iQUILA

SOFTWARE DEFINED NETWORKS

iQuila FAQ on Overlay Networks

iQ22061r2

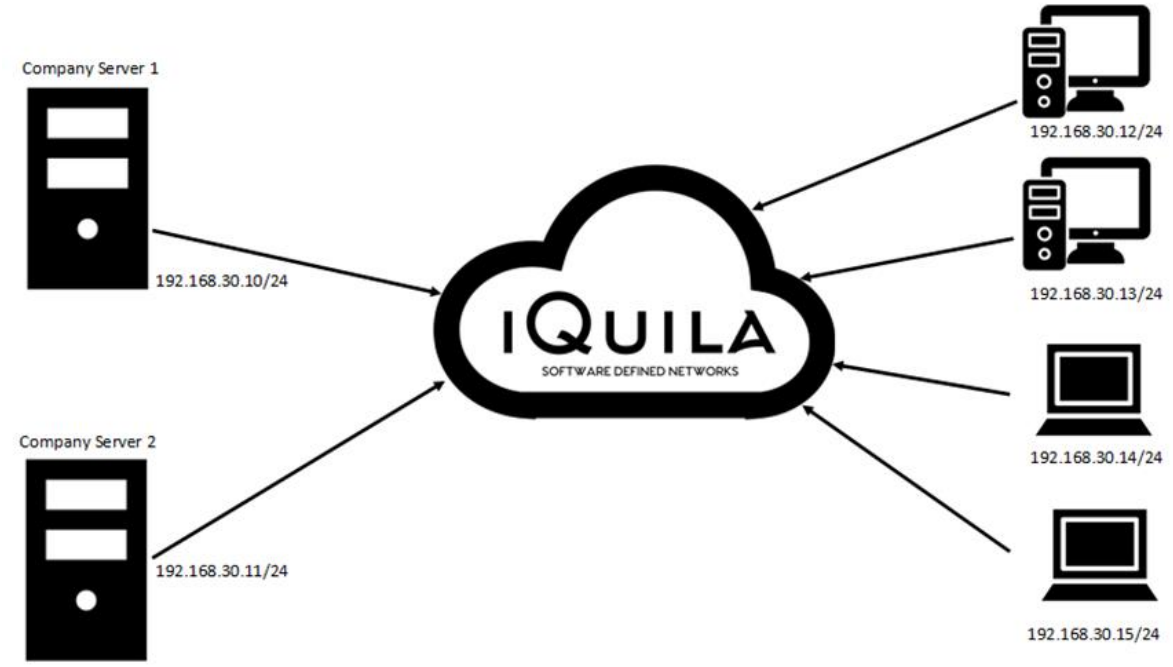
This Document Applies to:

iQuila Cloud

iQuila Cloud Overlay Network.

iQuila Cloud Overlay Network.

