

## DELTA SUMMARY

This document is a condensed description of the changes in **McAfee Web Gateway** Version **8.0** compared to McAfee Web Gateway Version 7.8.2.

Planned RTW: October 9<sup>th</sup>, 2018

This release has the following updates:

| Change                                                 | Impact Level |
|--------------------------------------------------------|--------------|
| 1) <u>McAfee Web Gateway support on Azure platform</u> | NEW          |
| 2) <u>HLS Stream Detection</u>                         | NEW          |
| 3) <u>RTF Opener</u>                                   | NEW          |
| 4) <u>EML Opener</u>                                   | NEW          |
| 5) <u>Support for Private GTI cloud</u>                | NEW          |
| 6) <u>DNSFastFallBack</u>                              | UPDATED      |



## McAfee Web Gateway support on Azure platform

### Value

With the introduction of this feature, customers will be able to bring up McAfee Web Gateway (MWG) over a Hyper-V installed on a Microsoft Windows 2016 Azure Virtual Machine.

### Overview

This document describes how to get McAfee Web Gateway up and running on Microsoft Azure.

### Important Concepts

Below is the detailed description of the steps needed to successfully install McAfee Web Gateway:

- Bringing up a Windows 2016 Server on Azure
- Installing Hyper-V on the Windows 2016 Server
- Setting up a Network Address Translation (NAT) for getting internet access in MWG
- Installing MWG on Hyper-V
- Enabling access to MWG

### Minimum Requirements

- Windows 2016 Server

Any Azure Virtual Machine higher than 'D3\_v3' or 'E3\_v3' configuration from the marketplace which supports nested virtualization to run Hyper-V. The below mentioned minimum requirements for MWG sizing are to be noted while selecting Windows 2016 Server.

- 'McAfee Web Gateway' Virtual Machine Sizing Chart:

| Use                                                                      | Memory<br>(RAM in GB) | Hard disk<br>space (in<br>GB) | CPU<br>cores |
|--------------------------------------------------------------------------|-----------------------|-------------------------------|--------------|
| Functional testing (one user) or Central Management console (no traffic) | 4                     | 80                            | 2            |
| Production (minimum)                                                     | 16                    | 200                           | 4            |
| Production (recommended)                                                 | 32                    | 500                           | at least 4   |

### Using this Feature

Details of the above steps are mentioned here:

- 1) Bringing up a Windows 2016 Server on Azure
  - a. Login to **Azure Portal** (portal.azure.com) with correct account information.
  - b. Go to **Create a Resource** and search for **Windows Server 2016 Virtual Machine** in the marketplace.
  - c. Select **Windows Server 2016 Datacenter** from the list.
  - d. Select deployment model as **Resource Manager** and hit **Create**
  - e. Refer to the below image for filling up the details and click OK.

Home > New > Create virtual machine > Basics

## Create virtual machine

**1** Basics  
Configure basic settings

**2** Size  
Choose virtual machine size

**3** Settings  
Configure optional features

**4** Summary  
Windows Server 2016 Datacent...

### Basics

\* Name  
Win2k16forMWG ✓

VM disk type ⓘ  
Premium SSD ▼

\* Username  
mwguser ✓

\* Password  
..... ✓

\* Confirm password  
..... ✓

Subscription  
CorpProducts Engineering - McAfee V ▼

\* Resource group ⓘ  
☒ Create new ☐ Use existing  
Win2k16forMWG ✓

\* Location  
South India ▼

OK

- f. In the section: **2. Choose Virtual Machine Size**, search for **v3**, as these machines will support nested virtualization. Select any system higher than 'D3\_v3' or 'E3\_v3' or other higher configurations supporting nested virtualization.

Home > New > Create virtual machine > Choose a size

### Create virtual machine

- 1 Basics  
Done
- 2 Size  
Choose virtual machine size
- 3 Settings  
Configure optional features
- 4 Summary  
Windows Server 2016 Datacent...

### Choose a size

Browse the available sizes and their features

Search: v3
Compute type: Current generation
Disk type: All disk types

| RECOMMENDED | SKU       | TYPE     | COMPUTE...     | VCPUS | GB RAM | DATA DIS... | MAX IOPS | LOCAL SSD |
|-------------|-----------|----------|----------------|-------|--------|-------------|----------|-----------|
| ★           | E2s_v3    | Standard | Memory optimi  | 2     | 16     | 4           | 3200     | 32 GB     |
|             | E4s_v3    | Standard | Memory optimi  | 4     | 32     | 8           | 6400     | 64 GB     |
|             | E4-2s_v3  | Standard | Memory optimi  | 2     | 32     | 8           | 6400     | 64 GB     |
|             | E8-4s_v3  | Standard | Memory optimi  | 4     | 64     | 16          | 12800    | 128 GB    |
|             | E8-2s_v3  | Standard | Memory optimi  | 2     | 64     | 16          | 12800    | 128 GB    |
|             | E16-4s_v3 | Standard | Memory optimi  | 4     | 128    | 32          | 25600    | 256 GB    |
|             | D2_v3     | Standard | General purpos | 2     | 8      | 4           | 4x500    | 50 GB     |
|             | D4_v3     | Standard | General purpos | 4     | 16     | 8           | 8x500    | 100 GB    |
|             | E2_v3     | Standard | Memory optimi  | 2     | 16     | 4           | 4x500    | 50 GB     |
|             | E4_v3     | Standard | Memory optimi  | 4     | 32     | 8           | 8x500    | 100 GB    |

Select

g. In the section: **3. Configure Optional features**, Select the public inbound ports as needed. Preferably, SSH and RDP:

Home > New > Create virtual machine > Settings

### Create virtual machine

- 1 Basics  
Done
- 2 Size  
Done
- 3 Settings  
Configure optional features
- 4 Summary  
Windows Server 2016 Datacent...

### Settings

(new) Win2k16forMWG-vnet

\* Subnet (10.0.1.0/24)

\* Public IP address (new) Win2k16forMWG-ip

Network Security Group

Basic Advanced

\* Select public inbound ports

2 selected

- ☐ No public inbound ports
- ☐ HTTP
- ☐ HTTPS
- ☒ SSH (22)
- ☒ RDP (3389)

Accelerated networking

Disabled Enabled

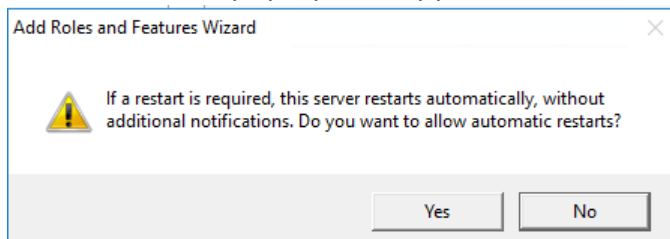
OK

h. Click on **OK**. Verify the summary on the next page and finally click on **Create** to initiate the deployment of the server.

