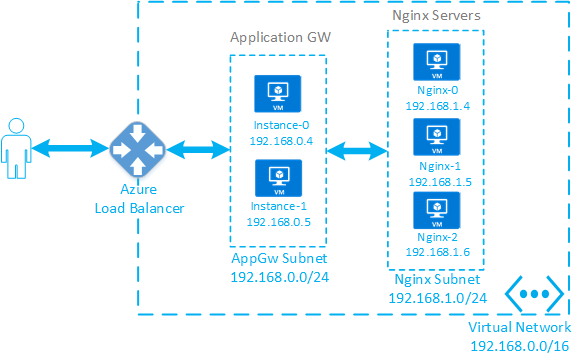
使用应用程序网关的环境下配置NSG的注意事项

**背景介绍**

大家在使用应用程序网关时，出于对安全方面的考虑，经常会进行一些额外的NSG配置来减小系统暴露在互联网上所带来的风险。如果大家对Azure应用程序网关的工作原理不甚了解，在配置NSG的时候经常会导致应用程序网关无法正常访问。本文通过对应用程序网关工作原理的介绍，阐述在使用应用程序网关的环境下配置NSG的注意事项。

**应用程序网关工作原理**

Azure应用程序网关采用的是类似于反向代理服务器的工作方式，客户端直接访问应用程序网关的公网地址而无法感知后端实际的服务器。当应用程序网关接收到客户端的请求之后，它会以自身实例在虚拟网络内部的地址作为源地址对后端池内部的服务器发起新的请求来获取数据，再将获取的数据通过原先跟客户端建立的连接返回给客户端。

如上图所示，我们部署了三台Nginx 服务器在应用程序网关后端。应用程序网关部署在AppGw 子网之内，Nginx服务器部署在Nginx 子网之内。应用程序网关本质上是由多个虚拟机实例组成的群集，默认情况下建立的应用程序网关包含两个实例，每个实例都会占用子网内的一个地址，如上图所示**实例-0**占用地址192.168.0.4，**实例-1**占用地址192.168.0.5。当客户端对应用程序网关发起请求时，Azure前端的负载均衡器会将请求发送到对应的应用程序网关实例，应用程序网关上面的服务会以实例本身的内网地址向后端服务器发起新的请求。比如客户端的请求被发送到**实例-0**，该实例会以192.168.0.4作为源地址对后端服务器发起请求。

如果客户端所用的公网IP地址为1.2.3.4， 应用程序网关开放的是公网80端口，应用程序网关与后端服务器也使用80端口进行通信，则在每个物理点的实际网络数据应该类似于下表所示。

|  |  |  |
| --- | --- | --- |
| **物理点** | **通讯包** | **说明** |
| 客户端 | [1.2.3.4]:random <->[AppGW VIP]:80 | 客户端只有跟应用程序网关公网IP之间的通讯包。 |
| 应用程序网关实例 | [1.2.3.4]:random <->[192.168.0.4|192.168.0.5]:80 | 由于Azure层面的NAT，客户端发包的目的地址被转化成应用程序网关的实例地址。 |
| [192.168.0.4|192.168.0.5]:random <-> [192.168.1.4|192.168.1.5|192.168.1.6]:80 | 应用程序网关发起新的TCP连接向后端服务器发起数据请求。这里的发包也包括应用程序网关发出的健康探测包。 |
| 后端服务器 | [192.168.0.4|192.168.0.5]:random <-> [192.168.1.4|192.168.1.5|192.168.1.6]:80 | 后端服务器对应用程序网关的请求进行回复。 |

**配置NSG时的注意事项**

一般来说，在使用应用程序网关的环境下配置NSG有以下几个注意事项。

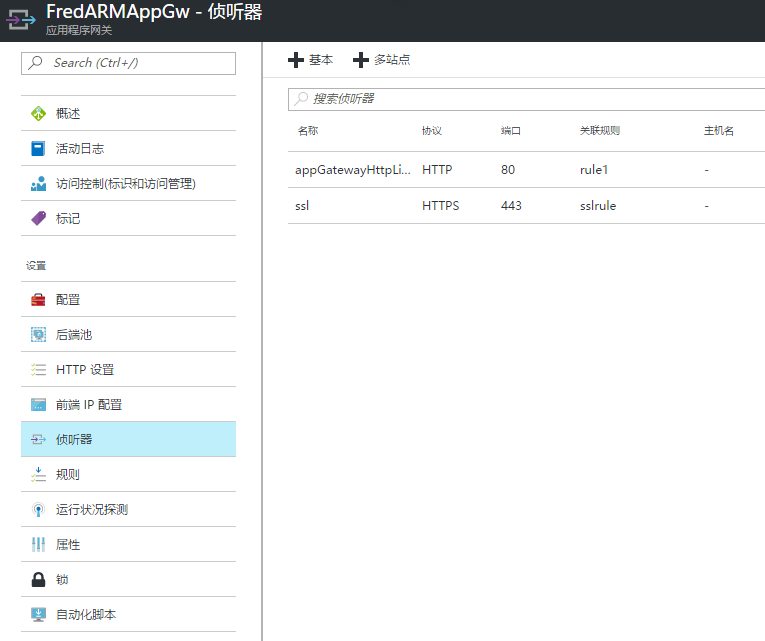
1. 应用程序网关实例所在的子网NSG需要允许互联网对前端服务端口的访问。
2. 应用程序网关实例所在的子网需要能够与后端服务器所在的子网进行通讯。
3. 后端服务器网卡绑定的NSG需要允许应用程序网关实例所在的子网对后端服务端口的访问。

