Положа руку на сердце, все ли из нас являются экспертами по вопросам безопасности?

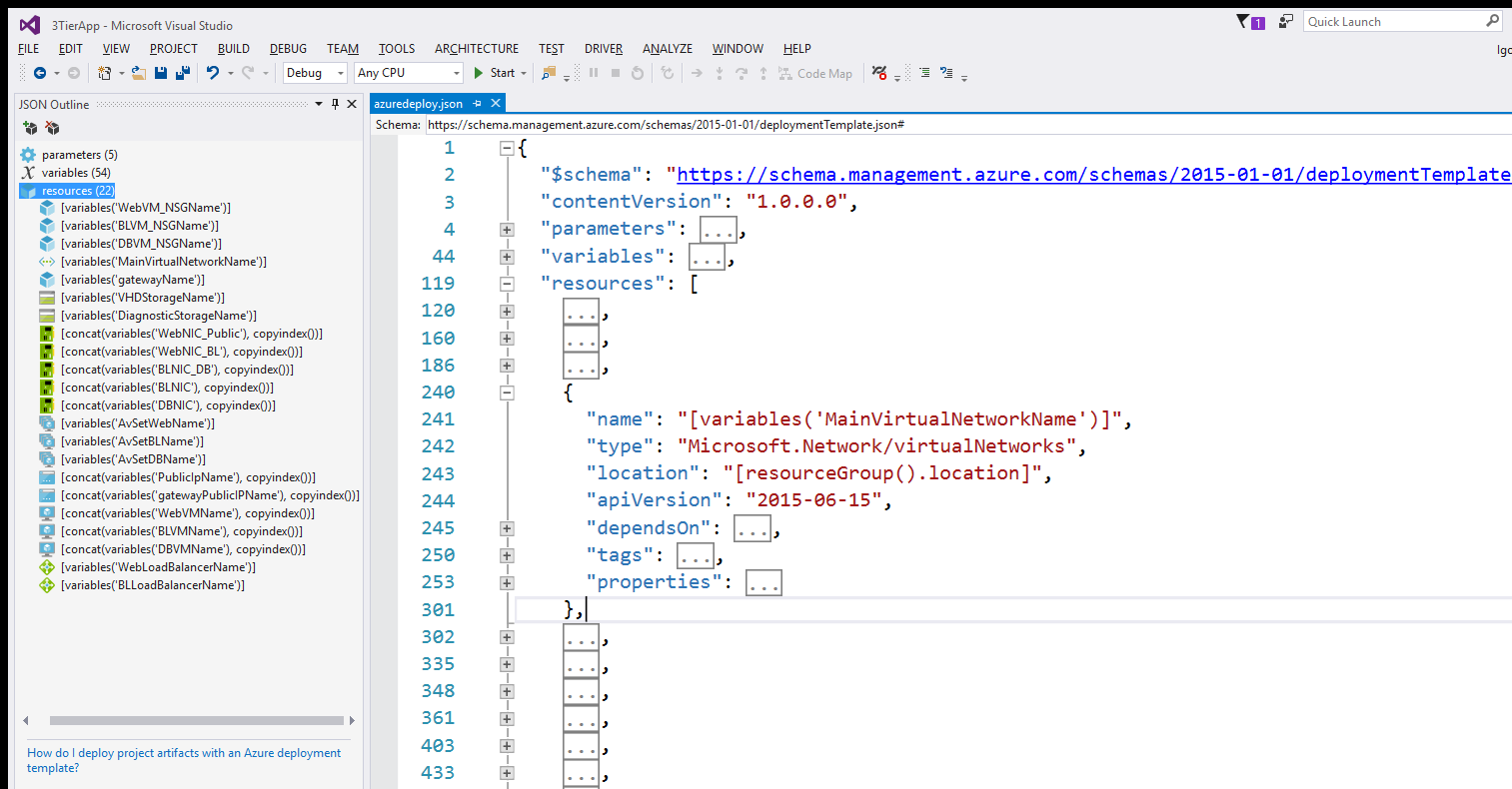
Лично я таким не являюсь, и очень хотел бы, чтобы какой-то искусственный интеллект подумал про безопасность и сказал мне- где у меня потенциальные дырки… а дальше я уже разберусь.