- i. Once deployed, go to **All resources** (on the left pane), and click on the Virtual Machine that you have created (search the name if you have more resources).
- j. Note down the Public IP. Now connect to this Virtual Machine using RDP using the username and password added in step e.

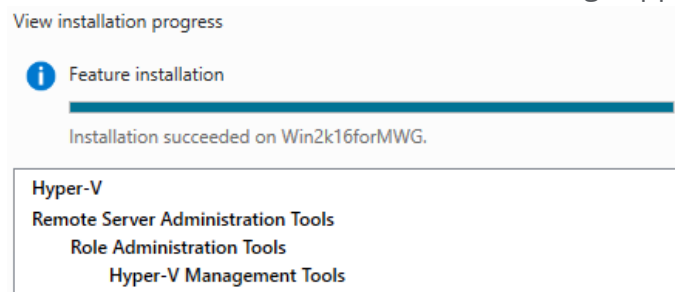
## 2) Installing Hyper-V on the Windows 2016 Server

- a. Login to the Windows 2016 Server created on Azure using RDP.
- b. Click on Start button, and open **Server Manager** from the menu.
- c. Click on **Manage** on the top-right corner and select **Add Roles and Features** from the sub-menu.
- d. During **Installation Type** section, Select **Role-based or feature-based installation** and **Select a server from the server pool** in the next section.
- e. In the **Server Roles** section, tick **Hyper-V**, a pop-up appears showing feature that are required for Hyper-V, tick **Include management tools (if applicable)** in the pop-up window and click on **Add Features**.
- f. Click Next until the **Virtual Switches** section, tick the Ethernet interface with the name **Microsoft Hyper-V Network Adapter**, and click **Next** till **Confirmation** section.
- g. On the **Confirmation** section, tick on **Restart the destination server automatically if required**.
- h. Click **Yes** on the pop-up that appears and click **Install**.



NOTE: Once installation is complete, you will lose access to RDP until restart completes!

- i. Again, login onto the server using RDP after the restart procedure is complete. The installation will continue and below message appears to mark installation done:

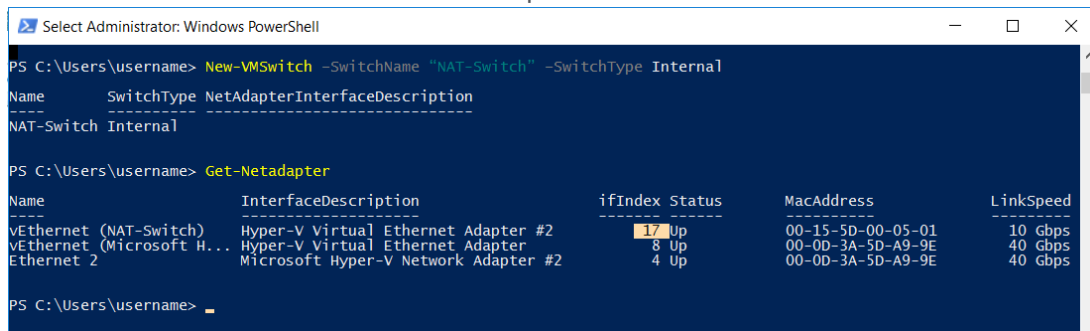


### 3) Setting up a Network Address Translation (NAT) for enabling internet connectivity in MWG

- a. Open **Powershell** in **Administrator** mode on Windows 2016 Server.
- b. Type in the following command to create an **Internal vSwitch** which will be configured as a **NAT Gateway** for MWG:

```
New-VMSwitch -SwitchName "NAT-Switch" -SwitchType Internal
```

- c. Type in the command **Get-NetAdapter** and note down the **ifIndex** (interface index) of the vSwitch that was created in the previous command.



```
PS C:\Users\username> New-VMSwitch -SwitchName "NAT-Switch" -SwitchType Internal
```

| Name       | SwitchType | NetAdapterInterfaceDescription |
|------------|------------|--------------------------------|
| NAT-Switch | Internal   |                                |

```
PS C:\Users\username> Get-NetAdapter
```

| Name                       | InterfaceDescription                 | ifIndex | Status | MacAddress        | LinkSpeed |
|----------------------------|--------------------------------------|---------|--------|-------------------|-----------|
| vEthernet (NAT-Switch)     | Hyper-V Virtual Ethernet Adapter #2  | 17      | Up     | 00-15-5D-00-05-01 | 10 Gbps   |
| vEthernet (Microsoft H...) | Hyper-V Virtual Ethernet Adapter     | 8       | Up     | 00-0D-3A-5D-A9-9E | 40 Gbps   |
| Ethernet 2                 | Microsoft Hyper-V Network Adapter #2 | 4       | Up     | 00-0D-3A-5D-A9-9E | 40 Gbps   |

The highlighted text (i.e. 17) is the ifIndex of the Internal Switch created in step b.

- d. Before running the next command, i.e. to create a NAT gateway, we need to select a different network other than the Windows Server 2016. For ex: If the Windows 2016 Server has been assigned the network 10.0.0.0/24, then let the NAT gateway be configured statically to 192.168.200.0/24 network. For this example, we are selecting the network **192.168.200.0/24**
- e. Run the following command to create a NAT gateway

```
New-NetIPAddress -IPAddress 192.168.200.1 -PrefixLength 24 -InterfaceIndex 17
```

The IP Address will be assigned as the IP of the NAT gateway, and the interface index is the one noted in step c.