下面对这几个注意事项进行详细的描述。

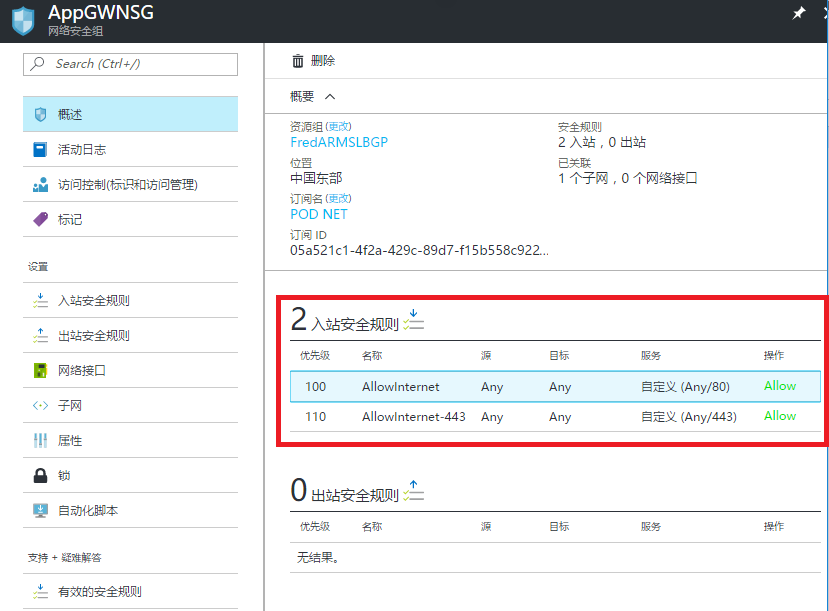
**1）应用程序网关实例所在的子网需要允许互联网对前端服务端口的访问**

在使用应用程序网关的环境下，应用程序网关实例会接收所有公网访问的流量，所以必须对应用程序网关实例所在的子网放行互联网对前端服务端口的访问。

比如我们配置应用程序网关启用了80和443端口的侦听器如下所示。



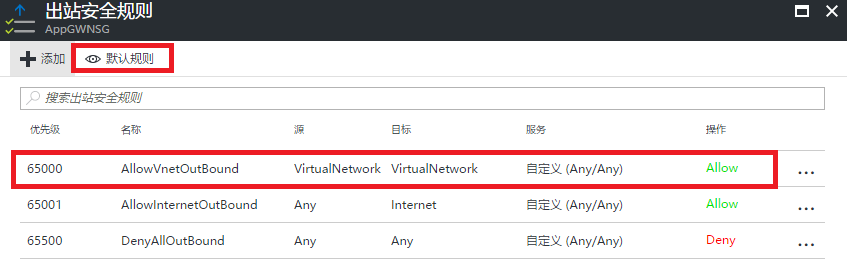
当应用程序网关实例所在的子网启用了NSG时，如下图所示，我们至少需要在入站规则里面开放公网对80端口以及443端口的允许访问规则。



NSG规则里面的目标地址必须选为Any而不要设定为某些固定的内网IP地址，这主要是因为应用程序网关实例所占用的内网地址是动态分配的，而且如果修改了应用程序网关的实例个数也会导致应用程序网关占用更多的子网里面的IP地址，这样就会导致规则无法应用到所有的应用程序网关实例。

**2）应用程序网关实例所在的子网需要能够与后端服务器所在的子网进行通讯**

对于绑定到虚拟网络子网的NSG来说，其在创建的时候会添加如下图所示的默认规则来允许虚拟网络内部的通信（查看时需要点击“默认规则”按钮）。如果没有配置新的规则来覆盖这个优先级为65000的规则时，一般不会出现问题。

