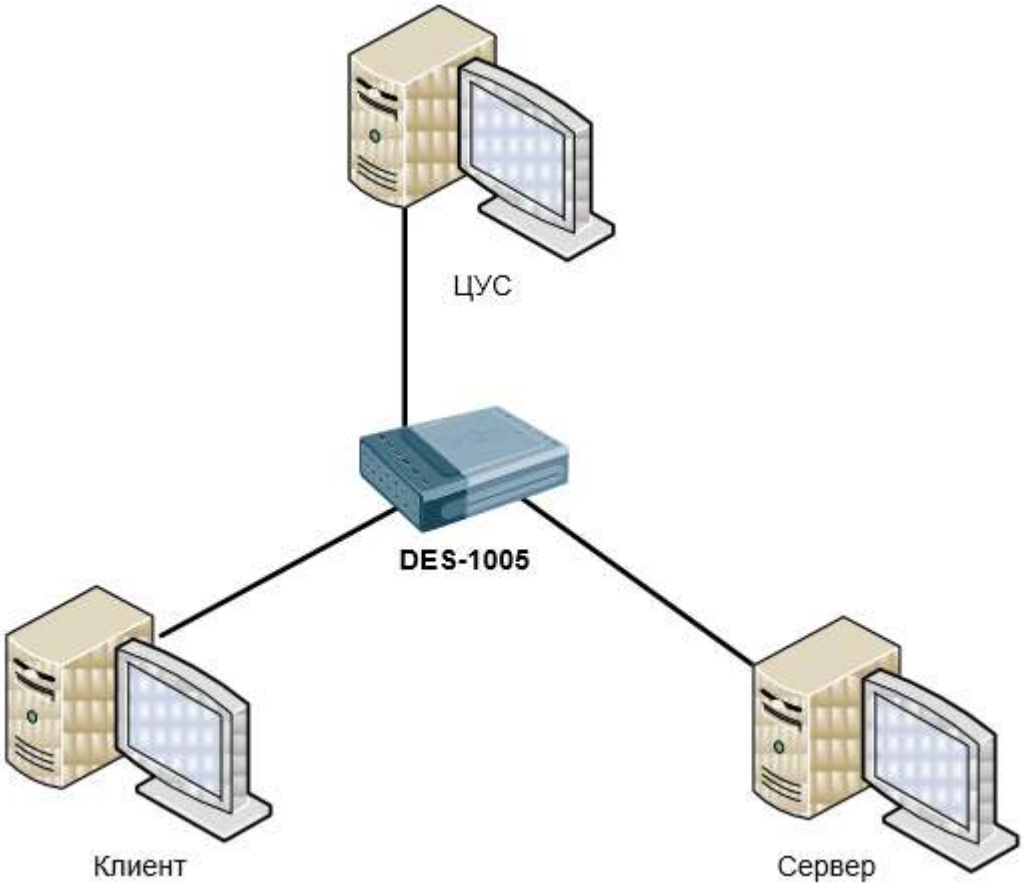


Рис.14

2. Изучите главу «Протокол SSL/TLS» теоретического пособия, а также главу «Центр управления сертификатами на базе пакета OpenSSL» в пособие по настройке ОС Linux

3. Запустите веб-сервис на сервере.

4. Инициируйте соединение клиента с веб-сервером и с помощью утилиты tcpdump убедитесь, что данные передаются без шифрования.

5. Создайте центр управления сертификатами (ЦУС) средствами openssl.

6. Создайте сертификат для веб-сервера. Настройте веб-сервер на работу с сертификатом.

7. Инициируйте соединение клиента с веб-сервером по протоколу HTTPS. Средствами браузера изучите сертификат. С помощью tcpdump изучите передаваемые пакеты и убедитесь, что передаваемая информация шифруется.

Контрольные вопросы:

Базовый уровень:

1. Трансляция адресов
2. Системы трансляции адресов.

Повышенный уровень:

3. Жизненый цикл TCP-соединения.
4. Межсетевой экран.