*If the interface index in this step is given that of an external interface, you will lose all the connections to the Windows 2016 Server. So be careful while typing in the interface index. If access is lost, please refer to [Resolving Issues Point 1](#).*

- f. The next command will create a NAT Network which will be available for MWG to connect to:

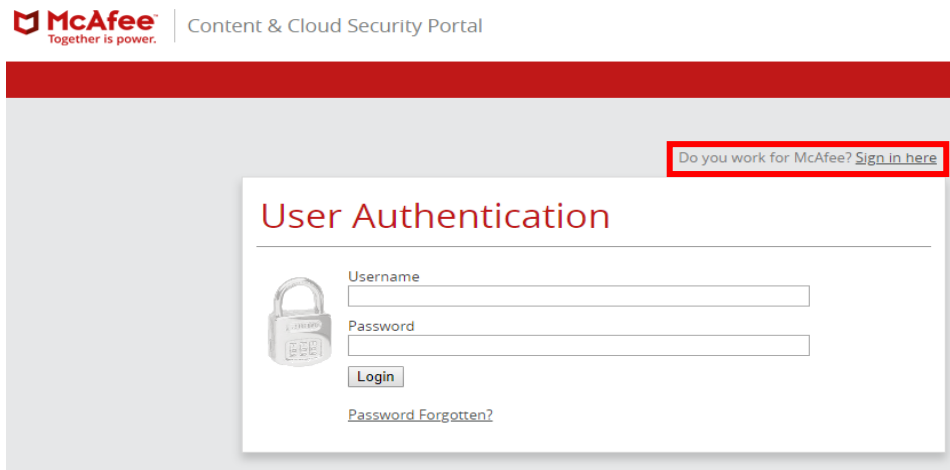
```
New-NetNat -Name NATNetwork -InternalIPInterfaceAddressPrefix 192.168.200.0/24
```

Here the network is the one used in step e.

#### 4) Installing MWG on Hyper-V

##### i. Getting the ISO for MWG

- a. Go to <https://contentsecurity.mcafee.com>
- b. Click on **Sign in here** as shown below:

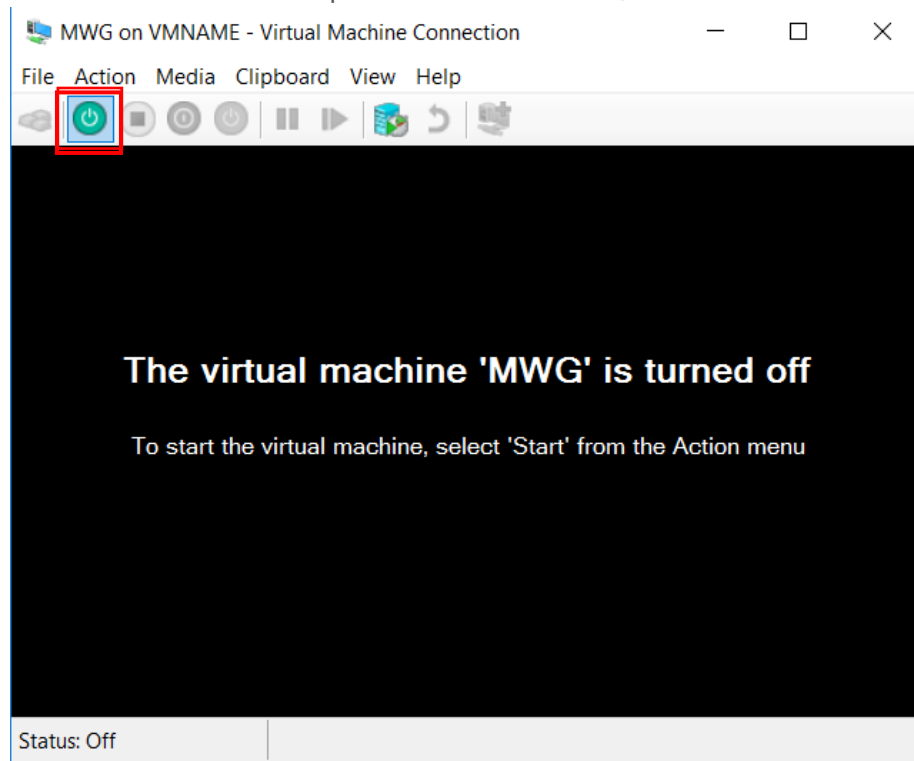


- c. After logging in, under **Latest Product Updates** click on **McAfee Web Gateway Main Release**
- d. Under required **McAfee Web Gateway Release**, click on **.iso** link. This will trigger the download, save the .iso file.

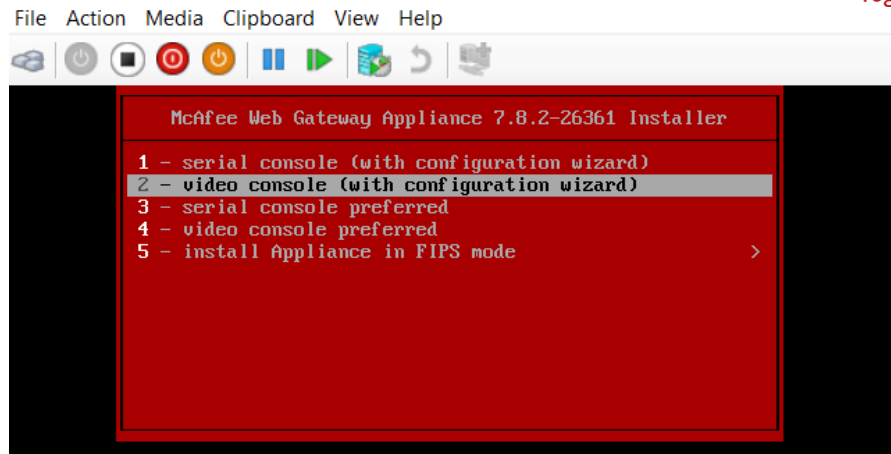
##### ii. Setting up the Virtual Machine on Hyper-V

- a. Open **Hyper-V Manager** by Clicking Start, point to **Windows Administrative Tools**, and then click **Hyper-V Manager**.
- b. In left pane, select the server below Hyper-V Manager.
- c. From the **Actions** pane, click **New**, and then click **Virtual Machine**.
- d. From the New Virtual Machine Wizard, click Next.
- e. On the **Specify Name and Location** section, specify a name for the virtual machine and where you want to store it, and then click Next.
- f. On the **Specify Generation** section, select **Generation 1**, and then click Next.
- g. On the **Assign Memory** section, specify memory as per your requirements from [this section](#). Minimum 4096 MB required to run MWG, and then click Next.  
 Option **Use Dynamic Memory for this virtual machine** is not supported by MWG.
- h. On the **Configure Networking** section, select the connection created in [Sec 3.b](#).

