RRC

# Основы грамотной политики управления брандмауэром

Перевод: Pete Kuzeev, Security Engineer, RRC Moscow

По работам: Reuven Harrison, CTO, Tufin Technologies
Michael Hamelin, Chief Security Architect for Tufin Technologies

RRC

# С чего нужно начинать?

Когда речь заходит политике безопасности, у профессионала в этой области сразу возникают ассоциации с ясной, интуитивной и четко организованной системой. Ваша задача построить систему, способную дать администраторам возможность быстро находить необходимые правила или добавлять новые и принимать правильные решения для обеспечения непрерывности бизнес-процессов. Позвольте дать вам несколько советов:

- создавайте чёткую и ясную документацию, затрагивающую каждое правило и сетевой объект, с помощью которой даже новый специалист мог разобраться с работающей системой

-избегайте использования одного и того же правила для различных задач, это может подкупить своей простотой, но является весьма небезопасным и не поддающемся управлению процессом

- группируйте правила в зависимости от задач бизнеса и добавляйте описания к каждому, воспользовавшись специальным разделом ПО в зависимости от вендора

# Правила хорошего тона

1. **С лёгкостью устранять проблемы сетевой доступности**

Если сеть стала работать не так как ожидалось, то первое устройство к которому будут претензии – это брандмауэр. У вас должно быть чёткое понимание какое правило вызывает проблему и на каком из устройств вам необходимо её устранить

2. **Возврат к более ранней конфигурации при необходимости**

Когда политика безопасности  становится причиной отказа сети передачи данных  вы можете, воспользовавшись удобными инструментами аудита, отследить изменение политики, повлекшее данный отказ и быстро устранить его вернувшись к предыдущей конфигурации

3. **Документирование на постоянной основе доступное для всех**

Каждое правило должно быть документировано создателем, по факту создания и быть доступно для понимание каждым из администраторов

# Правила хорошего тона

**4. Лёгкая для изучения и понимания**

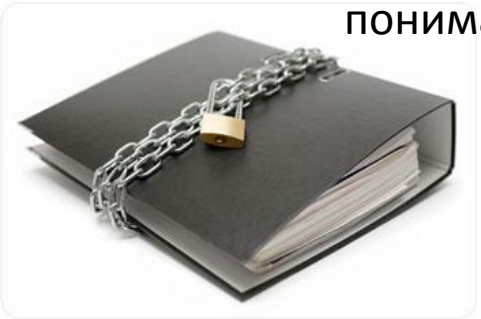
Когда новый администратор приходит в коллектив, он должен быстро составить чёткое понимание о устройстве сети и значении всех используемых брандмауэром правил

**5. Единое понимание политики, даже в смешанном окружении**

Не важно – сколько у вас устройств и от каких они вендоров, правило должно однозначно пониматься и выполняться на любом из них

**6. Подробная документация**

Каждое правило и каждый объект используемый в правилах вашей политики должны быть подробно описаны, до степени однозначности понимания и идентификации каждым из администраторов



# Правила хорошего тона

**7. Каждое правило – под чётко определенные задачи**

Правило не должно давать пользователю больше возможностей, чем ему требуется для конкретных бизнес-задач, все временные правила четко ограничивайте по времени действия, регулярно удаляйте потерявшие актуальность объекты и правила – у вас должен быть некий механизм взаимодействия, позволяющий уточнять актуальность того или иного правила перед его удалением

**8. Политика безопасности высокого уровня**

Политика правил вашего брандмауэра – это всего лишь первая ступенька к глобальной политике безопасности и отнюдь не последняя! Вы должны убедиться в том, что правила вашего брандмауэра гармонично вписываются в политику безопасности вашей компании, отлично документированы и позволяют сделать представление о структуре глобальной политики, принятых стандартах условных условных обозначений и процедур внесения изменений

# Аутсорс для безопасности

В России этот заголовок у многих вызовет улыбку, но в Европе и США, где многие компании существуют только лишь благодаря аутсорсу и SOHO данная услуга является весьма востребованной.

Если попробовать посчитать, то получается, что около 90% рабочего времени высококлассные специалисты занимаются «саморазвитием», а отнюдь не написанием тех или иных правил или настройкой каких-либо устройств , поэтому существенная экономия средств для средней, не говоря уже о небольшой компании – на лицо.

Существует ряд правил, соблюдая которые вы можете получить от аутсорса максимальный эффект, привести свою глобальную политику безопасности к стандартизованному виду, например ITIL и обеспечить максимальную защиту своих данных и пользователей.

