iQuila Cloud to Overlay Networks

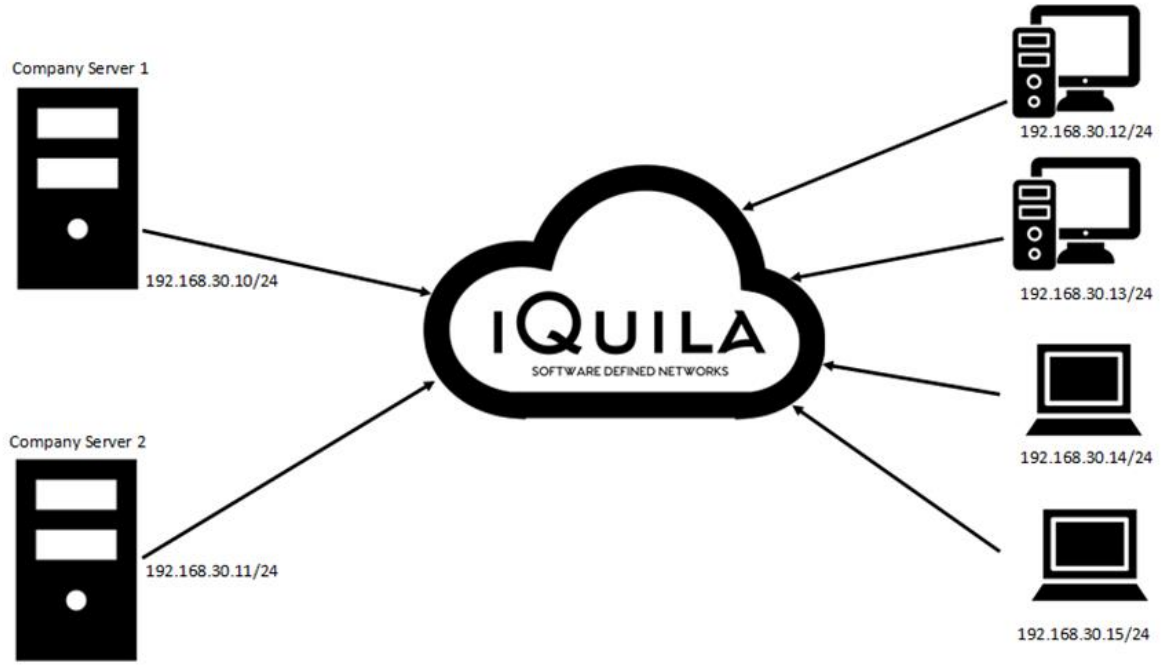
IQ22061r2

This Document Applies to:

iQuila Cloud

iQuila Cloud Overlay Network.

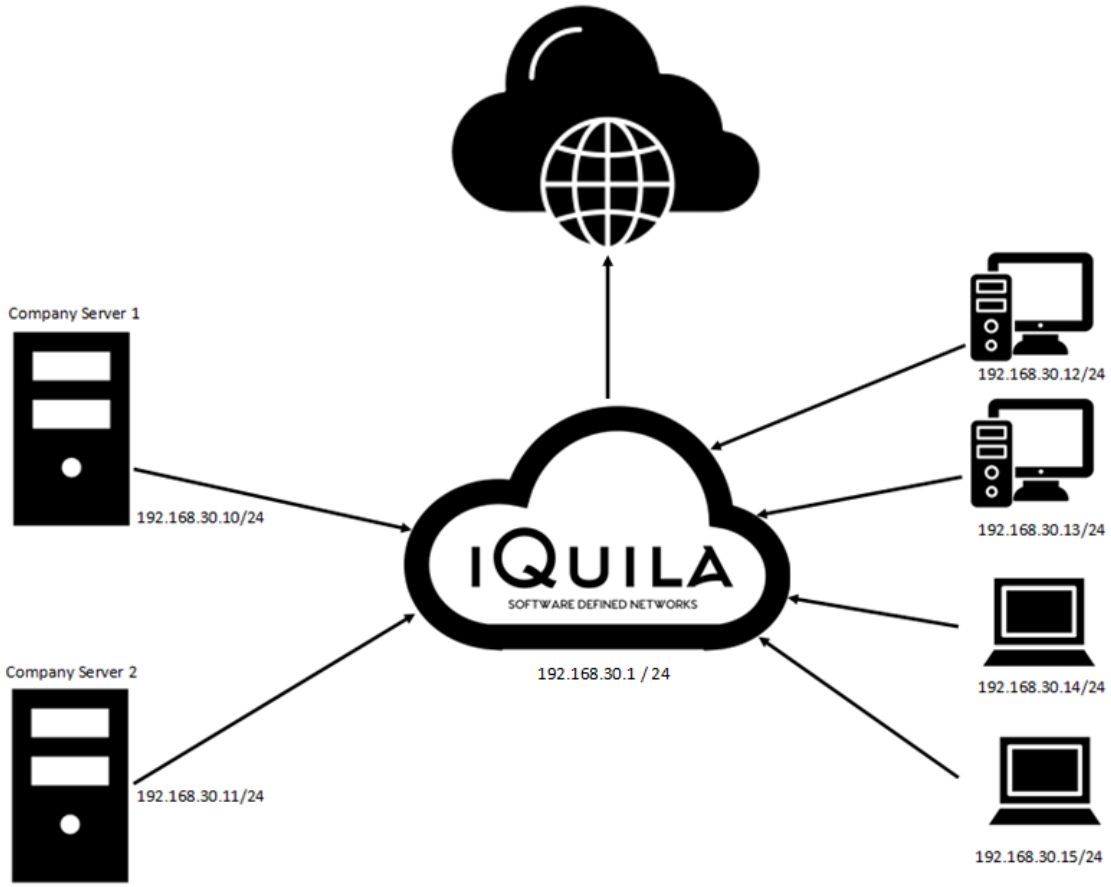
This configuration is quick and simple to deploy giving all remote users always-on secure connectivity to the office Servers.