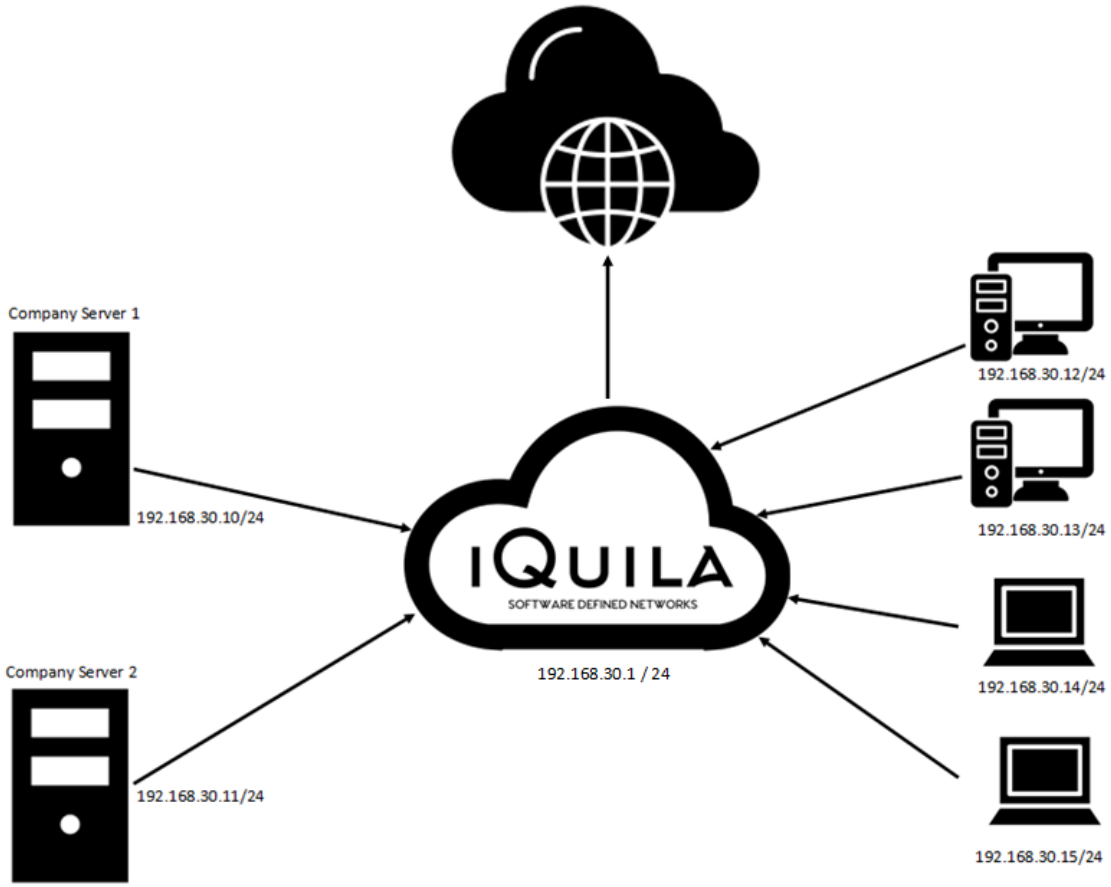
This basic, default Overly Network configuration is a quick and simple deployment to give all remote users always-on, secure, connectivity to Server based resources e.g., Fileserver, SQL, Accounting.



With this basic Overlay Network configuration, NAT is enabled on the iQuila Cloud Portal. The iQuila Cloud Client, is deployed, onto the company servers and onto the remote client computer and laptops. The iQuila Cloud will issue a 192.168.30.* address range by default to all iQuila Client VEN connections. DNS Resolution to internal hostnames are automatic and dynamically updated in the iQuila Cloud. Internet access is local to the remote users location and mapped drives are also possible in this configuration.

iQuila Cloud Overlay Network with Secure NAT routing.

This configuration is the same as the basic Overlay Network configuration, but internet access is now routed via the iQuila Cloud Secure Gateway Server.

