МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание,
_____ «_____» _____20____г.
(по

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Внедрение инфраструктуры кибербезопасности в учебный процесс_____

Специальность Системы Информационной Безопасности_____

Выполнил(а) Герцен Михаил Иванович_____ Группа СИБ-16-2___
(

Научный руководитель Альмуратова Камшат Бимуратовна
(ученая степень, звание,
Консультанты:
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич_____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных_____

Кафедра «Системы Информационной Безопасности»_____

Специальность «Системы Информационной Безопасности»_____

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Герцену Михаилу Ивановичу_____
(Ф.И.О.)

Тема проекта «Внедрение инфраструктуры кибербезопасности в учебный процесс»_____

Утверждена приказом по университету № _____ от «___» _____2020 г.

Срок сдачи законченного проекта «____» _____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – _____

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы –

Основная рекомендуемая литература:

Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. — МГТУ им. Н. Э. Баумана, 2002. — 306 с. — ISBN 5-7038-2059-6.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Создание топологии виртуальной сети	17.02.2020 – 20.02.2020	
Настройка виртуальной среды под необходимые задачи	21.02.2020 – 28.02.2020	
Запуск виртуальных устройств, первичная настройка	01.03.2020 – 08.03.2020	
Углубленная настройка межсетевого экрана	09.03.2020 - 18.03.2020	
Создание правил безопасности (SR)	19.03.2020 – 27.03.2020	
Сравнение характеристик разных межсетевых экранов	28.03.2020 - 07.04.2020	
Написание раздела БЖД	08.04.2020 - 18.04.2020	
Написание раздела рисков ИБ	19.04.2020 - 30.04.2020	

Аннотация

Данный дипломный проект посвящен теме внедрения и разворачивания инфраструктуры кибербезопасности в учебный процесс. Цель выполнения проекта заключалась в создании настраиваемой, легковесной и расширяемой среды для получения практических навыков в области сетевой безопасности в целом и в работе с межсетевыми экранами в частности.

Для выполнения поставленной задачи был проведен анализ текущих решений в области сетевой безопасности, были изучены компоненты инфраструктуры и доступные ресурсы, необходимые для функционирования брандмауэра. В ходе работы над проектом был получен новый теоретический опыт, впоследствии закрепленный практическим применением.

Annotation

This graduation project is dedicated to the topic of introducing and deploying cybersecurity infrastructure in the educational process. The goal of the project was to create a customizable, lightweight and extensible environment for gaining practical skills in the field of network security in general and about firewalls in particular.

To accomplish this task, an analysis of current solutions in the field of network security was carried out, the components of the infra structure and available resources necessary for the functioning of the firewall were studied. In the course of work on the project, new theoretical experience was obtained, subsequently fixed by practical application.

АҢДАТПА

Бұл дипломдық жоба оқу процесінде киберқауіпсіздік инфрақұрылымын енгізу және қолдану тақырыбына арналған. Жобаның мақсаты желінің қауіпсіздігі және, атап айтқанда, брандмауэр туралы тәжірибелік дағдыларды алу үшін икемделетін, жеңіл және кеңейтілетін ортаны құру болды.

Осы тапсырманы орындау үшін желілік қауіпсіздік саласындағы ағымдағы шешімдерге талдау жасалды, инфрақызыл құрылымының компоненттері және брандмауэр жұмыс істеуі үшін қажетті ресурстар қарастырылды. Жоба бойынша жұмыс барысында жаңа теориялық тәжірибе жинақталды, кейін практикалық қолдану арқылы бекітілді.

Содержание

Введение

Современные компании, имеющие множество узлов корпоративной сети и других сетевых устройств, нуждаются в использовании средств их защиты от угроз извне. Сейчас таким решением, которое будет оптимально по множеству пунктов, включая себестоимость, окупаемость, уровень защиты и т.д., может являться межсетевой экран или брандмауэр.

Использование Интернета для компании не только позволяет осуществлять свою деятельность и обеспечить непрерывность бизнеса, но и открывает множество путей для угроз, которые извне могут получить доступ к внутренней конфиденциальной информации. Для обеспечения должного уровня безопасности, на каждом узле сети компании может быть установлено антивирусное ПО, однако учитывая разницу в операционных системах, конфигурации и платформах сетевых устройств, такое решение, вероятно, было бы непрактичным и слишком дорогостоящим. Альтернативой этому, выступают средства информационной безопасности, основанные не на локальной защите конечных узлов, а на обеспечении безопасности всех (либо определенных) участков локальной сети. Межсетевые экраны создают единственную точку входа-выхода между внутренней и глобальной сетями, что, в свою очередь, облегчает задачи введение средств информационной безопасности и аудита. Как правило, брандмауэр состоит из пары устройств, одно из которых является коммутатором, а второе – персональный компьютер, с которого осуществляется конфигурация первого.

Глобально, можно выделить несколько областей, которые находятся под контролем межсетевого экрана:

- Управление службами. Данная область «ответственности» брандмауэра является основной, так как доступ во внешнюю сеть, как и из неё, осуществляется посредством сетевых служб.
- Маршрутизация. Для обеспечения безопасности всей локальной сети, её участки должны быть разделены, например, между отделами или другими структурными подразделениями. При корректной настройке маршрутизации, даже если часть сети оказалась под угрозой, остальные её участки останутся в безопасности.
- Управление пользователями. Данная функция необходима для распределения прав доступа и ролей между пользователями компании. Причем они могут быть как локальными, так и внешними (с использованием алгоритмов аутентификации).
- Эвристический или поведенческий анализ. Межсетевой экран можно настроить таким образом, чтобы подозрительный трафик не попадал во внутреннюю сеть, настроив соответствующие шаблоны. К примеру, запрет рассылки спама на внутреннюю электронную почту.

Соответственно, к межсетевым экранам выставляется ряд требований, без которых не может быть достигнут надлежащий уровень безопасности сети. К примеру, брандмауэр должен быть единственным пунктом

прохождения трафика из внешней сети во внутреннюю и наоборот. Также для межсетевого экрана всегда будет действовать правило «запрещено всё, что не разрешено», что означает необходимость ведения политик безопасности, соответствующих нуждам и требованиям компании.

Однако межсетевые экраны не могут быть единственным механизмом защиты от внешних угроз, даже для небольшой компании. Это связано с некоторыми ограничениями, а в частности:

- Некоторые сетевые устройства на предприятии могут обращаться напрямую к провайдеру, минуя межсетевой экран.
- Уязвимости во внутренней сети. Если источник угрозы находится внутри корпоративной сети, к примеру, сотрудник компании, находящийся в сговоре со злоумышленником извне – то в этом случае, брандмауэр будет бесполезен.
- Сетевые устройства (особенно переносные) компании могут быть заражены, находясь за периметром защиты, и после подключены к внутренней сетевой инфраструктуре.
- Если в компании функционирует беспроводная локальная сеть, то подключенный к ней удаленно злоумышленник уже окажется внутри периметра защиты.

1 Классификация межсетевых экранов

В зависимости от методов фильтрации трафика и режимов работы, брандмауэры можно разделить на несколько категорий: межсетевые экраны пакетной фильтрации, МЭ проверки состояния, МЭ NAT, МЭ прикладного уровня и гибридные МЭ.

Брандмауэры пакетной фильтрации обеспечивают выборочную маршрутизацию пакетов, как для внешних, так и для внутренних хостов. Блокировка или пропуск пакетов осуществляются в соответствии с правилами политики безопасности.

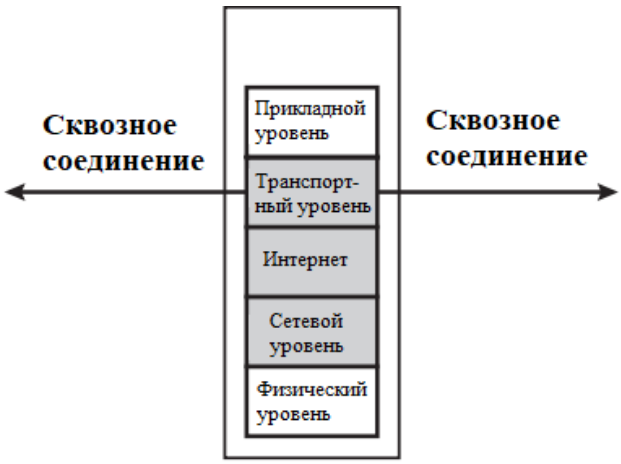


Рисунок 1.1 – Схема межсетевого экрана пакетной фильтрации

Преимущество брандмауэров пакетной фильтрации заключается в том, что они фактически незаметны для пользователей и обладают высоким быстродействием. Но так как они работают на недостаточно высоких уровнях, атаки на прикладном уровне не смогут быть отражены межсетевым экраном. Использование более низких уровней OSI так же не даёт возможность использовать продвинутые алгоритмы аутентификации пользователей. Атаки, эксплуатирующие уязвимости стека протоколов TCP/IP, такие как подмена IP адреса (IP spoofing) также не могут быть отражены большинством брандмауэров пакетной фильтрации.

Межсетевые экраны проверки состояния являются модифицированными МЭ пакетной фильтрации, но в отличие от последних позволяют, во-первых, отслеживать атрибуты пакетных наборов, а не каждого пакета по отдельности, а во-вторых, такие МЭ способны определить, в каком состоянии находится текущее TCP подключение – инициализация, передача данных либо закрытие соединения. Некоторые брандмауэры проверки состояния отслеживают данные таких протоколов FTP, IM, SIPS, чтобы узнать больше информации о текущих подключениях и их состоянии.[8]

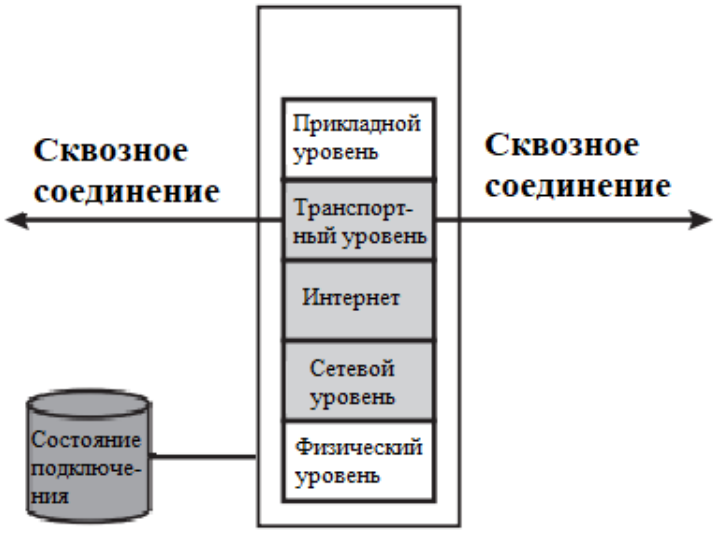


Рисунок 1.2 - Схема межсетевого экрана проверки состояния

Брандмауэры NAT позволяют использовать технологию Network Address Translation для функционирования корпоративной сети. Все сетевые устройства внутри периметра защиты будут иметь внутренние IP-адреса, которые будут преобразовываться для работы с внешними сетями. Само по себе, такое преобразование не является мерой защиты, однако будет полезно для скрытия топологии корпоративной сети. Механизмы работы таких межсетевых экранов могут отличаться. Один внутренний адрес может соответствовать единственному внешнему адресу. Такой подход существенно замедлит работу сетевых подключений. Также возможно динамически выделять адрес внешнего хоста каждый раз, когда с внутреннего адреса пытаются инициализировать подключение. В этом случае будет ограничено количество внутренних хостов, которые могут одновременно получить доступ к сети Интернет. Еще одним решением может быть использование переброса портов для того чтобы несколько устройств могли использовать один и тот же внешний сетевой адрес. Однако самым эффективным механизмом является динамическое создание пары из внешнего адреса хоста и номера порта для каждого внутреннего устройства, инициализирующего подключение к внешней сети.

Межсетевые экраны прикладного уровня – это набор программного обеспечения, которое позволяет удаленно разрешить, либо запретить прохождение трафика. Обмен данными проходит через шлюз прикладного уровня, который выступает в роли прокси и позволяет осуществлять обмен данными с удалёнными устройствами. Для доступа к брандмауэру пользователю необходимо предоставить данные для аутентификации через внешнее TCP/IP приложение. Такие МЭ считаются более безопасными, чем экраны пакетной фильтрации, так как вместо запрета или одобрения на прохождение конкретных пакетов на уровнях TCP и IP, необходимо выбрать несколько доверенных приложений, а брандмауэр после исследования их атрибутов определит все доступные разрешения для прохождения трафика.

Такой подход даёт широкие возможности по ведению журналов всего приходящего и выходящего трафика на прикладном уровне.

Гибридные МЭ является следствием комбинирования механизмов работы нескольких брандмауэров разного типа. Примером такого объединение может служить добавление функций пакетной фильтрации в МЭ прикладного уровня для того, чтобы обеспечить лучшую поддержку протокола UDP. По этому же принципу, разработчики МЭ пакетной фильтрации и МЭ проверки состояния добавляют некоторые функции брандмауэров прикладного уровня для расширения возможностей аутентификации пользователей и журналирования событий. Такое решение позволяет предприятиям оптимизировать нагрузку на межсетевые экраны и при этом обеспечить должный уровень безопасности. Гибридные брандмауэры используют механизмы пакетной фильтрации для событий невысокого риска, проверку состояния пакетов для трафика с более высоким уровнем риска и шлюзы прикладного уровня там, где необходимо обеспечить безопасность от атак более высокого уровня.

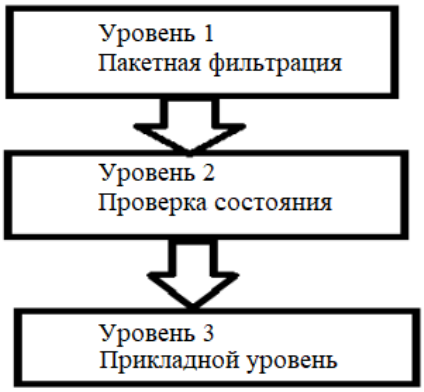


Рисунок 1.3 – Структурная схема гибридных межсетевых экранов

Ниже в таблице приведена сравнительная характеристика межсетевых экранов разных типов по следующим признакам: доступность (видимость) трафика, механизмы защиты, сложность аудита и их особенностям.

Таблица 1.1 – Сравнение типов межсетевых экранов

Тип межсетевого экрана	Пакетной фильтрации	Проверки состояния	NAT	Прикладного уровня	Гибридный
Доступ к трафику	Видимость сетевых адресов и протоколов	Видимость сетевых адресов, либо данных состояния	Видимость сетевых адресов двух типов и сетевых портов	Видимость полного содержимого пакета	Видимость полного содержимого пакета

Механизм защиты	Сканирование по правилам прохождения трафика	Сканирование по содержимому пакетов: заголовок либо поле данных	Недоверенные адреса не попадают в периметр защиты	Правила прохождения трафика, аутентификация пользователей	Сканирование по содержимому пакетов
Сложность аудита	Аудит затруднен	Аудит возможен	Аудит возможен	Широкие возможности для аудита	Чаще всего активно подвержен аудиту
Особенности	Сложность правил прохождения трафика	Обнаружение только известных атак	Не имеет механизма сканирования	Прокси заменяют правила для трафика	Требуется добавление белых листов

1.1 Классификация межсетевых экранов по объектам защиты

Как правило, для брандмауэра выделяется одна отдельная машина под управлением операционной системы, основанной на Unix. Однако также распространение получили и специальные программные модули, встроенные в маршрутизаторы или коммутаторы. По расположению межсетевого экрана в корпоративной сети, условно выделяют 3 варианта: узел-бастион (Bastion-host), брандмауэры для конечных узлов и персональные брандмауэры.

Узел-бастион – это критически важный элемент всей безопасности предприятия. Обычно он представляет собой отдельную машину, расположенную на внешней стороне демилитаризированной зоны. Такой узел чаще всего является платформой для разворачивания межсетевых экранов прикладного уровня. Узел-бастион состоит из множества прокси-модулей для управления DNS, FTP, SMTP-серверами, что позволяет собирать большое количество аудиторской информации, журналов событий, информации о длительности соединений и их текущем статусе. Конфигурация узла-бастиона позволяет установить дополнительные средства аутентификации для доступа к каждому прокси-модулю по отдельности. Такие прокси-модули имеют собственные настройки безопасности и имеют лишь ограниченный список команд, которые можно использовать для управления серверами, к которым они подключены. К тому же, прокси-модули не зависят как от самого узла-бастиона, так и от других модулей, что позволяет без вреда для других компонентов узла модифицировать такие модули. Количество прокси-модулей, устанавливаемых на узел-бастион ограничены только вычислительной мощностью последнего. Для обеспечения безопасности, изначально у модулей нет прав на исполнение или запись файлов, они могут исключительно считывать собственный конфигурационный файл. Для

функционирования, прокси-модулям не нужно прав супер-пользователя, а их директории хранятся на узле-бастионе в зашифрованном виде.

Брандмауэры конечных узлов используются для защиты устройств внутри корпоративной сети и чаще всего устанавливаются на сервера предприятия. Работа таких межсетевых экранов заключается в фильтрации всех проходящих пакетов, согласно правилам прохождениям трафика и политикам безопасности. Обычно такие межсетевые экраны имеют гибкую настройку под необходимые задачи хостов и работу с конкретными приложениями и сервисами. Из-за независимости от топологии корпоративной сети, использование таких брандмауэров позволяет совместить их функционал с функционалом межсетевых экранов других классов и уровней, что обеспечивает дополнительный уровень информационной защиты от угроз, как из глобальных внешних сетей, так и из внутренней сети.

Персональные брандмауэры контролируют входящий и исходящий трафик между конечными устройствами и глобальной сетью, что позволяет использовать их как для персональных компьютеров, так и внутри корпоративных сетей. Обычно, такие межсетевые экраны встроены в базовый набор ПО современных операционных систем и имеет встроенную конфигурацию для базовой защиты ПК от внешних угроз. Основная их задача состоит в запрете неавторизованного доступа к ресурсам компьютера извне. Несмотря на то, что персональные брандмауэры не имеют средств для гибкой и глубокой конфигурации, как межсетевые экраны более высоких классов, их функционала достаточно для обнаружения и нейтрализации подозрительного ПО и вирусов.

1.2 Классификация топологий сетей с межсетевыми экранами

Цель применения брандмауэров всегда одна и заключается в отделении внешнего потенциально опасного трафика от внутреннего, однако вариантов размещения таких программно-аппаратных средств существует множество. Ниже приведены наиболее актуальные варианты топологии сети с применением межсетевых экранов.

Сети с DMZ предполагают размещение внешнего межсетевого экрана на границе внутренней сети, вместе с роутером, который обеспечивает непосредственный доступ к глобальной сети. Внутренний межсетевой экран (один или несколько) будет обеспечивать защиту внутренний сети. Сеть, соединяющая два брандмауэра, называется DMZ – демилитаризированная зона. Внутри таких сетей обычно размещают сервера и службы, доступ к которым часто осуществляется из внешних сетей, но которым необходима базовая защита от угроз. Примерами таких служб могут быть DNS-служба, сервер корпоративной почты, внутренний сайт компании и так далее. Такая конфигурация позволяет устанавливать разные правила для внутренних и внешних межсетевых экранов, например внутренним брандмауэрам уже не нужно будет пропускать потенциально опасный трафик, который был

предназначен для сервисов внутри DMZ. Использование нескольких внутренних межсетевых экранов позволит защитить участки корпоративной сети даже в том случае, если источник угрозы находится внутри неё.

Использование частных виртуальных сетей (VPN) позволяет гибко настраивать сетевую инфраструктуру компании, однако сама по себе технология подразумевает использование глобальной сети и требует дополнительных мер защиты, таких как аутентификация и шифрование каналов с помощью специальных протоколов, таких как OpenVPN, PPTP, IPsec и SSTP. Потенциальные угрозы безопасности, связанные с использованием Интернета для доступа к виртуальным частным сетям не мешают сетевым администраторам активно их использовать для разгрузки корпоративных серверов и удаленного доступа сотрудников к ресурсам компании. Для работы VPN необходимы средства аутентификации и шифрования, которые обеспечивает межсетевой экран или маршрутизатор. Однако если брандмауэр будет работать с протоколом IPSec и весь трафик виртуальной частной сети будет зашифрован в оба конца, то межсетевой экран утратит возможность фильтрации трафика, журналирования или сканирования угроз.

Межсетевые экраны выделенного типа позволяют объединить ресурсы брандмауэров конечных узлов с автономными брандмауэрами. Такое объединение позволит управлять большим количеством межсетевых экранов как на корпоративных серверах компании, так и на конечных устройствах удаленных пользователей. Очевидным преимуществом выделенных межсетевых экранов будет удобство сбора всей аудиторской и аналитической информации со всех подключенных устройств.

1.3 Сравнение межсетевых экранов нового поколения (NGFW)

В качестве основного программного решения для дипломного проекта был выбран брандмауэр от компании Palo Alto. Однако для понимания необходимости его использования, как в качестве защитной меры, так и как средства для получения практических навыков и знаний в рамках учебного курса, имеет смысл провести сравнительную характеристику с другим программным решением – брандмауэром от компании CheckPoint.

Оба решения имеют схожее назначение и стоимость, поэтому сравнение будет проводиться по схожим признакам и особенностям. Однако имеет смысл определить точки расхождения в задачах, выполняемых брандмауэрами.

Межсетевые экраны нового поколения от компании CheckPoint работают лучше всего вместе с другими продуктами компании и чаще всего устанавливаются в составе целого комплекса решений по сетевой безопасности.

Решение от Palo Alto обеспечивает лучшую производительность, управление и расширяемость отдельно от других программных и программно-аппаратных средств обеспечения защиты сети. Именно функциональная независимость от других компонентов позволяет удешевить установку и последующее обслуживание межсетевого экрана Palo Alto.

Таблица 1.3 – Сравнительная характеристика

Характеристика	Palo Alto	Check Point
Исполнение	Аппаратное, виртуальное (VMware ESXi, Citrix SDK, KVM, Nutanix, Microsoft Hyper-V, OpenStack, Cisco ACI, AWS, Azure, vCloud Air, Google Cloud, Oracle Cloud, Alibaba Cloud)	Аппаратное, виртуальное (Cisco ACI, VMware NSX,ESXi, Microsoft Hyper-V, Openstack, KVM)
Операционная система	Собственная - PanOS	Собственная – Gaia (на базе Red Hat Linux)
Поддержка облачной среды	Amazon AWS, Microsoft Azure, vCloud Air, Google Cloud, Oracle Cloud, Alibaba Cloud	Amazon AWS, Microsoft Azure, Google Cloud, Oracle Cloud, Alibaba Cloud, IBM Cloud
Управление	WebGui, CLI, электронная почта, REST API, SNMP, bash-скрипты	REST API, SNMP, плагин Chrome, приложение Splunk, система управления Panorama

Поддержка технологий DNAT, SNAT	Да	Да
Технологии трансляции сетевых адресов	Static NAT (IPv4/IPv6), Dynamic NAT (IPv4,IPv6), NAT64, IPv6 NPTv6 (Network Prefix Translation)	Static NAT, Hide NAT, NAT64
Алгоритмы шифрования	DES, 3DES, AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-CCM, AES-128-GCM, AES-256-GCM	NSA Suite-A, Suite-B
Собственные средства для VPN	GlobalProtect VPN Client	Нет
Средства для туннелирования	IPsec site-to-site, IPsec client-to-site, LSVPN, SSL client-to-site, GRE, GTP, VXLAN, Cisco SGT, HTTP/2, 802.1q	IPsec site-to-site VPN, SSL VPN
Механизмы кеширования	Нет	Нет
Механизмы для поведенческого анализа	Zone protection, корреляционные правила, правила для бот-сетей	Модуль Anti-Bot
IDS/IPS системы	Единый модуль для обнаружения приложений, IPS и антивируса	Модуль IPS с собственными сигнатурами
Добавление собственных сигнатур	Импорт в формате SNORT, Professional Service по написанию сигнатур приложений	В формате SNORT и индикаторы по REST API
Блокирование нераспознанных приложений	Да	Да
Наличие открытой базы данных приложений	Applipedia	CheckPoint Threat Wiki
Собственные антивирусные средства	Да, лаборатория UNIT42 по разработке антивирусного движка	Антивирусный движок Kaspersky Lab и BitDefender

2 Межсетевой экран Palo Alto

Брандмауэры нового поколения от компании Palo Alto позволяют выстроить защиту корпоративной сети вокруг трех типов объектов - пользователей, приложений и данных.

Рисунок 2.1 – Физическое исполнение межсетевого экрана

Межсетевые экраны проверяют весь входящий и исходящий трафик, все приложения и пакеты с привязкой с конкретным пользователям, не зависимо от их местоположения и типа устройства, которые они используют.

Основные механизмы защиты, используемые в брандмауэрах Palo Alto:

- Просмотр всего трафика, пользователей, приложений, сервисов? независимо от используемого порта
- Уменьшение рисков информационной безопасности путем блокировки всех приложений, которые не внесены в разрешенный список
- Наблюдение и контроль за каждым пользователем и устройством, не зависимо от их расположения в корпоративной сети
- Централизованное управление всеми событиями информационной безопасности для отражения внутренних и внешних угроз

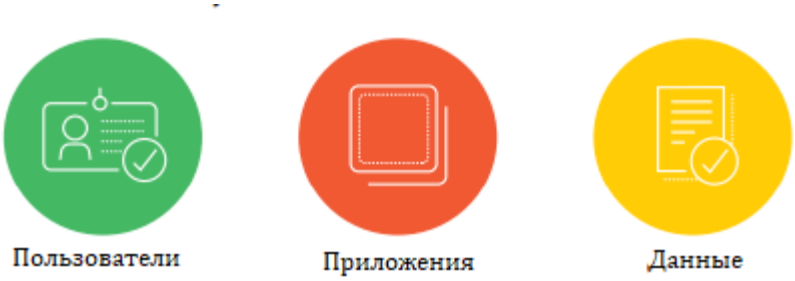


Рисунок 2.2 – Основные объекты защиты для брандмауэров нового поколения (NGFW)

Устаревшая модель защиты внутренних сетей, согласно которой угрозы могут быть только внешними, а все внутренние объекты являются безопасными, больше не может использоваться для современных компаний. Это обусловлено тем, что угрозы, проникнувшие во внутреннюю сеть незамеченными, получают полную свободу действий, что является критическим нарушением информационной безопасности предприятия. Современная модель защиты напротив, обеспечивает гораздо больший

уровень надёжности благодаря принципу "запретить всё, что не разрешено", помимо этого, текущие стратегии построения ИБ должны обеспечивать минимальные права доступа к критическим ресурсам компании.