Лабораторная работа №9 Защита удаленного управления
(4 часа)

Содержание:

1. Туннелирование соединений с использованием протокола SSL
2. Удаленное управление по защищённому протоколу SSH

Цель работы:

Изучение принципов безопасного обмена информации с использованием протокола SSL и ОС Linux. Изучение протокола SSH и способов его применения в ОС Linux

Теоретические сведения:

SSL (Secure Sockets Layer, уровень защищённых сокетов) – криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создаётся защищённое соединение между клиентом и сервером. SSL изначально разработан компанией Netscape Communications. Впоследствии на основании протокола SSL 3.0 был разработан и принят стандарт RFC, получивший имя TLS. TLS является протоколом более низкого уровня, хотя на модели TCP/IP это не отражается (и SSL, и TLS – протоколы прикладного уровня).

Использует шифрование с открытым ключом для подтверждения подлинности передатчика и получателя. Поддерживает надёжность передачи данных за счёт использования корректирующих кодов и безопасных хэш-функций. Обычно применяются следующие алгоритмы:

1. Для обмена ключами: RSA, Diffie-Hellman, ECDH, SRP, PSK.
2. Для аутентификации: RSA, DSA, ECDSA.
3. Симметричные шифры: RC4, Triple DES, AES, IDEA, DES, или Camellia. В старых версиях SSL также использовался RC2.
4. Для криптографических хэшей: HMAC-MD5 или HMAC-SHA для TLS, MD5 и SHA для SSL.
5. В старых версиях SSL также использовались MD2 и MD4.

SSL состоит из двух уровней. На нижнем уровне многоуровневого транспортного протокола (например, TCP) он является протоколом записи и используется для инкапсуляции (то есть формирования пакета) различных протоколов (SSL работает совместно с таким протоколами как POP3, IMAP, XMPP, SMTP и HTTP). Для каждого инкапсулированного протокола он обеспечивает условия, при которых сервер и клиент могут подтверждать друг другу свою подлинность, выполнять алгоритмы шифрования и производить обмен криптографическими ключами, прежде чем протокол прикладной программы начнёт передавать и получать данные. Если некоторая программа не поддерживает SSL/TLS, можно воспользоваться программой для создания защищенных туннелей stunnel.

SSH (Secure Shell) – это сетевой протокол, используемый для удаленного управления компьютером и для передачи файлов. SSH похож по функциональности на протоколы telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH позволяет передавать через безопасный канал любой другой сетевой протокол. Также, SSH может использовать сжатие передаваемых данных для последующей их шифрации.

Первая версия протокола, SSH-1, была разработана в 1995 году исследователем Tatu Ylönen из Технологического университета Хельсинки, Финляндия. SSH-1 был написан для обеспечения большей конфиденциальности, чем протоколы rlogin, telnet и rsh. В 1996 году была разработана более безопасная версия протокола, SSH-2, уже несовместимая с SSH-1. Протокол приобрел еще большую популярность и к 2000 году его использовало уже порядка двух миллионов пользователей. В 2006 году протокол был утвержден рабочей группой IETF в качестве Интернет-стандарта.

Однако, до сих пор в некоторых странах (Франция, Россия, Ирак и Пакистан) требуется специальное разрешение в соответствующих структурах для использования

определенных методов шифрования, включая SSH (см. закон Российской Федерации "О федеральных органах правительственной связи и информации").

Распространены две реализации SSH: коммерческая (закрытая) и свободная (открытая). Свободная реализация называется OpenSSH. К 2006 году 80% компьютеров Интернет использовало именно OpenSSH. Коммерческая реализация разрабатывается организацией SSH Inc., http://ssh.com/ - закрытая реализация, бесплатная для некоммерческого использования. Свободная и коммерческая реализации SSH содержат практически одинаковый набор команд.

В первой версии протокола есть существенные недостатки, поэтому в настоящее время SSH-1 практически нигде не применяется Наверное, вы помните знаменитый эпизод из фильма "Матрица-2: Перезагрузка", в котором Тринити использует эксплоит SSHNuke для взлома городской электростанции? Вначале она нашла уязвимый SSH-сервер, просканировав сеть программой Nmap. Затем, через "дыру" "SSH1 CRC2", она получила максимальные права доступа к этому серверу.