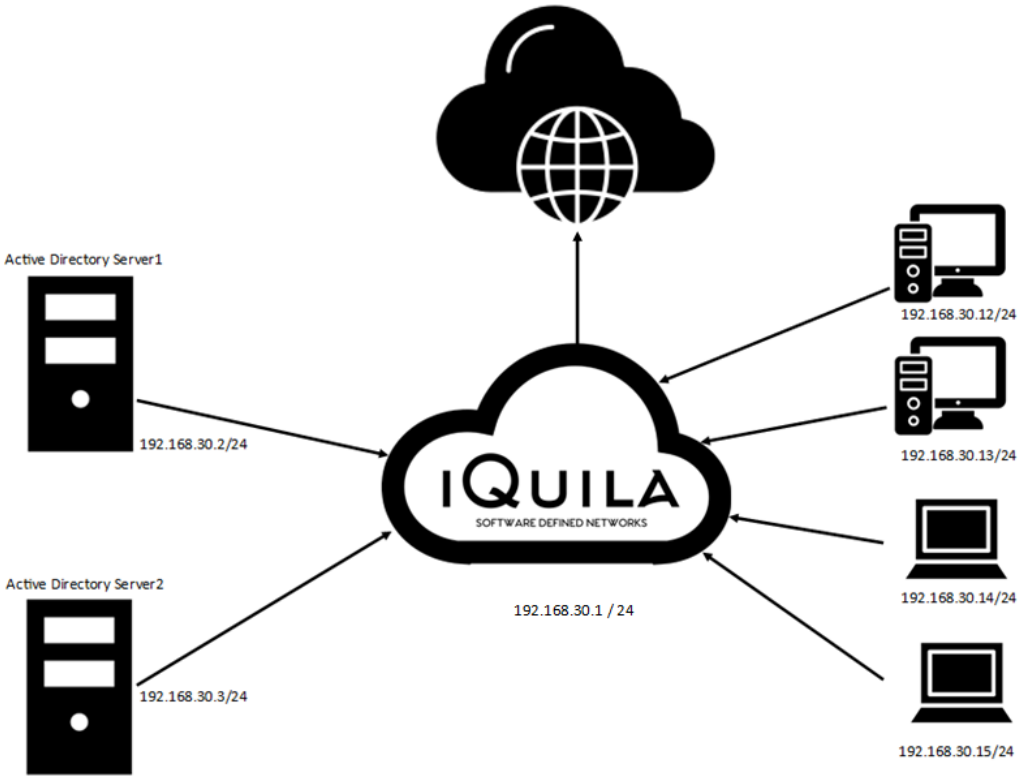


With this Overlay Network configuration, NAT is enabled on the iQuila Cloud Portal but also Secure Gateway is enabled on the iQuila Cloud Portal. All access to the Server resources is the same but the difference being that all remote user's internet access is now being routed via the iQuila Cloud Portal Secure Gateway Server at the location in which the iQuila switch was located. e.g., UK, USA, Europe.

Changes can be made to the routing matric to enable remote users to breakout to the internet locally at their ISP location, if it is deemed not necessary for users to route to the internet via the iQuila Secure Gateway Server.

iQuila Cloud Overlay Network with Secure NAT routing and Full Active Directory Login.

With this configuration all remote users can use the companies Active Directory Server to securely log their domain connected device remotely with full Active Directory Login at the computer GPO level.



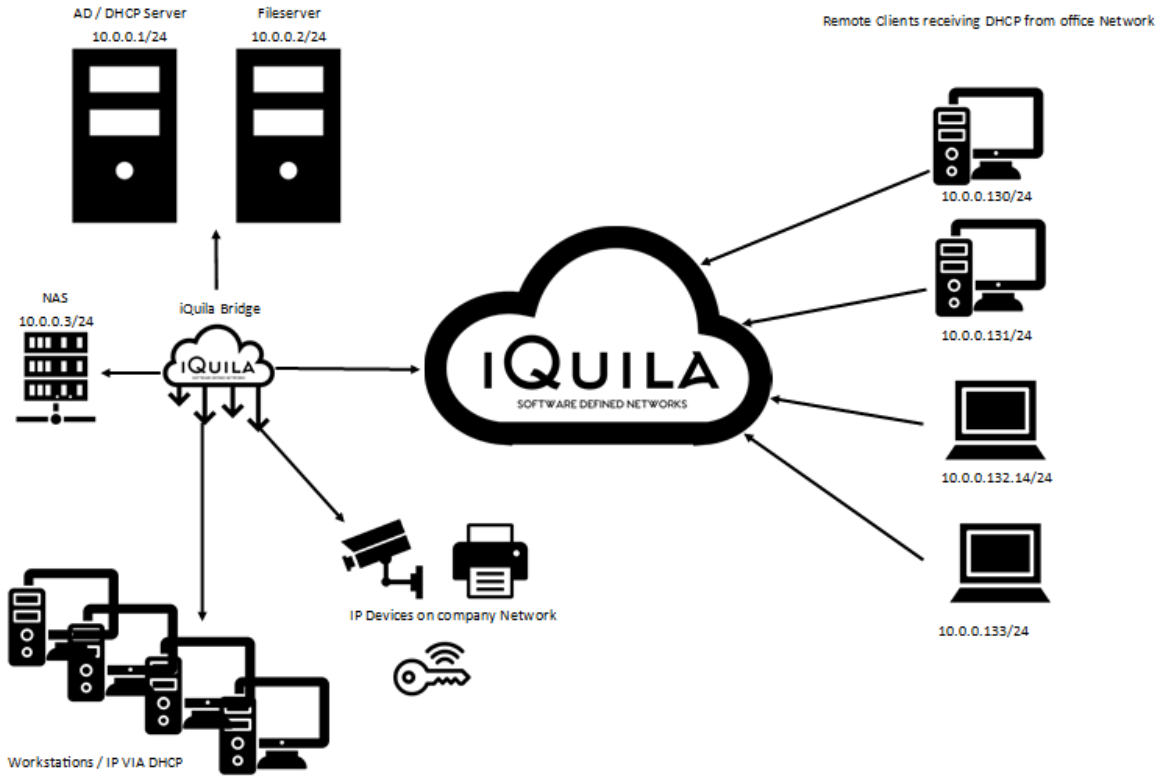
In this configuration, the Overlay network, NAT, and Secure Gateway are **enabled** on the iQuila Cloud Portal and the iQuila Cloud Client is deployed to the company servers and to the remote user's computers or laptops. The iQuila Cloud will issue a 192.168.30.* address range as default to all iQuila clients and a Gateway address of 192.168.30.1