Межсетевые экраны нового поколения также должны использовать механизмы защиты пользовательских данных, потому что чаще всего кража данных для входа в учетные записи сотрудников и клиентов компаний являются целью проведения большинства сетевых атак. Для предотвращения атак такого типа, брандмауэр Palo Alto используют следующие механизмы:

- Блокировка доступа к фишинговым сайтам с помощью URL-фильтрации и единой базы данных вредоносных ресурсов.
- Запрет для пользователей на отправку данных для входа на сайты, которых нет в разрешенных "белых" списках. Такой алгоритм будет полезен при попытке неизвестных вредоносных сайтов получить доступ к учетным записям сотрудников и клиентов.
- Многофакторная аутентификация (MFA) позволяет защитить учетные записи даже после того, как данные для входа были украдены. В качестве дополнительного этапа входа в учетную запись могут быть использованы SMS-сообщения, приложения-аутентификаторы, биометрические данные и т.д.
- Подключение дополнительных технологий. Например, внедрение поведенческого анализа, который позволяет отслеживать изменения в действиях, производимых пользователей (технология UEBA). Так же, брандмауэр может работать как составная часть SIEM-системы, которая будет следить за исполнением политик безопасности в режиме реального времени.

Для обеспечения должного уровня информационной безопасности внутри корпоративной сети, в брандмауэрах Palo Alto используется механизм «User-ID», суть которого заключается в глубоком аудите всех внутренних и внешних пользователей компании, а так же всего, что с ними связано. Пользователи со схожими по организационной структуре предприятия характеристиками объединяются в группы. Политики безопасности работают не с сетевыми или MAC-адресами, а напрямую с организационными единицами. Таким образом, доступ к критическим серверам компании можно выделить только системным администраторам, соответственно получать доступ они смогут не зависимо от того, на каком участке сети они находятся в данный момент или какое устройство используют. Дополнительным преимуществом такой стратегии может являться то, что при возникновении ситуации, угрожающей информационной безопасности компании со стороны какого-либо структурного подразделения или конкретного сотрудника, можно будет получить обширный доклад о всех действиях со стороны источника угрозы ИБ.

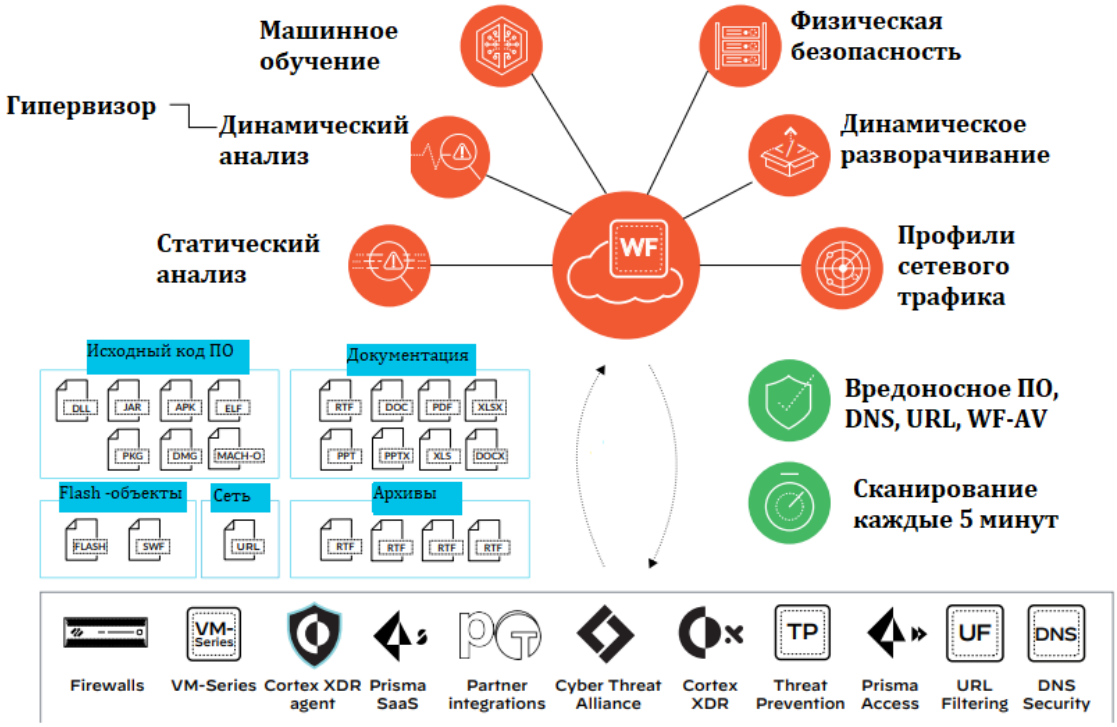


Рисунок 2.3 – Механизмы функционирования брандмауэра Palo Alto

Современные брандмауэры должны также обеспечивать защиту от продвинутых угроз. В брадмауэрах Palo Alto реализованы механизмы, которые способны противодействовать таким угрозам, отражая или локализуя их ущерб:

- Встроенная служба предотвращения угроз (IPS) содержит средства блокировки эксплойтов, сканирования портов, переполнения буфера. Механизмы IPS-системы также позволяют защитить данные межсетевого экрана от обфускации и перехвата управления.
- Блокировка доступа к вредоносным ресурсам с помощью URL-фильтрации.
- Технология WildFire. Собственная разработка Palo Alto, которая позволяет проводить анализ и отражение угроз с помощью технологий машинного обучения, динамической аналитики. Находясь в облачном ресурсе, эта технология обеспечивает защиту всей корпоративной сети, конечных узлов и других облачных сервисов.
- Защита DNS позволяет проводить глубокую аналитику и отражать атаки, направленные на службу доменных имен
-

Для оперативного реагирования на события информационной безопасности, современным межсетевым экранам необходимы средства для удобного, обширного и избыточного журналирования.

В брандмауэрах Palo Alto реализована технология Cortex Data Lake. Данная технология позволяет хранить логи в облачном сервисе, собирая данные со всех конечных узлов, а так же виртуальных и физических межсетевых экранов. Данная технология использует элементы машинного обучения, чтобы облегчить повседневные задачи, вроде корреляции событий, поиск отклонений от состояния безопасности и т.д.

В межсетевом экране реализован обширный функционал по созданию отчетов по событиям ИБ. Системный администратор может выбрать необходимые параметры и данные о текущем состоянии сетевой безопасности, и они будут автоматически собираться в регулярный отчет. Дополнительно можно настроить график отправки логов по электронной почте ответственным сотрудникам.

2.1 Конфигурация виртуальных машин

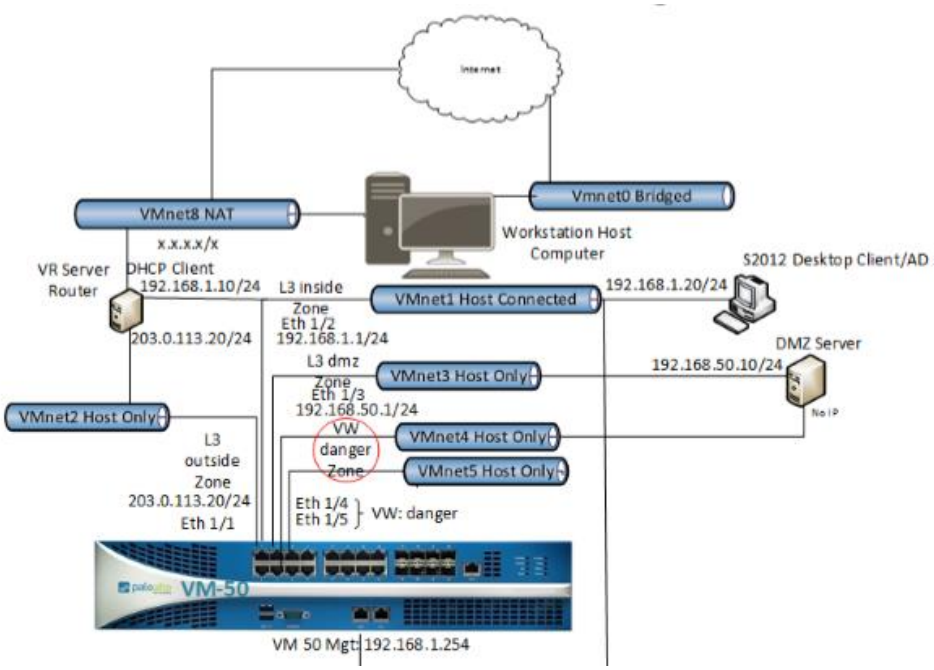


Рисунок 2.1.1 – Конфигурация сети предприятия

Топология, выбранная для использования сетевых устройств, состоит из 8-ми различных интерфейсов и 4-х основных устройств: межсетевого экрана, DMZ-сервера, рабочей станции и виртуального роутера. Доступ ко внешней сети может быть осуществлен только через виртуальные интерфейсы VMNet8 и VMNet0.

Для виртуальных машин было создано 8 интерфейсов, настройка первых семи отличается только IP-адресами подсетей.

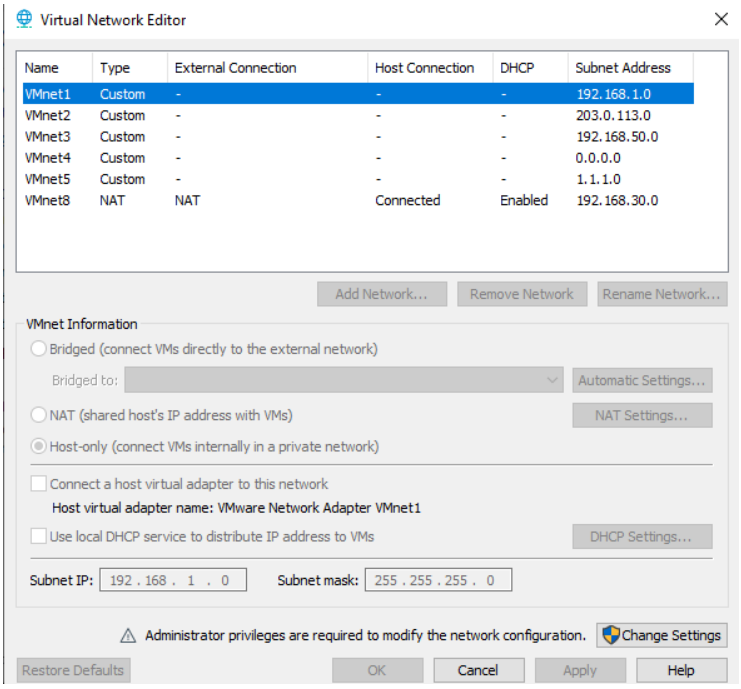


Рисунок 2.1.2 – Настройка сетевых адаптеров VMWare

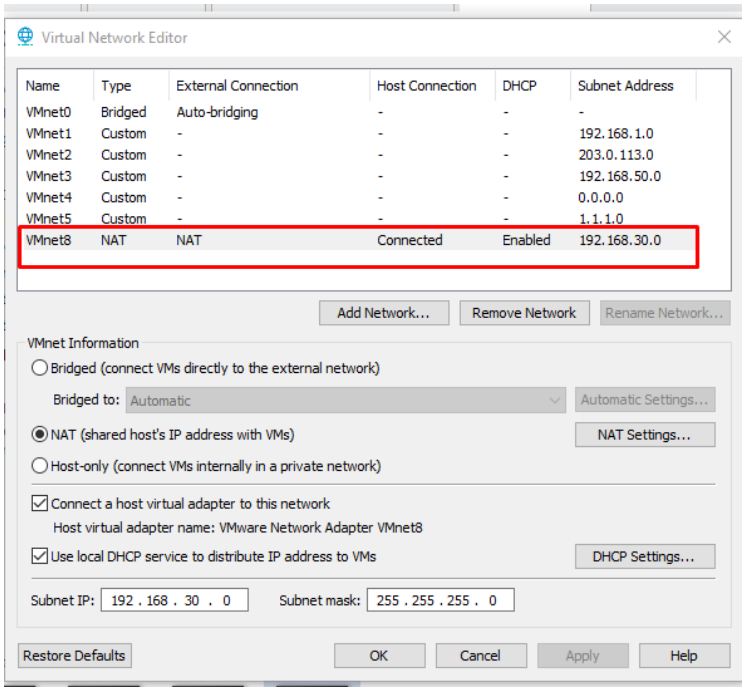


Рисунок 2.1.3 – Конфигурация сетевого адаптера для выхода во внешнюю сеть

Сетевые устройства, которые напрямую взаимодействуют с внешней сетью, подключены к сетевому интерфейсу с настроенным преобразованием сетевого адреса (VMNet8). Выход в глобальную сеть необходимо разрешить с рабочей станции и из виртуального маршрутизатора, на котором и будет установлено ПО нашего будущего межсетевого экрана.

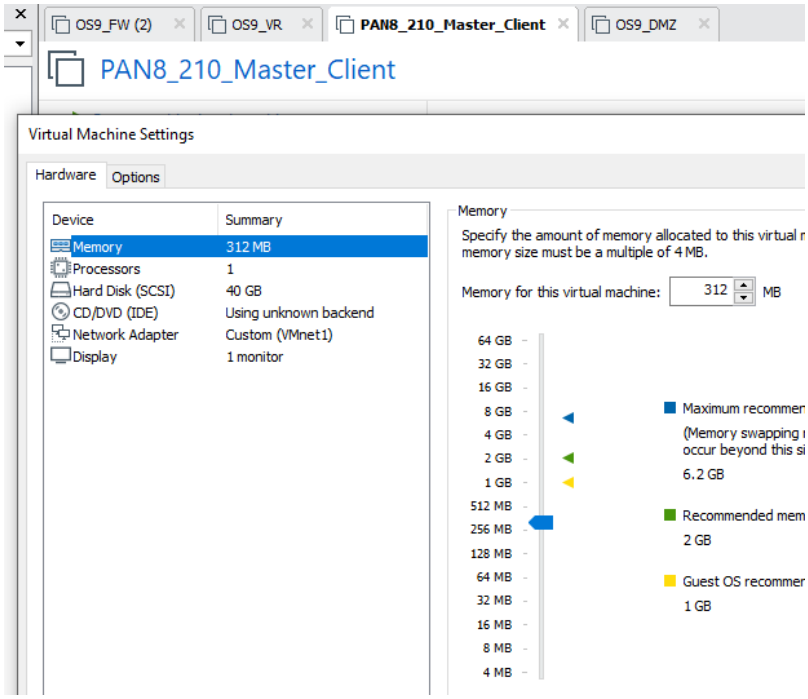


Рисунок 2.1.4 – Настройка виртуального рабочего ПК

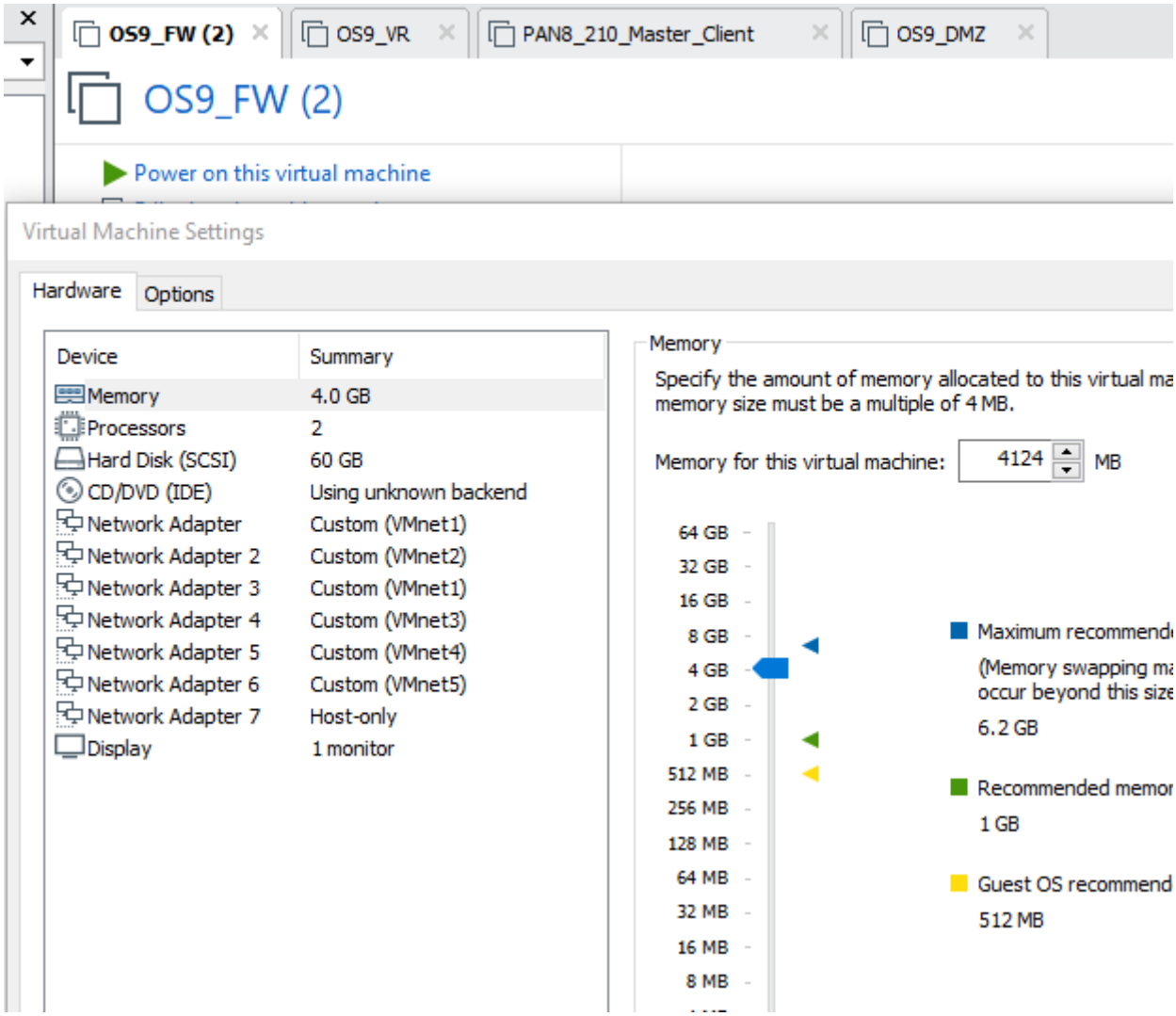


Рисунок 2.1.5 – Настройка виртуального Брандмауэра

На рисунке показана настройка виртуального оборудования для межсетевого экрана. Данная виртуальная машина является самой требовательной к ресурсам и её установка рекомендована на серверное оборудование. Минимальный объем оперативной памяти для работы с брандмауэром с ОС Palo Alto Networks составляет 4 гигабайта. Для использования всех виртуальных машин единовременно, требуется объем оперативной памяти около 12 Гбайт. Для стабильного функционирования всех компонентов настраиваемой инфраструктуры требуется использование средств распределения нагрузки между несколькими рабочими станциями с установленным на них ПО от VMWare или VirtualBox.

Остальные компоненты инфраструктуры являются менее требовательными – виртуальный маршрутизатор и DMZ-сервер используют операционные системы на ядре Unix. Рабочая станция использует ОС Windows, которая так же не требует больших ресурсов для запуска и функционирования.

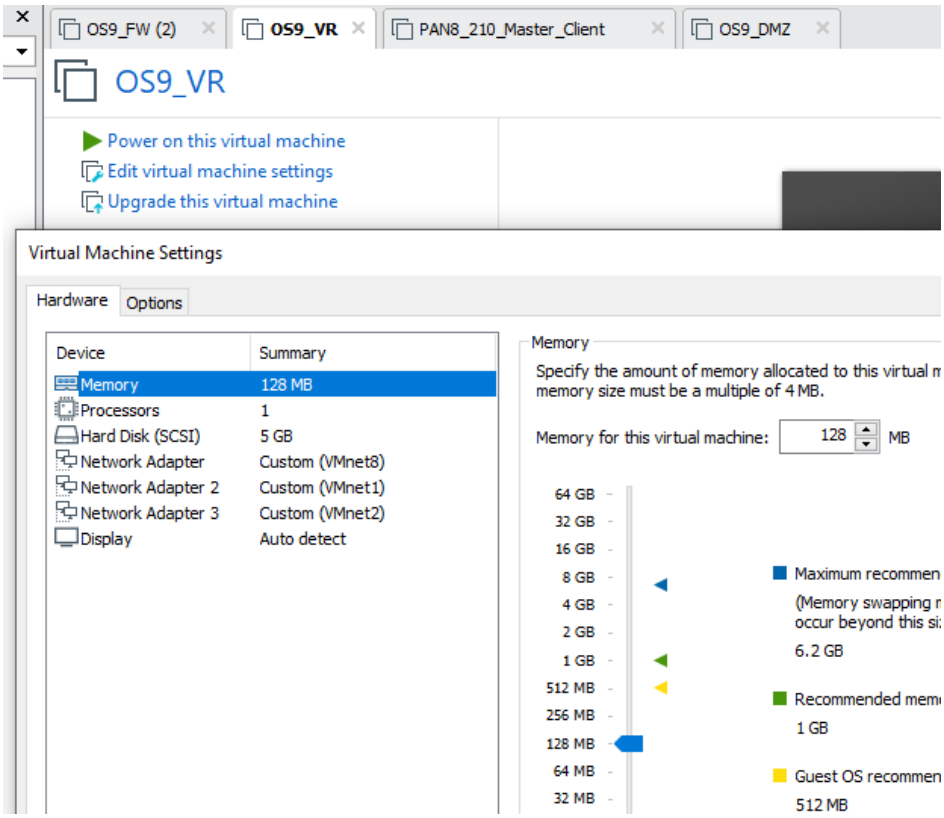


Рисунок 2.1.6 – Настройка виртуального роутера

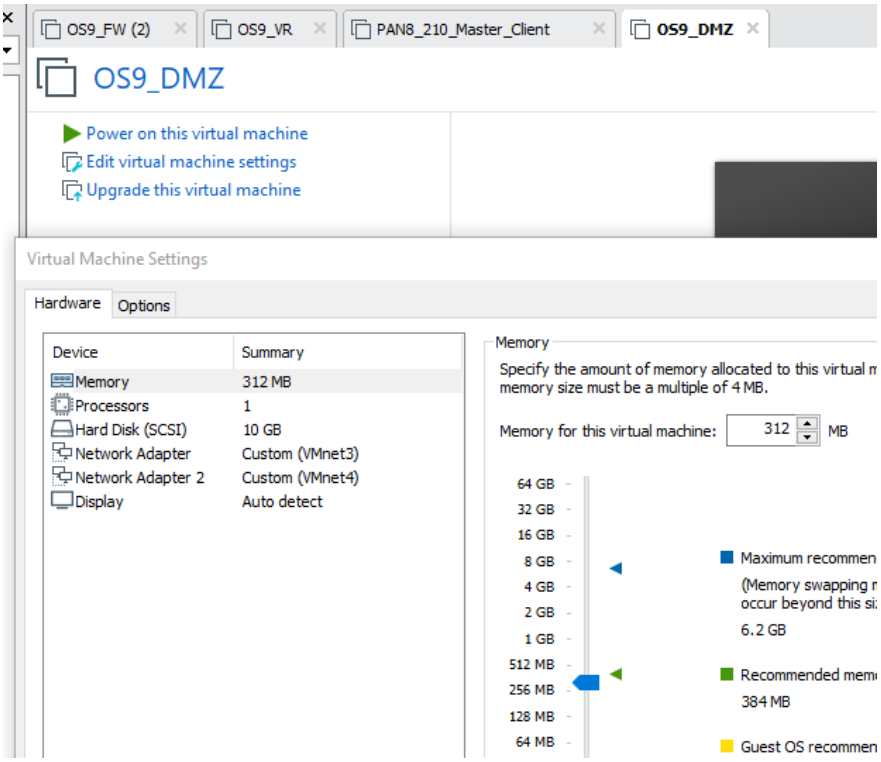


Рисунок 2.1.7 – Настройка DMZ-сервера

2.2 Настройка брандмауэра через сетевой интерфейс

Для подключения к межсетевому экрану через рабочую станцию необходимо убедиться, что все виртуальные машины работают и действительно объединены в общую сеть, для проверки можно использовать команду ping для обмена ICMP-пакетами.

