Разработка веб-интерфейса для авторизации и управления сетевым устройством (файрволом)

*Реализация веб интерфейса настройки фаервола для обеспечения безопасности сети*

Анализ существующих решений.

firewall (с англ. — противопожарная стена), или как его еще называют brandmauer (с нем. — противопожарная стена) в русском языке имеет два названия отображающих его назначение (меж)сетевой экран. Сетевой экран выполняет функцию блокировки доступа посторонних лиц к компьютеру посредством сети.

***Файрвол*** — это первая линия защиты в системе обеспечения безопасности данных. Межсетевые экраны предназначены для предотвращения несанкционированного доступа к ресурсам локальной сети, внешних и внутренних атак. Это может быть программный или аппаратный комплекс, либо комбинация и того, и другого. Основная функция межсетевого экрана заключается в фильтрации сетевого трафика в соответствии с установленными правилами, за счет чего осуществляется блокировка прохождения запрещенных запросов. В данной статье мы рассмотрим основные типы файрволов, их преимущества и потенциальные недостатки, а также перспективы развития данной технологии.

Условно можно выделить две основные технологии, реализуемые в файрволах: пакетная фильтрация и фильтрация на уровне приложений. При этом обе технологии могут быть реализованы в комбинации в рамках одного продукта.

**Пакетный файрвол (Packet-Filtering Firewall)**

В большинстве маршрутизаторов и коммутаторов используется технология пакетной фильтрации. Пакетные фильтры функционируют на сетевом уровне и осуществляют разрешение либо запрет прохождения трафика на основе анализа информации, находящейся в заголовке пакета. Такая информация включает тип протокола, IP адреса отправителя и получателя, номера портов отправителя и получателя. В некоторых случаях анализируются и другие параметры заголовка пакета, например для проверки является ли пакет частью нового либо уже установленного соединения. При поступлении пакета на любой интерфейс маршрутизатора, в первую очередь определяется, может ли пакет быть доставлен по назначению, а затем происходит проверка в соответствии с заданным набором правил — так называемым списком контроля доступа (ACL).

Определение правил фильтрации происходит на основе одного из двух взаимоисключающих принципов:

1) «Разрешено все, что не запрещено в явном виде»

Такой подход облегчает администрирование межсетевого экрана, так как не требует дополнительной настройки. Тем не менее, в случае неправильной настройки, когда не учитываются потенциальные несанкционированные действия, эффективность защиты стремится к нулю.

2) «Запрещено все, что не разрешено в явном виде»

Такой подход обеспечивает наиболее высокую степень эффективности. Относительным недостатком в данном случае является усложнение администрирования, так как необходима предварительная тонкая настройка базы правил.

С точки зрения безопасности более предпочтительным является второй вариант, при котором разрешается прохождение пакетов определенного типа и запрещается все остальное. С одной стороны такой подход упрощает настройку, так как количество запрещенных пакетов обычно гораздо больше, чем разрешенных. Кроме того, при появлении новых служб нет необходимости дописывать новые запрещающие правила — доступ к ним будет заблокирован автоматически. Тем не менее на каждый тип разрешенного взаимодействия необходимо прописать одно и более правил.

Преимущества:

\* Распространенность пакетных фильтров связана с тем, что эта технология проста и обеспечивает высокую скорость работы.

\* По умолчанию пакетный фильтр встроен в подавляющее большинство маршрутизаторов, коммутаторов, VPN-концентраторов. В связи с этим отпадает необходимость в дополнительных финансовых затратах на ПО.

\* Изучение данных в заголовках пакетов позволяет создавать гибкую схему разграничения доступа.

\* При создании правил фильтрации возможно использование помимо полей заголовков также и внешней информации, например, даты и времени прохождения сетевого пакета.

Недостатки:

\* Пакетные фильтры работают только с заголовками и могут пропустить поля, содержащие данные, противоречащие политике безопасности, например поле с командой на доступ к файлу паролей по протоколу FTP или HTTP, которая является потенциально опасной. Также пакетный фильтр может пропустить пакет от узла, с которым в данный момент не открыто никаких активных сессий.