The client software is then also deployed to every Active Directory server and the iQuila VEN connection on the AD servers are then assigned with a static IP address from the same subnet as the iQuila Cloud network. The DNS on the iQuila Cloud Portal should be configured to the assigned static IP address you set to the Active Directory servers.

The remote clients will now have full access to Active Directory login with full Group Policy down to the computer GPO level. This is achieved due to the iQuila Client service starting and operating thus connecting to the AD server before the device's logon screen is active.

Bridging; Extending your office network to the Cloud.

In this Overlay network configuration. The Layer 2 office network is bridge seamlessly to the iQuila Cloud using either, the iQuila Bridge Client software or an iQuila Hardware Bridge.



With a Bridged Network, the iQuila Cloud Portal is configured with the Overlay Network, NAT, and Secure Gateway **disabled**. A Bridge device is created on the Portal with the option "Allow DHCP over this link" set to ON allowing DHCP traffic on the Tunnel.

The Bridge Client software is installed on a server or PC in the office. The Enterprise Bridge (Hardware) is setup in the office and linked into the office switch. Configuration is then carried out to bring the Bridge online and bridge the office network to the iQuila Cloud. Please read the following documents.

Guide to Installing iQuila Bridge Client.

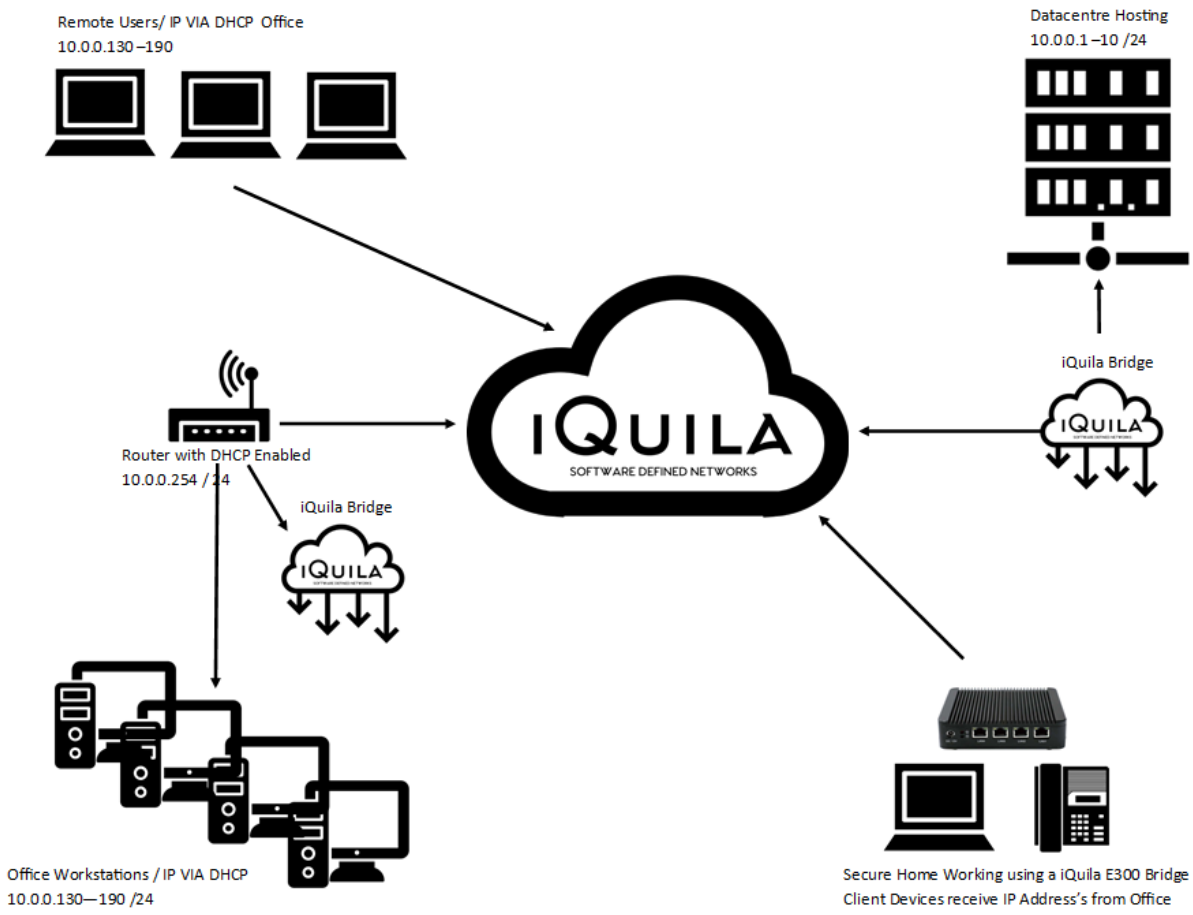
iQuila Enterprise 500 Hardware Bridge Installation Guide

All clients will now receive a DHCP address and routing from the Office DHCP server and will have the same functionality as if the user is in the office. All traffic for the Internet will route via the office gateway. All remote users will have access to any IP device on the internal office network and DNS will be to that of the office network.