Многие взломщики сканируют сеть в поиске открытого порта SSH. Поэтому в целях безопасности необходимо запрещать доступ по ssh для суперпользователя. Обычно злоумышленники подбирают именно пароль суперпользователя. Протокол SSH-2 устойчив к атакам "man-in-middle", в отличие от протокола telnet. То есть, прослушивание трафика, "снифинг", ничего не дает злоумышленнику. Протокол SSH-2 также устойчив к атакам путем присоединения посредине (session hijacking) и обманом сервера имен (DNS spoffing).

Далее по тексту под SSH имеется ввиду именно вторая версия протокола, SSH-2.

Для работы по SSH нужен SSH-сервер и SSH-клиент. Сервер прослушивает соединения от клиентских машин и при установлении связи производит аутентификацию, после чего начинает обслуживание клиента. Клиент используется для входа на удаленную машину и выполнения команд.

Задание:

Туннелирование соединений с использованием протокола SSL

1. Соберите топологию сети, представленную на рисунке 15.

2. Настройте «зеркалирование» (Port Mirroring) на коммутаторе следующим образом: порт «a» – приёмник, порт «b» – источник. Таким образом, злоумышленник сможет «прослушивать» весь трафик клиента.

3. Изучите главу «Протокол SSL/TLS» теоретического пособия, а также главу «Шифратор TCP-соединения Stunnel» в пособие по настройке ОС Linux.

4. Запустите на сервер POP3-сервер с авторизацией через /etc/passwd.

5. Получите почту пользователя root с машины клиента. Параллельно с этим процессом запустите утилиту tcpdump на компьютере злоумышленника. Обнаружьте пароль на почтовый ящик в перехваченных пакетах.

6. На сервере запустите утилиту stunnel на 995 порту для запуска почтового сервера.

7. Включите использование SSL/TLS на клиенте. Выполните шаг 5.

8. Сравните перехваченные утилитой tcpdump пакеты.

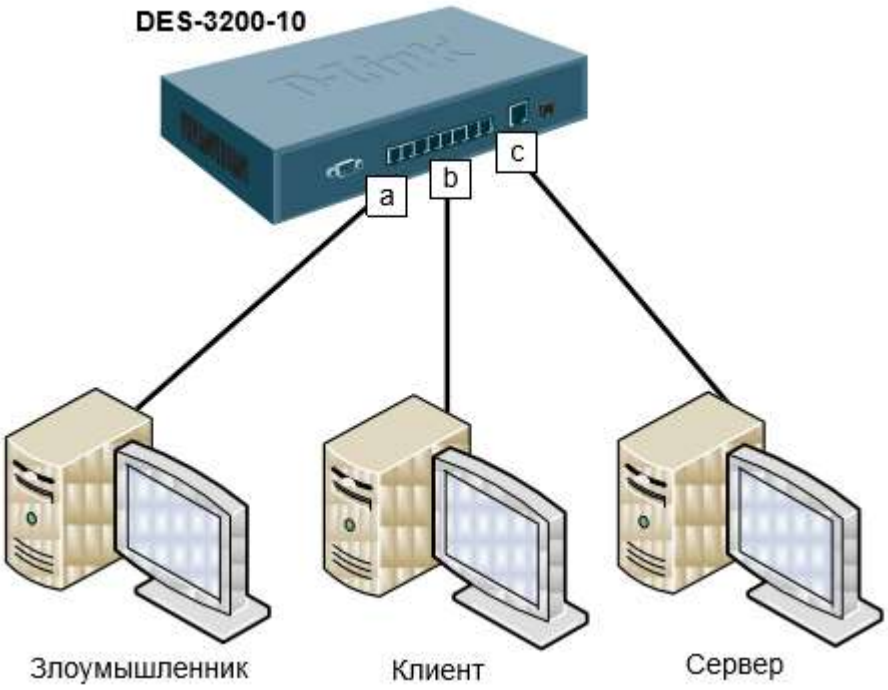


Рис.15.

Удаленное управление по защищённому протоколу SSH

1. Соберите топологию сети, представленную на рисунке 15.

2. Изучите главу «Протокол SSH» теоретического пособия, а также главу «Пакет OpenSSH» в пособие по настройке ОС Linux.

