Incorrect NSG Config_RDP SSH

Last updated by | Heath Rensink | Mar 2, 2023 at 9:11 AM PST

Tags

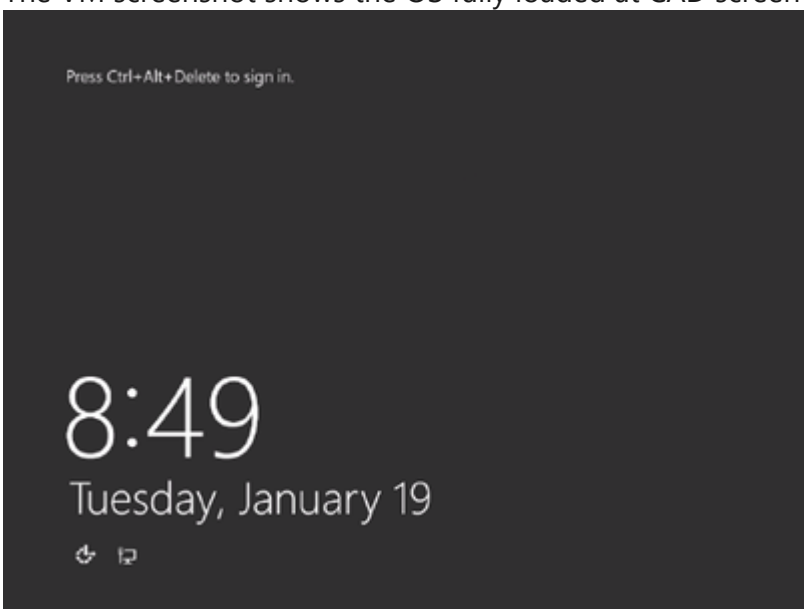
cw.TSG	cw.RDP-SSH

Contents

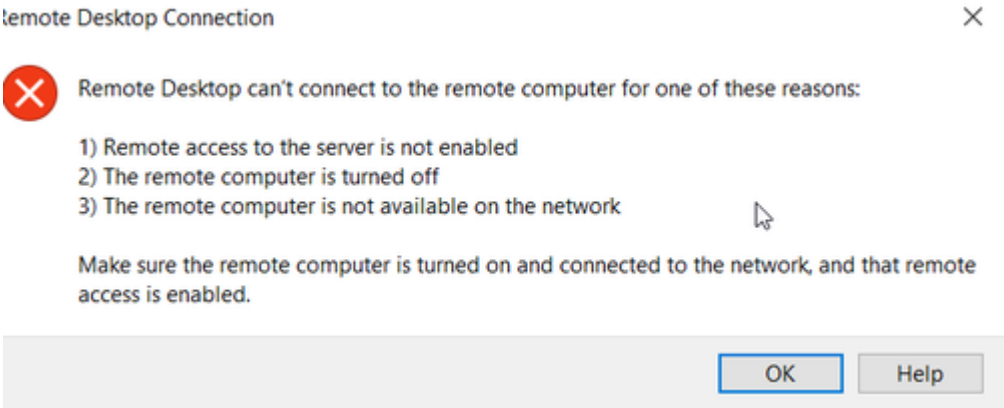
Symptoms

Symptom 1

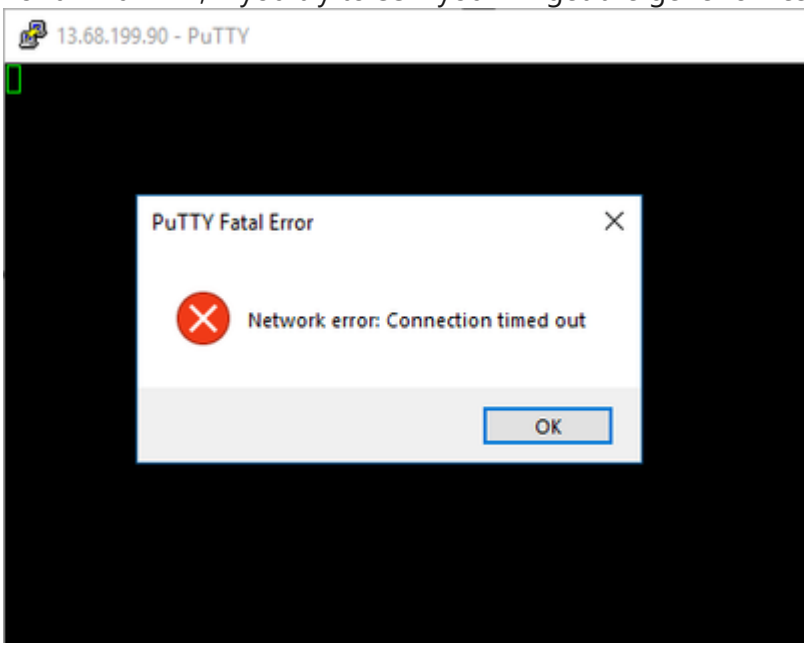
1. The VM screenshot shows the OS fully loaded at CAD screen (Ctrl+Alt+Del)