- i. On the **Connect Virtual Hard Disk** section, Select **Create a virtual hard disk** and specify a name, location, and size to create a virtual hard disk so you can install an operating system on it. See Minimum Req. For MWG at least 40 GB is required, so enter anything equal to or greater than 40 GB and then click Next.
  - j. On the **Installation Options** section, choose **Install an operating system from a bootable CD/DVD-ROM**, then select **Image file (.iso)** and **Browse** to the location of the .iso file, select it and click Next.
  - k. On the **Summary** section, Verify and click Finish.
- iii. Installation of MWG
- a. Right click on the Virtual Machine and select **Connect...**
  - b. Click on **Start** to boot up the Virtual Machine, as shown below:



- c. After the boot up, Select **Option 2** from the first screen of boot menu:



- d. When asked to Configure network interface eth0, select **No** in the auto-configure interface with DHCP page.
- e. Enter an IP from the network selected for the NAT. In our case, any IP from the network **192.168.200.0** can be selected. For this example, we are selecting **192.168.200.220** as the IP for **eth0**.
- f. Enter the netmask in accordance with the prefix.
- g. In the gateway address, enter the IP of the NAT gateway that was created in step **3.e**
- h. When asked for Primary DNS, please enter **168.63.129.16**. This is Azure's DNS IP address.
- i. In **Confirm changes** page check all the configurations, if everything looks good select **Yes** or else if something needs to be changed select **No**.
- j. Enter the root password, verify the password and hit Enter.
- k. Select **Default scheme with full Web Cache** in **Desired Volume Scheme** menu.
- l. MWG installation is complete.

## 5) Enabling access to MWG

Now we need to route all the traffic for MWG to the MWG Virtual Machine from base Windows Machine. To achieve this, we will have to configure Port Forwarding for the ports 4711 (HTTP UI access), 4712 (HTTPS UI access) and 9090 (Proxy Port). Also, by default, Azure Virtual Machines don't have these ports allowed for incoming or outgoing access, so merely changing the configuration on the Virtual Machines won't enable these ports. These ports should be allowed from the Azure Portal as well.

- Go to Azure Portal, click on the Virtual Machine and go to the **Networking** tab from the **Virtual Machine's** menu (on the 2<sup>nd</sup> left pane), under **Settings**.
- Allow **4711**, **4712** and **9090** ports to inbound traffic, by clicking **Add inbound port rule** and fill the appropriate **Destination port ranges** and **Name** for the same.

Add inbound security rule

Win2k16forMWG-nsg

Basic

\* Source ⓘ

Any

\* Source port ranges ⓘ

\*

\* Destination ⓘ

Any

\* Destination port ranges ⓘ

4711,4712,9090

\* Protocol

Any

TCP

UDP

\* Action

Allow

Deny

\* Priority ⓘ

330

\* Name

MWG\_Ports

Description

Add

- Now we need to add the Port Forwarding rules in the host machine configuration (i.e. Windows 2016 Server). Type in the following commands in an **Powershell** as

Administrator to forward traffic from the respective ports to MWG, the IP address mentioned below should be that of the MWG Virtual Machine you are working on (that is **192.168.200.220** in this example):

For Port 4711:

```
netsh int portproxy add v4tov4 listenport=4711 connectport=4711  
connectaddress=192.168.200.220
```

For Port 4712:

```
netsh int portproxy add v4tov4 listenport=4712 connectport=4712  
connectaddress=192.168.200.220
```

For Port 9090:

```
netsh int portproxy add v4tov4 listenport=9090 connectport=9090  
connectaddress=192.168.200.220
```

- d. Now the MWG can be accessed using the Windows 2016 Server's IP address followed by UI and Proxy ports.

## 6) Accessing MWG Proxy from the McAfee network

- a. The MWG UI will be accessible from the McAfee network. But redirecting the traffic to the newly created MWG Proxy won't work, as setting up another proxy on port 9090 is not allowed on McAfee network. For accessing the same we need to open another non-standard port on Windows 2016 Server following the instructions on **5.b** and **5.c**, and forward all the traffic from that port to port **9090** of the MWG Virtual Machine following the instructions on **5.d**
- b. Selecting a non-standard port, for example **40444**. Follow **5.b** and **5.c** for accessing the port on Windows 2016 Server externally.
- c. Start a **Powershell** in Administrator mode, and enter the command below to forward traffic from **40444** (that can be different in your case) to **9090** of MWG Virtual Machine:  

```
netsh int portproxy add v4tov4 listenport=40444 connectport=9090  
connectaddress=192.168.200.220
```
- d. Now for setting proxy on any browser set the **Proxy Address** as the Windows 2016 Server's IP and **Proxy Port** as the port selected in step **6.b** (i.e. **40444** in this example)

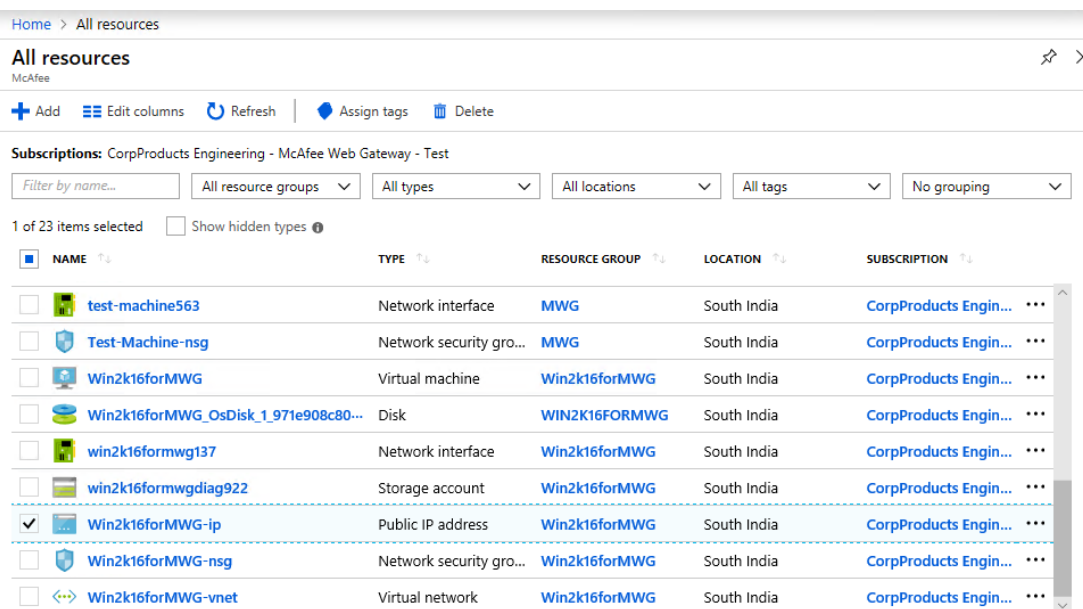
## Configuring the feature

Once the MWG is available, it can be configured using the guide as provided [here](#).