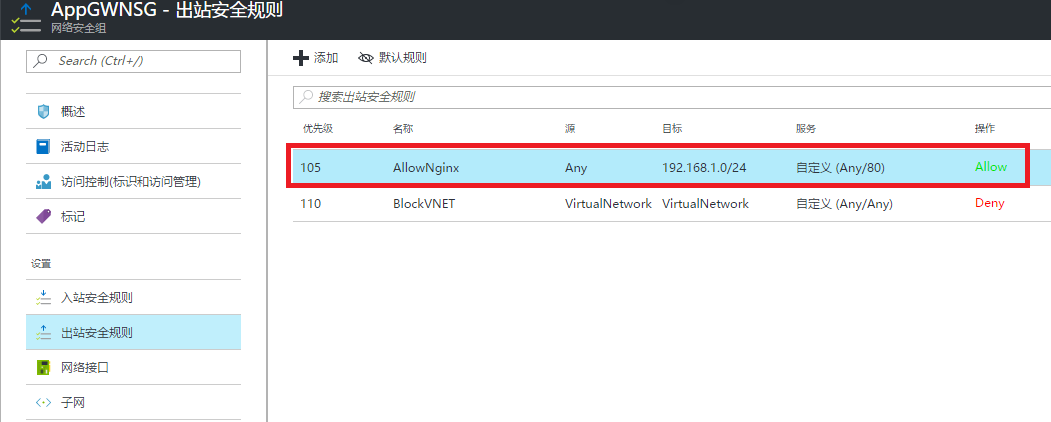
****

但当我们在虚拟网络的子网之间配置了NSG策略来进行访问控制时，我们至少要保证下面两点：

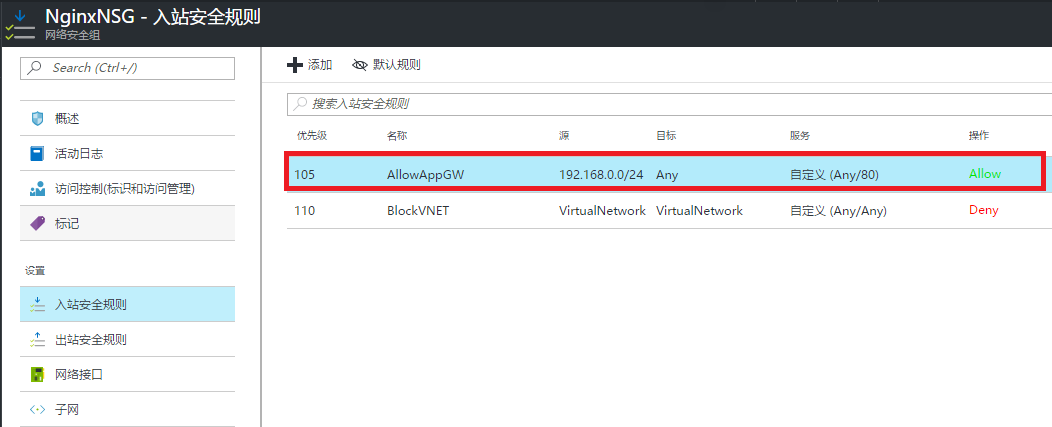
1. 应用程序网关实例所在的子网NSG的出站安全规则放行对后端服务器服务端口的访问
2. 后端服务器所在的子网NSG的入站安全规则放行应用程序网关实例所在的子网的访问请求。

比如在上面提到的测试环境中，我这边将名为AppGWNSG的NSG绑定到应用程序网关实例所在的子网，并将名为NginxNSG的NSG绑定到后端服务器所在的子网。

对于AppGWNSG，入站和出站规则我这边都添加了一条优先等级为110的Deny规则来禁止虚拟网络之间的通信，用此来模拟用户场景中可能出现的虚拟网络内部的流量控制策略。我们至少要在AppGWNSG的出站安全规则中添加更高优先级的规则来放行应用程序网关到后端服务器服务端口的访问。比如我这边建立优先级为105的名为AllowNginx的规则，允许访问Nginx Subnet 192.168.1.0/24网段的80端口。如果后端服务器不是监听在80端口，需要更改为对应端口或者配置为Any(\*)。

****

同样的对于NginxNSG，在入站和出站规则我这边都添加了一条优先等级为110的Deny规则来禁止虚拟网络之间的通信，用此来模拟用户场景中可能出现的虚拟网络内部的流量控制策略。我们同样也需要在入站安全规则里面添加更高优先级的规则来放行应用程序网关到后端服务器的访问。比如我这边建立优先级为105的名为AllowAppGW的规则，允许来自于AppGW subnet 192.168.0.0/24网段 访问80端口的流量。同样的，如果后端服务器不是监听在80端口，也需要更改为对应端口或者配置为Any(\*)。

****

**3）后端服务器网卡绑定的NSG需要允许应用程序网关实例所在的子网对后端服务端口的访问**

如果后端服务器的网卡绑定了NSG，我们也需要在NSG中配置访问策略来允许应用程序网关的访问。从前面的分析中我们知道应用程序网关会以实例的内网地址向后端服务器进行访问请求以及健康探测，所以我们只需要在入站规则中放行应用程序网关实例所在的子网对服务器服务端口的访问就行，而不需要开放公网对服务端口的访问。

如下图所示，我这边将名为VM\_NSG的NSG绑定到后端服务器，我们只需要在入站安全规则里面添加允许源为AppGW subnet192.168.0.0/24网段的访问即可。可以看到NSG默认会阻止来自于Internet的访问，在这种配置下应用程序网关仍然能够正常工作。