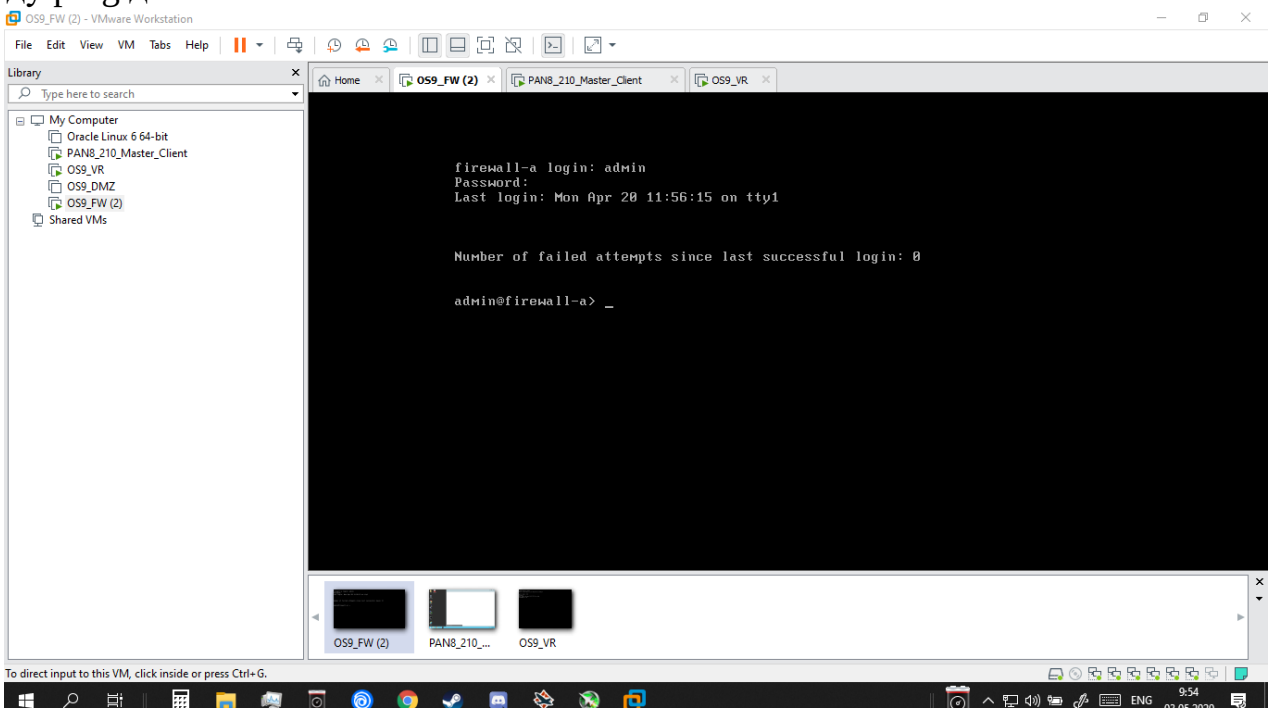


Рисунок 2.2.1 – Запуск виртуальной машины с брандмауэром

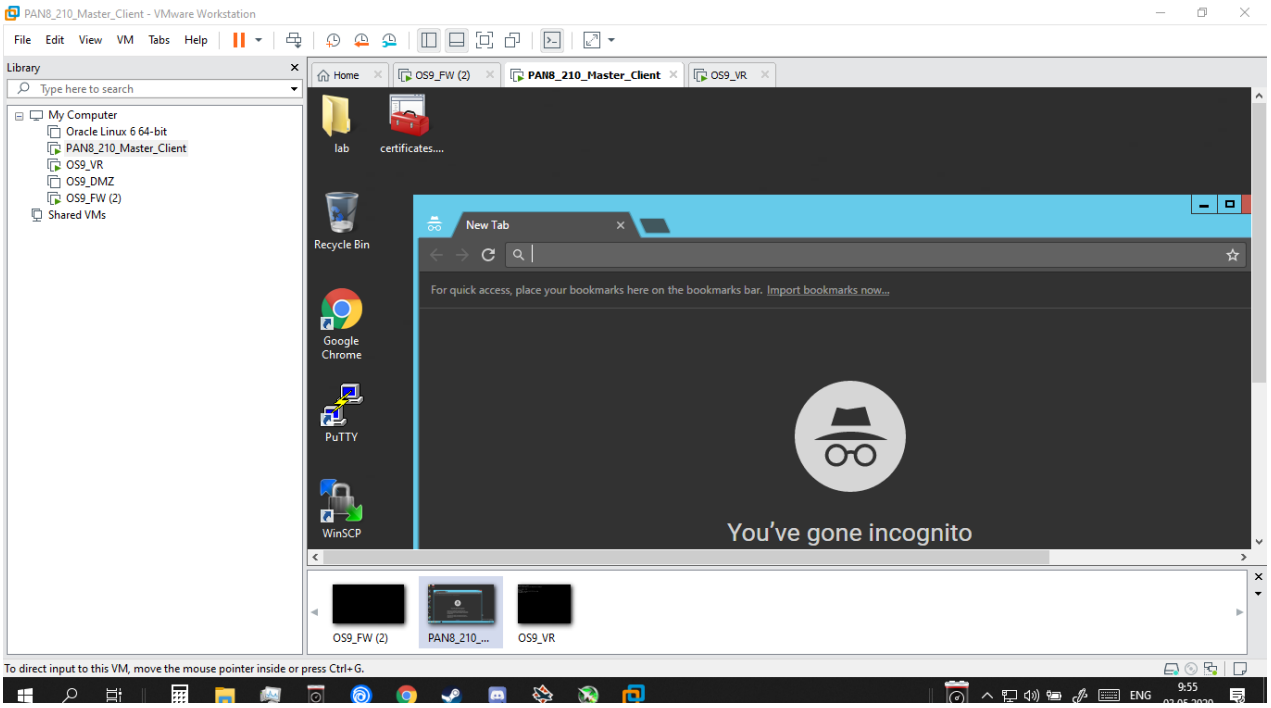


Рисунок 2.2.2 – Запуск клиентской виртуальной машины

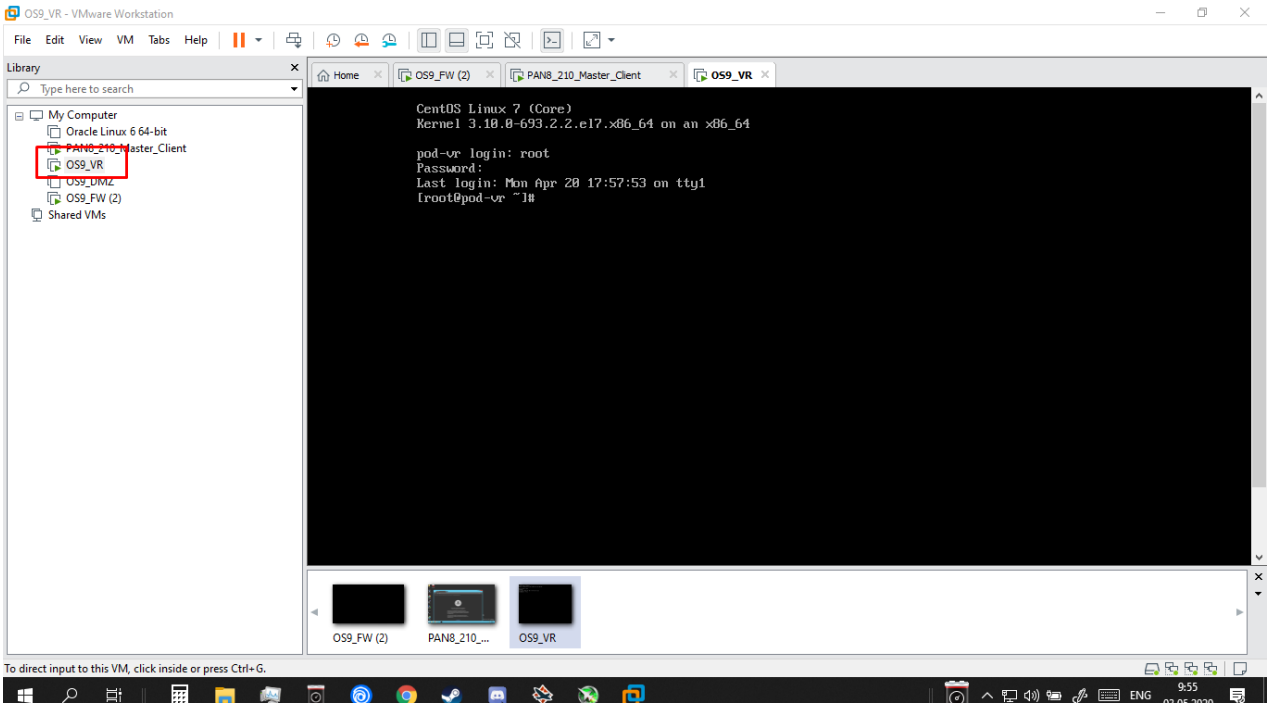


Рисунок 2.2.3 – Запуск виртуального маршрутизатора

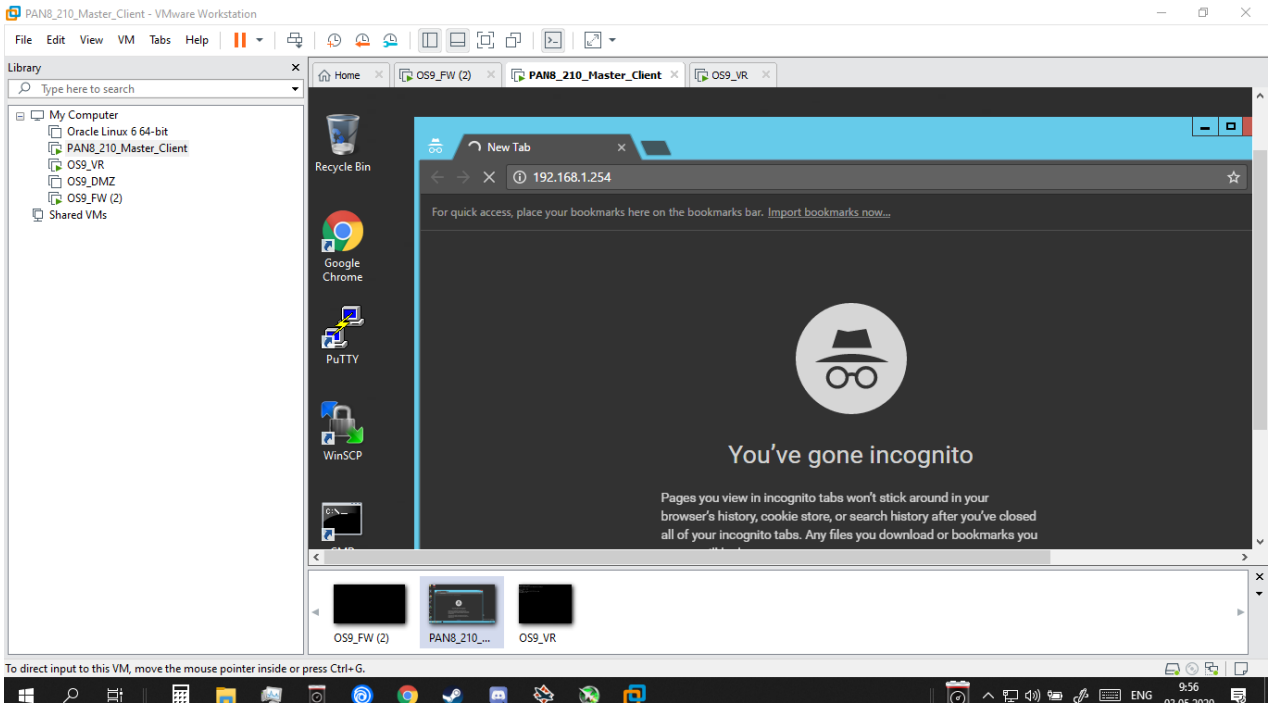


Рисунок 2.2.4 – Попытка подключения к брандмауэру

Подключение к Web-интерфейсу межсетевого экрана в виртуальной среде выглядит так же, как и для подключение к физическому устройству. Убедившись в том, что устройства действительно находятся в одной сети, выполняется переход по адресу виртуального межсетевого экрана.

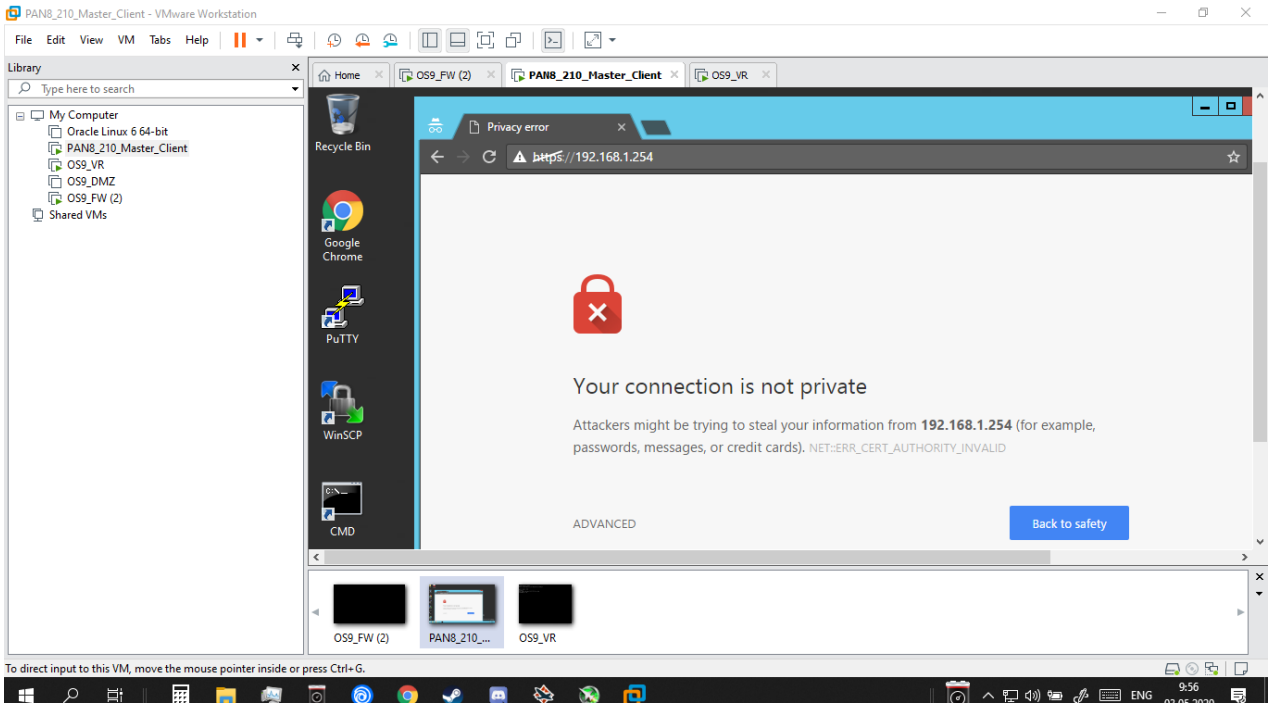


Рисунок 2.2.5 – Предупреждение об отсутствии HTTPS

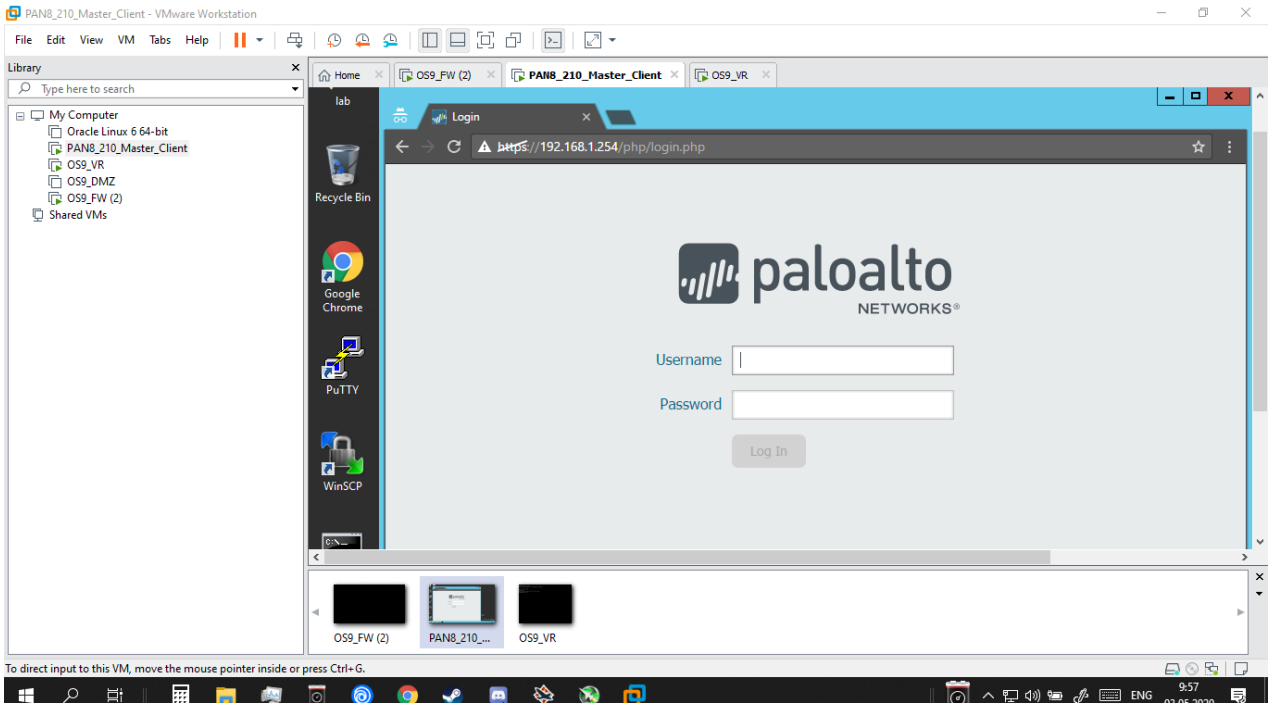


Рисунок 2.2.6 – Поля для авторизации межсетевого экрана

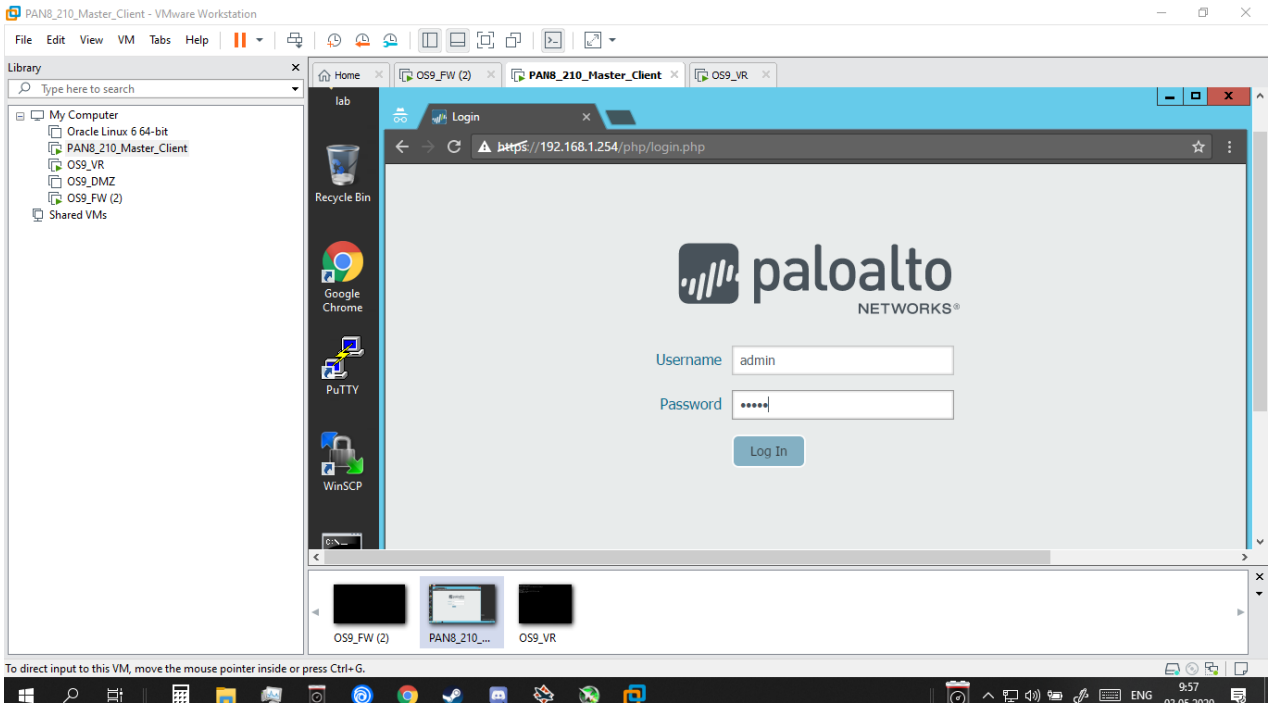


Рисунок 2.2.7 – Подключение к стандартной администраторской учетной записи

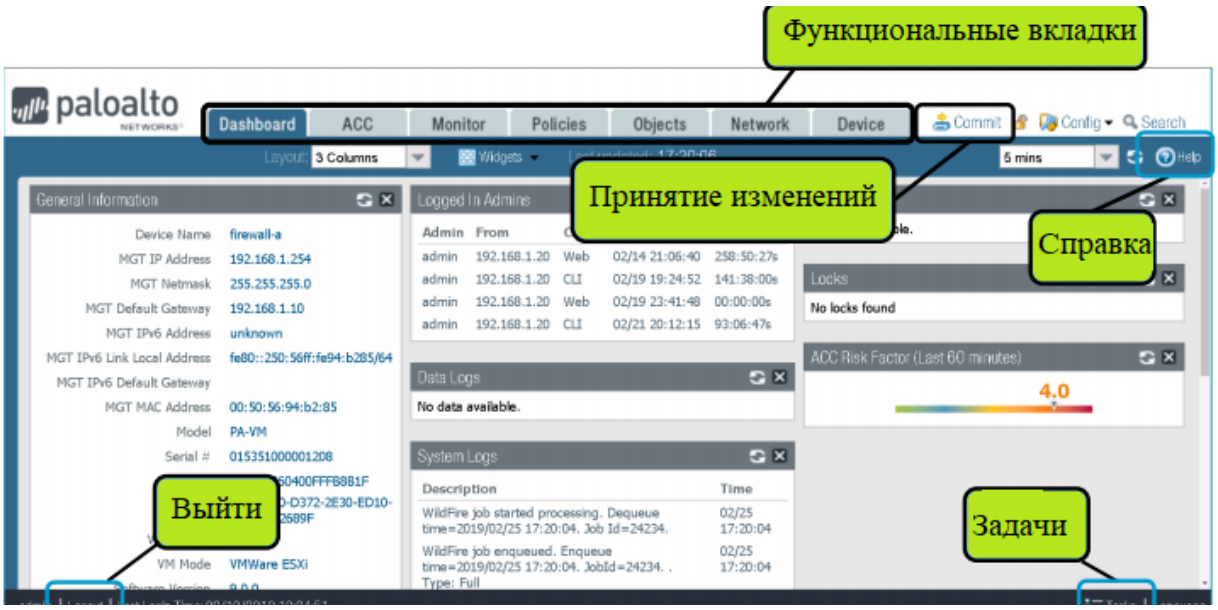


Рисунок 2.2.8 – Главная страница для администрирования брандмауэра

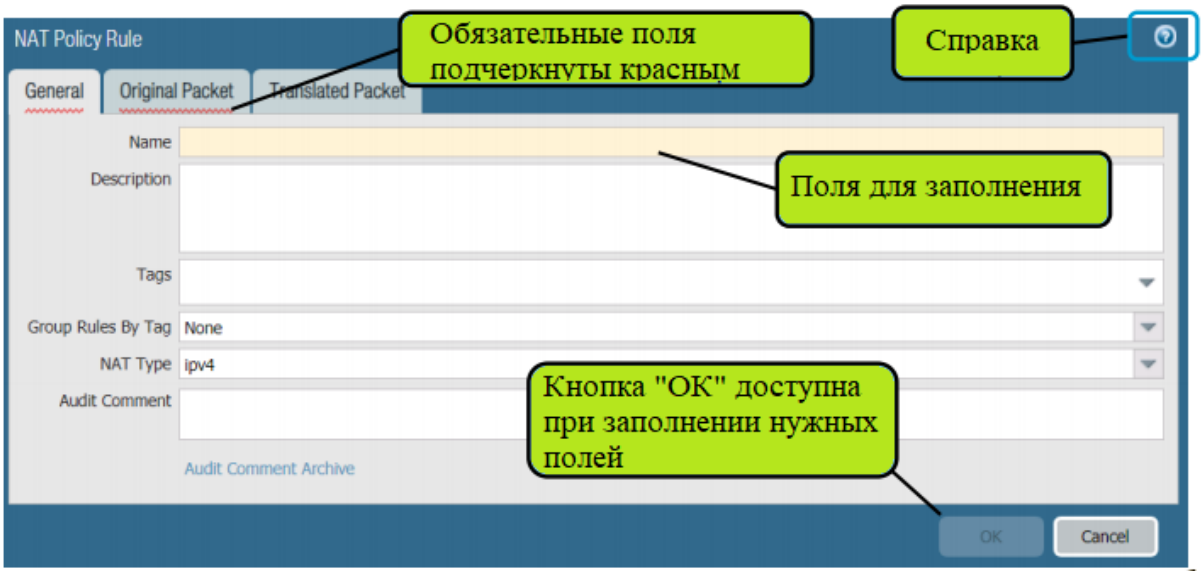


Рисунок 2.2.9 – Основные поля для создания правила прохождения сетевого трафика

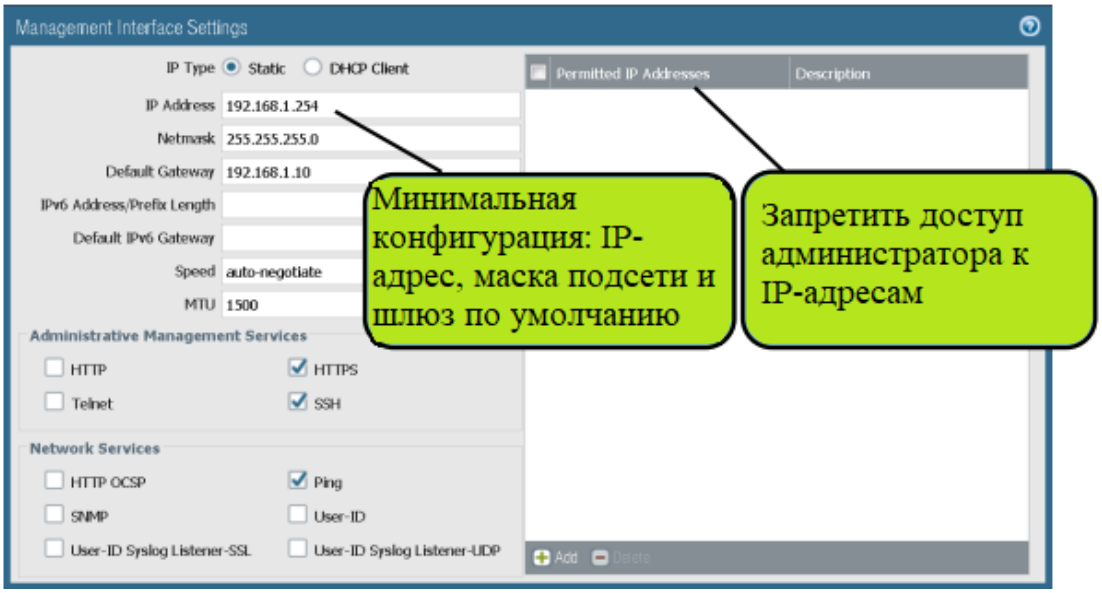


Рисунок 2.2.10 – Управление интерфейсами

Системные администраторы, управляющие функциями межсетевого экрана обладают средствами разделениями участков внутренней сети на участки и зоны. Данная функция используется для распределения уровней доступа для различных подразделений компании. Например, структурное подразделение бухгалтерии не может иметь доступ к участкам сети, кроме собственных, а управлению системного администрирования важно иметь доступ к интерфейсам других организационных единиц для их конфигурации и аудита.

Межсетевые экраны нового поколения Palo Alto используют алгоритмы шифрования с целью дешифровки подозрительного трафика для того, чтобы устранить потенциальные угрозы сетевой безопасности. Однако, если работа ведется с чувствительной информацией - то гибкие настройки управления позволят сохранить данные в зашифрованном виде. Так же, пользователям не дозволено переходить по ссылкам на те сайты, которые используют истёкшие, недоверенные или самоподписанные сертификаты безопасности. Дополнительно, ведется контроль версии TLS сайтов, так как старые версии протокола могут потенциально открыть точки входа в корпоративную сеть извне.