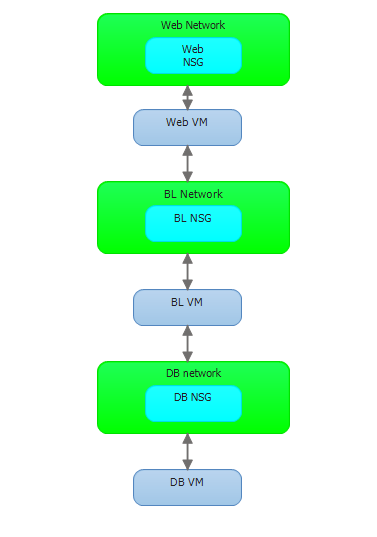
В Azure в preview появилась достаточно полезная фича- Azure Security Center <https://azure.microsoft.com/en-us/services/security-center/> , которая умеет анализировать вашу инсталляцию (виртуальные машины, сети, наличие firewall и еще несколько моментов <https://azure.microsoft.com/en-us/documentation/articles/security-center-policies/> ).

Давайте посмотрим, что он может.

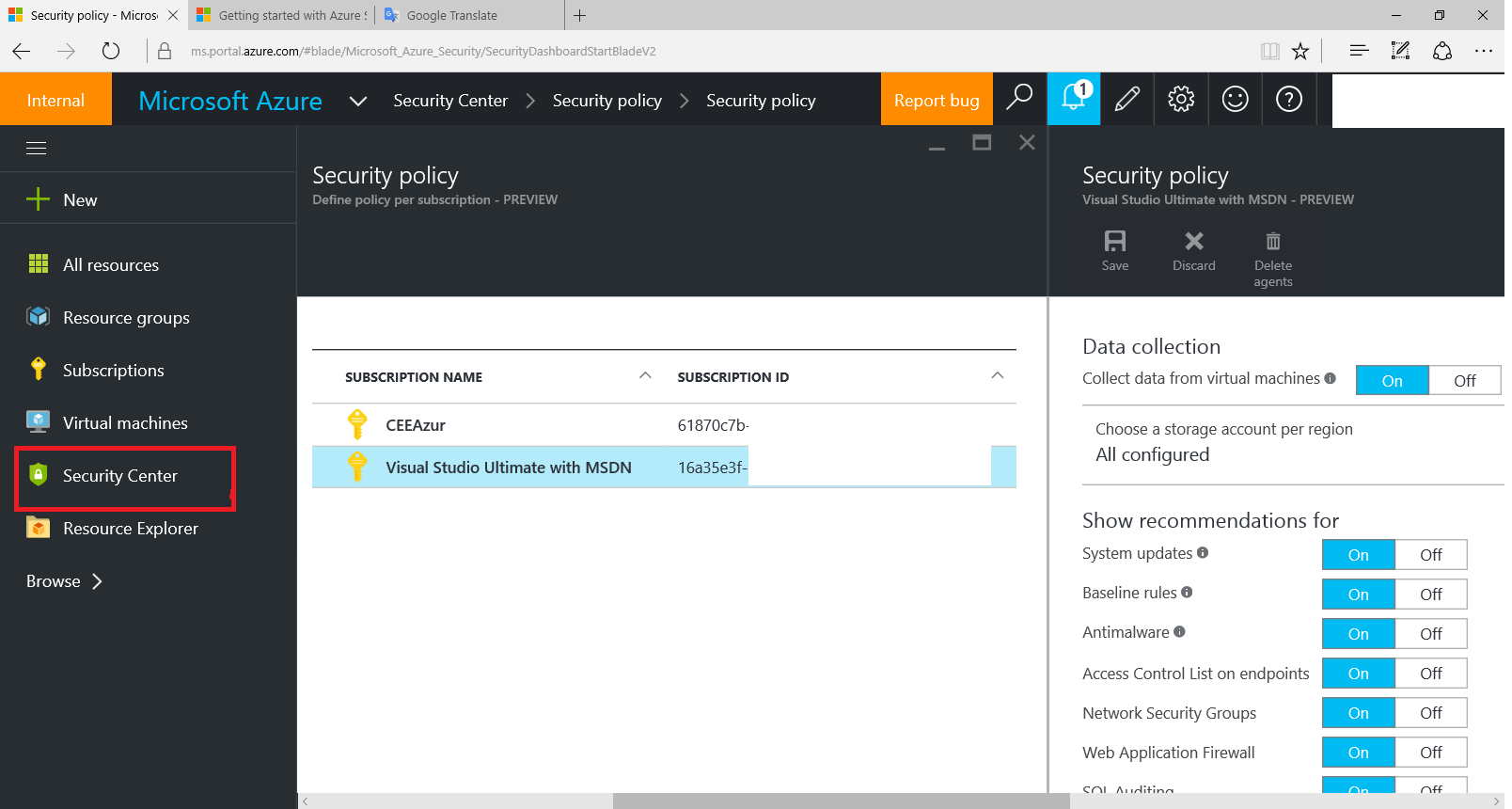
Для начала задеплоим что-нибудь в Azure. Я для тестов буду использовать этот ARM шаблон <https://github.com/msftrupfe/ARM/tree/securityPost>