## Resolving Issues

### 1. Lost RDP connection to Virtual Machine hosted on Azure due to interference with external interface

- i. Login to Azure portal with your credentials.
- ii. Open the Virtual Machine properties that has lost RDP connection from **Dashboard** or **All Resources**.
- iii. Click on **Stop** on top of the Virtual Machine property window, to shut down the Virtual Machine
- iv. Go to the **Networking** tab and click on **Detach network interface** for the existing network interface.
- v. Click on **Attach network interface -> Create network interface**
- vi. Enter the **Name** and click on **Create**
- vii. After the network interface is created, you will be redirected to the **Attach network interface**, select the newly created interface from the drop down and click on **OK**
- viii. Click on **All resources** and click on the **Public IP address** element as shown below:



| NAME                                 | TYPE                     | RESOURCE GROUP       | LOCATION           | SUBSCRIPTION                 |
|--------------------------------------|--------------------------|----------------------|--------------------|------------------------------|
| test-machine563                      | Network interface        | MWG                  | South India        | CorpProducts Engin...        |
| Test-Machine-nsg                     | Network security gro...  | MWG                  | South India        | CorpProducts Engin...        |
| Win2k16forMWG                        | Virtual machine          | Win2k16forMWG        | South India        | CorpProducts Engin...        |
| Win2k16forMWG_OsDisk_1_971e908c80... | Disk                     | WIN2K16FORMWG        | South India        | CorpProducts Engin...        |
| win2k16formwg137                     | Network interface        | Win2k16forMWG        | South India        | CorpProducts Engin...        |
| win2k16formwgdiag922                 | Storage account          | Win2k16forMWG        | South India        | CorpProducts Engin...        |
| <b>Win2k16forMWG-ip</b>              | <b>Public IP address</b> | <b>Win2k16forMWG</b> | <b>South India</b> | <b>CorpProducts Engin...</b> |
| Win2k16forMWG-nsg                    | Network security gro...  | Win2k16forMWG        | South India        | CorpProducts Engin...        |
| Win2k16forMWG-vnet                   | Virtual network          | Win2k16forMWG        | South India        | CorpProducts Engin...        |

- ix. Click on **Dissociate** if the **Public IP address** is attached to some interface and click **Yes**, as shown below:

Home > All resources > Win2k16forMWG-ip

**Win2k16forMWG-ip**  
Public IP address

Search (Ctrl+/,)

Associate X Dissociate → Move Delete

**Overview**

- Activity log
- Access control (IAM)
- Tags

**Settings**

- Configuration
- Properties

**Essentials**

|                                                      |                  |
|------------------------------------------------------|------------------|
| Resource group (change)                              | SKU              |
| Win2k16forMWG                                        | Basic            |
| Location                                             | IP address       |
| South India                                          | 104.211.209.49   |
| Subscription name (change)                           | DNS name         |
| CorpProducts Engineering - McAfee Web Gateway - T... | -                |
| Subscription ID                                      | Associated to    |
| 3fdb8811-7a7b-4170-a688-bee3b42d0988                 | win2k16formwg137 |
|                                                      | Virtual machine  |
|                                                      | Win2k16forMWG    |

- x. Click on **Associate**, and select **Network interface** from the list, then select the network interface that you attached to the Virtual Machine in step **vi** above and click **OK**
- xi. Go to the Virtual Machine property from **All resources** and click on **Start** to boot up the machine.
- xii. In the properties, below you will find the new **Public IP address** that is assigned to the Virtual Machine on successful bootup.

All the properties of the interface are reset, so now you can successfully RDP to the Virtual Machine.

## References

- NAT Rules: - <https://anandthearchitect.com/2018/01/06/windows-10-how-to-setup-nat-network-for-hyper-v-guests/>
- Nested Virtualization: - <https://azure.microsoft.com/en-in/blog/nested-virtualization-in-azure/>
- Dv3 and Ev3 Machines: - <https://azure.microsoft.com/en-in/blog/introducing-the-new-dv3-and-ev3-vm-sizes/>
- MWG Documentation: - [https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT\\_DOCUMENTATION/27000/PD27276/en\\_US/mwg\\_780\\_pg\\_product\\_0a00\\_en-us.pdf](https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27276/en_US/mwg_780_pg_product_0a00_en-us.pdf)

## Abbreviations

|     |                             |
|-----|-----------------------------|
| CPU | Central Processing Unit     |
| GB  | Giga Byte                   |
| MWG | McAfee Web Gateway          |
| NAT | Network Address Translation |
| RAM | Random Access Memory        |
| RDP | Remote Desktop Protocol     |
| SSH | Secure Shell                |



## HLS Stream Detection

### Value

This feature allows user to detect HLS streams.

### Overview

HTTP Live Streaming (also known as HLS) is an HTTP-based media streaming communications protocol.

This feature adds

- HLS detection capability to Stream detector
- HLS playlist (.m3u8) file, media type detection

### Important Concepts

The HLS streaming protocol chops the video content down into small chunks and then delivers these short clips to viewers. Generally, the protocol splits video files, into short segments with the .ts file extension.

As the stream is played, the client downloads the extended M3U playlist (.m3u8) file of mime type “**application/vnd.apple.mpegurl**” at the beginning of the streaming session. The extended M3U playlist file serves as an index for the video segments.

The HTTP Live Streaming is based on the RFC8216.