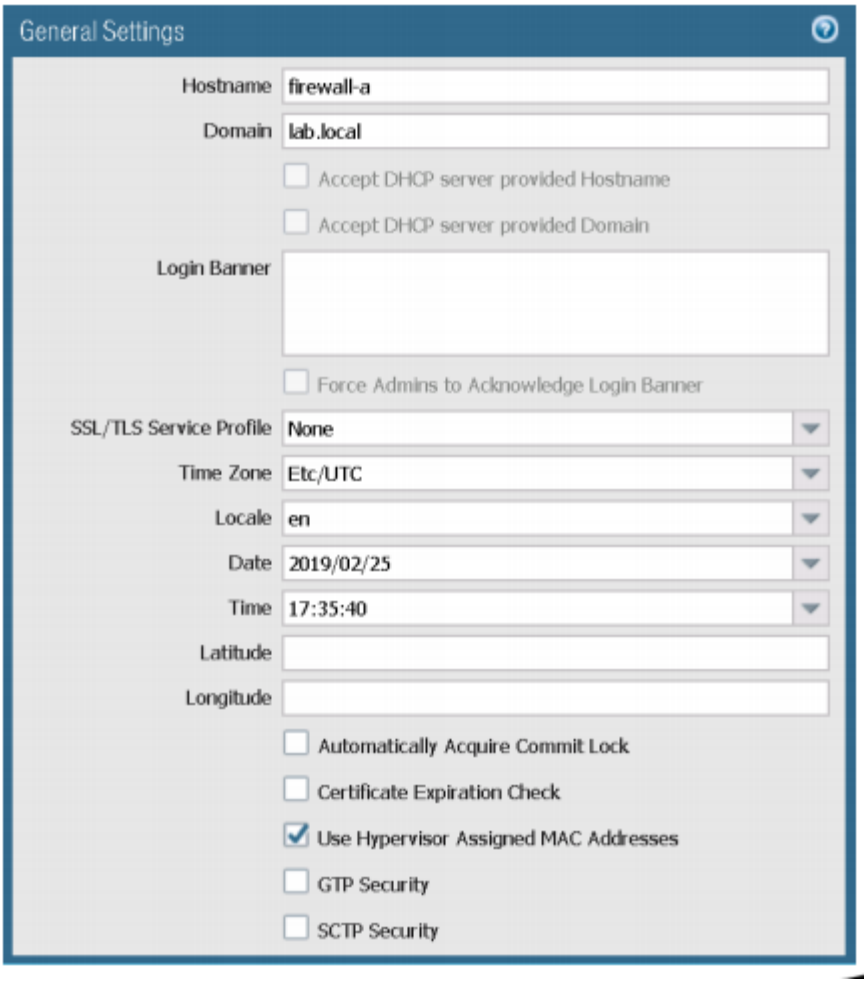


Рисунок 2.2.11 – Глобальные настройки межсетевого экрана

Для корректной работы всех функций брандмауэра необходимо настроить точное время, дату, местоположение, домен и т.д.

Так как на практике межсетевой экран работает внутри корпоративной сети функционирующего предприятия, необходимо настроить конфигурацию других сетевых сервисов, в том числе DHCP, DNS, Proxy и другие.

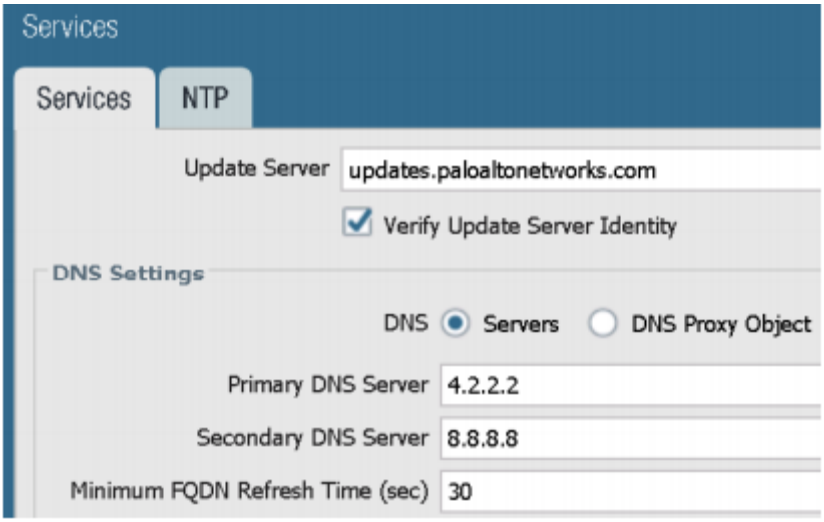


Рисунок 2.2.12 – Настройка сервисов внутри корпоративной сети

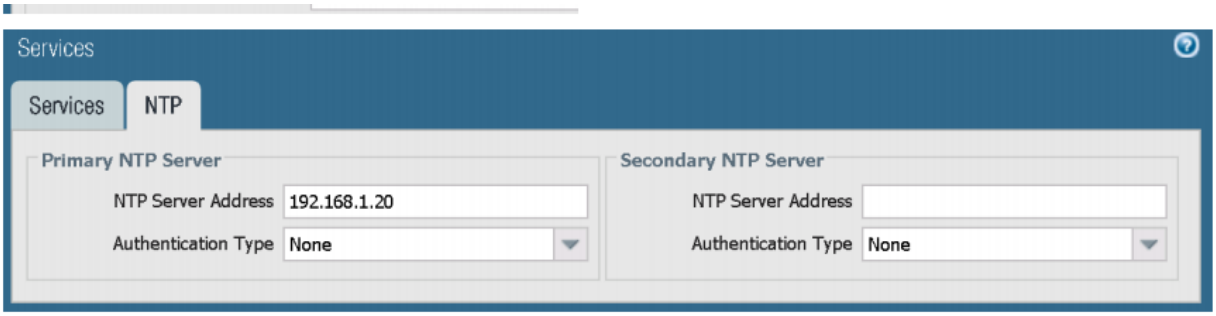


Рисунок 2.2.13 – Настройка NTP-серверов

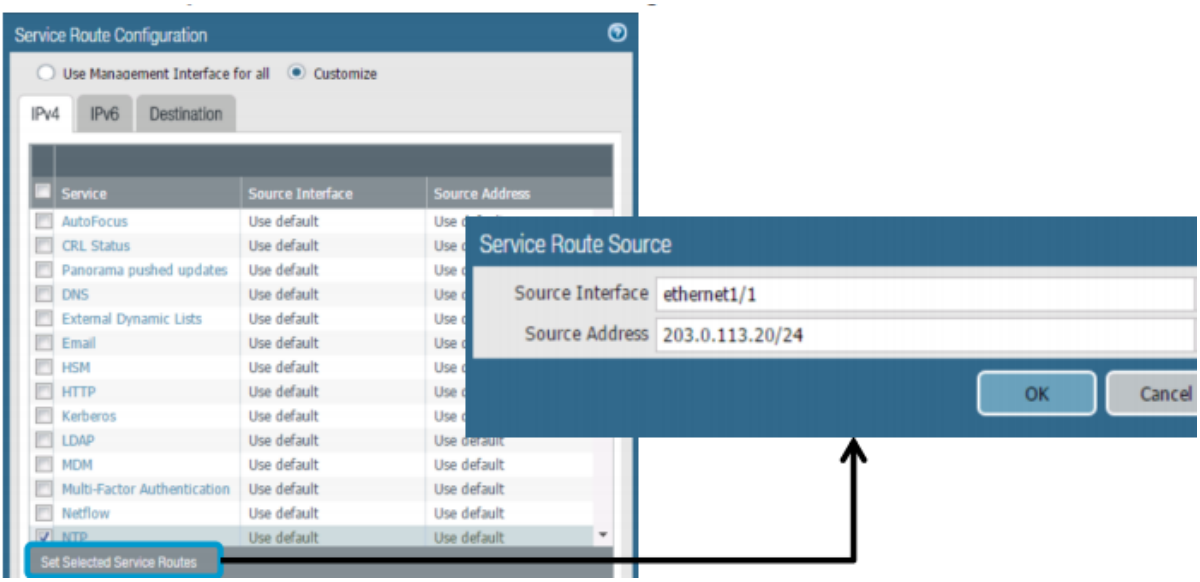


Рисунок 2.2.14 – Управление доступными сетевыми сервисами

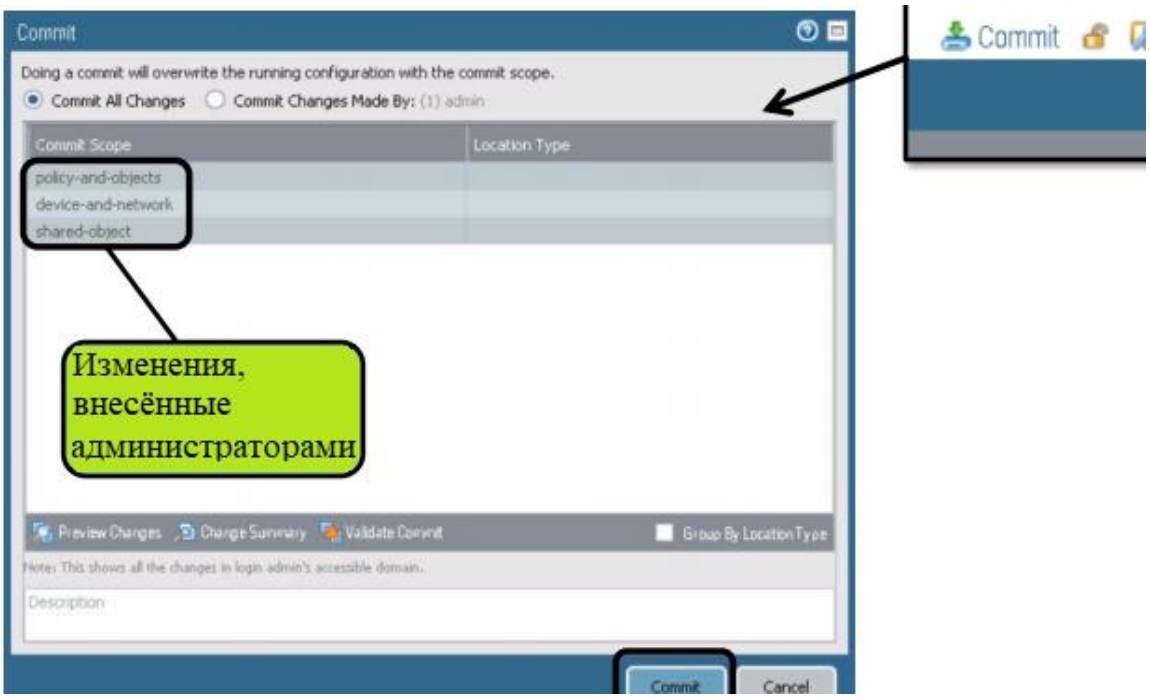


Рисунок 2.2.15 – Подтверждение внесенных изменений

Функция, которая будет полезна как при изучении функций межсетевого экрана несколькими студентами, так и при одновременной

настройке его функций несколькими администраторами заключается в том, что изменения, внесенные с каждой учетной записи, могут быть приняты в любой последовательности независимо друг от друга.

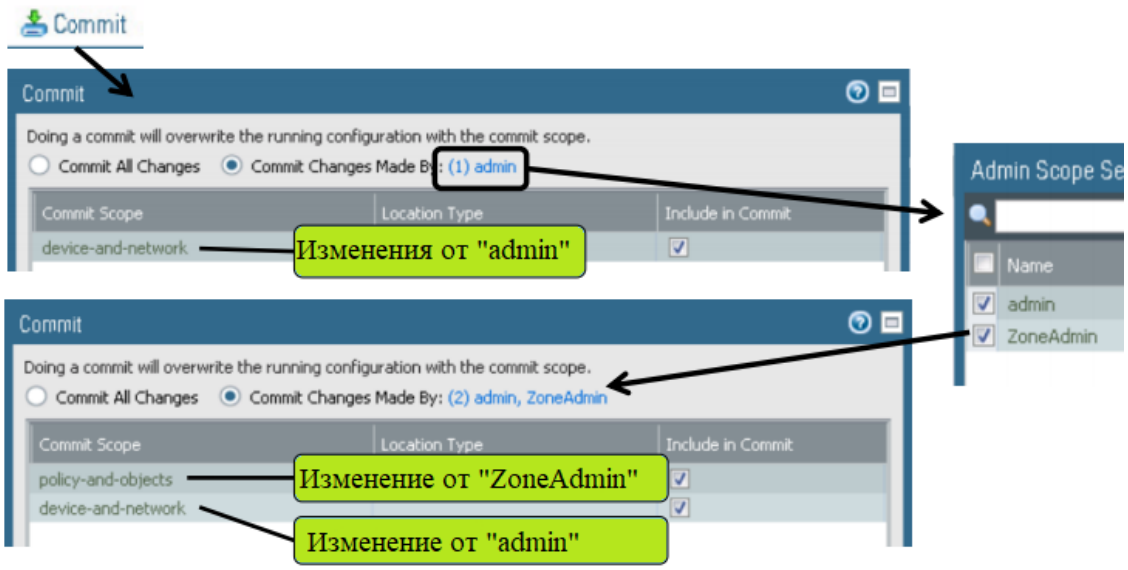


Рисунок 2.2.16 – Управление брандмауэром несколькими администраторами

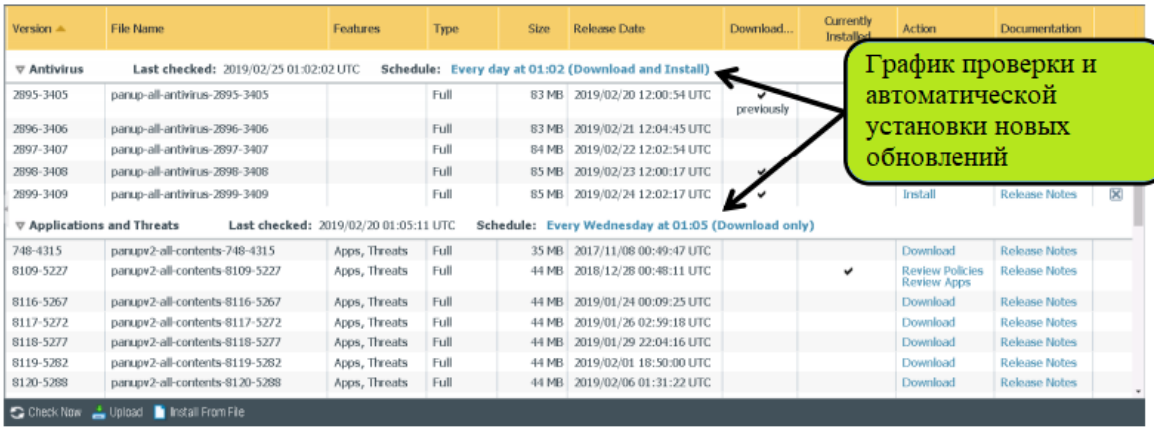


Рисунок 2.2.17 – Сведения о доступных обновлениях для ПО

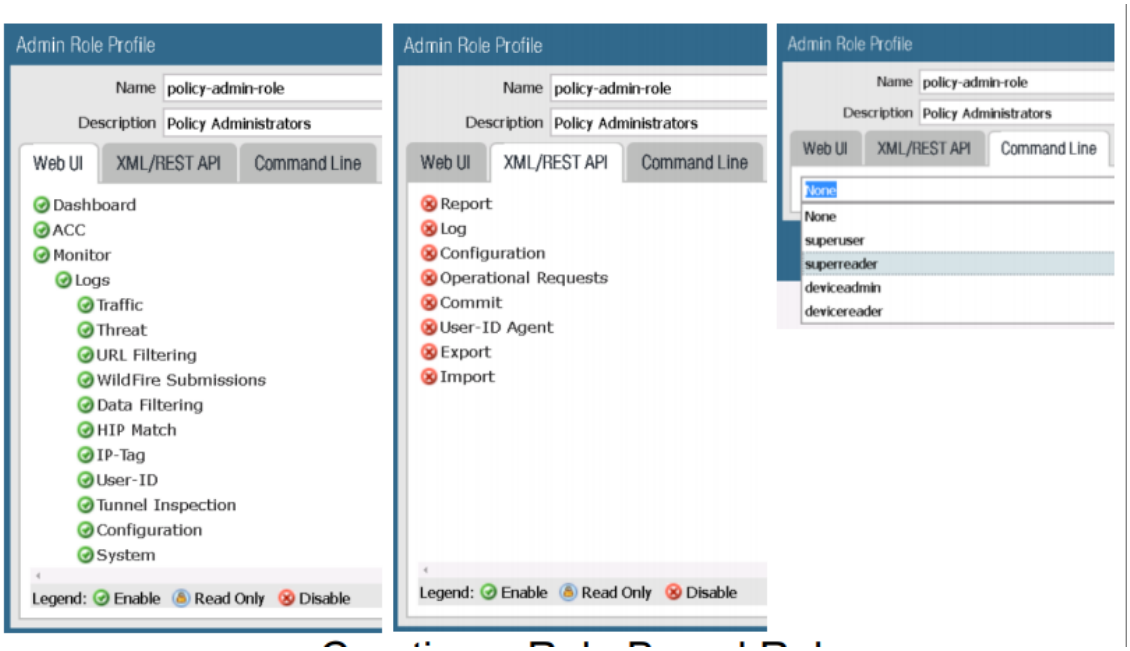


Рисунок 2.2.18 – Выбор роли для администраторской учетной записи

Межсетевой экран Palo Alto содержит множество надстроек для администраторов. Этого требует сложная структура организационных единиц совеременных предприятий. Так, например, администратор, ответственный за топологию корпоративной сети не сможет выполнять функционал администратора групповых политик и наоборот.

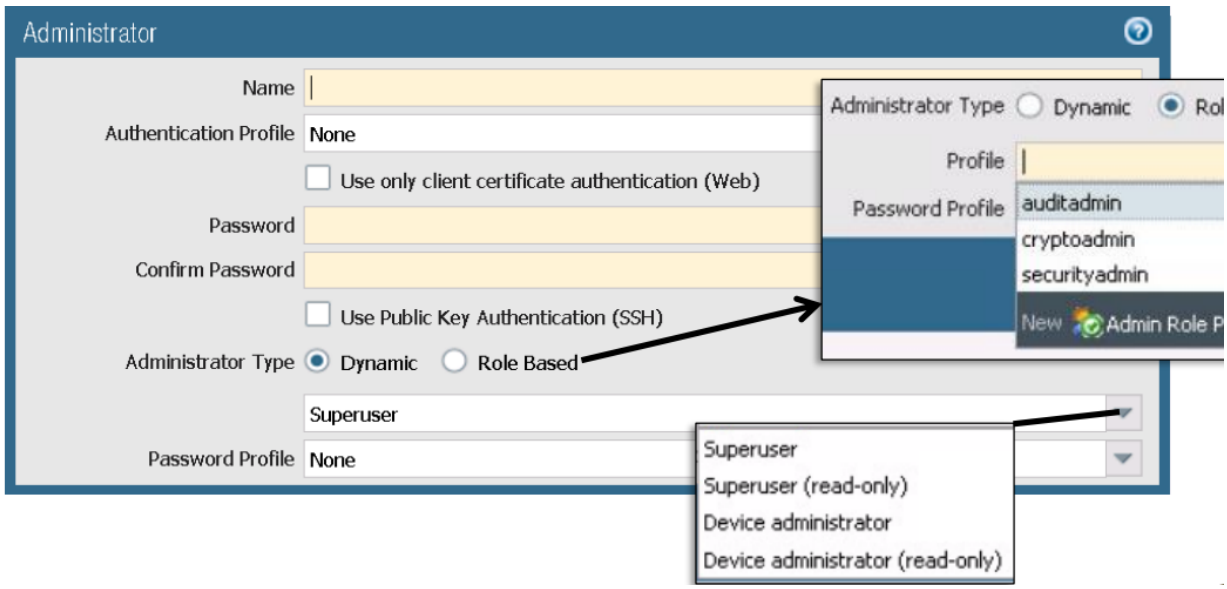


Рисунок 2.2.19 – Настройки администратора

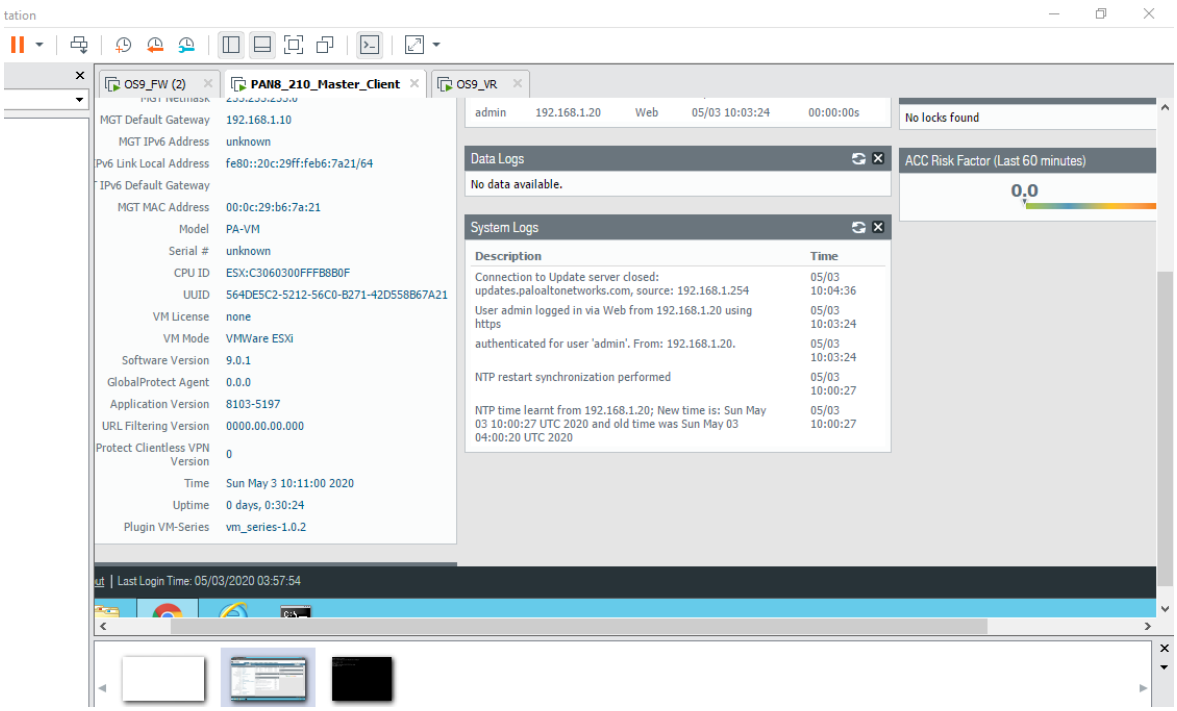


Рисунок 2.2.20 – Панель управления межсетевым экраном

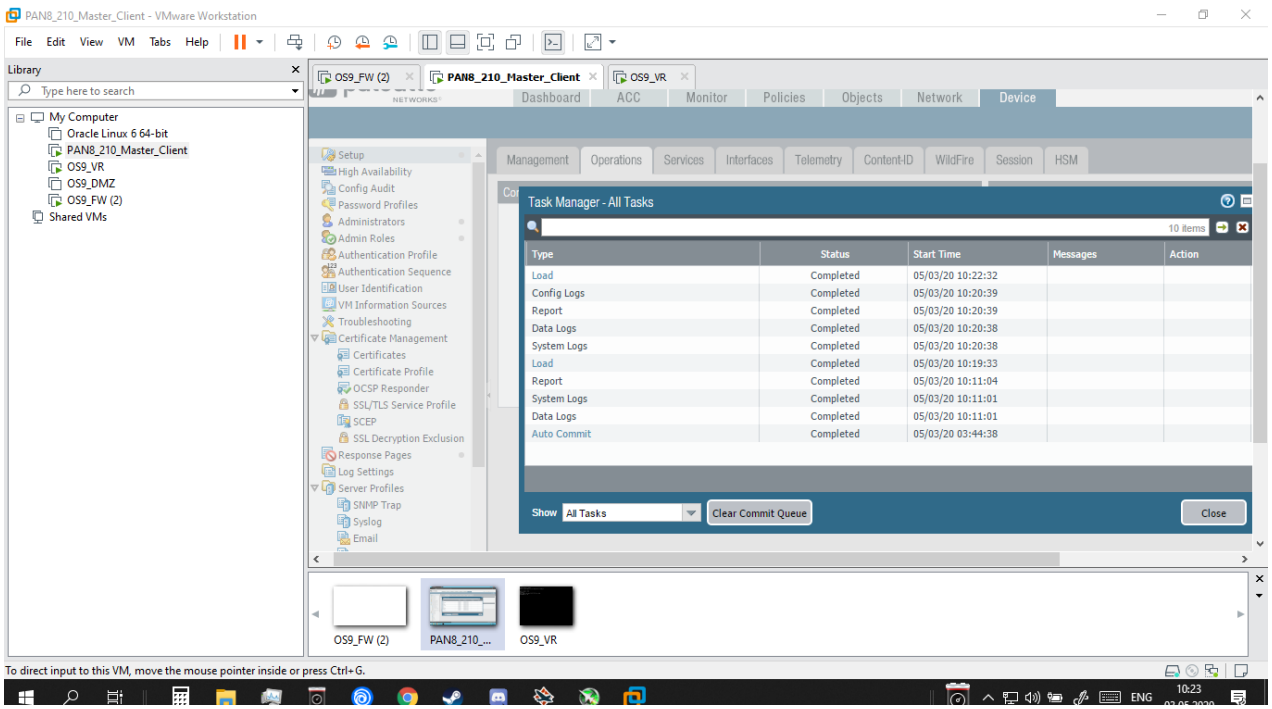


Рисунок 2.2.21 – Встроенный диспетчер задач

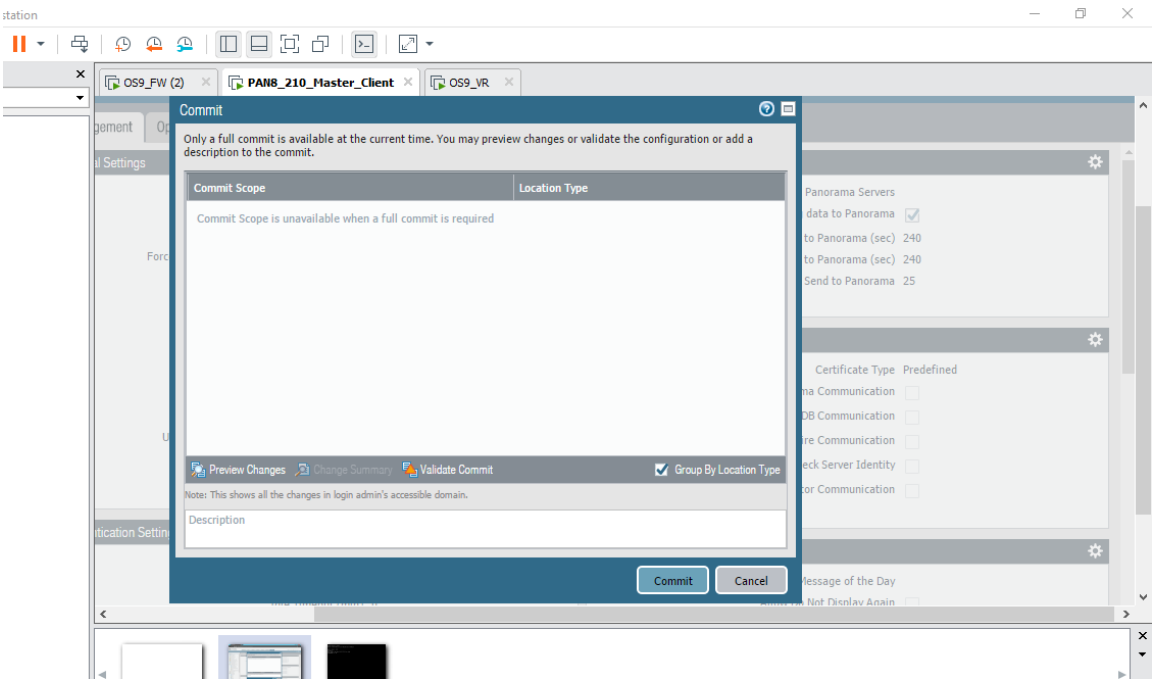


Рисунок 2.2.22 – Окно принятия изменений

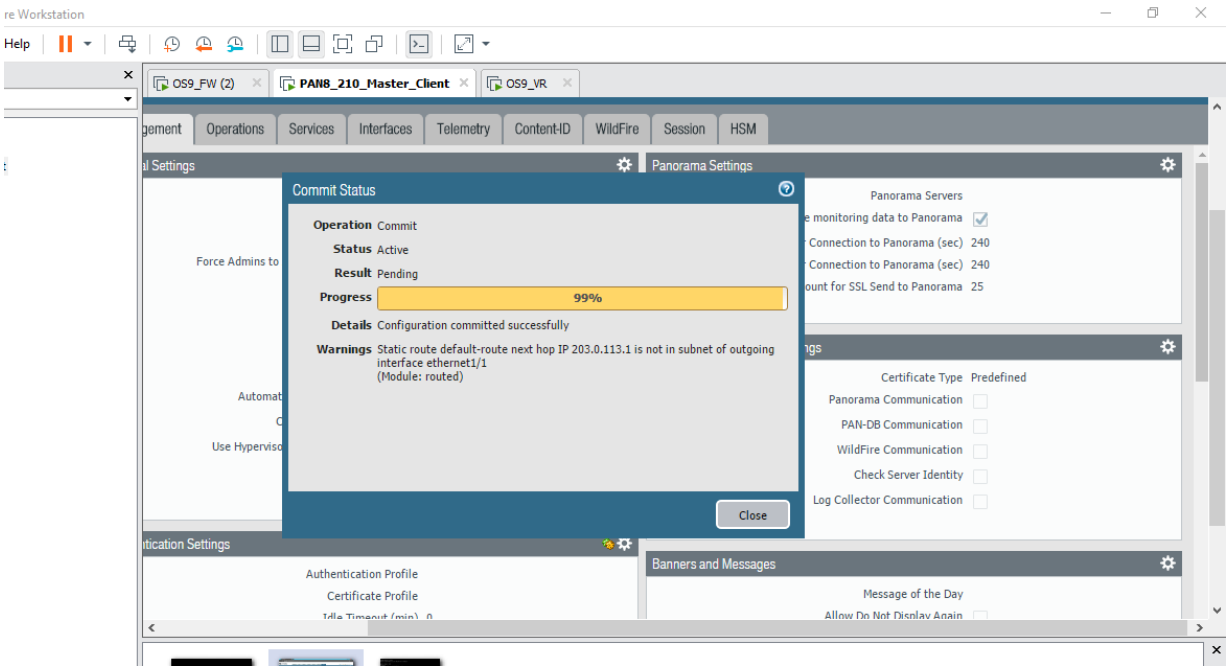


Рисунок 2.2.23 – Ошибки и предупреждения при принятии изменений

Для удобства управления, объекты для настройки брандмауэра могут быть объединены по схожим признакам в единую группу. Такими объектами могут быть политики, пользователи, зоны, интерфейсы и т.д.