Что он в себя включает: это приложение с 3 слоями. 1-N виртуальных машин в веб слое (windows server 2012r2), 1-N виртуальных машин в слое бизнеслогики(windows server 2012r2), 1-N в слое данных (SQL server на windows server 2012r2). Виртуальные машины в availability группах. 1 сеть, с 3 подсетями (1 между базой и логикой, 1 между логикой и вебом и одна по сути DMZ). Каждая подсеть содержит свою network security group, в которой определены inbound/outbound security rule (считайте для простоты- что правила для firewall, которые лобо разрешают трафик на определенные ip, либо запрещают). Визуально как-то так:

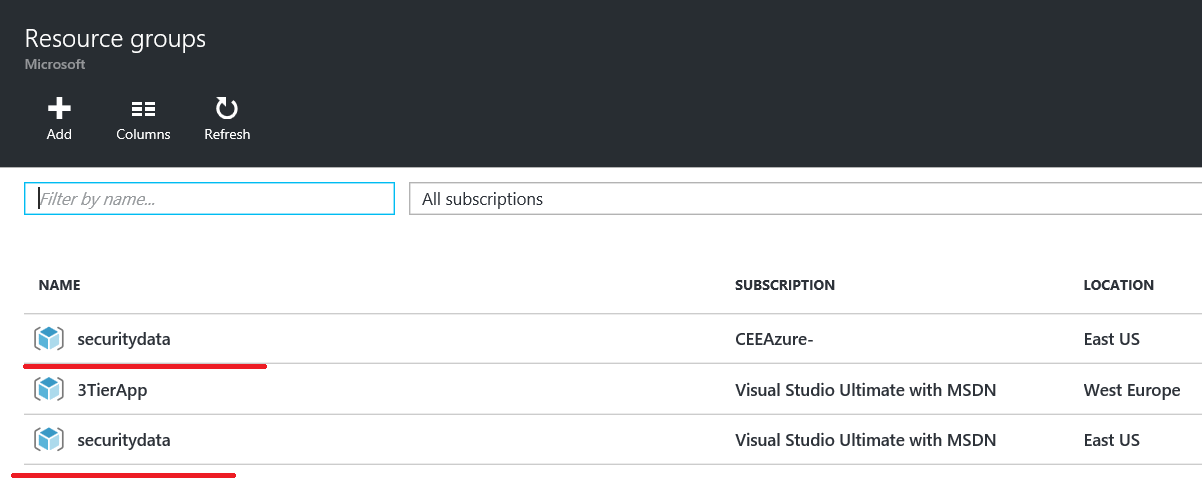




Теперь давайте включим сбор данных для security center:

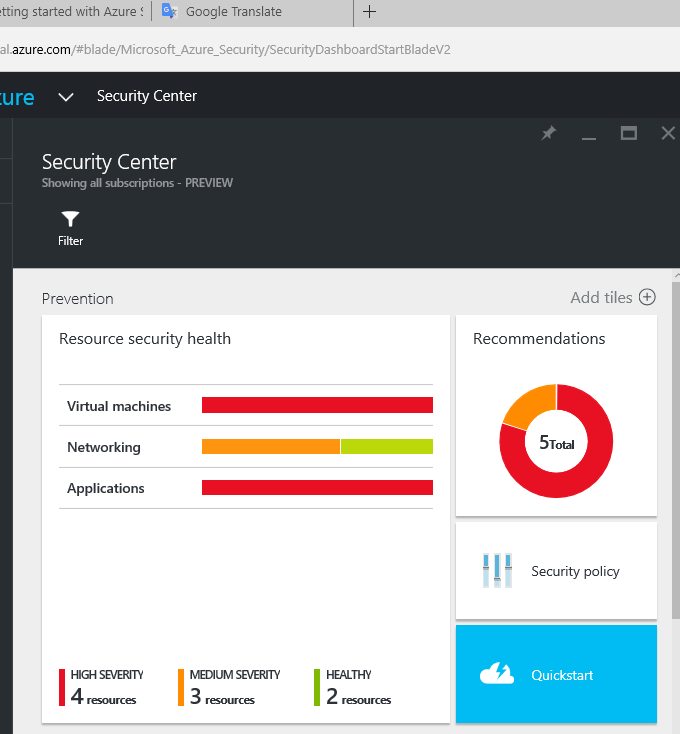


Security Center создаст для сбора данных resource group и storage account.



Вы заметите, что у меня таких группы 2- это потому, что у меня 2 подписки и данные собираются для каждой подписки отдельно.