\* Пакетные фильтры не анализируют трафик на прикладном уровне, что открывает возможность для совершения множества видов атак.

\* Настройка достаточна сложна и требует от администратора высокой квалификации и глубокого понимания принципов работы протоколов стека TCP/IP.

**Файрвол прикладного уровня** (Application Firewall)

Данный тип файрвола включает в себя прикладное программное обеспечение и играет роль промежуточного звена между клиентом и сервером. Аппликативные файрволы обеспечивают защиту на прикладном уровне, используя для блокировки вредоносных запросов информацию о специфических особенностях приложений. Технология фильтрации на уровне приложений позволяет исключить прямое взаимодействие двух узлов. Файрвол выступает в качестве посредника между двумя узлами, перехватывает все запросы и после проверки допустимости запроса устанавливает соединение. Файрвол прикладного уровня предоставляет возможность аутентификации на пользовательском уровне, протоколирование трафика и сетевых событий, а также позволяет скрыть IP-адреса хостов локальной сети.

Преимущества:

\* Файрволы прикладного уровня обеспечивают более высокий уровень защиты по сравнению с пакетными фильтрами, так как имеют больше возможностей для анализа всего сетевого пакета, а не только заголовка TCP пакета.

\* Прикладные файрволы создают более детализированные логи.

Недостатки:

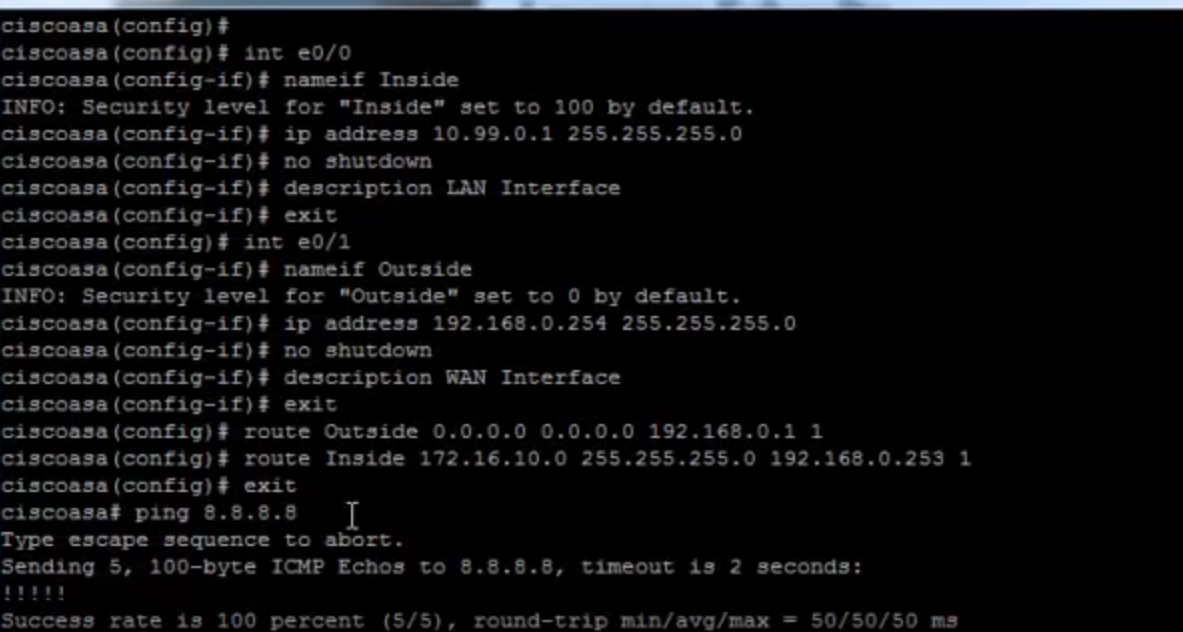
\* Данная технология является более медленной, так как значительная процессорная нагрузка для осуществления сервисов отрицательно сказывается на скорости работы. Глубокий анализ полей данных заметно снижает производительность межсетевого экрана, увеличивает время отклика и пропускную способность сети.