3. Проверьте, работает ли на компьютерах ssh-сервер (ps ax | grep ssh). Если не работает, то запустите его командой.

4. Попробуйте подключиться с клиента на сервер с использованием протокола SSH. Изучите переданные пакеты с помощью tcpdump. Посмотрите, какие события были отмечены в файле журнала /var/log/auth.log.

5. Перезагрузите удалённый сервер, не подключаясь к нему.

6. Удалённо перезапустите демон ssh без подключения.

7. Подключитесь к удалённому серверу и перезапустите демон ssh. Обратите внимание на то, что сеанс не завершился.

8. Запустите FTP-сервис на сервере.

9. Выполните передачу файла через FTP с помощью утилиты wget. Анализируйте проходящие пакеты с помощью утилиты tcpdump (-XX). Запомните скорость передачи.

10. Выполните передачу файла через ssh. Анализируйте проходящие пакеты с помощью tcpdump (-XX). Запомните скорость передачи. Сравните передаваемые пакеты и скорость передачи данных.

11. Включите сжатие ssh и повторите замер скорости. В каждом тесте анализируйте результаты для файла, состоящего из нулей, для файла, содержащего случайную последовательность (dd if=/dev/urandom of=file bs=1M count=10), для текстового конфигурационного файла и для бинарного файла.

12. Напишите скрипт, который будет создавать файл размеров 10МБ со случайными данными, архивировать его и передавать с удалённой на локальную машину.

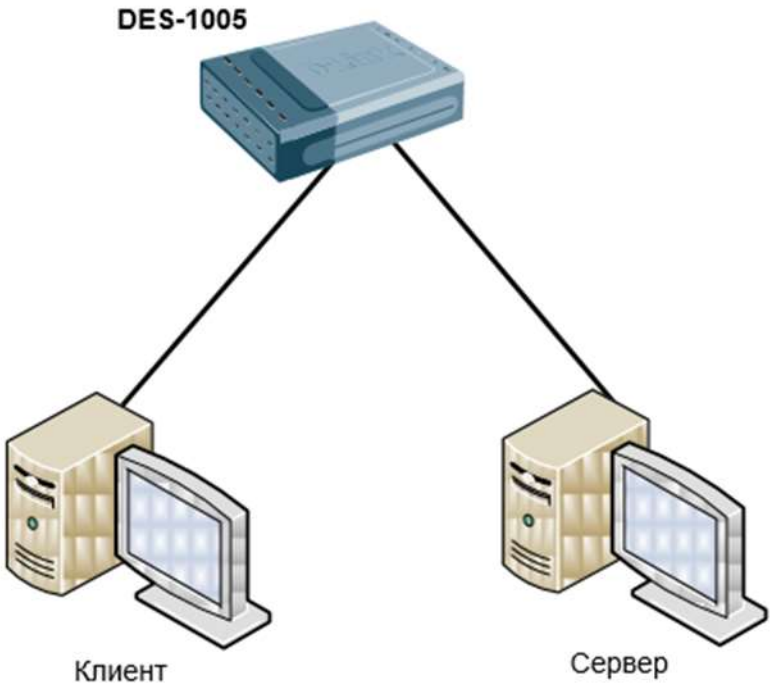


Рис.15.

Контрольные вопросы:

Базовый уровень:

1. Для чего применяется удаленное управление.
2.Что такое туннелирование.

Повышенный уровень:

3.Опишите протокол SSL
4. Опишите протокол SSH

Методические указания к самостоятельной работе студентами

СОДЕРЖАНИЕ

Введение

Целью изучения дисциплины «Основы построения защищенных компьютерных сетей» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, обучение принципам и методам защиты информации в компьютерных сетях, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации.