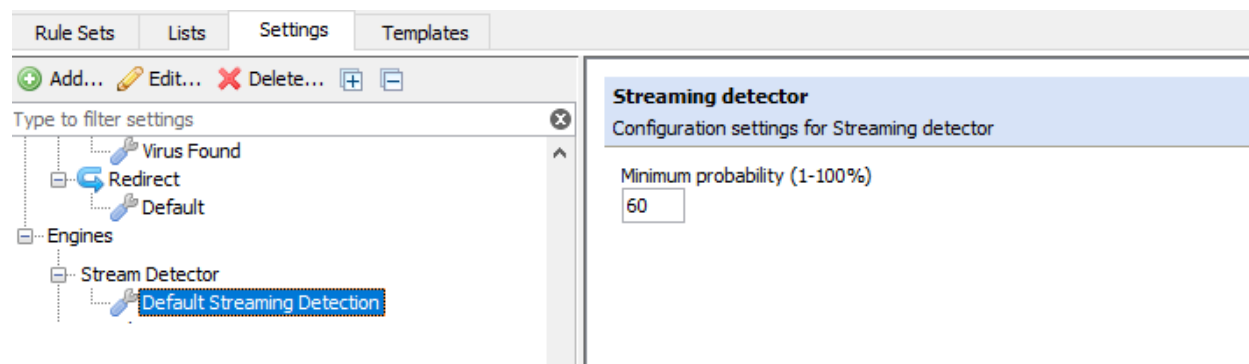
### Using this Feature

To use this feature, follow these steps:

- 7) Use the property “**StreamDetector.IsMediaStream**” in the rules, to enable stream detection.

## Configuring the feature

Video and Audio streams are detected based on the configured probability value of Streaming Detector. The default probability for Stream detection is 60, please update the same according to your preferences.





## RTF Opener

### Value

This feature would allow user to open RTF (Rich Text Format) files and scan for embedded objects.

### Overview

The Rich Text Format (often abbreviated RTF) is a document file format. RTF file usually contains formatted text and graphics.

This change will help in extraction and detection of objects embedded within a RTF file.

### Important Concepts

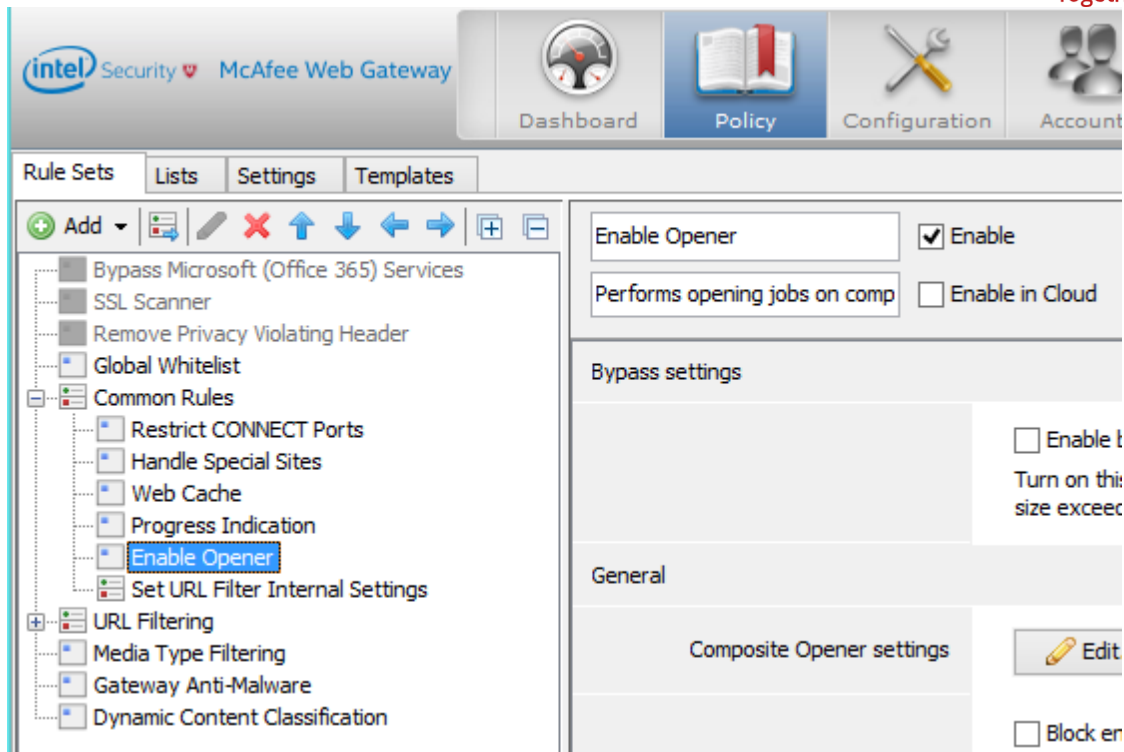
The current RTF opener implementation is based on RTF Specification 1.9.1. This specification can be found at <https://www.microsoft.com/en-in/download/details.aspx?id=10725>.

### Using this Feature

To use this feature, follow these steps:

- 1) "Enable opener" in the MWG default policy must be enabled.

### Related Screenshots



intel Security McAfee Web Gateway

Dashboard Policy Configuration Account

Rule Sets Lists Settings Templates

+ Add [Icons]

- Bypass Microsoft (Office 365) Services
- SSL Scanner
- Remove Privacy Violating Header
- Global Whitelist
- Common Rules
  - Restrict CONNECT Ports
  - Handle Special Sites
  - Web Cache
  - Progress Indication
  - Enable Opener**
  - Set URL Filter Internal Settings
- URL Filtering
  - Media Type Filtering
  - Gateway Anti-Malware
  - Dynamic Content Classification

Enable Opener ☒ Enable

Performs opening jobs on comp ☐ Enable in Cloud

Bypass settings

☐ Enable t

Turn on thi:  
size exceed

General

Composite Opener settings  Edit

☐ Block en



## EML Opener

### Value

This feature would allow user to open EML files and scan for embedded objects.

### Overview

EML is an e-mail message file format. These files contain email messages and email file attachments.

This change will help in extraction and detection of objects embedded within an EML file.

### Important Concepts

EML is a file extension for an e-mail message saved to a file in the MIME RFC 822 standard format by Microsoft Outlook Express as well as some other email programs. EML files can contain plain ASCII text for the headers and the main message body as well as hyperlinks and attachments.

### Using this Feature

To use this feature, follow these steps:

- 1) "Enable opener" in the MWG default policy must be enabled.

### Related Screenshots

The screenshot displays the McAfee Web Gateway Policy configuration interface. The top navigation bar includes the Intel Security logo, the text 'McAfee Web Gateway', and icons for Dashboard, Policy (selected), Configuration, and Account. Below the navigation bar, there are tabs for Rule Sets, Lists, Settings, and Templates. The main content area is divided into a left sidebar and a right configuration panel.