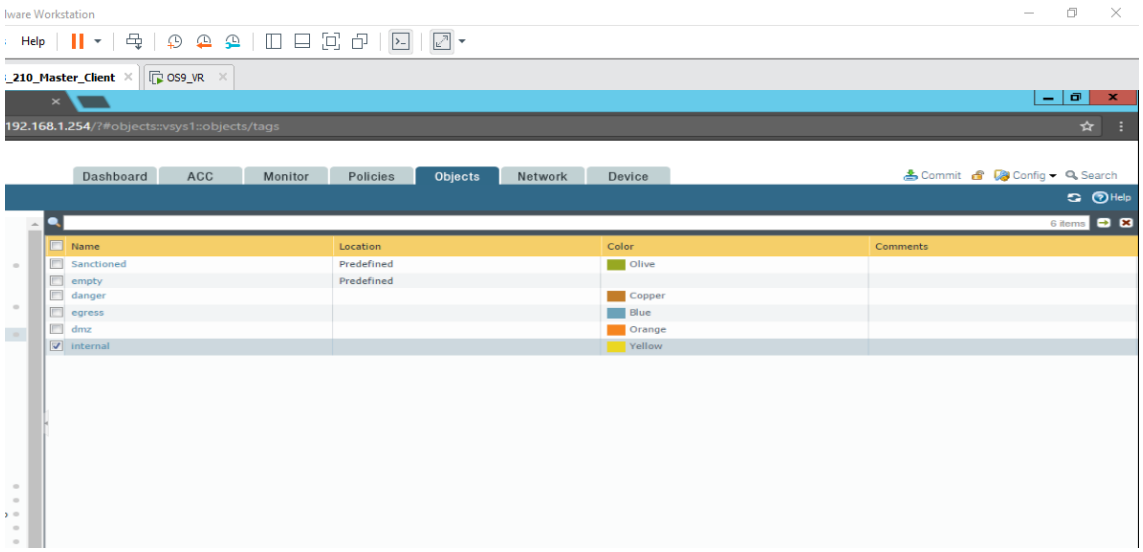


Рисунок 2.2.24 – Объекты межсетевого экрана

Для удобства администрирования, для данного межсетевого экрана реализовано разделение всей сети на «зоны безопасности». К примеру, если необходимо реализовать доступ к DMZ из внешней сети, но важно не пропустить трафик дальше демилитаризованной зоны – во внутреннюю сеть. В таком случае будет разумным создать две зоны безопасности, первая из которых будет включать в себя DMZ-сеть, а вторая – остальную часть внутренней сети.

Другими словами, «зона безопасности» - это логическое объединение ключевых компонентов корпоративной сети со схожими требованиями к безопасности и доступности. Настройки безопасности по умолчанию будут запрещать трафику проходить из одной «зоны безопасности» в другую, однако позволят устройствам видеть друг друга и обмениваться данными, если они находятся в пределах единой «зоны безопасности»