Задачи дисциплины:

1. изучение типовых угроз безопасности в компьютерных сетях;
2. изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
3. приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
4. овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
5. овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные и практические работы, самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области построения защищенных компьютерных сетей. На лабораторных и практических работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным и практическим работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных и практических работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

– самостоятельное изучение учебного материала по заданным темам;

– подготовка к лабораторным работам, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

– работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);

– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

– составление плана и тезисов ответа или графическое изображение структуры ответа;

– составление таблиц для систематизации учебного материала;

– изучение нормативных документов;

– ответы на контрольные вопросы;

3) для формирования умений:

– подготовка к практическим и лабораторным занятиям;

– решение задач и практических и лабораторных заданий;

– подготовка отчетов по практическим и лабораторным занятиям;

– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические и лабораторные занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим и лабораторным занятиям, а также варианты тестовых заданий.

2. Самостоятельное изучение тем лекций

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
	Самостоятельное изучению тем лекций	1,2,3,4	1,2,3	1,2	1,2,3,4
1	Самостоятельное изучение «Угрозы безопасности сети»	3,4	1,3	1,2	1
2	Самостоятельное изучение «Защита инфраструктуры сети»	2,3	1,2	1,2	2,3
3	Самостоятельное изучение «Основы IP-адресации и маршрутизации»	1,2,	1,2,3	1	4,2

3. Вопросы для собеседования по практическим занятиям

Практическое занятие 1: Настройка операционной системы Cisco IOS
Базовый уровень:

1. Сохранение настроек в энергонезависимую память
2. Базовые средства среды имитационного моделирования Cisco Packet Tracer

Повышенный уровень:

1.Настройка прав доступа в Cisco Packet Tracer

2. Модули линейных карт и сетевых интерфейсов на маршрутизаторах и коммутаторах Cisco

Практическое занятие 2: Защита инфраструктуры маршрутизации

Базовый уровень:

1. Средства обеспечения отказоустойчивости и масштабирования. Задачи, решаемые на каждом уровне иерархической модели данной СПД

2. Команды, используемых для настройки протокола OSPF

Повышенный уровень:

1. Для каждого маршрутизатора определить его характеристики, роли и свойства в рамках протокола OSPF.

2.Протокол MD5

Практическое занятие 3: Защита инфраструктуры коммутации

Базовый уровень:

1. Механизмы защиты виртуальных ЛВС.

2. Атаку типа «VLAN hopping».

Повышенный уровень:

1.Базы данных VLAN

2.Маршрутизация VLAN на коммутаторе уровня ядра-распределения ЛВС.

Практическое занятие 4: Защита ЛВС от петель на канальном уровне

Базовый уровень:

1. Работе механизмов BPDU Guard, BPDU Filter и Root Guard. Область применения и назначение каждого из этих механизмов защиты.

2. Механизма Root Guard.

Повышенный уровень:

1. DoS-атаки на сетевую инфраструктуру.

2. Атака типа BPDU spoofing на протокол STP.

Практическое занятие 5: Защита ЛВС от атак канального уровня

Базовый уровень:

1. .Атака MAC-flooding

2. Атака MAC-spoofing

Повышенный уровень:

1. Метод статического назначения разрешенных MAC-адресов

2. Динамически изменяемая сетевая инфраструктура

Практическое занятие 6: Построение маршрутизируемой ЛВС

Базовый уровень:

1. Механизмы и средства обеспечения отказоустойчивости и масштабирования.

2. Достоинства полностью маршрутизируемых ЛВС

Повышенный уровень:

1. Реализации политик безопасности (межсетевом экранировании, организации VPN) при построении маршрутизируемых ЛВС

2.Ассиметричная маршрутизация

Практическое занятие 7: Защита сетевой инфраструктуры

Базовый уровень:

1. Основные настройки безопасности

2. Планировщика задач для обеспечения возможности передачи ресурсов процессам управления

Повышенный уровень:

1. Сеть внутриполосного управления

2. Доступа в сеть управления из ЛВС передачи данных

Практическое занятие 8: Тема: Защита периметра сети

Базовый уровень:

1.Технология NAT

2.Проанализировать политику безопасности управления информационными потоками.