2. When you try to RDP you get the generic error that the VM is unreachable



3. For a Linux VM, if you try to SSH you will get the generic message that the connection is timing out:



4. There's no connectivity to the virtual machine on its VIP or DIP, verified with [VM Port Scanner](#).

5. If you try to RDP/SSH from the jumpbox, either RDP or PUTTY responds just fine and is awaiting for credentials

6. You can verify this in ASC where the Stateful Test will fail and specifically call out NSG security rule(s):

```
Traffic Test
================================================
Traffic Direction:      InternetIn              [used to simulate inbound traffic coming from internet]
Source IP:              8.8.8.8                 [you can enter your home IP address here, the same you might e
Source Port             3389                    [doesn't matter]
Destination IP          10.0.0.4 (NIC:default)  [The IP of the VM in this scenario]
Destination Port        3389                    [RDP]
Transport Protocol      TCP                     [or UDP]

Traffic Test Results
================================================
Overall Result                  ❌ Traffic BLOCKED
Overall Customer RCA            Access Control BLOCKS this INBOUND traffic by default security rule: DenyAllIn
Overall Customer Mitigation     If the access control (security rules) result is not desired, view the Effecti

Stateful Test (NSG Layer)
Test Result                     ❌ Traffic BLOCKED.
Customer RCA                    Access Control BLOCKS this INBOUND traffic by default security rule: DenyAllIn
Customer Mitigation             If the access control (security rules) result is not desired, view the Effecti
Rule Name                       DefaultRule_DenyAllInBound
Rule Priority                   65500
Rule Type                       block
Condition Source Ports          0-65535
Condition Destination Ports     0-65535
Condition Source IP             0.0.0.0/0,0.0.0.0/0

Stateless Test (Routing Layer)
Test Result                     ✅ Traffic: ALLOWED.
Customer RCA                    Routing ALLOWS this INBOUND traffic at the routing layer using a default rule.
Customer Mitigation             If the routing result is not desired, view the Effective Route Table to determ
Rule Name                       VNET_VFP_RULE_IPV4_IN_MAC_REWRITE
Rule Priority                   1200
Rule Type                       mapmacin
```

Symptom 2

1. The cx is an internal MSFT employee (as in their email ends with `@microsoft.com`).
2. If they use the `Network security group test` blade from the Portal to test RDP connectivity through the NSG, it will show a security rule called `BlockHighRiskTCPPortsFromInternet` is blocking 3389. This rule is not visible in any accessible NSG.
3. Similarly, you can verify this in ASC where the Stateful Test will fail and specifically call out the `Azure Virtual Network Manager (Microsoft.Network/NetworkManagers)` rule(s):

```
Traffic Test
================================================
Traffic Direction:      InternetIn              [used to simulate inbound traffic coming from internet]
Source IP:              8.8.8.8                 [you can enter your home IP address here, the same you might e
Source Port             3389                    [doesn't matter]
Destination IP          10.0.0.4 (NIC:default)  [The IP of the VM in this scenario]
Destination Port        3389                    [RDP]
Transport Protocol      TCP                     [or UDP]

Traffic Test Results
================================================
Overall Result                  ❌ Traffic BLOCKED
Overall Customer RCA            Access Control BLOCKS this INBOUND traffic using an Azure Virtual Network Mana
Overall Customer Mitigation     If this is not desired, please contact your Azure network administrator who ma

Stateful Test (NSG Layer)
Test Result                     ❌ Traffic BLOCKED.
Customer RCA                    Access Control BLOCKS this INBOUND traffic using an Azure Virtual Network Mana
Customer Mitigation             If this is not desired, please contact your Azure network administrator who ma
Rule Name                       BlockHighRiskTCPPortsFromInternet_8e593d16-5f9d-4b25-b3b2-df7b6951a08b
Rule Priority                   98
Rule Type                       block
Condition Source Ports          1-65535
Condition Destination Ports     20-20,21-21,22-22,23-23,111-111,119-119,135-135,137-137,138-138,139-139,161-16


Stateless Test (Routing Layer)
Test Result                     ✅ Traffic: ALLOWED.
Customer RCA                    Routing ALLOWS this INBOUND traffic at the routing layer using a default rule.
Customer Mitigation             If the routing result is not desired, view the Effective Route Table to determ
Rule Name                       VNET_VFP_RULE_IPV4_IN_MAC_REWRITE
Rule Priority                   1200
Rule Type                       mapmacin
```