2.3 Создание правил прохождения трафика

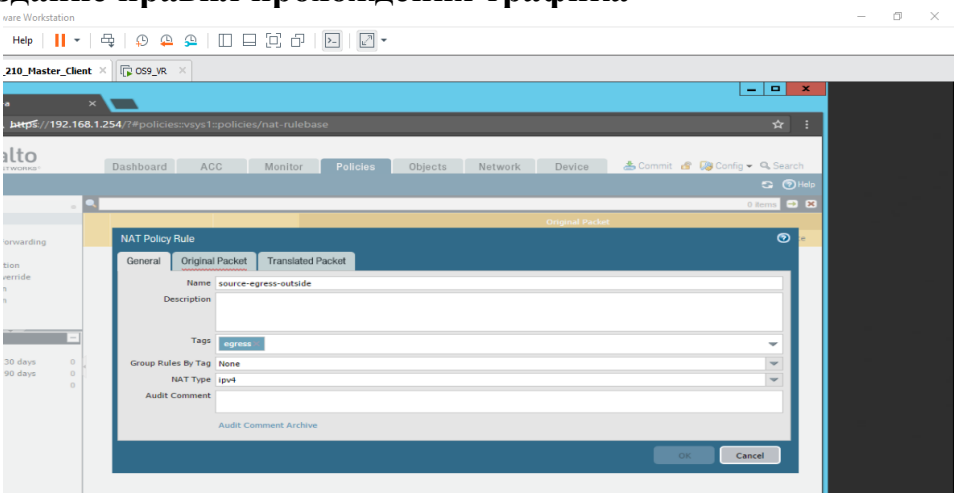


Рисунок 2.3.1 – Создание политики NAT

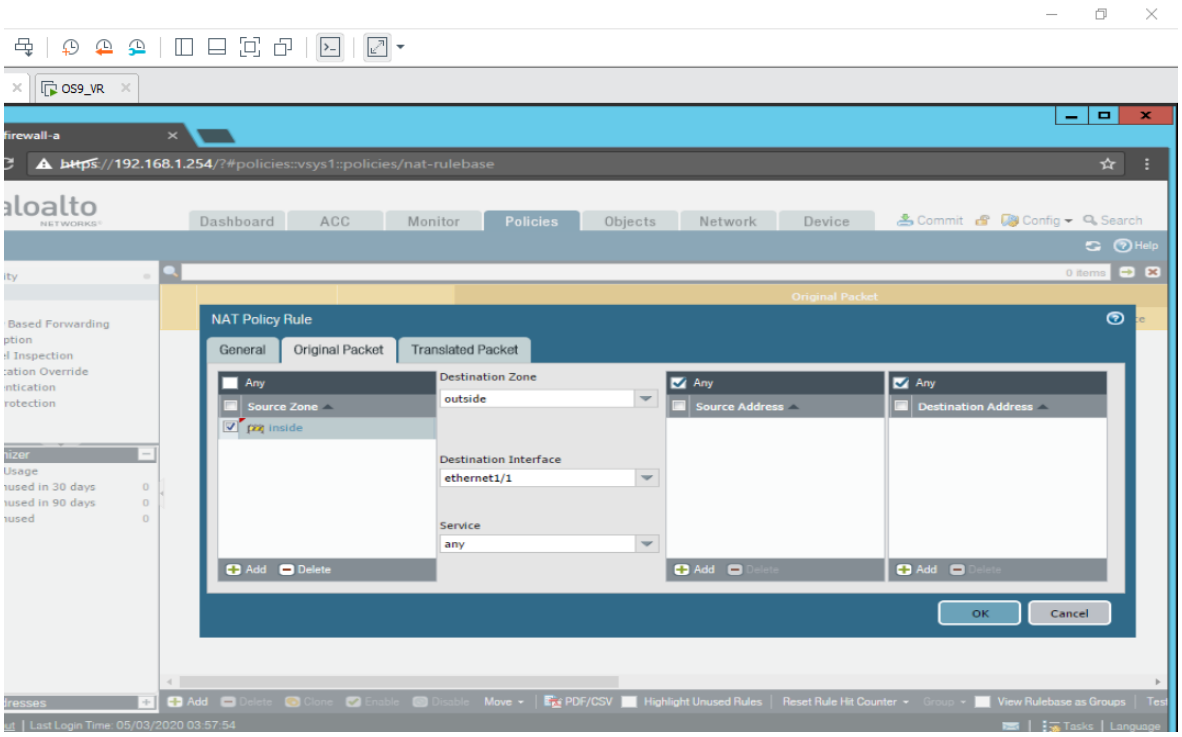


Рисунок 2.3.2 – Свойства политики

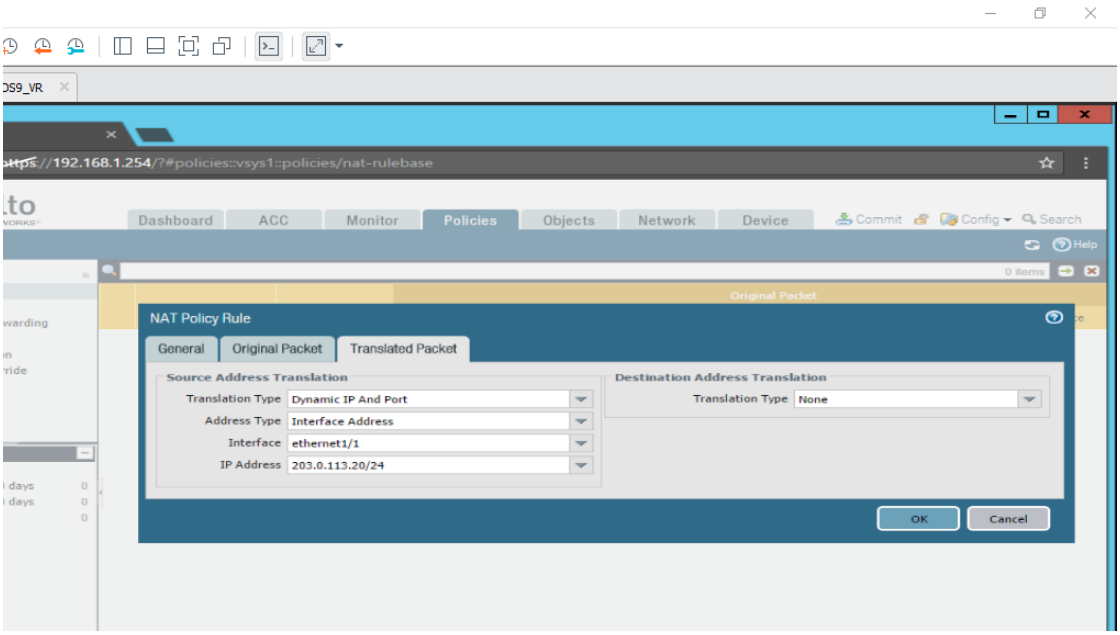


Рисунок 2.3.3 – Свойства передаваемых пакетов для политики NAT

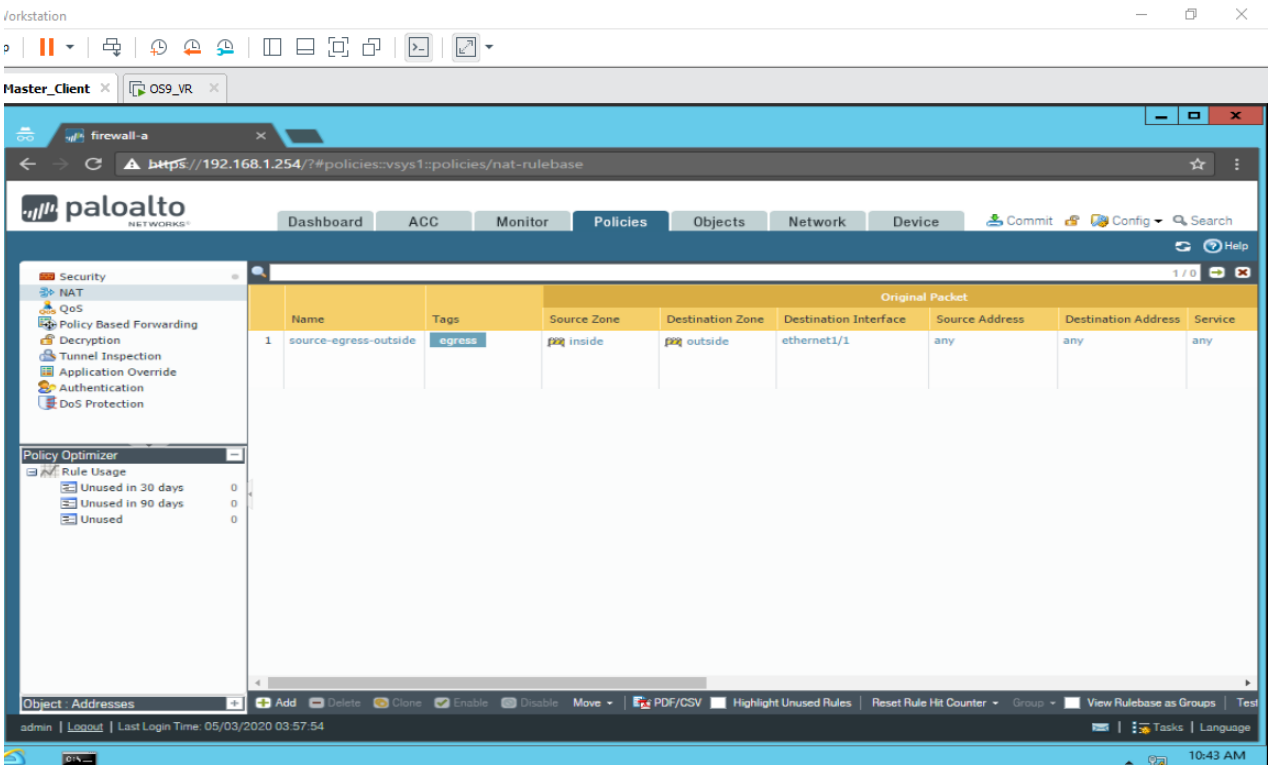


Рисунок 2.3.4– Готовая политика NAT в соответствующем разделе

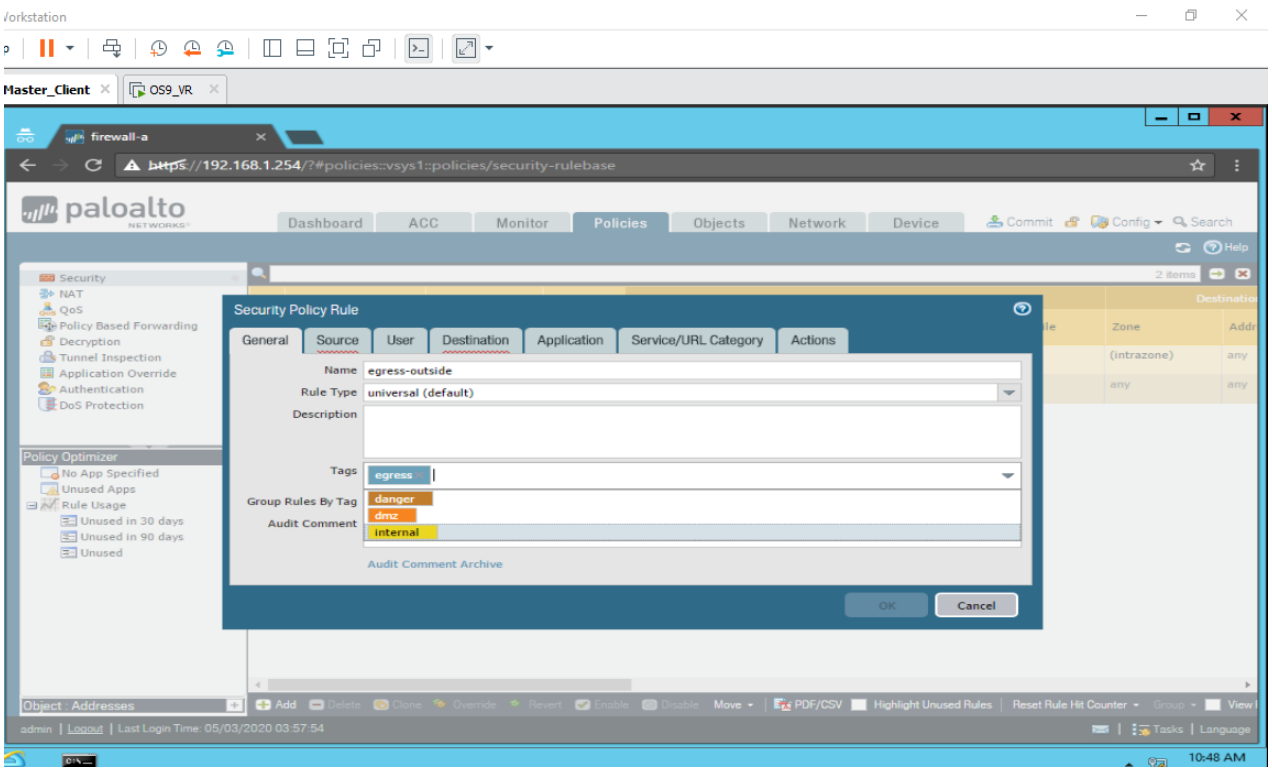


Рисунок 2.3.5 – Свойства политики безопасности

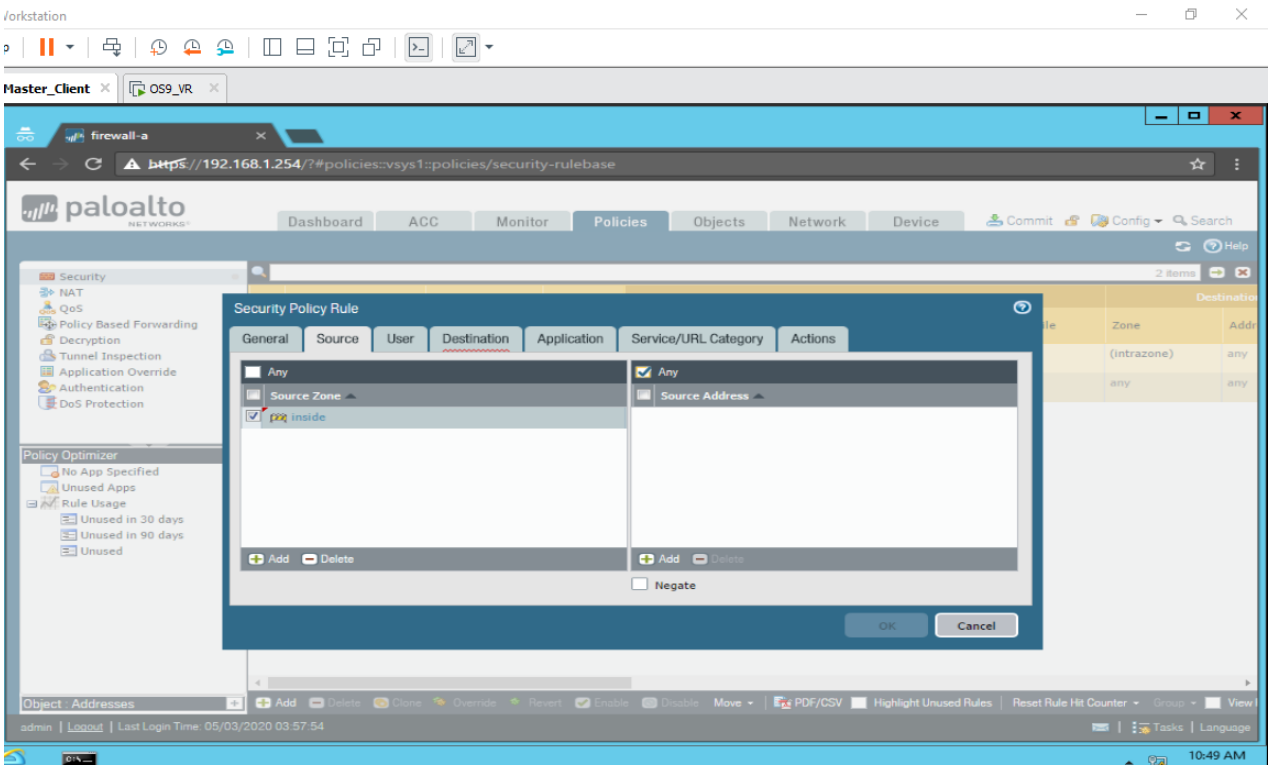


Рисунок 2.3.6 – Настройка источника трафика

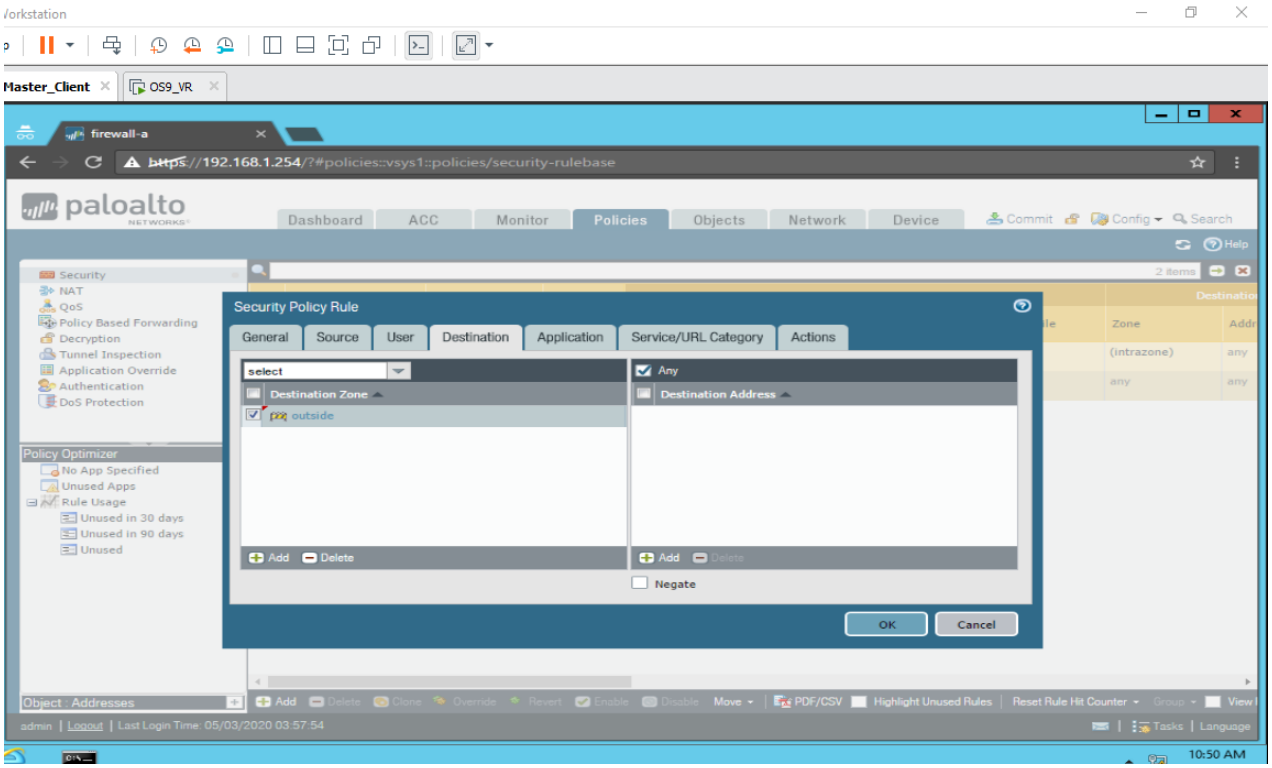


Рисунок 2.3.7 – Настройка назначения трафика

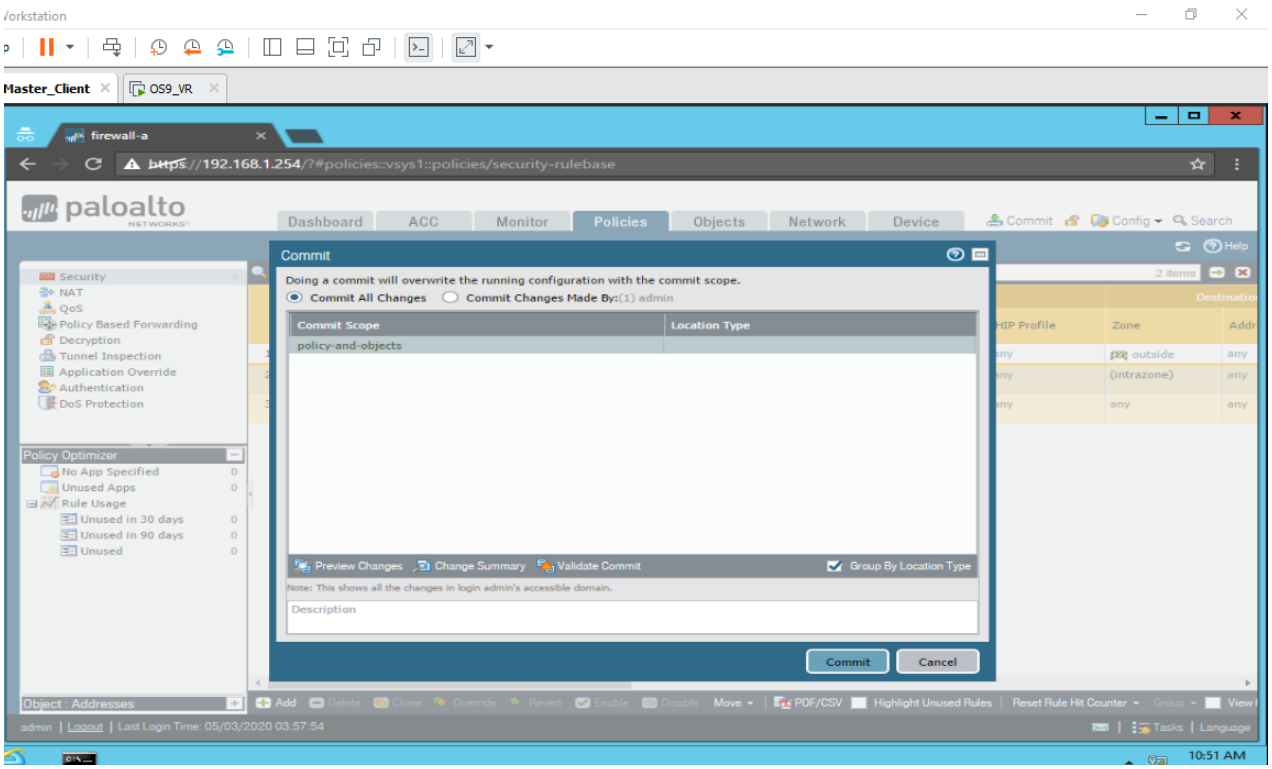


Рисунок 2.3.8 – Принятие изменений

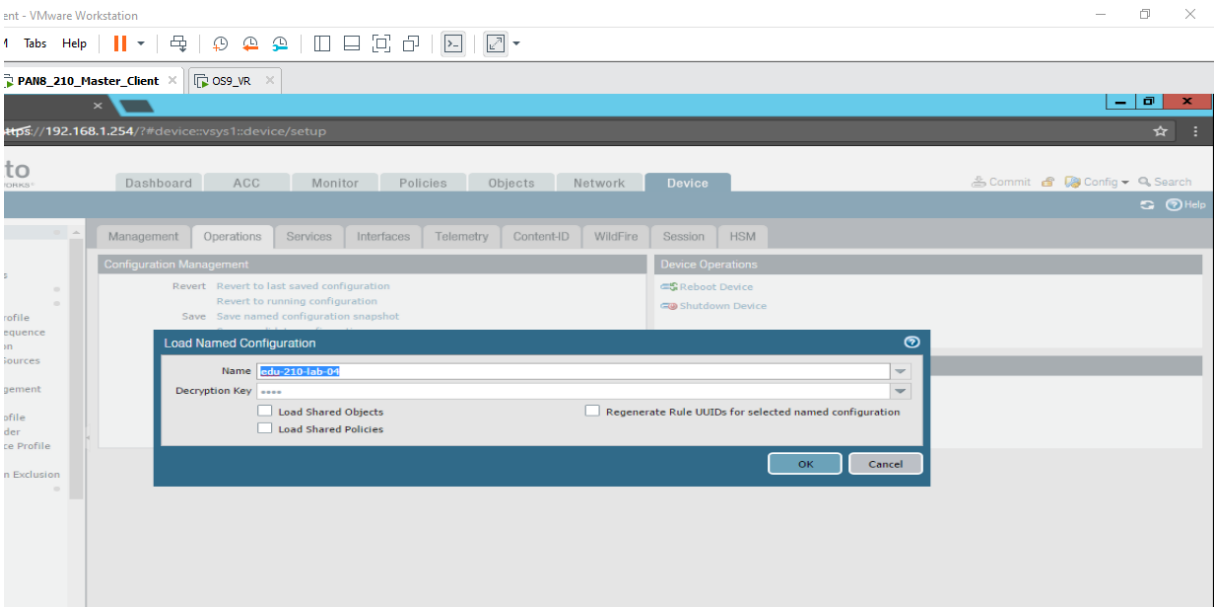


Рисунок 2.3.9 – Импорт готовой конфигурации

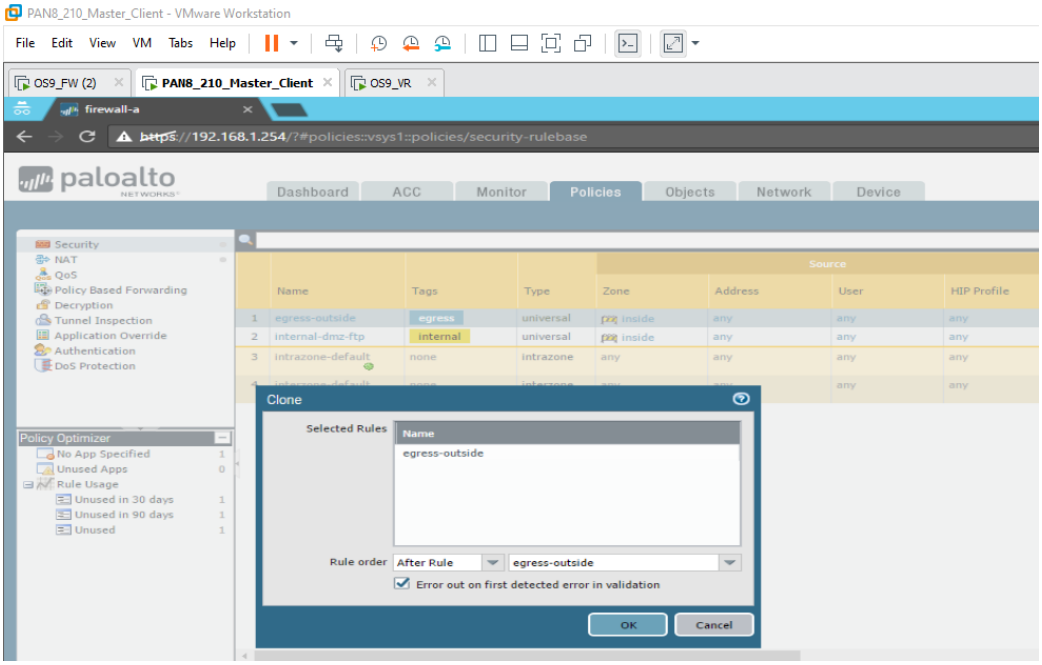


Рисунок 2.3.10 – Дублирование политики безопасности

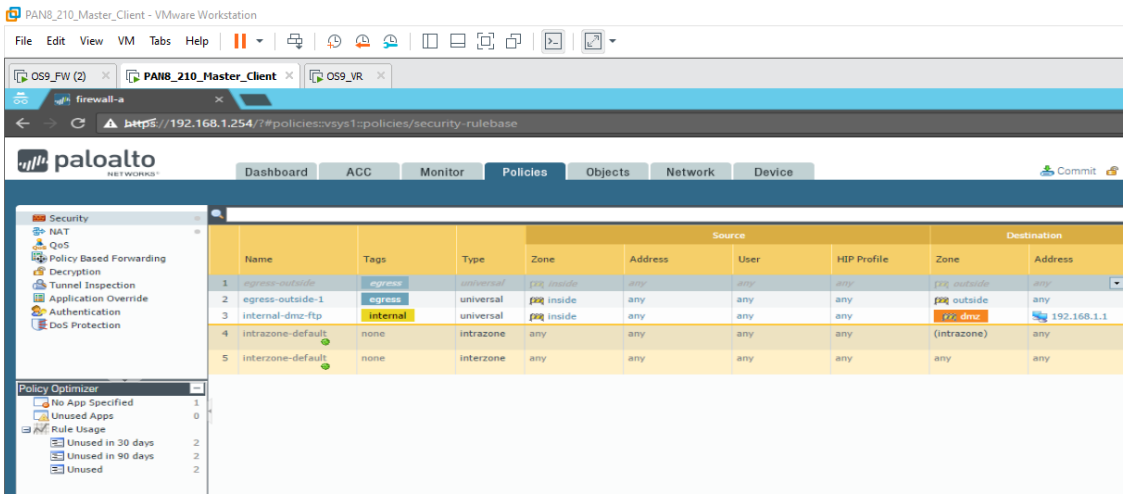


Рисунок 2.3.11 – Сортированные политики безопасности

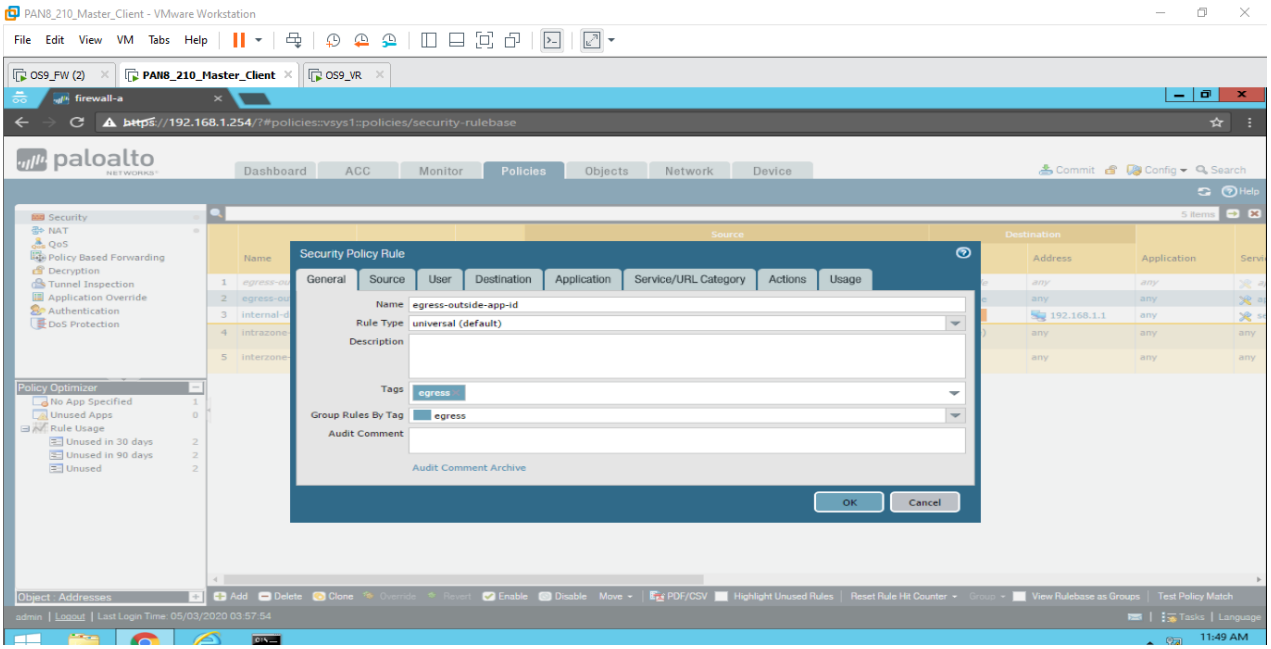


Рисунок 2.3.12 – Создание политики на выход за пределы корпоративной сети (Egress)

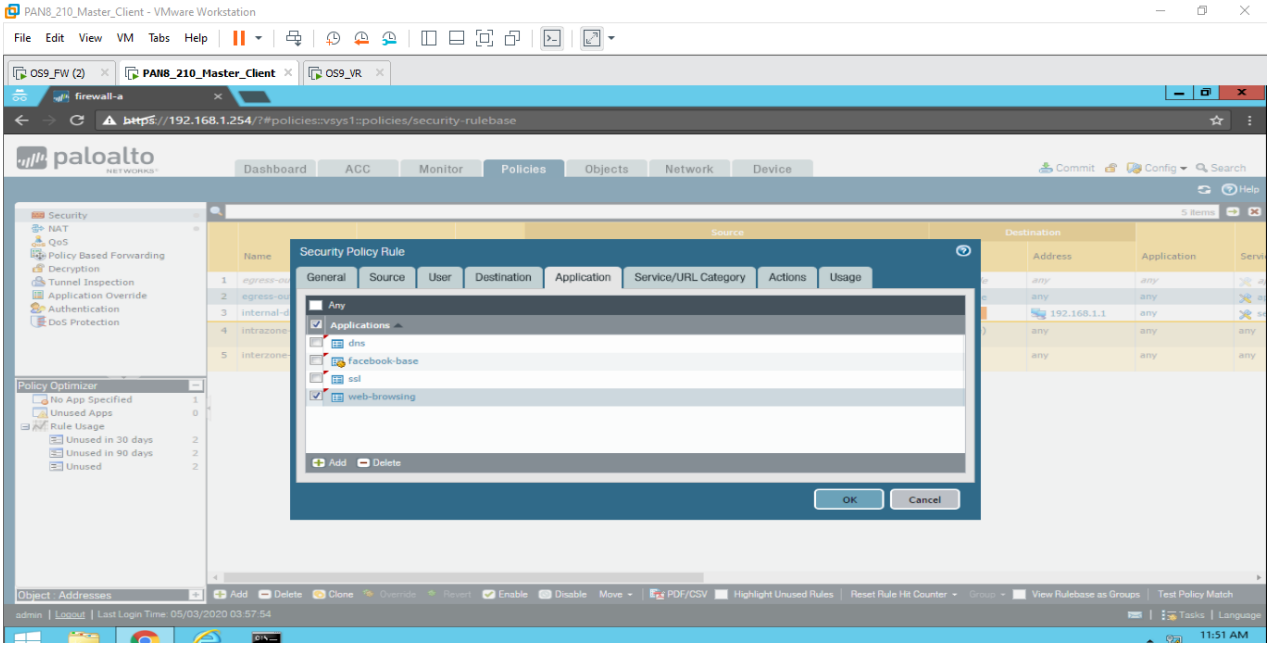


Рисунок 2.3.13 – Используемые приложения

Работу с приложениями в корпоративной сети, брандмауэры Palo Alto используют технологию App-ID. Она позволяет собирать сведения о ПО, особенности их поведения и сопутствующие риски. Для каждого приложения формируется сигнатура, которая и будет определять его для брандмауэра, так же, при необходимости компоненты ПО могут быть расшифрованы. Для удобства управления политиками, все используемые сотрудниками приложения могут быть собраны в группы по различным признакам - уровни риска, назначение ПО, используемые протоколы и так далее.

Основное преимущество создания динамических наборов приложений, заключается в удобстве и расширяемости применяемых политик безопасности. Так, например, настроив фильтр на приложения, использующих протоколы SSL\TLS и имеющие высокий уровень риска, можно одной политикой запретить использование целого списка приложений для конкретной группы сотрудников или сотрудника.

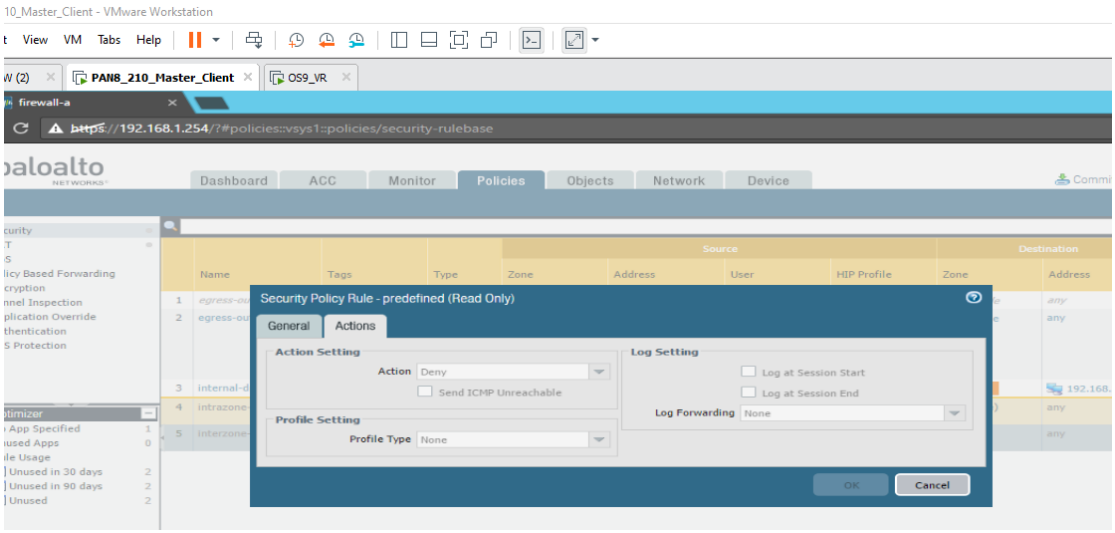


Рисунок 2.3.14 – Действия при срабатывании политики

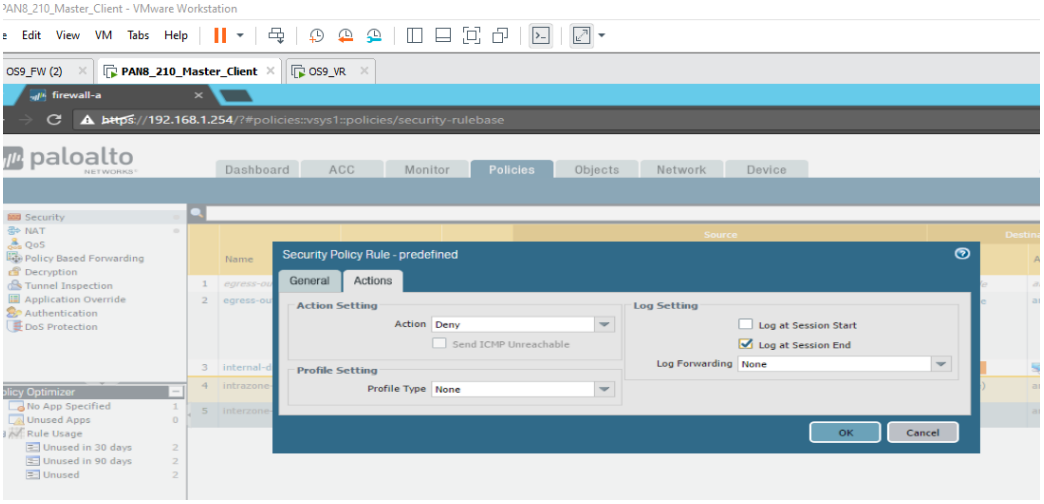


Рисунок 2.3.15 – Запрет прохождения трафика

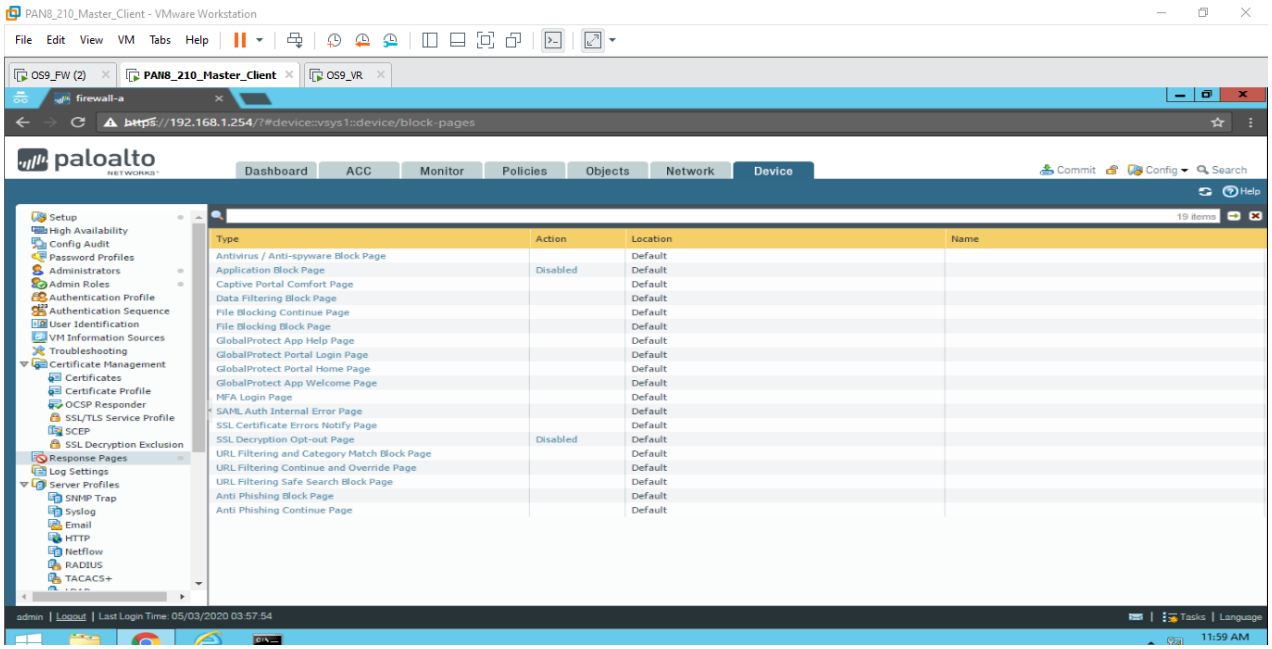


Рисунок 2.3.16 – Результат выполнения политики

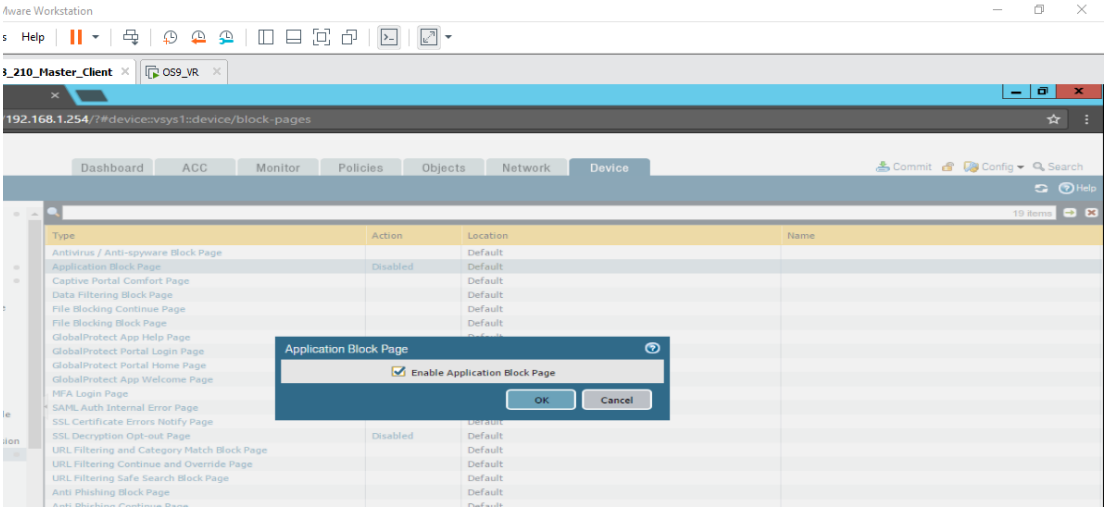


Рисунок 2.3.17 – Настройка всплывающего окна при блокировке приложения

Рисунок 2.3.18 – Политика для конкретного порта (для FTP)

Рисунок 2.3.19 – Политика для конкретного приложения

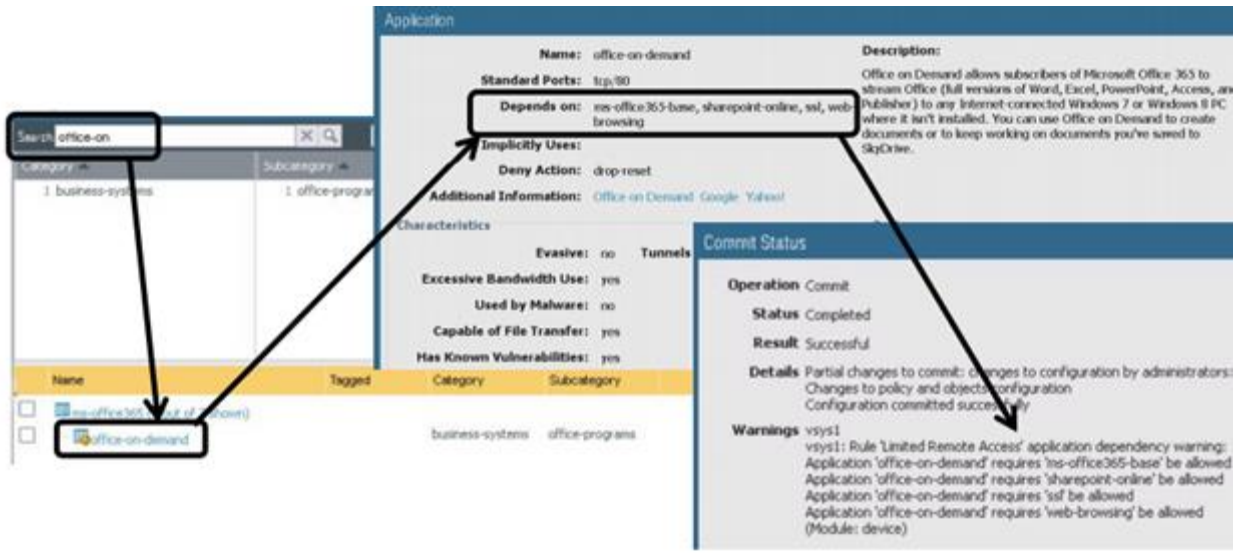


Рисунок 2.3.20 – Отслеживание зависимостей при принятии политик

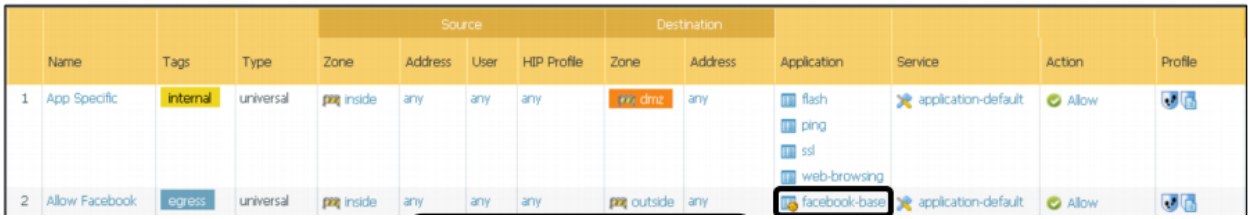


Рисунок 2.3.21 – Политика для сайтов на основе facebook.com

Такая политика будет распространятся не только на основной сайт, но и на все его поддомены.