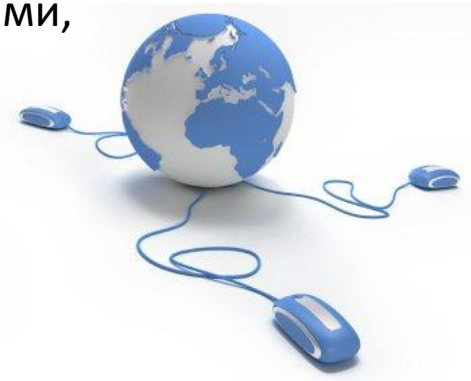
# Правила аутсорса

1. **Используйте стандартизованную систему управления (например, ITIL)**

Никогда не перекладывайте решение своих внутренних проблем на организацию, осуществляющую вашу поддержку, ваше общения с ней должно ограничиваться официальными чёткими указаниями на необходимость выполнения той или иной настройки и на желаемый результат

2. **Не нужно надеяться только на брандмауэр**

Не забывайте, что файрвол это всего лишь верхушка айсберга – обязательно приведите свою информационную систему к соответствию одному из стандартов безопасности (например, PCI, HIPAA, DPA), это позволит вам внести прозрачность в управления периферийными устройствами, регистрацию изменений настроек, согласование работ



# Правила аутсорса

**3. Взаимопонимание**

Для оптимальной работы у вас должна быть устойчивая связь в обоих направлениях, по одному ответственному сотруднику с каждой стороны, способных быстро решать все поступающие задачи

**4. Доверяй, но проверяй**

У вас должна быть возможность - проверять работу обслуживающей вас организации, хотя бы раз в месяц, посредством стороннего аудита и отслеживать совершаемые на устройствах действия

**5. Уровень обслуживания**

Сразу договоритесь о уровне обслуживания, времени в течение которого происходит обработка вашего обычного запроса и высоко приоритетного, обсудите формат внесения изменений в устройство, в идеале – четыре действия: запрос от вас, предложения по настройкам от обслуживающей организации, подтверждение от вас, применение настроек аутсорсером

# Правила аутсорса

**6. Проверьте вашего аутсорсера**

Обязательно проверьте репутацию организации, которая будет обслуживать ваши информационные системы, нанесите визит им в офис, удостоверьтесь в том, что они не являются посредниками – такое иногда бывает, узнайте о их собственной системе безопасности, о том, как они набирают персонал, пригласите с собой знакомого или стороннего эксперта, пусть он побеседует с их специалистами и составит представление о квалификации

**7. Доступ на чтение**

У вас всегда должен быть доступ на чтение к любому периферийному устройству – так вы сможете отслеживать текущее состояние и факт выполнение работ на самом устройстве, не нужно полагаться на систему закрытия тикетов самого аутсорсера

# Распространенные ошибки

Моим первым провалом было то, что я устроил одновременную перезагрузку всех маршрутизаторов компании, я написал скрипт, в котором была ошибка и вместо того, чтобы перезагрузить все маршрутизаторы по очереди – он перезагрузил их все одновременно. Я думал меня уволят, к счастью – нет, вместе с шефом, воспользовавшись планом аварийного восстановления, мы восстановили работоспособность сети в течение нескольких часов.

Хорошие новости состоят в том, что сбои не так часты, плохие – в том, что их наступление невозможно предсказать, какие-либо неверные настройки могут вызвать сбой через день, а могут – через год.

Существует ряд весьма распространённых ошибок – попробуем рассмотреть в кратце самые существенные из них!

# Распространенные ошибки

1. **Создание обезличенных групп брандмауэра**

Каждая созданная вами группа должна иметь четкую характеристику, старайтесь избегать использования операторов подобных ANY

2. **Используйте свежую версию ПО для вашего устройства**

Не нужно стремиться использовать самую свежую версию ПО для вашего устройства, однако, если разница составляет более 15 релизов – бегите заниматься обновлением вашего устройства сразу после прочтения

3. **Не путайтесь в технологиях**

Если мы обратимся к практике, то аудиторы с удивлением выслушали администратора, который считал, что пароль и брандмауэр – являются разновидностью двухфакторной аутентификации

# Распространенные ошибки

**4. Несчастные случаи**

Администратор щёлкнул мышкой не там где нужно, следует быть внимательным, когда речь идет об обслуживании важных систем

**5. Скудная документация**

Когда предыдущий администратор был со скандалом уволен, оказалось что никто не знает значения многих правил сконфигурированных на брандмауэре – пришлось потратить много времени для наведения порядка

**6. Создание избыточных правил**

Создание правил, где любой трафик между некоторыми сетями запрещён или разрешён, за редким исключением такие правила не нужны

**7. Использование правил маршрутизации в политике безопасности**

Редактирование того или иного правила требует внесения изменений в таблицу маршрутизации, это может озадачить нового администратора

# Распространенные ошибки

**8. Использование интернет имени (DNS) в объекте политики**

Все современные популярные веб-ресурсы кластеризованы и могу иметь много ip адресов ассоциированных с данным именем

**9. Внесение изменений в конфигурацию в режиме «паники»**

Часто, при решении тех или иных задач, мы весьма ограниченны во времени и если у нас что-то не получается мы начинаем исправлять, отключать или удалять не понятные нам правила и объекты. Когда мы в конце концов находим «виновника» к нам начинает приходить понимание того, что многие исправленные правила не имели к ней никакого отношения, а вернуть их в начальное состояние не представляется возможным или затянется не на один день