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link or url to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.

  Deploy to Azure

Root Cause Analysis

Root Cause Analysis 1

Symptom 1 only

The Network Security Group rules are not properly set and thus the NSG is not allowing the RDP/SSH traffic.

Root Cause Analysis 2

Symptom 1 only

Customer could also have enabled Just-in-time (JIT) access to lock down inbound traffic to the Azure VM.

Root Cause Analysis 3

Symptom 2 only

For a lot of MSFT internal cx this access is blocked by default using the policy created by Azure Network Manager: https://msazure.visualstudio.com/AzureWiki/_wiki/wikis/AzureWiki.wiki/86366/Simply-Secure-V2-Network-Security-Rules.

References

- Network security groups
- How to manage NSGs using the Azure portal
- IP address types and allocation methods in Azure
- https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time
- Troubleshooting connectivity problems between Azure VMs

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Networks*	*Routing Azure Virtual Network V3\Connectivity\Cannot connect to virtual machine using RDP or SSH*	*Root Cause - Windows Azure\Virtual Network\NSG\Configuration\Customer misconfiguration*	

To know how to flag a bug on a case please refer to How to do Proper Case Coding

Customer Enablement

- Cannot RDP to a VM because RDP port is not enabled in NSG

Mitigation

Mitigation 1

Bear in mind of the following scenarios:

- Currently the portal experience to deploy a VM, by default is prepopulating to not open any port on the VM
    1. When you create a new virtual machine you will have a set of default NSGs that are automatically applied. However, any customization performed by the cx could be locking them out of the VM:

Network security group [redacted] attached to network interface [redacted]
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
300	RDP	3389	TCP	Any	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

2. You could easily be in this scenario if the customer didn't open the inbound port rule when the Vm was created. By default, *None* is selected in the portal:

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports ⓘ ◉ None ○ Allow selected ports

Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

3. However, sometimes you will run into issues if the customer customized these rules incorrectly. This usually happens when the customer wrongly setup the source port to 3389:

Add inbound security rule

Basic

* Source ⓘ
Any

* Source port ranges ⓘ
3389

* Destination ⓘ
Any

* Destination port ranges ⓘ
3389

* Protocol
Any | TCP | UDP

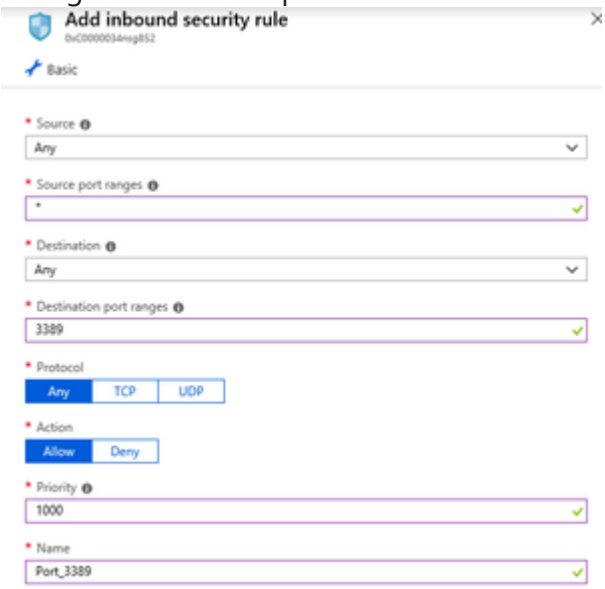
* Action
Allow | Deny

* Priority ⓘ
310

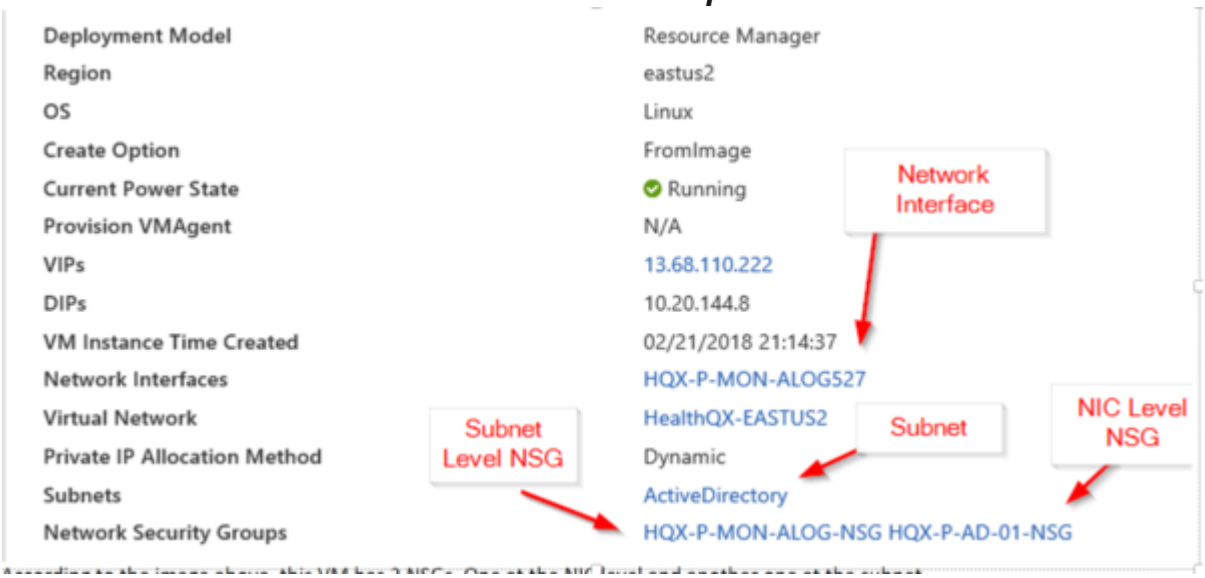
* Name
Port_3389

4. This configuration will not work as it will force the computer that is initiating the session to use 3389 as its source port and it is very unlikely that could happen unless any onprem device is forcing all of their outbound connections to use port 3389. In order to access the virtual machine, you want to

configure the source port as *.



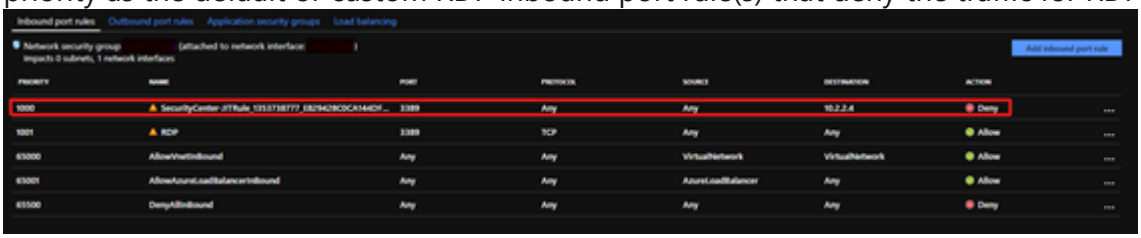
5. If the customer sets up an IP range on the NSG it could inadvertently block the access the same way the source IP could be blocking your access. This IP range could be internal or public for the source IP. If the customer setup a range on the source IP, anything outside that IP range will not be able to access.
6. Furthermore, if that is not your case, then check if the customer has setup an NSG on the VNET level on that specific subnet because if there's any Deny rule in there, will overwrite the ones on the VM level.
   - To identify if the customer has a NIC Level NSG and a Subnet Level NSG please refer to the below sample. Based on this image, this VM has 2 NSGs. One at the NIC level and another one at the subnet level. ***The rules at the subnet level will take precedence over*** the NIC Level NSG.