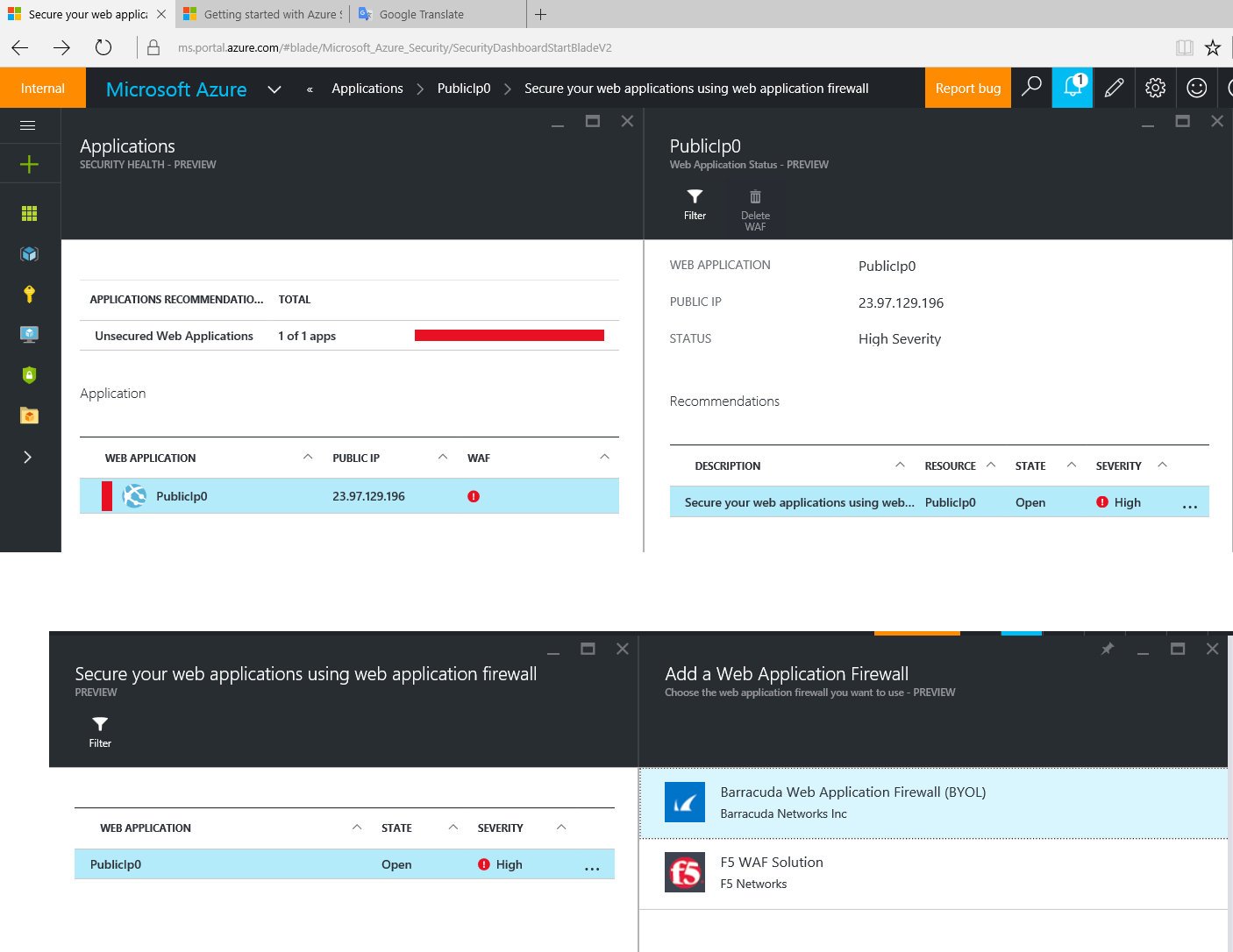
Давайте откроем Blade с Security Center и посмотрим, как все плохо.



Я в целом догадывался, что у меня дыра в безопасности (хорошо, что хоть что-то в безопасности), но выглядит как-то совсем печально и надо разбираться.

