[SSIS IR] Regarding concerns of allowing outbound port 80 for Azure-SSIS IR joining VNet

Last updated by | Jackie Huang | Jan 4, 2022 at 12:24 AM PST

Background

When client is dealing with signed certificate, it will need to download Certificate Revocation List (CRL) to verify whether the cert is revoked or not.

https://social.technet.microsoft.com/wiki/contents/articles/2303.understanding-access-to-microsoft-certificate-revocation-list.aspx

So we ask customer to allow outbound port 80 when join IR into VNet, as usually client will download CRL from below site:

- crl.microsoft.com:80
- mscrl.microsoft.com:80
- crl3.digicert.com:80
- crl4.digicert.com:80
- ocsp.digicert.com:80
- cacerts.digicert.com:80

Since Network Security Group not support tag to include whatever FQDN, so now we document that customer need to open outbound port 80 to INTERNET web site which customer might have concern.

Solution

We can suggest customer to redirect outbound traffic to NVA or Azure Firewall after IR join Vnet.

See [SSIS IR] Support Traffic Routing to Virtual Network Appliance for IR join VNet for details.

Then they can whitelist below FQDN for port 80

- crl.microsoft.com:80
- mscrl.microsoft.com:80
- crl3.digicert.com:80
- crl4.digicert.com:80
- ocsp.digicert.com:80
- cacerts.digicert.com:80

The downside of this solution right now is

- Customer need to monthly check IP list under BatchNodeManagement service tag in case any new IP need to be updated into UDR.

> It will be improved after Network team support service tag in UDR, ETA is not determined right now

- Customer need to afford COGS of NVA or Azure Firewall. If customer already has it or plan to use NVA\AzureFirewall to do auditing for all outbound traffic, it won't be any problem

How good have you found this content?