Повышенный уровень:

1. Информационные потоки правилами

2. Политику безопасности управления

Практическое занятие 9: Криптографическая защита каналов передачи данных

Базовый уровень:

1. Протокол ESP

2. Транспортный режим работы IPSec

Повышенный уровень:

1. Криптографическая защиты протоколов IPSec

2. Параметры и ключи криптографической защиты IPSec

Практическое занятие 10: Защита беспроводной ЛВС

Базовый уровень:

1. Механизмами обеспечения безопасности беспроводной сети

2. Угрозы безопасности беспроводной сети

Повышенный уровень:

1. Подходы к построению беспроводных ЛВС

2. Доступ из беспроводного сегмента к ЛВС корпоративной сети

Практическое занятие 11: Сбор предварительной информации

Базовый уровень:

1. Этапы анализа защищенности сети

2. Методы получения информации

Повышенный уровень:

1. Механизмы защиты для противодействия методам предварительного сбора информации о сети

2. Сбор данных о номерах автономных систем исследуемой сети

Практическое занятие 12: Идентификация узлов и портов сетевых служб

Базовый уровень:

1. Ограничение доступа к сетевым службам

2. Методы сканирования

Повышенный уровень:

1. ARP SCAN

2. Идентификация узлов методом IP Probing

Практическое занятие 13: Идентификация служб и приложений

Базовый уровень:

1. Использования служб прикладного уровня для идентификации веб-серверов

2. Анализ заголовков

Повышенный уровень:

1. Метода анализа параметров повторной передачи

2. Особенности реализации механизмов идентификации служб и приложений в сканерах nmap и amap.

Практическое занятие 14: Идентификация операционных систем

Базовый уровень:

1. Методы идентификации ОС в сетевых сканерах

2. XSpider, Nessus и Nexpose

Повышенный уровень:

1. Опрос стека TCP/IP

2. Методы идентификации ОС, которые могут быть выполнены стандартными

сетевыми средствами (командами) ОС (например, telnet, ssh, ping).

Практическое занятие 15: Идентификация уязвимостей сетевых приложений по косвенным признакам

Базовый уровень:

1. Косвенные признаки уязвимости защиты
2. Классификация уязвимостей

Повышенный уровень:

1. Сетевые службы SSH, FTP.
2. Сетевые службы DNS, HTTP

Практическое занятие 16: Идентификация уязвимостей на основе тестов

Базовый уровень:

1. Атака грубой силы
2. Методы подбора учетных записей

Повышенный уровень:

1. Механизм DoS-атаки, используемой для разрыва соединения с сервером S.
2.Подбор паролей.

Практическое занятие 17: Сканирование уязвимостей веб-приложений

Базовый уровень:

1. Назначение сканеров безопасности
2. Атака типа внедрение операторов SQL

Повышенный уровень:

1. Атака на веб-приложения типа «Подделка межсайтовых запросов» (CSRF).
2. Атаки CSRF- и XSS-атак

Практическое занятие 18: Сканирование уязвимостей корпоративной сети

Базовый уровень:

1. Классификация сканеров безопасности
2. Политика сканирования уязвимостей

Повышенный уровень:

1. Настройка сканирования сети
2. Аудит отладочной информации процесса сканирования

4.2. Вопросы для собеседования по самостоятельному изучению лекций

Тема №2. Угрозы безопасности сети

Базовый уровень:

1.Вирус, червь и троян
2.Кибербезопасность
3.Протоколы сетевого уровня.

Повышенный уровень:

1.Методы противодействия вирусам червям и троянам.
2.Методы противодействия программам вымогателям.

Тема №4. Защита инфраструктуры сети

Базовый уровень:

1.Факторы, влияющие на структуру сети.
2.Основные требования к безопасности современный сетей.
3. Способы предотвращения типовых угроз безопасности сетей.

Повышенный уровень:

1.Главные принципы построения защищенной сети.
2.Подготовка безопасной коммуникационной среды?