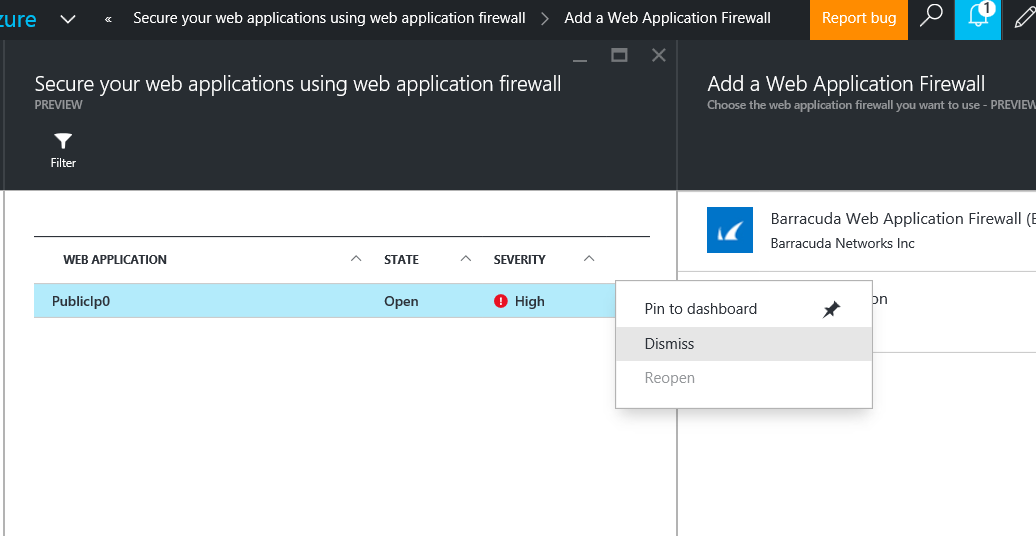
Начнем с вкладки Applications

Я не совсем согласен с картинкой, которую использовала продуктовая команда, но суть понятна- где ваш firewall перед public ip вашего приложения?

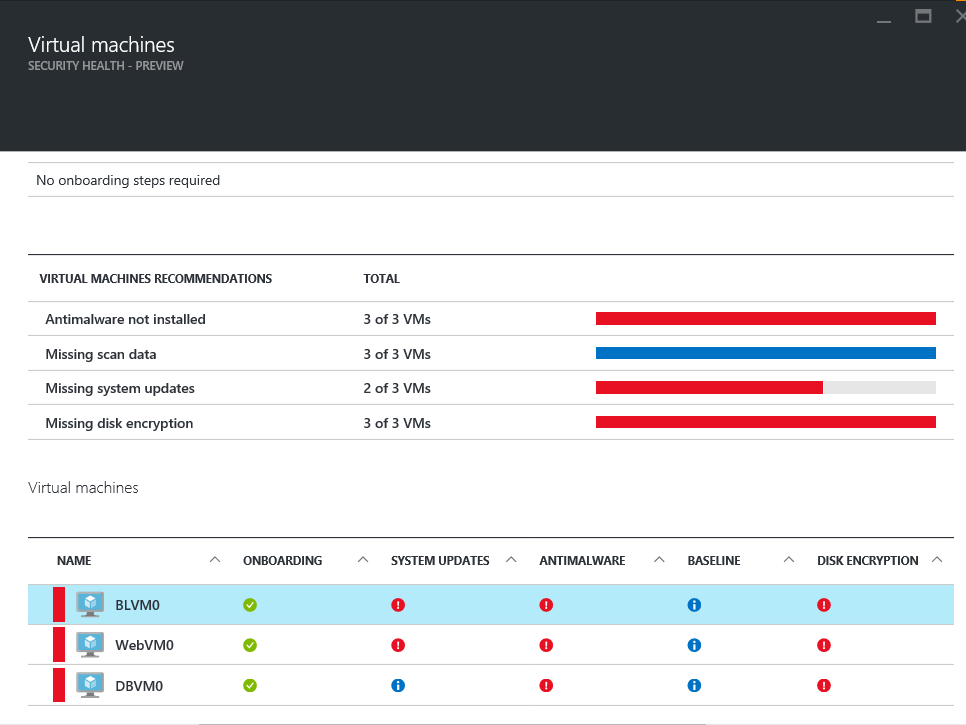


Сразу предлагается фикс- добавить firewall от внешнего вендора (не спешите его добавлять, почитайте про его возможности, про цены, может быть вам этот public ip и не нужен).