**Left Sidebar (Rule Sets):**

- Bypass Microsoft (Office 365) Services
- SSL Scanner
- Remove Privacy Violating Header
- Global Whitelist
- Common Rules
  - Restrict CONNECT Ports
  - Handle Special Sites
  - Web Cache
  - Progress Indication
  - Enable Opener** (highlighted)
  - Set URL Filter Internal Settings
- URL Filtering
  - Media Type Filtering
  - Gateway Anti-Malware
  - Dynamic Content Classification

**Right Configuration Panel:**

- Enable Opener:** ☒ Enable
- Performs opening jobs on comp:** ☐ Enable in Cloud
- Bypass settings:**
  - ☐ Enable t
  - Turn on this size exceed
- General:**
- Composite Opener settings:** [Edit](#)
- ☐ Block en



## Support for Private GTI cloud

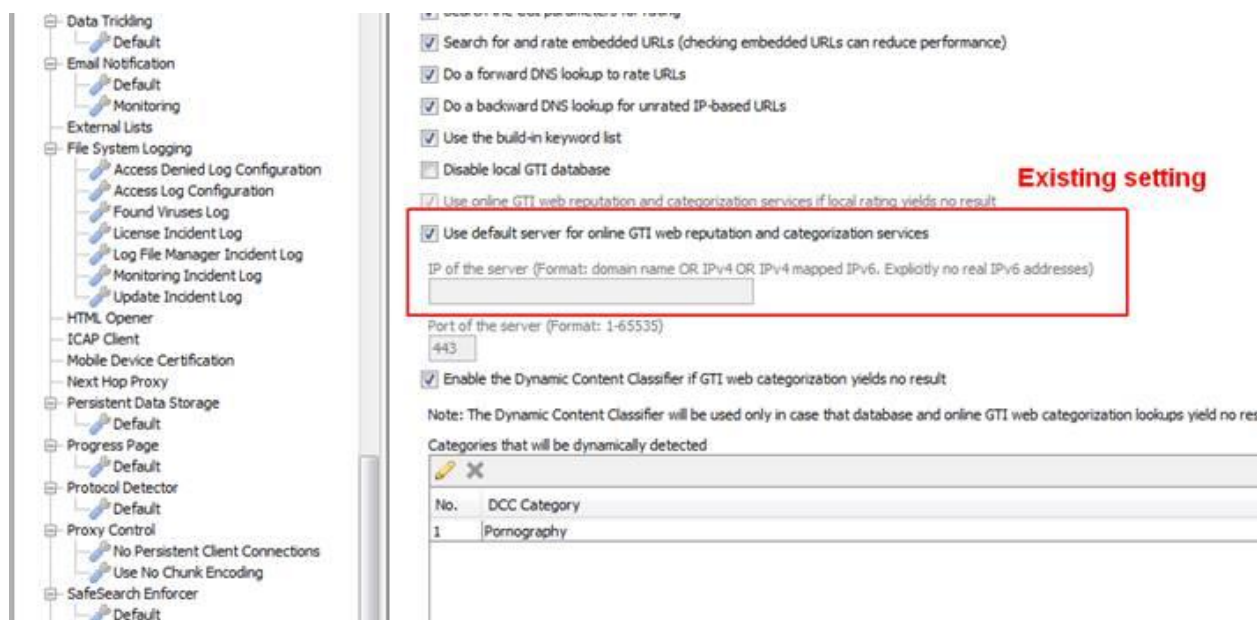
### Value

This feature allows users to leverage a private GTI cloud, that runs on premise instead of the public GTI.

### Overview

The Private GTI service implements the same API as public GTI cloud service but runs on premise and is under full control of a customer. MWG has to connect to a custom server, accept customer-defined server certificate and provide customer-defined client certificate to connect to PGTI service. That's why URL filter configuration in MWG now allows to overwrite server address (existing setting), server and client certificates (new in 8.0 and a non-announced feature in 7.8.2.2 to get a contract).

### Related Screenshots



**Existing setting**

☒ Use default server for online GTI web reputation and categorization services

IP of the server (Format: domain name OR IPv4 OR IPv4 mapped IPv6. Explicitly no real IPv6 addresses)

Port of the server (Format: 1-65535)

443

☒ Enable the Dynamic Content Classifier if GTI web categorization yields no result

Note: The Dynamic Content Classifier will be used only in case that database and online GTI web categorization lookups yield no res

Categories that will be dynamically detected

| No. | DCC Category |
|-----|--------------|
| 1   | Pornography  |

- Coaching
  - Default
- Composite Opener
  - Default
- Data Loss Prevention (Classifications)
- Data Loss Prevention (Dictionaries)
- Data Tricking
  - Default
- Email Notification
  - Default
  - Monitoring
- External Lists
- File System Logging
  - Access Denied Log Configuration
  - Access Log Configuration
  - Found Viruses Log
  - License Incident Log
  - Log File Manager Incident Log
  - Monitoring Incident Log
  - Update Incident Log
- HTML Opener
- ICAP Client
- Mobile Device Certification
- Next Hop Proxy
- Persistent Data Storage
  - Default
- Progress Page
  - Default
- Protocol Detector
  - Default
- Proxy Control
  - No Persistent Client Connections
  - Use No Chunk Encoding
- SafeSearch Enforcer
  - Default
- SAML Request
- SAML Response
- Secure Reverse Proxy Filter
- Secure Token
- Single Sign On
- SSL Client Certificate Handling
- SSL Client Context with CA
  - Default CA
- SSL Client Context without CA
- SSL Scanner
  - Default Certificate Verification
  - Enable Content Inspection
- SSO Certificates
- SSO Private Keys
- Statistics
  - Default

Set...