To allow remote clients to breakout out locally on their internet and not via the office gateway (this is called split tunnelling), simply change the matric on the iQuila Virtual Network Adaptor (VEN) to a higher value (45). Internet traffic will now route from the user's location, but all office network access will still be available.

iQuila Cloud Bridge, extending your Cloud network into your office.

In this configuration there are two bridges installed, one is located at the data centre and the other is located at the company's office.



With a Bridged Network the iQuila Cloud Portal is configured with the Overlay Network, NAT, and Secure Gateway **disabled**. The two bridges are deployed, one in the datacentre, the other in the office. The Bridge connection between the iQuila Cloud to the Datacentre has DHCP disabled and just bridges the Datacentre to the Cloud. The Bridge connection from the iQuila Cloud to the Companies Office as DHCP enabled and is located behind the Router / Firewall that is running the DHCP service for the office, (although this could be run from the datacentre). Remote users connecting to iQuila Cloud will get a DHCP IP address from the office DHCP server. App, Printers, and any IP addressed device at the company office that reside on the same subnet as the hosting environment will be available to all. Also in this configuration is a secure home worker accessing very confidential information and using a IP phone is achieved using an iQuila 500 hardware bridge.

iQuila Cloud, Bridging multiple Office and Public Cloud Hosting.

In this configuration, we are linking 3 offices, Public cloud Hosting, and giving Seamless secure always-on remote working. A bridge is installed at each office location, each office is configured on the same subnet and the client have seamless access to the service of both locations, installing the iQuila client on the Public hosted server also brings this server into the network securely enabling the hosted firewall to be restricted, applications such as Veeam and VMware can we used for Replication from office to office with instant failover and no need for reconfiguration of IP addresses.