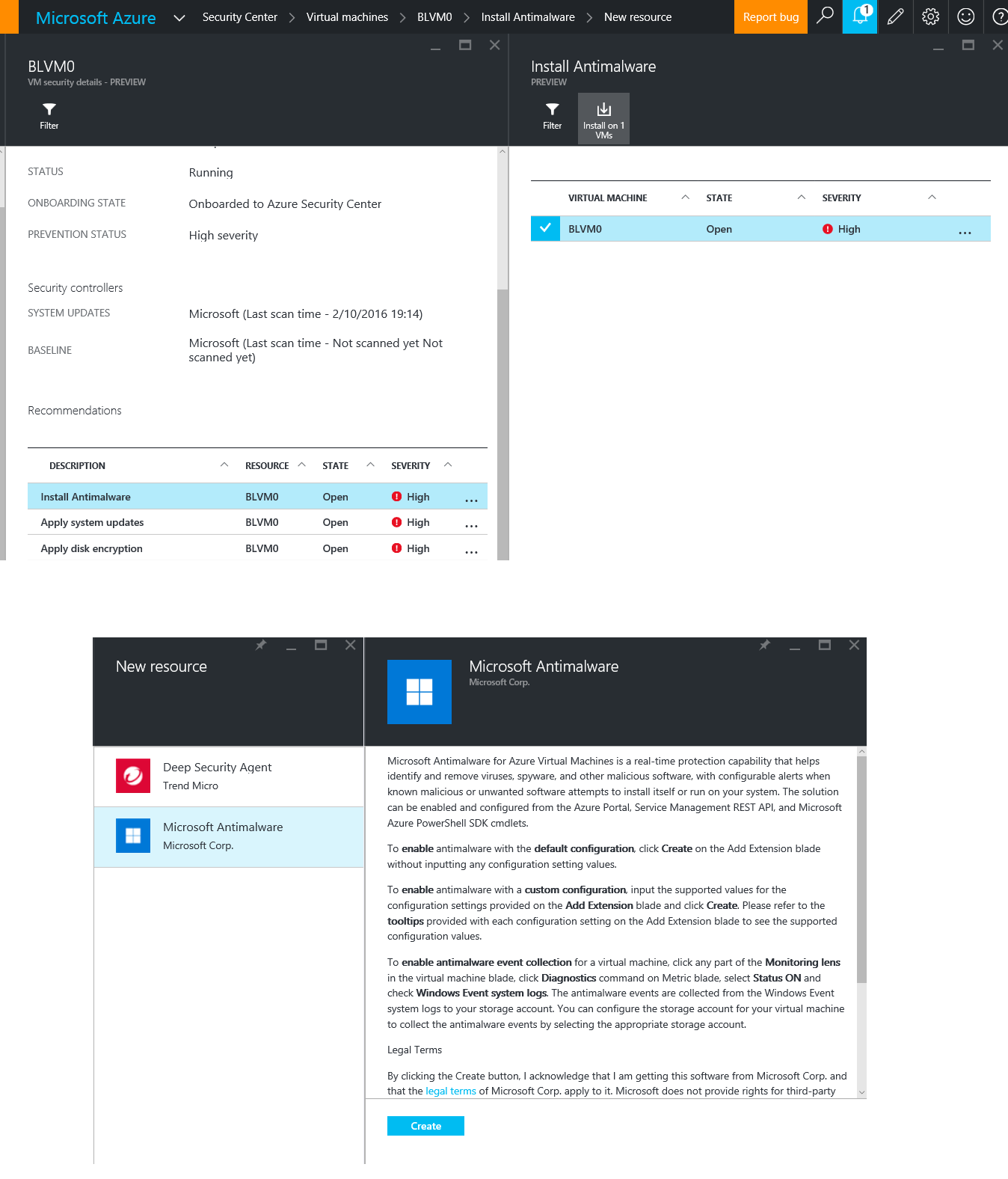
Как и любая другая ошибка, найденная роботом- она должна быть обдумана человеком, и я лично решил проигнорировать ее и чтобы она мне глаза не мозолила сделал dismiss



