iQuila FAQ

on Routing through Secure Gateways

iQ22101r1

This Document Applies to:

iQuila Cloud

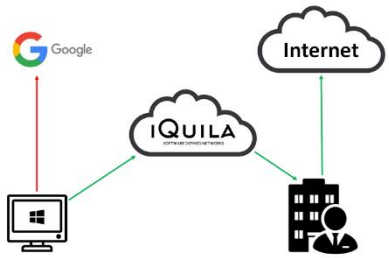
Routing through Secure Gateways

Split tunnelling with iQuila Cloud in Bridging Mode.

There are several, options available when requiring split tunnelling on iQuila Cloud.

1. Local Split tunnelling – this is where only traffic destined for the remote network is sent over the iQuila Link.

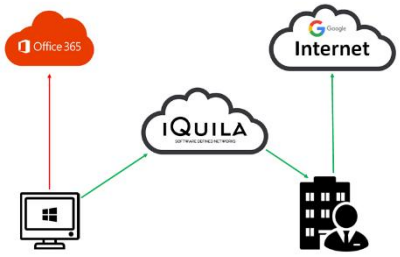
   - Advantage – Reduced load and bandwidth on the iQuila link.
   - Disadvantage – All traffic destined for the iQuila link is sent locally and therefore cannot be managed/filtered and can leave the endpoint at risk of malware and vulnerable for man in the middle attacks.



   Please see documents on changing the Gateway Metric for Local Routing. (IQ22068r4)

2. Setting selected applications to route locally and all other traffic to route over the iQuila connection.

   - Advantage – Reduced load and bandwidth on the iQuila link.
   - Disadvantage – Although you may trust the destination that you would like to set for local routing you can still leave your system unprotected against MTM, (Man in the middle attacks).



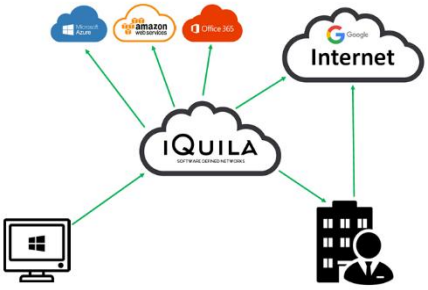
   To route a selected application such as Microsoft Office 365 locally and not over the iQuila link please run the local script on your system. Copy the script to notepad and save it as a .bat file. Insert the IP address and subnet of the application you would like to route locally, and change the iQuilaConnectionsName to the connections name of your iQuila account, you can add as many routes to the script as you require.

```
vencmd localhost /client /CMD accountdisconnect iQuilaConnectionName
@echo off
set "ip="
for /f "tokens=2,3 delims={,}" %%a in ('"WMIC NICConfig where IPEnabled="True" get
DefaultIPGateway /value | find "I" "') do if not defined ip set ip=%%~a
route add [application ip address]  mask [subnet] %ip%
echo  Homenet GW Address is: %ip%
pause
vencmd localhost /client /CMD accountconnect iQuilaConnectionName
```

Note: You must have iQuila Command line tools installed to run this script.

3. Enabling the iQuila Cloud Secure Gateway.

Utilising iQuila Cloud offers a secure gateway that enables you to route traffic from the client out through the iQuila Cloud gateway protecting the client from endpoint attacks and (MTM) man in the middle attacks. To enable secure gateway, select Networking, then advance networking from your iQuila cloud portal account, If you are using a bridge when enabling secure gateway please assign the secure gateway an IP address on the same subnet as your LAN.



- Advantage – Endpoints are fully protected as all data is routed via the secure gateway and Cloud services are secured by installing either iQuila Cloud client on your cloud services or locking down access to the public IP address of the iQuila gateway servers.
- Disadvantage – none.

(Configuring secure gateway is a new feature of iQuila cloud, if your cloud account does not have this function, please contact support to have your account upgraded)

4. Utilising RFC 3442 Push paths.

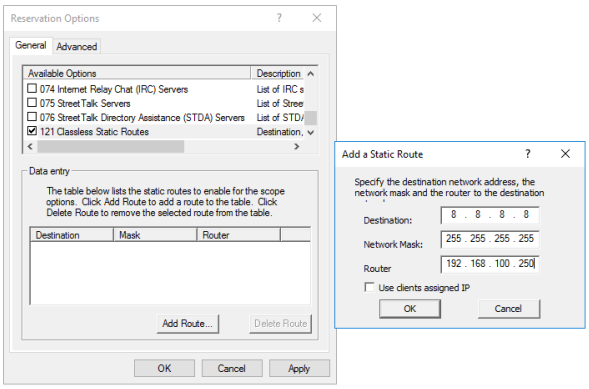
The iQuila Client adaptors fully support RFC 3442 standards enabling the use of push paths. Push paths can easily be configured from your DHCP server once the iQuila Secure gateway has been enabled, or via the iQuila Cloud DHCP server.

Configuring Windows Server DHCP to Push Routes:
If you are using a Windows DHCP server and wish to push routes to clients, you will need to have a good understanding of your network topology. Please remember if you are pushing routes from your DHCP server this can affect all clients, both local to the LAN and remote. If you do not want these routes to affect local LAN clients you have several options.

- Create revisions and assign the route to the revisions.
- Create a separate VLAN and configure a new scope for these clients.
- Disable DHCP filtering on the iQuila Bridge and configure DHCP on your cloud portal account.

5. Creating a route in Microsoft DHCP Server under revisions.

Create revisions for the clients you would like to push routes to. On the revisions, select 'configure options' then select option 121, "Classless Static Routes", Select Add Route and enter the IP address of the destination along with its subnet mask, then enter the IP address of the iQuila Cloud Secure Gateway and click ok. Add any further routes as required, once all the routes have been applied click ok, once your DHCP server updates, the new routes will be pushed to the client.



6. Configuring iQuila Cloud for DHCP and pushing routes from iQuila Cloud.

First, you will need to create a new exclusion range of IP addresses on your Local DHCP server, this eliminates conflicts with the DHCP scope you are about to configure on the iQuila Cloud.

On your Windows DHCP server select Address Pool then create a new exclusion range

Enable DHCP on the cloud portal and configure a DHCP scope, to do this login to your portal account and select networking then advance networking, enable the option for DHCP server and assign a DHCP address range, under DNS enter the IP address of your internal LAN DNS servers, under gateway enter the gateway you would like the internet traffic to go through, if you enter the Cloud Gateway IP address then all traffic as default will route out via the iQuila Cloud Secure gateway, you can then enter the routes under the Split Tunnelling section that you would like to route via your office gateway, alternatively enter your office LAN gateway address and use split tunnelling to enter the routes you would like traffic to route via the Secure gateway servers.

For routes to take effect please make sure your iQuila Virtual Network adaptor's metric is set to Automatic.

7. IP Address of iQuila Secure Gateway Endpoints.

iQuila Cloud Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements.

United Kingdom
193.33.117.0/24, 185.127.19.102/32. 83.229.69.24/32, 194.146.24.80/32, 185.79.109.0/24

Europe
83.229.85.165/32, 63.250.56.195/32

North America
52.144.45.106/32, 138.128.245.166/32, 138.128.242.146/32, 104.225.143.25/32

Middle East
212.80.205.174/32

Asia
45.126.124.72/32, 45.126.126.230/32