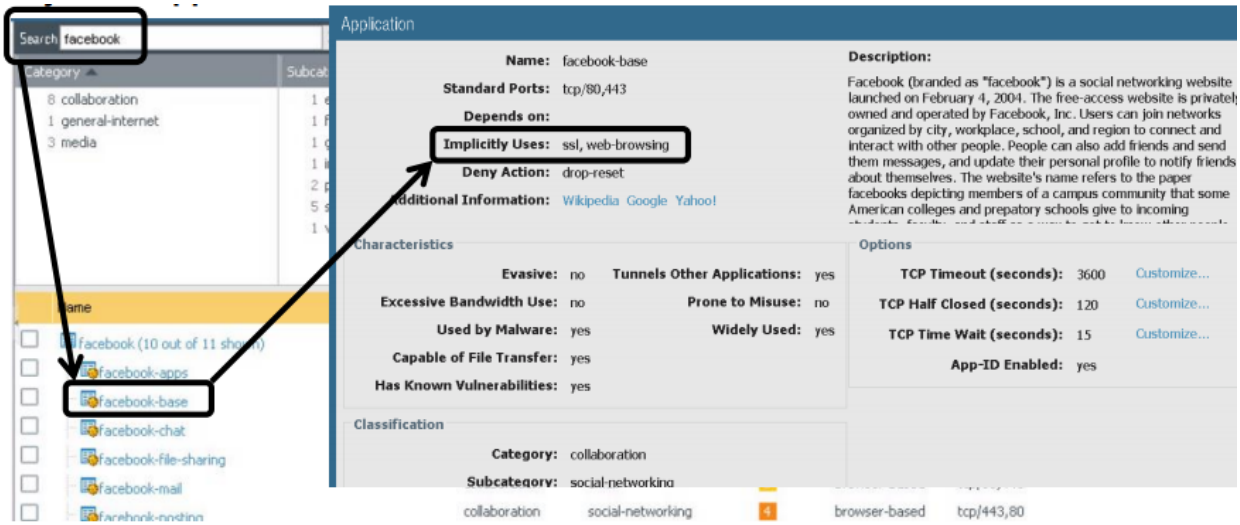


Рисунок 2.3.22 – Зависимости при блокировании приложений сайта facebook.com

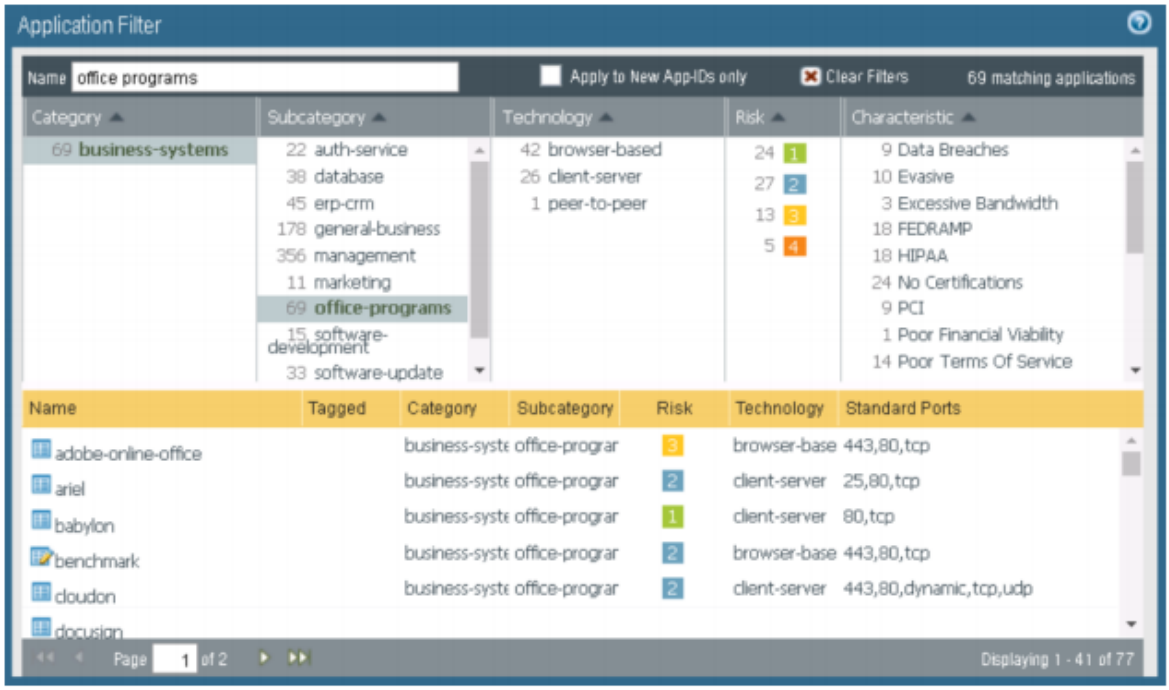


Рисунок 2.3.23 – Настройка политик для приложений по выбранным фильтрам

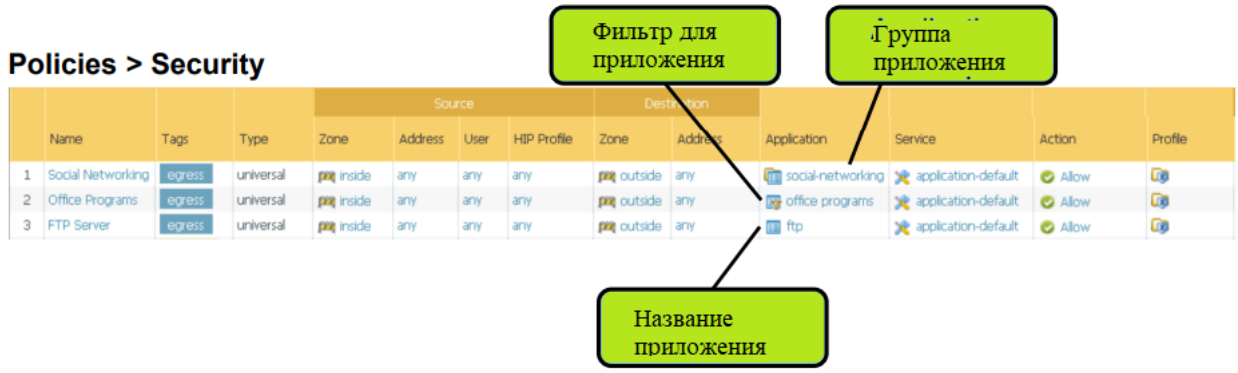


Рисунок 2.3.24 – Политики безопасности с фильтрами приложений

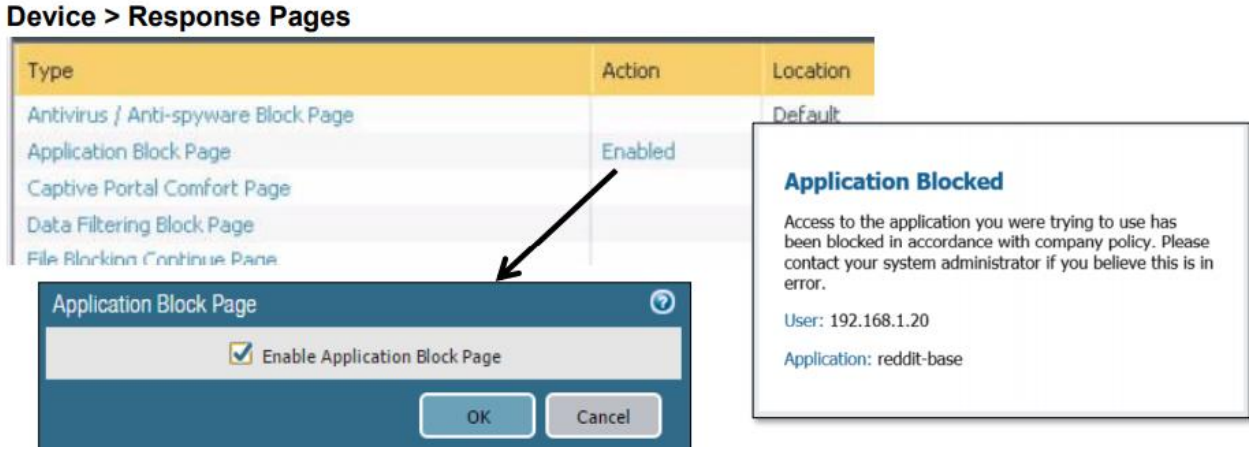
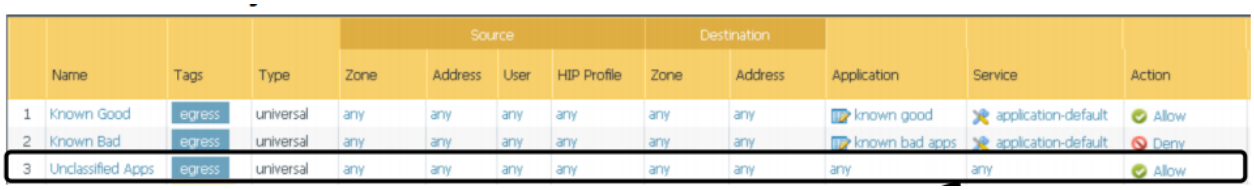


Рисунок 2.3.25 – Настройка уведомлений при срабатывании политики



	Name	Tags	Type	Source				Destination		Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address			
1	Known Good	egress	universal	any	any	any	any	any	any	known good	application-default	Allow
2	Known Bad	egress	universal	any	any	any	any	any	any	known bad apps	application-default	Deny
3	Unclassified Apps	egress	universal	any	any	any	any	any	any	any	any	Allow

Рисунок 2.3.26 – Политика для неизвестных приложений

3 Охрана труда

В качестве темы дипломной работы было выбрано введение в учебный процесс инфраструктуры киберзащиты. Это означает, что основным местом эксплуатации такой инфраструктуры будет помещение на базе учебной аудитории, оснащенное персональными компьютерами и огороженным помещением под серверное оборудование.

Для данного помещения будут актуальны санитарно-эпидемиологические правила и нормативы СанПиН от 2.2.2/ 2.4.1340-03 - гигиенические требования к персональным электронно-вычислительным машинам и организации работы[5]. Большинство вредных физических факторов офисных помещений связаны с:

- повышенные уровни шума, запыленности, ЭМИ и МП, статического электричества, ионизации воздуха и ионизирующих излучений;
- повышенные или пониженные температура, влажность и подвижность воздуха; недостаток освещенности/
- недочеты при расчете кратности воздухообмена.

Психофизические вредные факторы серверного помещения

Многие из перечисленных выше видов вредного воздействия также могут являться причиной избыточной негативной психоэмоциональной нагрузки. Например, шум, неверно организованное освещение рабочего места, сквозняки, затхлый воздух и т.д.

В целом же к психофизическим вредным факторам относят психоэмоциональные перегрузки, вызванные, в том числе, монотонностью работы, перенапряжением анализаторов органов слуха, зрения, осязания, повторяющиеся операции, способные привести к возникновению профессиональных заболеваний.

В совокупности или по отдельности воздействие вредных факторов может быть причиной появления острых и хронических общих и профессиональных (ГОСТ 12.0.002-80 «ССБТ. Термины и определения») заболеваний, в том числе ведущих к стойкой потере трудоспособности.

Государство нормирует количественные показатели вредных производственных факторов на любом рабочем месте, включая офис. Разработанные нормативы — часть законодательства РК, их соблюдение возложено на работодателя. Для выяснения соответствия параметров рабочих мест требованиям государственных стандартов предусмотрена специальная оценка условий труда (СОУТ).

ПК, ПлПК, ноутбуки и ВТ размещаются в специально построенных, пристроенных, реконструированных помещениях, а также в помещениях первого этажа жилых домов с отдельным входом, не совмещенным с подъездом жилого дома или на любых этажах общественных зданий, при обеспечении звукоизоляции и вентиляции помещений с устройством изолированных от жилых помещений вентиляционных каналов для отвода загрязненного воздуха выше уровня кровли здания. В помещениях для

размещения и эксплуатации ПК, ПлПК, ноутбуков и ВТ обеспечиваются условия для соблюдения нормируемых параметров освещенности, микроклимата (Таблица 2). Помещения для работы с ПК, ПлПК, ноутбуками и ВТ не размещаются в подвальных и цокольных помещениях. Рабочие места с ПК, ПлПК, ноутбуками и ВТ не размещаются в местах, где расположены силовые кабели, высоковольтные трансформаторы, технологическое оборудование. Также помещения для работы с ПК, ПлПК, ноутбуками и ВТ не размещаются в подвальных и цокольных помещениях. Рабочие места с ПК, ПлПК, ноутбуками и ВТ не размещаются в местах, где расположены силовые кабели, высоковольтные трансформаторы, технологическое оборудование.

Для отделки помещений применяют материалы, допускающие уборку влажным способом с применением моющих средств.

Поверхность пола в помещениях, где оборудуются ПК, ПлПК, ноутбуки и ВТ, выполняется без выбоин и щелей, из материалов, обладающих антистатическими свойствами. Помещения с использованием ПК, ПлПК, ноутбуками и ВТ, мебель и оборудование содержатся в порядке и чистоте. Дефекты в отделке помещения и поломки оборудования, мебели подлежат своевременному ремонту и замене.

Помещения, где размещаются ПК и ВТ, оборудуются защитным заземлением.

Расстановка компьютеров (ПК, планшетные персональные компьютеры, ноутбуки) используется одним из трех 3-х вариантов: периметральная, рядные (2-3-рядная), центральная.

При периметральной расстановке, расстояние между стеной с оконными проемами и столами 0,5 метров (далее - м), стеной и столами - 0,4 м.

При рядной расстановке расстояние между тылом поверхности одного видеомонитора и экраном другого - не менее 2 м, между боковыми поверхностями видеомониторов не менее 1,2 м, при двух-трехрядной расстановке одноместных столов с компьютерами расстояния в каждом ряду между боковыми поверхностями столов не менее 0,5 м.

При центральной расстановке рабочие столы с компьютерами устанавливаются в центре, в два ряда без разрыва и экраны видеомониторов обращены в противоположные стороны, располагаясь в шахматном порядке, или напротив друг друга тыльными сторонами мониторов, при этом расстояние между тылом поверхности одного видеомонитора и экраном другого - не менее 2 м[1].

Размеры рабочей поверхности (подробнее в Таблице 1):

1) высота рабочей поверхности стола (от пола) регулируется в пределах 640 - 800 миллиметров (далее - мм);

2) ширину рабочей поверхности стола 800, 1000, 1200 и 1400 мм;

3) рабочий стол имеет пространство для ног высотой не менее 580 мм, шириной - не менее 500 мм, глубиной - не менее 450 мм.

Экран видеомонитора находится от глаз пользователя на расстоянии 600-700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

В помещениях, где для занятия с ПК, ПлПК, ноутбуками и ВТ оборудуются одноместными столами, предусматривают следующую конструкцию одноместного стола для работы с ПК, ПлПК, ноутбуков и ВТ:

1) две раздельные поверхности: одну горизонтальную для размещения ПК с плавной регулировкой по высоте в пределах 520 - 760 мм и вторую подвижную для клавиатуры с регулировкой по высоте соответственно горизонтальной рабочей поверхности;

2) ширина поверхностей для ПК, ПлПК, ноутбуков и ВТ клавиатуры составляет не менее 750 мм, глубина - не менее 550 мм;

3) ширина пространства для ног не менее 500 мм, глубина не менее 450 мм, а высоту принимать в соответствие с ростом;

4) увеличение ширины поверхностей до 1200 мм при оснащении рабочего места принтером.

Основные размеры рабочего места при работе с компьютерами высота края стола и высота пространства для ног соответствуют росту.

Непрерывная длительность занятий в дошкольных организациях и школах непосредственно с ВТ, ПК, ПлПК и ноутбуками в течение учебного часа соответствует:

дошкольных организациях и 1 классах - не более 15 минут;

2 - 3 классах - не более 20 минут;

3) 4-5 классах - не более 25 минут;

4) 6 - 8 классах - не более 30 минут;

5) 9 - 11(12) классах - не более 35 минут.

Продолжительность непосредственной работы с ВТ и ПК, ПлПК и ноутбуками рекомендуется не более двух часов. В период работы проводятся профилактические мероприятия: упражнения для глаз через каждый 20-25 минут и физкультурная пауза через 45 минут во время перерыва.

Компьютерные игровые занятия в дошкольных организациях проводятся не чаще 2 раз в неделю.

Занятия с ВТ, ПлПК, ноутбуками и ПК не проводятся за счет времени, отведенного для сна, дневных прогулок и оздоровительных мероприятий.

Одновременное использование одного ВТ, ПК, ПлПК, ноутбуков двумя и более людьми, независимо от возраста не рекомендуется.

Для сбора мусора с объектов, размещенных на первых этажах многоквартирного жилого дома, в частном домовладении, во встроено - пристроенных помещениях используются общие мусоросборники жилого дома или контейнеры.

Не используются ПК, ВТ, ПлПК, ноутбуки без наличия документов, подтверждающих их качество и безопасность.

Обработка составляющих частей компьютера (клавиатуры, монитора, процессора и т.д.) осуществляется средствами, предназначенными для ухода

ПК, ПлПК, ноутбуков и ВТ. Предусматривается отдельное помещение для хранения неисправных и вышедших из строя компьютеров, недоступное для детей.

Не эксплуатируются объекты, размещенные в аварийных зданиях и помещениях.

В помещениях, где расположены ПК, ПлПК, ноутбуки и ВТ, обеспечиваются допустимые параметры микроклимата в соответствии с приложением 2 к настоящим Санитарным правилам.

Помещения с ПК, ПлПК, ноутбуками и ВТ оборудуются системами отопления, вентиляцией, кондиционерами.

Перед началом работы и после каждого академического часа занятий осуществляют сквозное проветривание.

Помещения, где размещаются ПК, ПлПК, ноутбуки и ВТ имеют естественное освещение.

Искусственное освещение в помещениях для эксплуатации ПК и ВТ осуществляется системой общего равномерного освещения. В производственных и административно-общественных помещениях на рабочем месте, применяют системы комбинированного освещения (к общему освещению дополнительно устанавливаются светильники местного освещения, предназначенные для освещения зоны рабочего места).

Освещенность на поверхности рабочего стола составляет: при комбинированном освещении не менее 300 люкс (далее - лк) от общей системы, 500 лк от местной системы; при наличии только общей системы освещения - 400 лк. Освещение выполняется таким образом, чтобы обеспечить отсутствие бликов на поверхности экрана. Освещенность поверхности экрана не более 200 лк.

В качестве источников света при искусственном освещении используются люминесцентные лампы. В светильниках местного освещения допускается применение ламп накаливания, в том числе энергосберегающие.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПК ПлПК, ноутбуков и ВТ своевременно заменяют перегоревшие лампы. Неисправные, перегоревшие люминесцентные лампы хранят в отдельном помещении. Не допускается выброс отработанных люминесцентных ламп в мусоросборные контейнеры. Вывоз и утилизация отработанных ламп проводится организациями, имеющими лицензию на данный вид деятельности.

Оборудование (печатающие устройства, серверы и другое), уровень шума которого превышает допустимый, размещается вне помещений, где оборудованы ПК, ПлПК, ноутбуки и ВТ.

Таблица 3.1 – Размеры рабочего места

Рост, сантиметров (далее - см)	Высота над полом, миллиметров (далее - мм)	
	поверхность стола	пространство для ног, не менее

100-115	460	320
116-130	520	400
131 - 145	580	520
146-160	640	580
161 - 175	700	640
Выше 175	760	700

Таблица 3.2 - Допустимые параметры микроклимата для помещений

Температура, С	Относительная влажность, не более, %	Скорость движения воздуха, м/с
18	66	< 0,1
19	62	< 0,1
20	58	< 0,1
21	55	< 0,1
22	52	< 0,1

Таблица 3.3 - Допустимые значения уровней звукового давления в октавных полосах частот и уровня звука, создаваемого ПЭВМ

Уровни звукового давления в октавных полосах со среднегеометрическими частотами									Уровни звука в дБА
31,5 Гц	63 Гц	125 Гц	250 Гц	500 Гц	1000 Гц	2000 Гц	4000 Гц	8000 Гц	
86 дБ	71 дБ	61 дБ	54 дБ	49 дБ	45 дБ	42 дБ	40 дБ	38 дБ	50

Подраздел 2 Расчёты для серверного помещения

В качестве объекта расчета была выбрана звукоизоляция (проверка уровня допустимого шума) для серверного помещения, на базе которого функционирует сетевая инфраструктура, описанное в данном дипломном проекте. Требования к звукоизоляции изложены в МСН 2.04-03-2005 «Защита от шума». Согласно этому документу, Основным источником шума в зданиях различного назначения является технологическое и инженерное оборудование[1].

Шумовыми характеристиками технологического и инженерного оборудования, создающего постоянный шум, являются уровни звуковой мощности L_w, дБ, в восьми октавных полосах частот со среднегеометрическими частотами 63-8000 Гц (октавные уровни звуковой мощности), а оборудования, создающего непостоянный шум, эквивалентные уровни звуковой мощности $L_{wэкв}$ и максимальные уровни звуковой мощности $L_{wмакс}$ в восьми октавных полосах частот. Расчетные точки в

производственных и вспомогательных помещениях промышленных предприятий выбирают на рабочих местах и (или) в зонах постоянного пребывания людей на высоте 1,5 м от пола. В помещении с одним источником шума или с несколькими однотипными источниками одна расчетная точка берется на рабочем месте в зоне прямого звука источника, другая - в зоне отраженного звука на месте постоянного пребывания людей, не связанных непосредственно с работой данного источника.[3]

Так как серверное помещение находится внутри учебной аудитории и ограждено тонкой стенкой, будет произведен расчёт октавного уровня звукового давления *L*, дБ (1) для дальнейшего расчёта требуемого снижения октавных уровней звукового давления $\Delta L_{тр}$ (2).

Таблица 3.4 – Допустимые уровни звукового давления

Назначение помещений или территорий	Уровень звукового давления (эквивалентный уровень звукового давления) L, дБ, в октавных полосах частот со среднегеометрическими частотами, Гц								Уровень $L_{Аэкв}$, дБА	Максимальный уровень звука, $L_{Амакс}$, дБА	
	1,5	3	25	50	00	000	000	000	8000		
Классные помещения, учебные кабинеты, аудитории учебных заведений, конференцзалы, читальные залы библиотек и т.д.	9	3	2	5	9	5	2	0	28	0	55

Октавный уровень звукового давления *L*, дБ, в расчетных точках соразмерных помещений (с отношением наибольшего геометрического размера к наименьшему не более 5) при работе одного источника шума следует определять по формуле

$$L = L_w + 10lg\left(\frac{\chi \cdot \Phi}{\Omega r^2} + \frac{4}{kB}\right), \quad (1)$$

где L_w - октавный уровень звуковой мощности, дБ;

χ - коэффициент, учитывающий влияние ближнего поля в тех случаях, когда расстояние *r* меньше удвоенного максимального габарита источника (*r* < $2\ell_{макс}$) (принимают по таблице 5);

Φ - фактор направленности источника шума (для источников с равномерным излучением $\Phi = 1$);

Ω - пространственный угол излучения источника, рад (принимают по таблице 6).

r - расстояние от акустического центра источника шума до расчетной точки, м (если точное положение акустического центра неизвестно, он принимается совпадающим с геометрическим центром);

k - коэффициент, учитывающий нарушение диффузности звукового поля в помещении (принимают по таблице 7 в зависимости от среднего коэффициента звукопоглощения α_{Φ});

B - акустическая постоянная помещения, м^2, определяемая по формуле

$$B = \frac{A}{1 - \alpha_{ср}}, \quad (2)$$

где *A* - эквивалентная площадь звукопоглощения, м^2, определяемая по формуле

$$A = \sum_{i=1}^{n} \alpha_i S_i + \sum_{j=1}^{m} A_j n_j, \quad (3)$$

где α_i - коэффициент звукопоглощения *i*-ой поверхности;

S_i - площадь i-ой поверхности, м^2;

A_j - эквивалентная площадь звукопоглощения *j*-го штучного поглотителя, м^2;

n_j - количество *j* - тых штучных поглотителей, шт;

$\alpha_{ср}$ - средний коэффициент звукопоглощения, определяемый по формуле

$$\alpha_{ср} = \frac{A}{S_{огр}}, \quad (4)$$

где $S_{огр}$ - суммарная площадь ограждающих поверхностей помещения, м^2[4].

Таблица 3.5 – Влияние ближнего поля

$r/\ell_{макс}$	χ
1,0	2
1,2	1,6
1,5	1,25
2	1

Таблица 3.6 - Пространственный угол излучения источника

Условия излучения	Ω, рад.	$101g\Omega$, дБ
В пространство – источник на колонне в помещении, на мачте, трубе	4 р	11
В полупространство – источник на полу, на земле, на стене	2 р	8
В 1/4 пространства – источник в двухгранном углу (на полу близко от одной стены)	р	5
В 1/8 пространства – источник в трехгранном углу (на полу близко от двух стен)	р/2	2

Таблица 3.7 – Коэффицент для нарушения диффузности поля

$\alpha_{ср}$	k
0,2	1,25
0,4	1,6
0,5	2,0
0,6	2,5

Так как в выбранном помещении, источник шума, всего один, то расчёт будет вестись по формуле (1).

n=2, то есть в серверном помещении будет установлено 2 штучных поглотителя из специального материала, а m=2, так как источник шума только один.

Рекомендуется использовать акустическую облицовку, средний коэффициент звукопоглощения α которой, в октавной полосе со среднегеометрической частотой 1000 Гц не превышал величины 0,25, а расчетные точки расположены преимущественно в зоне отраженного поля. То, есть наши входные данные для нахождения L выглядят так:

α=0.25;
n=2;
m=1;
S=13 м2;
χ=2;
Φ=1;
k=2.5;
r=1.5;
Ω=р;
$\alpha_{ср}$=0.6;
L_w=40; (Таблица 4)
A(1)=2 м2;

S(огр)=15 м2;

Но для начала, найдем А - эквивалентную площадь звукопоглощения по формуле (3). И получаем значение 9, рисунок из Mathcad приведен ниже:

$$\sum_{i=1}^{2}(0.25\cdot 10)+\sum_{j=1}^{1}(2\cdot 2)=9$$

Теперь находим В по формуле (2), но для этого необходимо найти

$\alpha_{ср}$ по формуле (4)

$\alpha_{ср}$ = 9/15=$\frac{3}{5}$, теперь приступаем к расчёту В по формуле (2)

В = $\frac{9}{\frac{3}{5}}$ = 13,3;

Теперь, получив все входные данные, произведем расчет L в среде Mathcad, итоговое решение со всеми входными данными показано ниже:

$$40+10\log\left[\left[\frac{(2\cdot 1)}{3.14\cdot 1.5^{2}}+\frac{4}{2.5\cdot 13.3}\right],10\right]=36.057$$

Таким образом, октавный уровень звукового давления L =36.057.