Давайте посмотрим что там с виртуальными машинами то



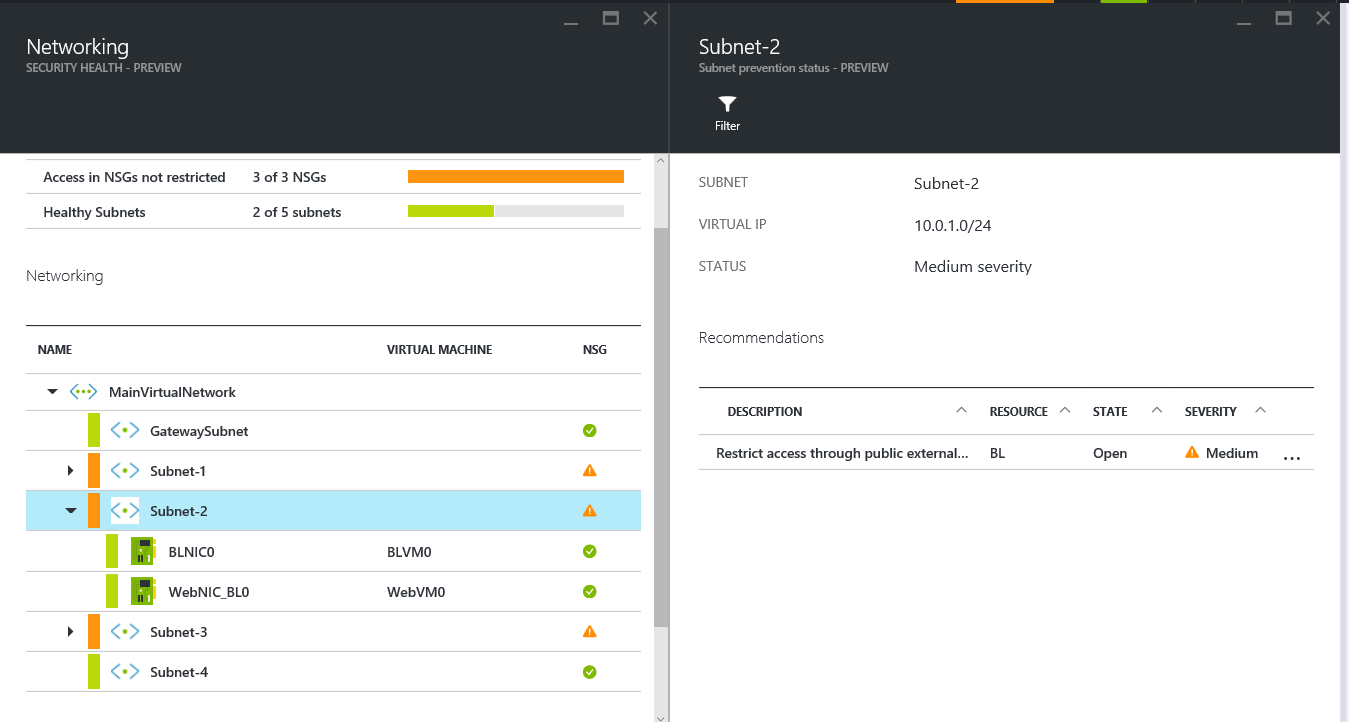
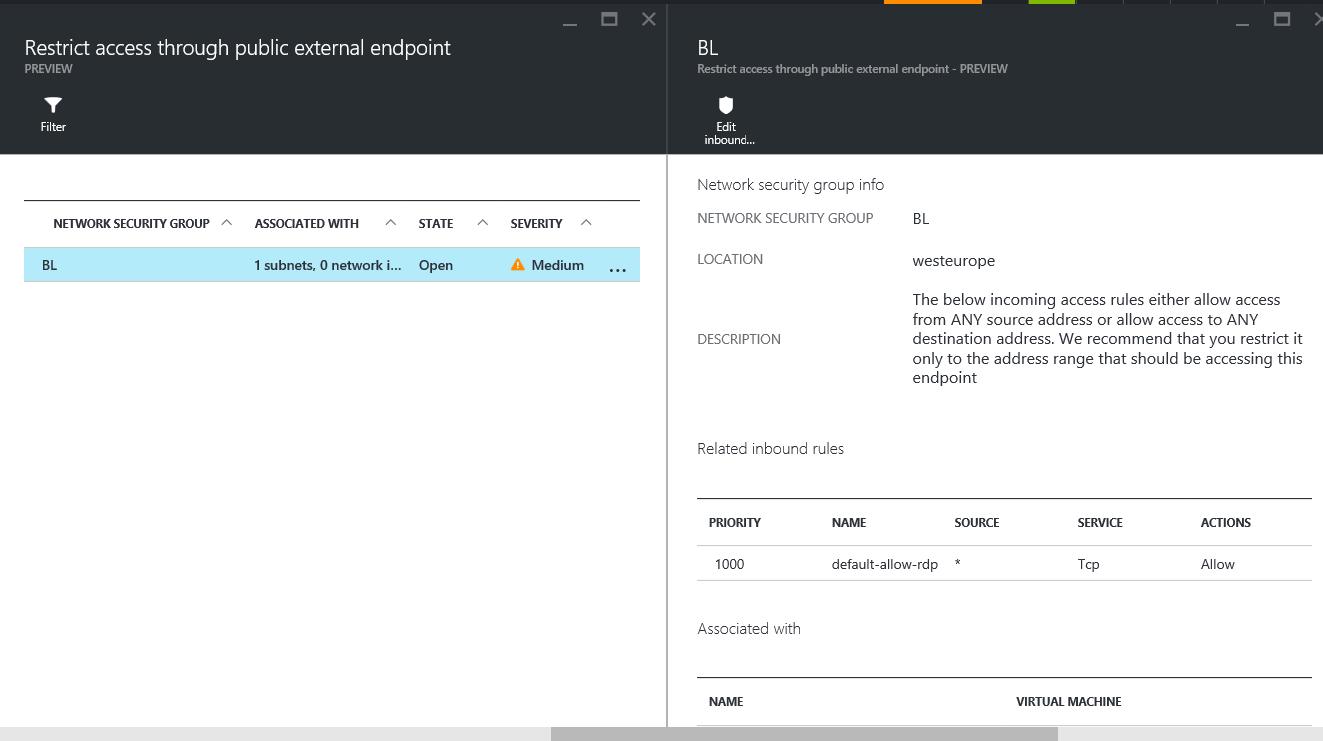
Опять печально, по всем 3 машинам есть потенциальные проблемы: диски не шифрованные(в azure только disk c может быть зашифрован bitlocker-ом), обновлений не хватает, антивируса нет. Для некоторых проблем, можно прям сразу нажать на кнопку решение. На пример установить антивирус в машину.