☒ Connect to GTI cloud via hostname also when a proxy is configured

☒ Try to bypass the proxy if unreachable

☒ Trust server certificate

New

**Subject**  
Common Name (CN) mwg  
Organization (O) mwg  
Organizational Unit (OU) <not set>

**Issuer**  
Common Name (CN) mwg  
Organization (O) mwg  
Organizational Unit (OU) <not set>

**Validity**  
Not Before 24.03.2016 14:43:05  
Not After 24.03.2026 14:43:05

**Extensions**  
Comment <not set>

**Fingerprint**  
9a 8b 5f d3 82 d4 fd dd 12 0f 79 fd da 97 17 7d 80 86 1a 78  
Import...

☐ Provide client certificate

**Subject**  
Common Name (CN)  
Organization (O)  
Organizational Unit (OU)

**Issuer**  
Common Name (CN)  
Organization (O)  
Organizational Unit (OU)

**Validity**  
Not Before -  
Not After -

**Extensions**  
Comment

**Fingerprint**  
-

**Private key**  
<not set>

**Client Certificate**
Import...
Export...
Export Key...

**Logging**
☐ Enable logging

Log Level  
03 INFO



## DNSFastFallBack

### Value

When a dns query results in multiple IPV4 or IPV6 address, this updated feature will define the order in which those IP addresses should be attempted to connect. Whether to attempt the IPV4 or IPV6 address is already defined in previous release. In this release we will define the order of addresses which should be attempted to connect within an address family (IPV4 addresses or IPV6 addresses).

### Overview

When we get multiple addresses belonging to same family, we need to sort those addresses. Following are the parameters based on which the sorting will happen.

- Precedence of the IP address.
- Scope of the IP address
- Connection/Roundtrip time.
- Least recently used IP address.

### Important Concepts

The values of the above factors affect our IP address selection. They are discussed in more detail below.

#### a) IP address precedence

Below table contains the IP address prefix and its corresponding precedence. While calculating the precedence ipv4 address is converted to ipv6 address. Example of this conversion is, if the IPV4 address is 10.10.10.10, then it's corresponding IPV6 is "::ffff;0a0a:0a0a" So, all IPV4 address will have same Precedence.

| Prefix        | Precedence | Label |
|---------------|------------|-------|
| ::1/128       | 50         | 0     |
| ::/0          | 40         | 1     |
| ::ffff:0:0/96 | 35         | 4     |
| *2002::/16    | 30         | 2     |
| *2001::/32    | 5          | 5     |
| *fc00::/7     | 3          | 13    |
| ::/96         | 1          | 3     |
| *fec0::/10    | 40         | 11    |
| *3ffe::/16    | 1          | 12    |
| *fec0::/10    | 1          | 11    |
| *3ffe::/16    | 1          | 12    |

We will use the IP addresses precedence in increasing order. Highest precedence IP will be selected to connect first. The order is same as the default precedence value in the rfc 6724, except for the entry \*fec0::/10.

b) Scope of the IP address.

Different scopes of IP addresses are

- Link Local
- Site Local
- Global

While sorting based on scope we give preference in the same order as defined above. Unique local addresses are given same scope as that of site local. If two IPs has same precedence value then only we sort using the scope.

c) Connection/Round trip time.

We will maintain the time taken to connect to an IP. This is the factor which is based on the connection history. For two IP addresses if above two factors (precedence and scope) measure same then only we sort using the Connection time. The round-trip time is updated while using http, https protocol

d) Least recently used IP.

We will be maintaining last used time for all IPs. For any two IPs, if all the above 3 factors (precedence, scope and roundtrip time) measure same, then least recently used IP will be given the preference.

Example.

Suppose the DNS AAAA query resolves to following IP Address.

"0:0:0:0:0:c0a8:14dd"

"3ffe:0:0:0:0:7823:9263"

"fc00:0:0:0:ad:34:ff:bc"

"2002:0:0:0:0:ffff:c0a8:14dd"

"fe80:0:0:0:0:6487:5458"

"2001:10:0:0:0:0:c0a8:14dd"

"0:0:0:0:0:ffff:c0a8:14dd"

"0:0:0:0:0:0:0:1"

"2001:10:0:0:0:0:c0a8:14de"

"2001:10:0:0:0:0:c0a8:14da"

The order of connection attempts and the reasons for that order are listed in the table below

| Order | IP Addresses              | Precedence | Scope        | Round-trip time in milli sec | Least Recently used         | Reason for the order                                                                                        |
|-------|---------------------------|------------|--------------|------------------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------|
| 1     | 0:0:0:0:0:0:1",           | 50         | Not Relevant | 100                          | Fri Sep 7 04:25:15 UTC 2018 | Highest Precedence so 1                                                                                     |
| 2     | "fe80:0:0:0:0:6487:5458"  | 40         | Link Local   | 100                          | Fri Sep 7 04:26:15 UTC 2018 | Same precedence as 3, 4,5,6, but second because it's scope is link local                                    |
| 3     | "fc00:0:0:0:ad:34:ff:bc"  | 40         | Unique Local | 200                          | Fri Sep 7 04:27:15 UTC 2018 | Same precedence as 2, 4,5,6, but 3rd because it's scope is Unique local                                     |
| 4     | "2001:10:0:0:0:c0a8:14dd" | 40         | Global       | 200                          | Fri Sep 7 04:28:15 UTC 2018 | Same precedence as 2, 3,5,6, but 4th because it's scope is Global                                           |
| 5     | "2001:10:0:0:0:c0a8:14de" | 40         | Global       | 300                          | Fri Sep 7 04:29:15 UTC 2018 | Same precedence as 2, 3,4,6, but 5th because it's scope is also Global and RTT is greater than the 4th one. |

|   |                               |    |              |     |                             |                                                                                                                                                    |
|---|-------------------------------|----|--------------|-----|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 6 | "2001:10:0:0:0:c0a8:14da"     | 40 | Global       | 300 | Fri Sep 7 04:30:15 UTC 2018 | Same precedence as 2,3,4,5, but 6th because it's scope is also Global and RTT is same as 5th, but the 4th one is least recently used than the 4th. |
| 5 | "0:0:0:0:0:ffff:c0a8:14dd"    | 35 | Not Relevant | 200 | Fri Sep 7 04:21:15 UTC 2018 | Because of Precedence                                                                                                                              |
| 6 | "2002:0:0:0:0:ffff:c0a8:14dd" | 5  | Not Relevant | 200 | Fri Sep 7 04:22:15 UTC 2018 | Because of Precedence                                                                                                                              |
| 7 | "0:0:0:0:0:0:c0a8:14dd"       | 1  | Not Relevant | 200 | Fri Sep 7 04:23:15 UTC 2018 | Because of Precedence                                                                                                                              |
| 8 | "3ffe:0:0:0:0:7823:9263"      | 1  | Not Relevant | 200 | Fri Sep 7 04:24:15 UTC 2018 | Because of Precedence                                                                                                                              |