В зависимости от сферы применения среди файрволов прикладного уровня выделяют WAF (Web-application firewalls), предназначенные для защиты веб-приложений, DAF (Database Access Firewalls), защищающие базы данных и т.д.

Что представляет из себя данное сетевое устройство.?

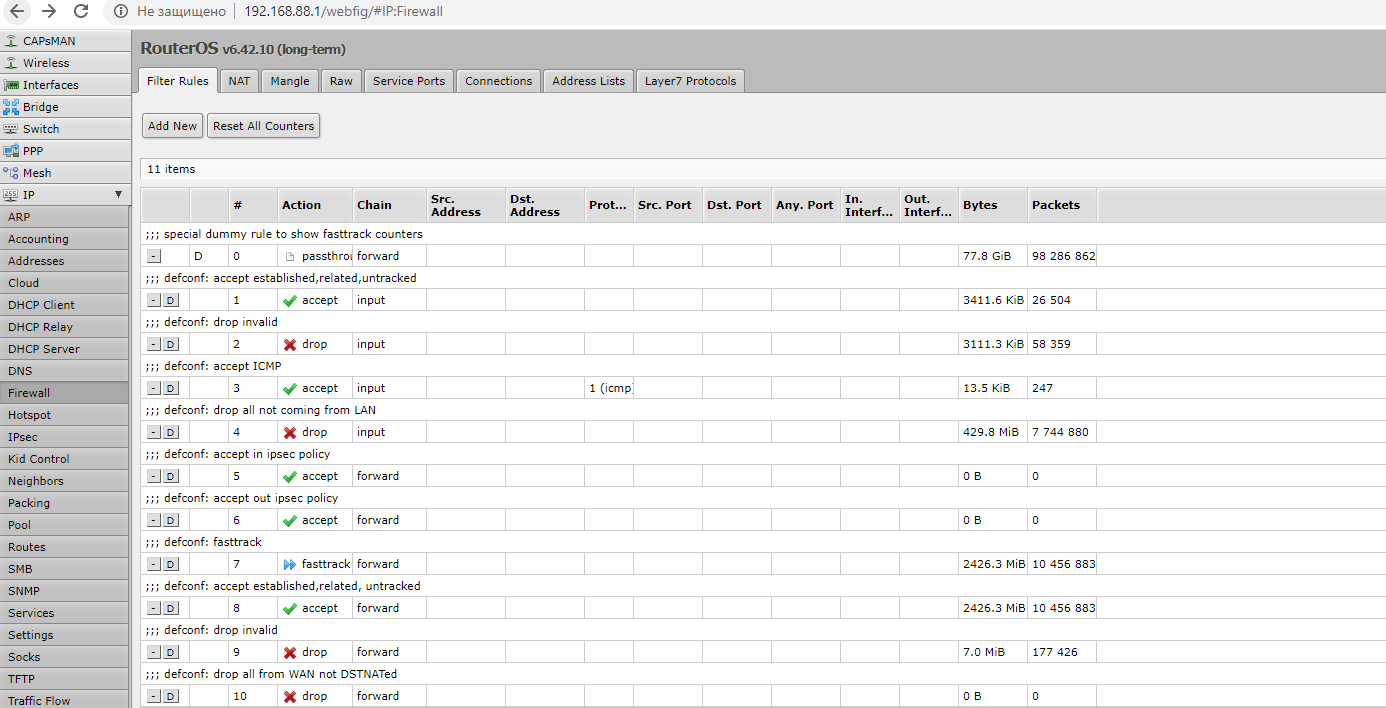
..2 порта, Ethernet между локальной и внешней сетью