   - Additionally, a rule should be setup on both NSGs (e.g. there should be a rule on each NSG to allow 3389/22 connectivity).
7. Another option that you could have here will depend on which IP allocation model the customer is selecting for the Public IP, this could be either allowing or denying all inbound traffic. Refer to [Compare Public IP Base and Standard tiers]

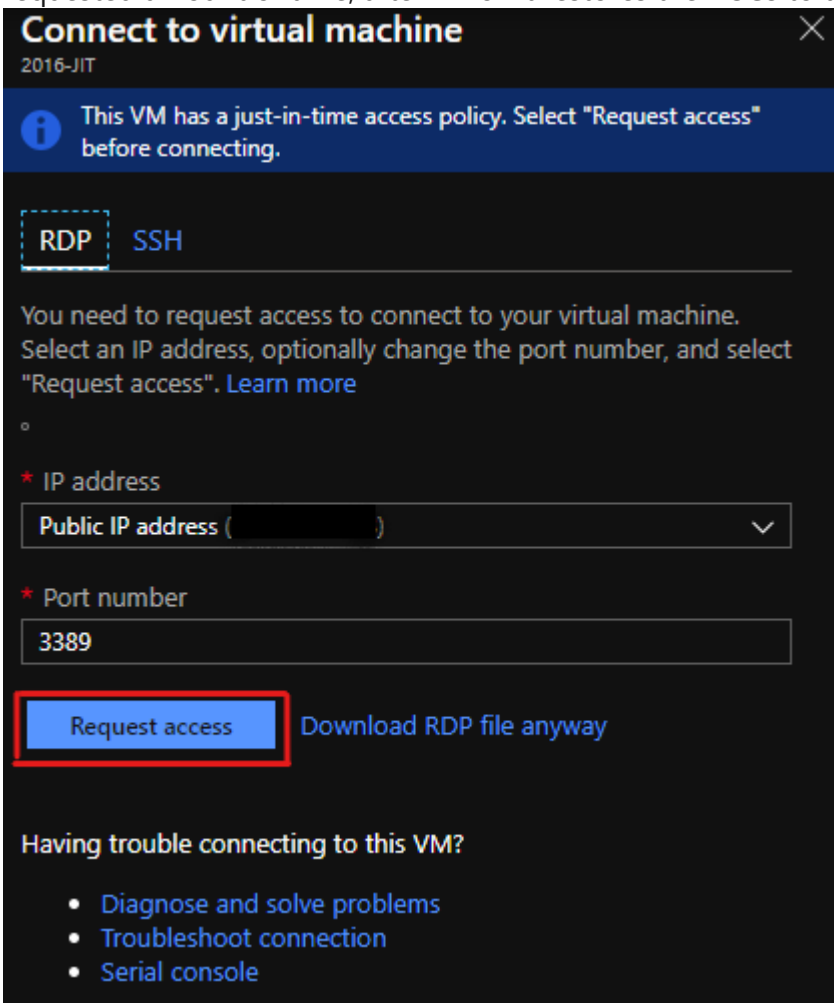
Mitigation 2

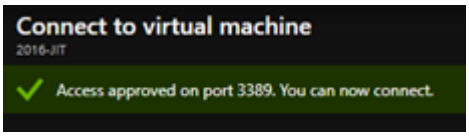
- If Just-in-time (JIT) access is enabled, the cx will find an inbound rule on the NIC view with a lower number priority as the default or custom RDP inbound port rule(s) that deny the traffic for RDP.



From Azure Support Center:

Security Center will decide whether to grant access upon user request based on Azure RBAC. If a request is approved, Security Center automatically configures the NSGs to allow inbound traffic to these ports for the requested amount of time, after which it restores the NSGs to their previous states.





Mitigation 3

Symptom 2 only

Here's the doc on how insecure ports are blocked by policy for our org (CSS): https://dev.azure.com/CSSAzSubGovernance/Public/_wiki/wikis/Public.wiki/58/Network-Security-Groups-(NSGs)-v2

As noted, the mitigation is to use JIT for 3389/22 access, or to scope the NSG rule solely to your IP address.

If the cx's situation is managed by Azure Network Manager, this can't be mitigated at the CSS level. The Azure Network Manager policy is executed above the NSG level. There's a process for internal MSFT employees to apply for a security exception here: https://msazure.visualstudio.com/AzureWiki/_wiki/wikis/AzureWiki.wiki/85823/Azure-Network-Manager-Simply-Secure-Network-Security-Rules-v2

You can see the above in AzNet's TSG on this: https://supportability.visualstudio.com/AzureNetworking/_wiki/wikis/Wiki/542465/Azure-Network-Manager

Need additional help or have feedback?

To engage the Azure RDP-SSH SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **RDP-SSH SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **RDP-SSH Feedback** form to submit detailed feedback on improvements or new content ideas for RDP-SSH. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **RDP-SSH Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!