Тема №10. Основы IP-адресации и маршрутизации

Базовый уровень:

1.Протокол ARP
2.Структура пакета ARP

3.Маршрутизация ARP

Повышенный уровень:

1.Механизмы безопасности в ARP

2. ARP-оповещение

4.3. Вопросы к экзамену

Вопросы для проверки уровня знаний

Базовый уровень:

1.Модель сетевой безопасности.
2.Обобщённый сценарий атаки.
3.Основные причины возникновения угроз защиты сети.
4.Типы угроз безопасности сети.
5.Процесс оценки состояния защиты.
6.Инфраструктура сети.
7.Защита физических устройств.
8.Защита административного интерфейса.
9.Методы авторизации.
10.Методы аутентификации.
11.Методы аудита.
12.Сервер сетевого доступа.
13.Проблема защиты удаленного доступа.
14.Эталонная модель TCP/IP.
15.Эталонная модель OSI.
16.Коммутация LAN.
17.Протокол распределенного связующего дерева.
18.Поиск и устранение неисправностей STP.
19.Обзор функций сетевого уровня.
20.IPv4-адресация и маршрутизация.
21.Протоколы стека TCP/IP.
22.Основы IPv6.
23.Адресация IPv6 и создание подсетей.
24.Протокол ARP.
25.Концепции коммутации в локальных сетях.
26.Защита от петлевых маршрутов с помощью протокола STP.
27.Сеть Фейстеля.
28.Распределение ключей.
29.Алгоритмы стандартного шифрования.
30.Расположение устройств шифрования.
31.Область применения криптографии открытого ключа.
32.Односторонняя кеш функция.
33.Безопасные кеш функции и HMAC.
34.Классификация межсетевые экраны.
35.Архитектура межсетевых экранов.
36.Фильтрация пакетов.
37.Транспортные шлюзы.
38.Шлюзы приложений.
39.Системы обнаружения атак и вторжений.
40.Классификация СОВ.
41.Классификация механизмов безопасности в сетях Wi-Fi.
42.Механизмы шифрования в беспроводных сетях.
43.Принципы аутентификации абонента.
44.Открытая аутентификация.

45.Дополнительные механизмы защиты.
46.Ограничение количества управляющих компьютеров.
47.Списки контроля доступа.
48.Протокол IEEE 802.1x.
49.Методы контроля доступа при использовании протокола IEEE 802.1x.
50.Концепция построения виртуальной частной сети.
51.Протокол IPSEC.
52.Протокол SSH.
53.Протокол SSL.

Повышенный уровень:

1.Типовые угрозы безопасности компьютерных сетей.
2.Основы построения компьютерных сетей.
3.Криптографические методы обеспечения безопасности сети.
4.Программно-аппаратные средства обеспечения безопасности компьютерных сетей.
5.Механизмы обеспечение безопасности бесповодных локальных сетей.
6.Механизмы обеспечения безопасности коммутируемых лоальных сетей.
7.Виртуальные частные сети.

Задачи для проверки умений и навыков

1.Задачи на построение компьютерной сети

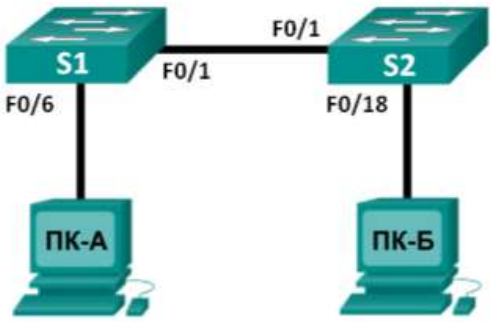


Рис.1.1.Топология сети

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	Недоступно	Недоступно	Недоступно
S2	VLAN 1	Недоступно	Недоступно	Недоступно
ПК-А	Сетевой адаптер	192.168.1.10	255.255.255.0	Недоступно
ПК-Б	Сетевой адаптер	192.168.1.11	255.255.255.0	Недоступно

Рис.1.2. Таблица адресации.

Базовый уровень:

1.Укажите, какие кабели и порты должны использоваться в сети.
2.Проложите кабели между устройствами.
3.Настройте на узлах статический IP-адрес на интерфейсах, которые подключены к локальной сети.
4.Проверьте связь между компьютерами с помощью утилиты ping.
5.Настройте имя узла, локальные пароли и баннер входа в систему для каждого коммутатора.
6.Сохраните текущие конфигурации.

Повышенный уровень:

1. Отобразите текущую конфигурацию коммутатора.

2. Отобразите версию IOS текущего коммутатора.

2.Задачи на обеспечение безопасности сетевых устройств

Рис.2.1.Топология сети

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Рис.2.2.Таблица адресации

Базовый уровень.