Теперь мы сможем найти требуемое снижение октавных уровней звукового давления ΔL(треб) по формуле (5),

$$\Delta L_{треб}=L_{i}-L_{доп}+10\cdot lgn \quad (5)$$

где Li — октавный уровень звукового давления или уровень звука i-го источника шума, рассчитанный в расчетной точке, дБ (дБА);

Lдоп — допустимый октавный уровень звукового давления, дБ, или уровень звука, дБА, определяемый по таблице 4;

n — общее число источников шума, учитываемых при расчете суммарного уровня в расчетной точке

ΔL=36.057-40+10lg1= 3,943дБ(дБА)

3.1 Расчет влагосодержания внутри серверного помещения

Воздух представляет собой физическую смесь различных газов, образующих атмосферу Земли. Чистый воздух – это смесь газов в относительно постоянном объемном соотношении: азот – 78,09 %, кислород – 20,95 %, аргон – 0,93 % и диоксид углерода – 0,03 %. Кроме того, воздух содержит незначительное количество других газов, таких как водород, озон, оксиды азота. Содержание паров воды в воздухе может достигать четырех объемных долей в % в зависимости от конкретных условий окружающей среды и характера деятельности человека. Основными параметрами воздуха являются его плотность, влажность, температура, давление, влагосодержание и др. [2]

Плотностью воздуха ρ называется отношение массы воздуха к его объему; плотность воздуха выражается в кг/м3 . Степень влажности воздуха определяется абсолютной и относительной влажностью. Абсолютная влажность “e” характеризуется массой водяных паров G(вп) в единице объема воздуха V и выражается в г/м3:

e = Gвп/V, (6)

Относительная влажность φ – это отношение абсолютной влажности воздуха e к максимальной (насыщенной) e(max) при данной температуре; относительную влажность воздуха выражают в %:

φ = e · 100 %/e(max), (7)

Температура воздуха показывает степень его нагрева; ее измеряют в градусах различных температурных шкал. В Международной практической температурной шкале различают температуры Кельвина (T, К) и Цельсия (t, °C), связанные между собой соотношением

t ≈ T – 273, (8)

Давление воздуха (барометрическое) Рб – это сумма парциальных давлений сухого воздуха Рсв и водяных паров Рп; измеряется в Паскалях (Па):

P(б) = P(св) + P(п), (9)

Давление водяных паров (парциальное) Рп – давление, под которым находятся водяные пары во влажном воздухе.

Влагосодержание воздуха d – это количество водяных паров, г, приходящихся на 1 кг сухого воздуха:

d = 0,623 · φ · Рн/(Рб – φ · Рн), (10)

где Рн – давление насыщенного пара, кгс/см2 , зависящее от температуры воздуха (Таблица 8). Удельная энтальпия влажного воздуха – это количество теплоты, необходимое для нагревания от 0 °C до данной температуры такого количества влажного воздуха, сухая часть которого имеет массу 1 кг[3].

Таблица 3.1.1 – Давление насыщенного пара

Температура, °C	Давление, кгс/см2	Удельная энтальпия пара, кДж/кг
0	0,0062	2493,1

Продолжение таблицы 3.1.1

5	0,0089	2502,7
10	0,0125	2512,3
15	0,0174	2522,4
20	0,0238	2532,0
25	0,0323	2541,7

Энтальпия влажного воздуха I складывается из энтальпии сухой его части Iсв и энтальпии водяных паров Iвп:

$I = I_{св} + I_{вп} = 1{,}005 \cdot t + [(2\,500 + 1{,}8 \cdot t) \cdot d \cdot 10–3]$, кДж/кг.

Рассчитаем влагосодержание для серверного помещения, имея входные данные:

$t = 20$ °C

Рб = 0,098 МПа (1кгс/см2)

$\varphi = 50$ %

$d = 0{,}623 \cdot 0{,}5 \cdot 0{,}0238/(1 – 0{,}5 \cdot 0{,}0238) = 0{,}0075$ кг/кг = 7,5 г/кг

Таким образом, влагосодержание воздуха будет равно 7,5 г/кг.

Вывод

На основании произведенных вычислений и собранного теоретического материала, было определено, что превышение допустимой мощности всего в ~4 дБА, является несущественным и тех средств звукоизоляции, что предусмотрены в серверном помещении, а именно – двух звукопоглотителей площадью в 2 квадратных метра каждый. – достаточно для обеспечения приемлемого уровня звукоизоляции.

Влагосодержание воздуха также является допустимым, это также было установлено с помощью расчётов с использованием всех необходимых входных данных. Результаты расчётов позволяют нам сделать выводы о приемлемых условиях труда и эксплуатации серверного оборудования.

4 Анализ и оценка рисков

Процесс управления направлен на определение событий, которые могут оказать влияние на организацию, и на управление связанным с этими событиями риском. При этом обеспечивается контроль над допустимым уровнем риска при разумной гарантии достижения целей организации. Управление рисками организации представляет собой непрерывный процесс, охватывающий всю организацию, осуществляется сотрудниками на всех уровнях организации (советом директоров, менеджерами и другими сотрудниками), используется при разработке и формировании стратегии, применяется во всей организации, на каждом ее уровне и в каждом подразделении и включает анализ портфеля рисков на уровне организации.

К мерам по управлению ИТ-рисками относятся: разработка нормативных документов; обеспечение физической безопасности и безопасности ИС; разграничение доступа к ресурсам компании; контроль состояния корпоративной ИС. Во-первых, определяется объект защиты — проводится инвентаризация информационных активов, оценивается их критичность для бизнес-процессов компании. Во-вторых, решается, от чего осуществляется защита. Для этого анализируются присущие системе уязвимости, определяется степень их критичности — вероятность того, что они могут быть реализованы.

4.1 Идентификация активов

Политика информационной безопасности одной из стратегий — это управление и расчет рисков.

Суть данной стратегии заключается в реализации важных аспектов политики информационной безопасности и анализа угроз. Риск появляется там где существует вероятность угрозы, при этом величина пропорциональная величине этой вероятности.

Оценивая размер выработать определенные меры и создать механизм контроля того, что остаточные риски не выходят за приемлемые ограничения. Следовательно, управление рисками включает процесс 2 видов деятельности: оценка рисков и выбор эффективных и выгодно экономических защитных регулирующих механизмов. Процесс можно разделить на несколько последовательных этапов:

1) Идентификация рисков;
2) Выбор анализируемых объектов;
3) Анализ угроз и последствий;
4) Выбор и реализация защитных мер;
5) Оценка остаточного риска.

При идентификации рисков следует учесть активы и информационные ресурсы, их ценности и защитные меры. Исследуя все компоненты информационной системы необходимо учесть всю инфраструктура

организации, одно из ключевых результатов процесс идентификации активов является получение детальной информации всей структуры организации и способы её использования.

Выбор объектов анализа, это следующий этап управления рисков, который заключается в разбиении на сектора и более важных частей или критичных участках, это позволяет минимизировать затраты, а также в данный этап входят объекты такие как компьютеры, периферия, системы защиты, сеть и программные объекты. Программным объектам относятся firewall, антивирус, различные сервисы итд.

Анализ угроз и последствий, производится на основе уже полученных данных из предыдущих этапов – активы, объекты. Исходя из этого производится оценка степени определенности угроз и максимальный риск. Максимальный риск в данном случае это пятибалльная таблица, следуя которой устанавливается приоритет. 1 – маловероятно и 5 – неизбежно. Данная структура позволяет обеспечивать наиболее важнейшую из многих задача для успешной ликвидации или уменьшения угрозы.

Выбор и реализация защитных мер. На данном этапе следует решение угрозы выявив оценки определенной угрозы на величину предполагаемого ущерба, необходимо реализовать дополнительные защитные меры уже имеющихся защитных систем, которые отличаются методами защиты т.е эффективностью и обладающие невысокой стоимостью.

Оценка остаточного риска необходимо для результата эффективности уже предпринятых мер и показателей оценки. Этот этап предполагает о валидности предпринятых мер, стоимость и пропорциальность к появлению дальнейших угроз с уже корректирующих мероприятий данной уязвимости.

Перечень активов:

– Корпоративная (внутренняя) сеть;
– Межсетевой экран;
– Виртуальный роутер;
– Рабочий ПК;
– DMZ-сервер;

4.2 Идентификация рисков

Для расчета рисков были выбраны следующие угрозы и уязвимости:

1. Перепад напряжения. Непредвиденное падение напряжения, которое может спросить текущую конфигурацию и несохраненные данные на сервере.
2. DDOS-атака. Уязвимость протокола передачи пакетов приведет к переполнению буфера, что в свою очередь дает возможность совершить DDOS-атаку на сервер.

3. Распространение вредоносного ПО. Анонимный доступ к файловому серверу позволит злоумышленнику подменить легитимным файлы сервера

4. Неверная настройка доступов. Была допущена ошибка при назначении прав и полномочий пользователям или группам.

5. Переполнение буфера памяти. Из-за ошибки в протоколе очереди межсетевого экрана, буфер памяти переполняется очень быстро, что приводит к отказу в обслуживании.

6. Внедрение бэкдора. Программист ОС встроил в вызов сервисов ядра бэкдор, который позволяет получать удаленный доступ к компьютеру с этой ОС.

7. НСД в ЛВС. Допущенная при проектировании ЛВС ошибка, например, открытый порт RG-45, приведет к получению злоумышленником несанкционированного доступа во внутреннюю сеть.

8. Установка ложного сертификата безопасности. Пользователь установил нелигитимный корневой сертификат, что позволяет злоумышленнику подменить сертификат VPN сервера и раскрыть шифрованную сессию.

9. Выход из строя комплектующих. Недостаточно хорошее техническое обслуживание узлов ЛВС, которое привело к физическим повреждениям ЛВС.

10. Удаленное управление зараженным компьютером. Неправильное правило ACL приведет к тому что трафик из внешней сети будет проходить к внутренним ресурсам корпоративной сети.

4.3 Расчёт рисков

В качестве параметров над которыми будут производится расчеты, используются:

-Коэфициенты показателей «Конфиденциальности», «Целостности», «Доступности»;

-Коэфициент уровня угрозы;

-Коэфифицент показателя степени уязвимости.

Согласно стандарту BS 77990 уровень риска вычисляется с учетом трех показателей – ценности ресурса, уровня угрозы и степени уязвимости. Формульный вид представлен ниже:

$$R = S * L(t) * L(v); \quad (1)$$

Где R - значение риска;

S - ценность актива/ресурса;

L(t) - уровень угрозы;

L(v) - уровень/степень уязвимости.

После расчета показателей уровня риска, производится введение мер, препятствующих реализации риска, в данном случае этими мерами должно служить введение программно-аппаратного комплекса. Перерасчет остаточного показателя риска после введения мер осуществляется по формуле ниже:

$$R_{\text{ост}} = S * L(t)_{\text{ост}} * L(v)_{\text{ост}} \quad (2)$$

Где $R_{ост}$ - остаточный риск;

S - ценность актива/ресурса;

$L(t)_{ост}$ - уровень угрозы после введения мер;

$L(v)_{ост}$ - уровень/степень уязвимости после введения мер.

По итогам расчетов должно сформироваться мнение, у специалиста, который производил расчеты, о эфективности вводимых мер защиты.

Таблица 4.3.1 – Расчёт рисков информационной безопасности

Код	**Угрозы**	**Уязвимости**	**Максимальный уровень риска**	**Меры по обработке риска**	**Остаточный уровень риска**	**Дата**	**Комментарии**
А. Межсетевой экран							
.1	Перепад напряжения	Непредвиденное падение напряжения, которое может спросить текущую конфигурацию и несохраненные данные на сервере.	94	UPS (ИБП)	43	27.06.2020	Установка источника электропитания, обеспечивающий при кратковременном отключении основного источника мощности питания, а также защиту от помех в сети основного источника
.2	Переполнение буфера памяти	Из-за ошибки в протоколе очереди межсетевого экрана, буфер памяти переполняется очень быстро, что приводит к отказу в обслуживании	38	Использование dev/null	15	28.06.2020	Перенаправление избыточной информации в бесконечный раздел /dev/null позволит защитить буфер от переполнения
В. Корпоративная сеть							

.1	НСД в ЛВС	Допущенная при проектировании ЛВС ошибка, например, открытый порт RG-45, приведет к получению злоумышленником несанкционированного доступа во внутреннюю сеть	38	Учет сетевых зон средстами брандмауэра Palo Alto	26	30.06.2020	Использование механизмов для учета каждого участка сети существенно упрощает аудит и журналирование
.2	Выход из строя комплектующих	Недостаточно хорошее техническое обслуживание узлов ЛВС, которое привело к физическим повредеждениям ЛВС	71	Резервное копирование	11	01.07.2020	Backup системы позволит всегда иметь стабильную версию всего необходимого ПО, к которой всегда можно вернуться при возникновении ошибок или сбоев.
С. Виртуальный маршрутизатор							
.1	DDOS-атака	Уязвимость протокола передачи пакетов приведет к переполнению буфера, что в свою очередь дает возможность совершить DDOS-атаку на сервер	46	Firewal Palo Alto	16	27.06.2020	Брандмауэр рассматривает каждый уникальный поток (на основе входной и выходной зоны, IP-адреса источника и назначения, протокола и приложения)
.2	Неверная	Была допущена ошибка при назначении	61	Ограничение прохождения	44	28.06.2020	Ограничения общего количество маршрутов,

	настройка доступов	прав и полномочий пользователям или группам		трафика			которые могут быть приняты BGP во время одной сессии
D. DMZ-сервер							
.1	Удаленное управление зараженным компьютером	Неправильное правило аксес листа приведет к тому что трафик из внешней сети будет проходить к внутренним ресурсам корпоративной сети	16	ACL	9	27.06.2020	В access-list заносятся записи, запрещающие доступ к PE по telnet из CE
E. Рабочий ПК							
.1	Распространение вредоносного ПО	Анонимный доступ к файловому серверу позволит злоумышленнику подменить легитимным файлы сервера	74	Политики безопасности	29	27.06.2020	Прописать все условия по безопасности в политике о неразглашении конфиденциальности, предоставить гарантийное письмо, подписание с компанией политики о кибербезопасности

.2	Установка ложного сертификата безопасности	Пользователь установил нелигитимный корневой сертификат, что позволяет злоумышленнику подменить сертификат VPN сервера и раскрыть шифрованную сессию.	76	Ruleset внутри межсетевого экрана	5	27.06.2020	Политика безопасности, регулирующая установку сертификатов безопасности защитит от установки непроверенных и вредоносных cert’ов
.3	Внедрение бэкдора	Внутренний пользователь встроил в сервис ядра ОС бэкдор, который позволяет получать удаленный доступ к компьютеру с этой ОС	76	Протоколы аутентификации	39	27.06.2020	Использование аутентификации в протоколах маршрутизации защитит внутреннюю сеть от нежелательного доступа извне.

4.4 Проекты Coras

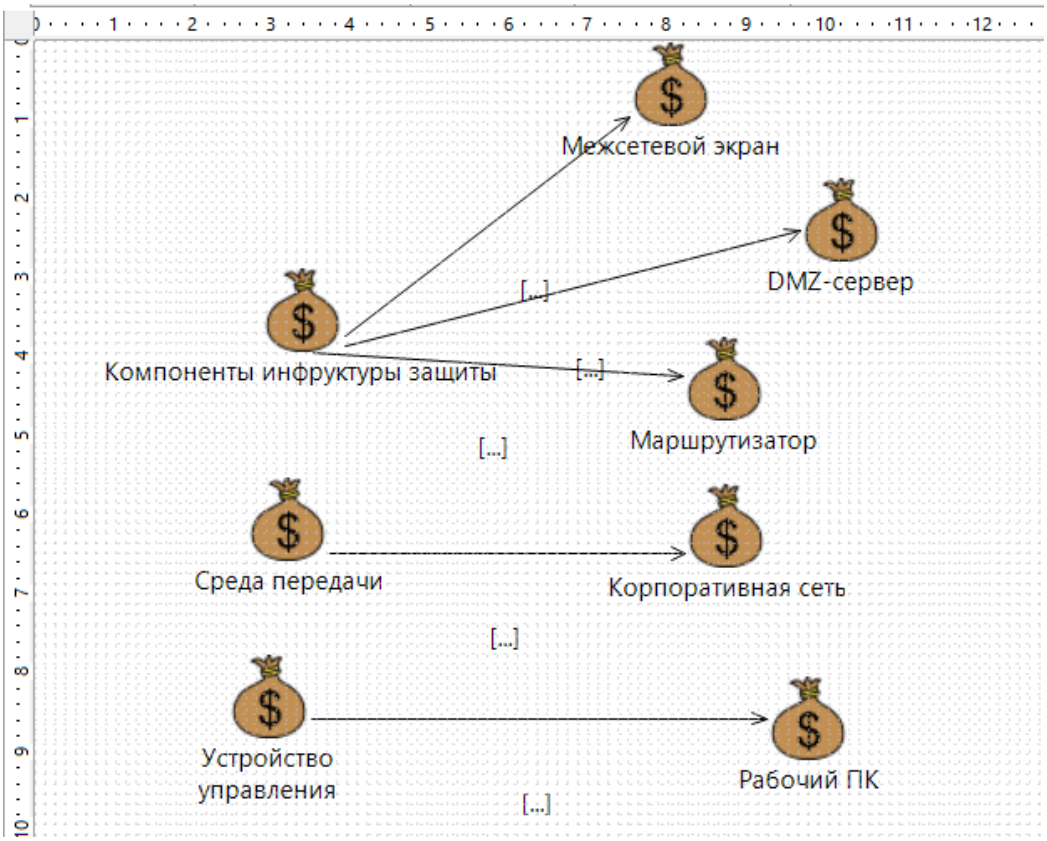


Рисунок 4.4.1 – Активы, выбранные для расчёта

Для удобства восприятия активы условно разделены на несколько категорий, в том числе: компоненты инфраструктуры защиты, которые являются основными инструментами выполнения дипломного проекта; среда передачи – это ЛВС, которая развернута в рамках учебной аудитории для соединения устройств в единую сеть; и устройство управления инфраструктурой – рабочий ПК под управлением OS Windows 2012.

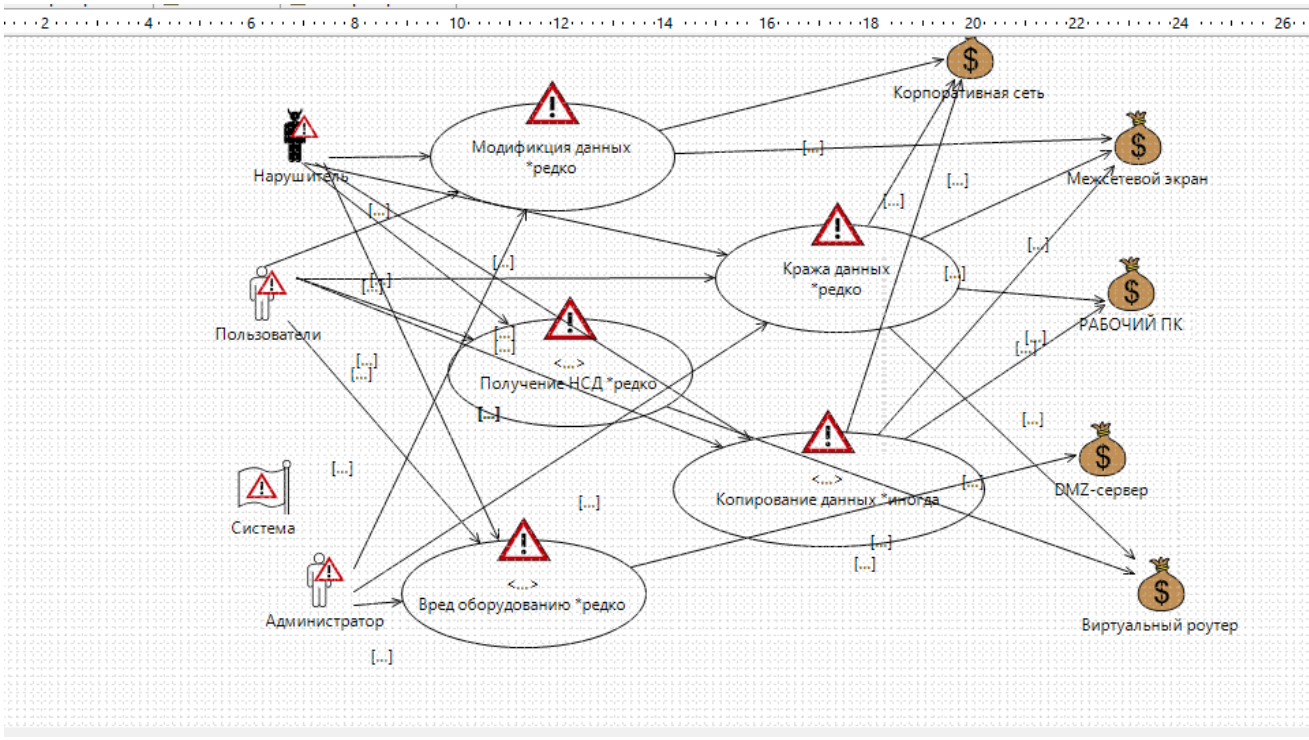


Рисунок 4.4.2 – Угрозы и вероятность их возникновения

Далее было определено, какие угрозы будут актуальными для выбранных активов. Стоит обратить внимание, что угрозы могут исходить как снаружи, так и изнутри внутренней корпоративной сети.

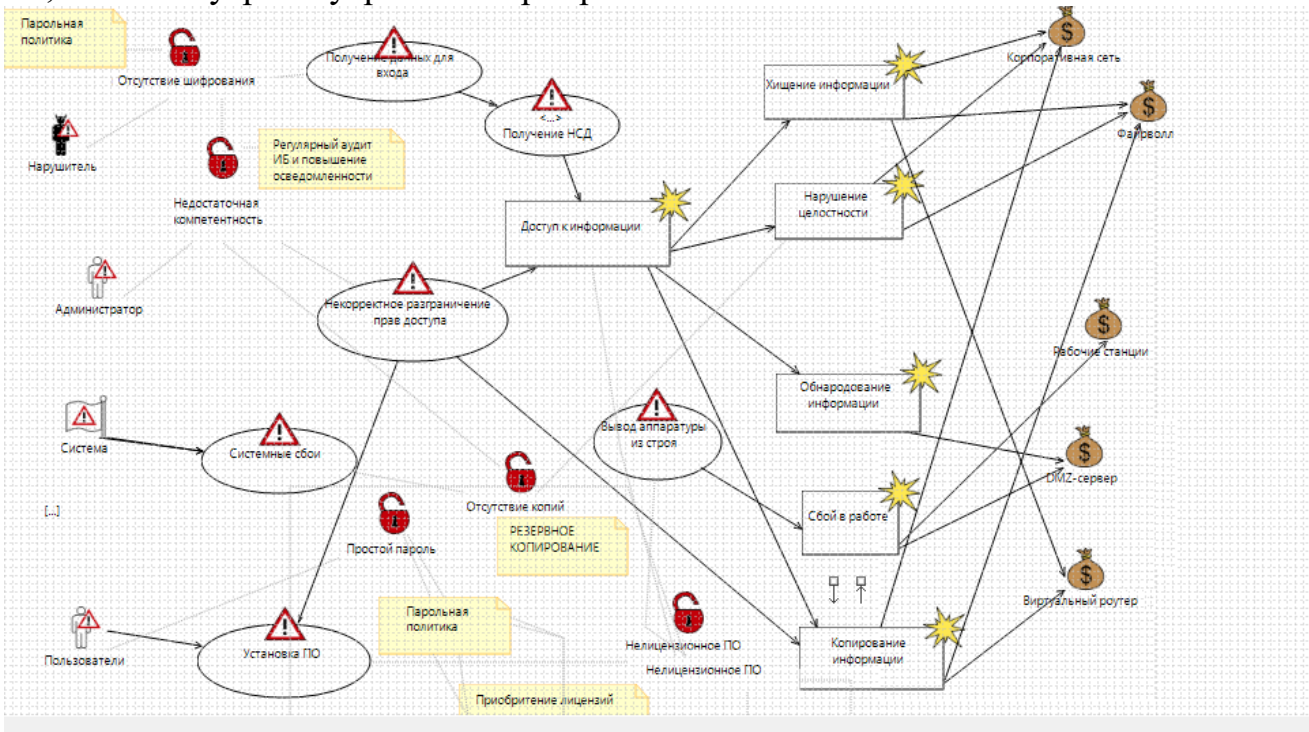


Рисунок 4.4.3 – Риски и вероятность возникновения

На Рисунке 3 мы можем видеть, как именно риски могут навредить нашим активам. Благодаря данной схеме наглядно демонстрируется, от кого

или чего исходят рисковые ситуации и как обычная угроза, с помощью эксплуатации определенной уязвимости, становится рисковой ситуацией.

Рисунок 4.4.4 – Диаграмма угроз с элементами СЗИ

На Рисунке 4 изображены способы «закрытия» рисковых ситуаций – какие-либо действия, направленные на сведение к минимуму возможного риска для наших активов. Зачастую, риск полностью оказывается убрать невозможно. В данном случае необходимо убедиться, что такой риск будет локализован и не навредит другим ценным активам.

Вывод

Результаты, полученные в результате расчетов, дают нам ясную картину, насколько дипломный проект может быть устойчив к рисковым ситуациям, насколько разумно будет применение тех или иных механизмов понижения рисков. Так, например, рисковая ситуация с перебоями напряжения для межсетевого экрана , которая по количественной шкале составляла 94 пункта, так как брандмауэры крайне чувствительны к перепадам напряжения, была фактически «закрыта» установкой модулей бесперебойного питания, что позволило сократить величину риска в два раза. Таким образом, проделанная работа даёт нам ясное понимание того, какие меры являются обоснованными и логичными, а какие будут чрезмерными и лишними.

Обращаясь к численным значениям, полученных в результате расчетов, можно делать вывод, что применимые меры являются достаточными и обоснованными как с финансовой, так и с технической точки зрения.

Согласно расчетам, в среднем, величина рисков после принятия мер составляет в 2.6 раз меньшее значение, чем изначальное.

Список литературы

1. Попов, А. А. Производственная безопасность [Электронный ресурс] / Попов А.А. — Москва : Лань, 2013 .— Рекомендовано УМО по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки «Безопасность жизнедеятельности» .— ISBN 978-5-8114-1248-8 . (дата обращения: 24.04.2020)
2. Белов, С. В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность) : [учебник для академического бакалавриата по дисциплине "Безопасность жизнедеятельности" для бакалавров всех направлений подготовки в вузах России] / С. В. Белов .— 5- е изд., перераб. и доп. — Москва : Юрайт, 2014 .— 702 с. : ил. ; 21 см .— (Бакалавр, Академический курс) (дата обращения: 22.04.2020)
3. СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений [Текст] / Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.
4. МСН 2.04-03-2005 «ЗАЩИТА ОТ ШУМА» (дата обращения: 21.03.2020)
5. Безопасность жизнедеятельности : учебное пособие / О. М. Зиновьева, Л. А. Лысов, А. М. Меркулова [и др.]. — Москва : МИСИС, 2019. — 134 с. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/116916 (дата обращения: 24.04.2020)
6. Митрошина Екатерина Валерьевна СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕЖСЕТЕВЫХ ЭКРАНОВ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО - УПРАВЛЯЮЩИХ СИСТЕМАХ // E-Scio. 2017. №1 (4). URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-mezhsetevyh-ekranov-v-raspredelennyh-informatsionno-upravlyayuschih-sistemah (дата обращения: 24.05.2020).
7. ГОСТ 12.1.003-2014 Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности (Переиздание) 2015 – 26с.
8. Национальная библиотека им Баумана //bmtsu: SIEM. 2020. URL://https://ru.bmstu.wiki/SIEM_(Security_information_and_event_management (дата обращения 07.04.2020).
9. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. — МГТУ им. Н. Э. Баумана, 2002. — 306 с. — ISBN 5-7038-2059-6. (дата обращения: 14.05.2020)