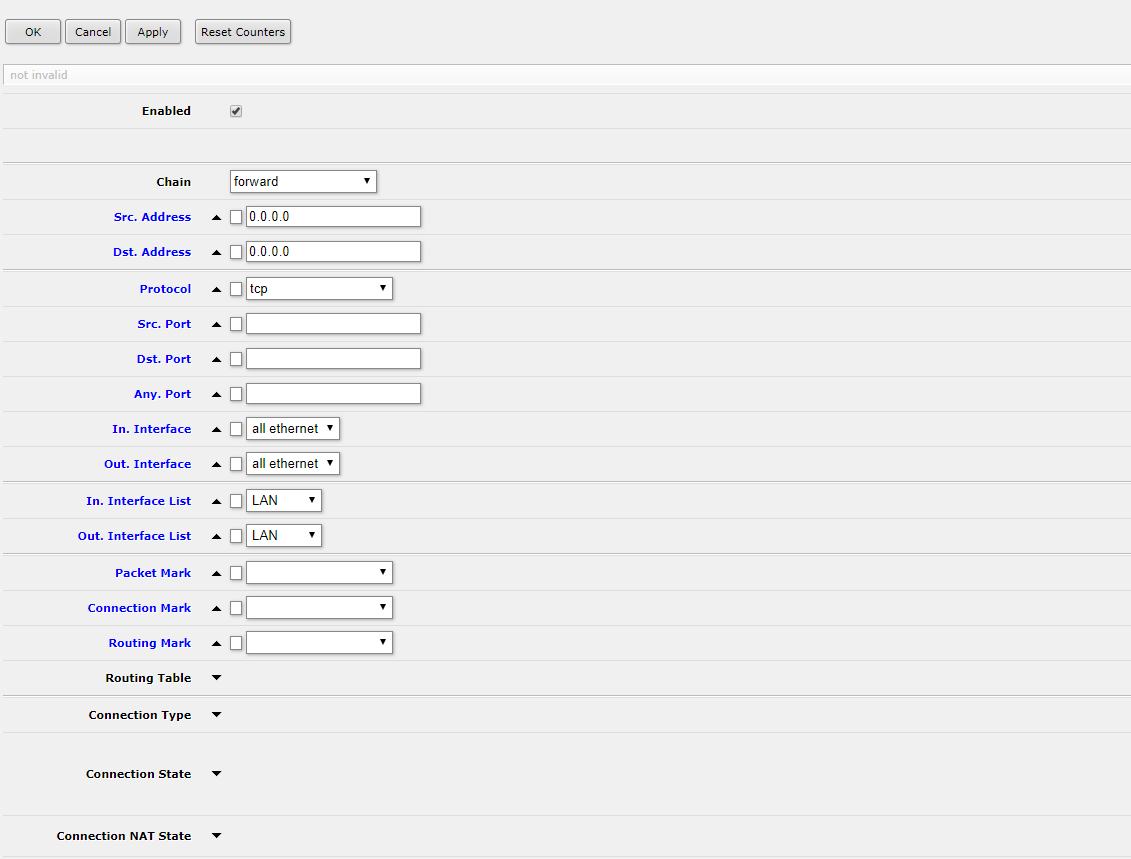
Фаервол Cisco



Не имеет графического интерфейса или веб интерфейса, команды нужно вводить вручную в терминале

Веб интерфейс micriotik





1. Анализ предметной области

Реализация:

Css, js, html.

Циско использует консоль, чтобы не дублировать функционал. Защищенность, юсб сложнее получить доступ чем через сеть, консоль защищенней.

**Почему стремимся к веб интерфейсу?**

Сформулировать цели

HP коммутаторы L2+ tplink производитель, модели

Найти как можно больше производителей сетевых устройст с возможностью настройки фаервола. 10-20 устройств, таблица, большинство устройств – фаерволы, или коммутаторы с фаерволом

План

1. Создать яндекс диск.
2. Оформить результаты анализа
   1. Какой функционал реализуется в циско и как
   2. Циско работает через консоль, удобно описывать и использовать (анализ удобства использования)
   3. Удобство веб интерфейса, безопасность и удобство (консоль это хорошо, но неудобно удаленно подключаться и обычному пользователю будет сложно) нужно обеспечить безопасность веб.
   4. Компромисс – сделать доступным веб, после подключения по консоли подключать – отключать
   5. Коммутаторы
3. Реализация html css js

Список производителей

Какие имеют фаервол

Какой функционал и как реализован

Добавить свое видение