7.Настройка основных параметров устройства.

8.Настройка основных мер обеспечения безопасности на маршрутизаторе.

Повышенный уровень.

3.Настройка основных мер обеспечения безопасности на коммуникаторе.

3.Задачи на сбор сведений о сетевых устройствах

Рис.3.1.Топология сети

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Рис.3.2.Таблица адресации

Базовый уровень:

9.Настройте оборудование в соответствии с топологией сети.

10.Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

11.Присвойте статический IP-адрес маршрутизатору PC-A NIC.

12.Настройте базовые параметры на маршрутизаторе R1.

13.Выполните базовую настройку коммутатора S1.

14.Проверьте подключение к сети.

Повышенный уровень:

4.Соберите информацию на R1 с помощью команд IOS CLI.

5.Соберите информацию на S1 с помощью команд IOS CLI.

6.Соберите информацию на PC-A с помощью команды CLI.

4. Список рекомендуемой литературы

4.1. Основная литература:

1. Одом У. - Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101, акад. изд.: Пер. с англ. - М.: ООО "И.Д. Вильямс", 2015. – 912 с.: ил. - Парал. тит. Англ.

2. Одом У. - Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд.: Пер. с англ. - М.: ООО "И.Д. Вильямс", 2015. - 736 с.: ил. - Парал. тит. Англ.

3.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов // Питер. – СПб.: Питер, 2012, 944 с.

4.Таненбаум Э., Уэзеролл Д. Компьютерные сети: Учебное пособие // Питер. – СПб.: Питер, 2012.-960 с.

4.2. Дополнительная литература:

1.Уэнстром М. Организация защиты сетей Cisco. Пер. с англ. М.: изд. дом "Вильямс", 2005, 768 с.

2.Столингс В.- Компьютерные сети, протоколы и технологии Интернета. СПб: Издательство: БХВ-Петербург, 2005. 832 с.

3.Ермаков А.Е. - Основы конфигурирования корпоративных сетей Cisco. Учебное пособие для бакалавров. — М.: УМЦ ЖДТ, 2013. - 247 с.

4.3. Методическая литература:

1. Теоретическое пособие «Сетевая безопасность». Типовой комплект учебного оборудования. Челябинск 2013.

2. Пособие по управлению «Сетевая безопасность». Типовой комплект учебного оборудования. Челябинск 2013.

3. Пособие по настройке «Сетевая безопасность». Типовой комплект учебного оборудования. Челябинск 2013.

4. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс / А.Н. Андрончик. - Екатеринбург : Издательство Уральского университета, 2014. - 179 с. - ISBN 978-5-7996-1201-6, экземпляров неограничено

5. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации : учеб. пособие для вузов / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко ; под ред. А. П. Пятибратова. - 3-е изд., перераб. и доп. - М. : Финансы и статистика, 2006. - 560 с. : ил. - Библиогр.: с. 539-541. - Предм. указ.: с. 553-559. - ISBN 5-279-02779-0, экземпляров 6

4.4. Интернет-ресурсы:

1. Юрин И.Ю.- Теоретические и практические основы защиты информации. 2012. http://library.sgu.ru/uch_lit/620.pdf

2. Cisco Systems, Inc. Cisco SAFE reference guide. http://cisco.com/go/safe.

3. Cisco Systems, Inc. High availability campus network design – routed access layer using EIGRP or OSPF system assurance guide. http://cisco.com/go/srnd.

4. Cisco Systems, Inc. Network security baseline. http://cisco.com/go/safe

4.5. Материально-техническое обеспечение дисциплины:

1.Для возможного обеспечения использования контролирующих программ предусматривается класс ПЭВМ в соответствующей комплектации.

2.Специализированная лаборатория «Обнаружение сетевых вторжений».

3.Специализированная лаборатория «Программно-аппаратные средства обеспечения информационной безопасности».

4.Специализированная лаборатория «Сетевые компьютерные технологии».

5.Типовой комплект учебного оборудования «Сетевая безопасность».

6.Программное обеспечение для комплекта учебного оборудования «Сетевая безопасность.

7.Среда имитационного моделирования «Cisco Packet Traicer».

8.Операционная система Linux.