Жмем кнопку создать и будем считать, что мы стали чуть-чуть безопаснее.

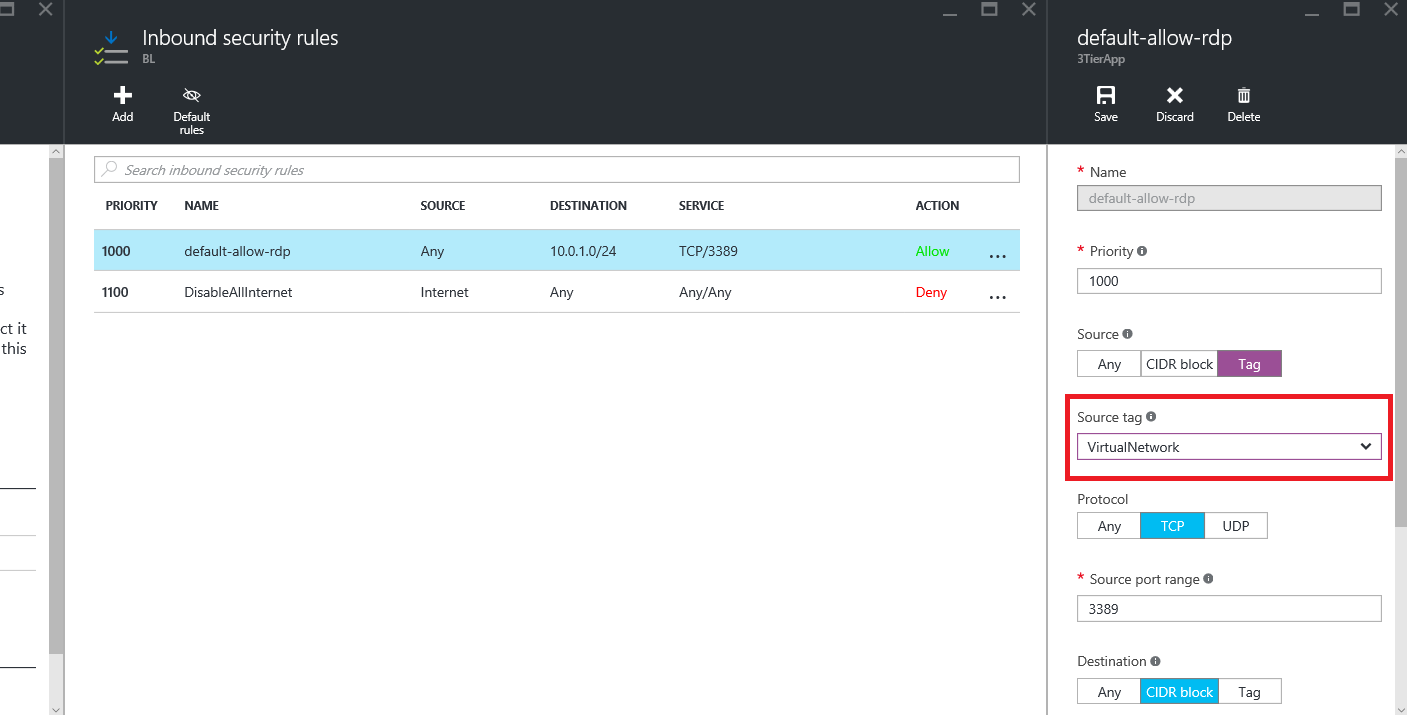
**Ну и самое важное- сеть**

Давайте посмотрим, что-же security center не нравится в конфигурации моих подсетей.



Ну понятно- правила по сути разрешают всем кому не лень отсылать трафик на любой ip в моей подсети и это не как не блокируется. Согласен- проблема и надо правила конфигурировать.

Я решил, что доступ к RDP я разрешу только из моей виртуальной сети.



Не скажу, что я закрыл все дыры, но спасибо что security center указал мне на самые базовые вещи, которые я быстро смог закрыть, чтобы хоть самые очевидные дары в безопасности закрыть.

Что вообще умеет проверять Security Center? Да мы по сути все и разобрали, кроме вещей связанных с sql. Еще SC умеет проверять включено ли шифрование на SQL <https://msdn.microsoft.com/en-us/library/dn948096.aspx> , и включен ли Audit <https://azure.microsoft.com/en-us/documentation/articles/sql-database-auditing-get-started/> на SQL.

Для preview сервиса- по моему не плохо. Есть пожелание что добавить? Вам сюда <https://feedback.azure.com/forums/216840-security-and-compliance>