In this configuration of the Overlay network, NAT is enabled on the iQuila Cloud. And all the clients are deployed to company servers and remote client computers/laptops. The iQuila cloud will issue a 192.168.30.* address range as default to all iQuila clients. DNS Resolution two internal hostnames are automatic and dynamically updated in the iQuila Cloud.

iQuila Cloud Overlay Network with Secure NAT routing.

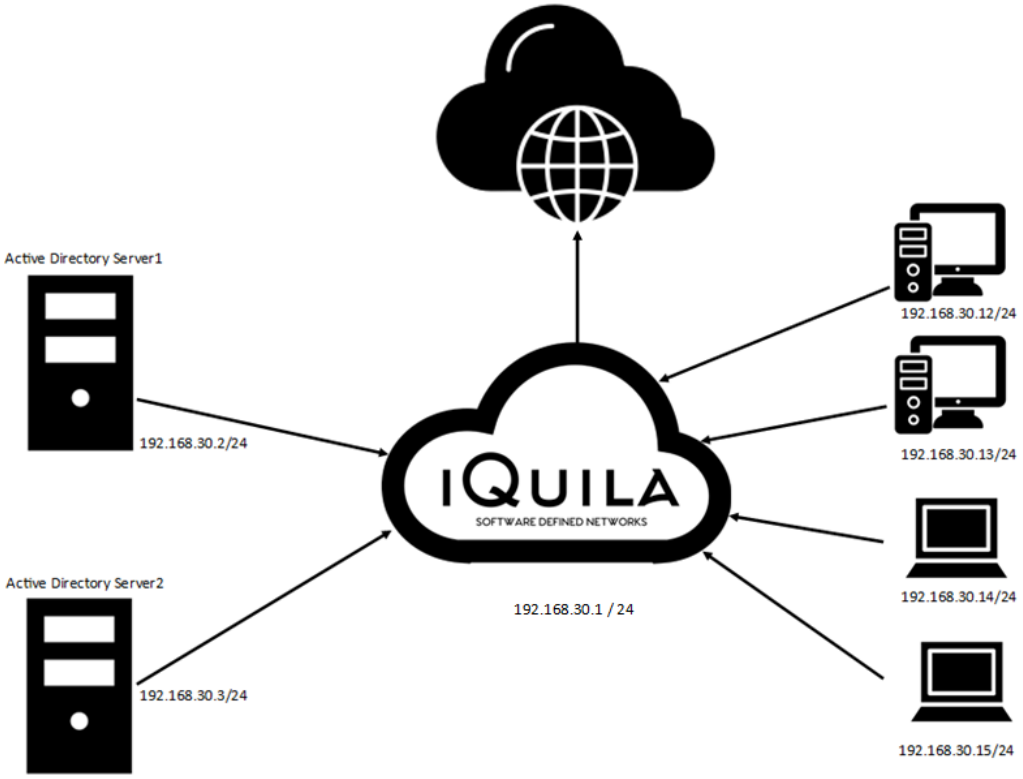
This configuration is a quick and straightforward way to deploy, giving all remote users always-on secure connectivity to the office servers.



In this configuration an Overlay network, NAT and Secure Gateway is enabled on the iQuila Cloud and the agent is deployed to company servers and remote client computers/laptops, the iQuila cloud will issue a 192.168.30.* address range as default to all iQuila clients and a Gateway of 192.168.30.1, DNS Resolution two internal hostnames is automatic and dynamically updated in the iQuila Cloud, Network Metric configured on the server to a higher value, this configuration will route all traffic for Clients via the datacentre, company traffic will be directed to the server and internet traffic is router via the datacentre keeping all client connections safe and protected against rogue Wi-Fi access points. Also, the server traffic routing as not changed.

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

This configuration is quick and simple to deploy giving all remote users always-on secure connectivity to the office servers with full active directory Login.

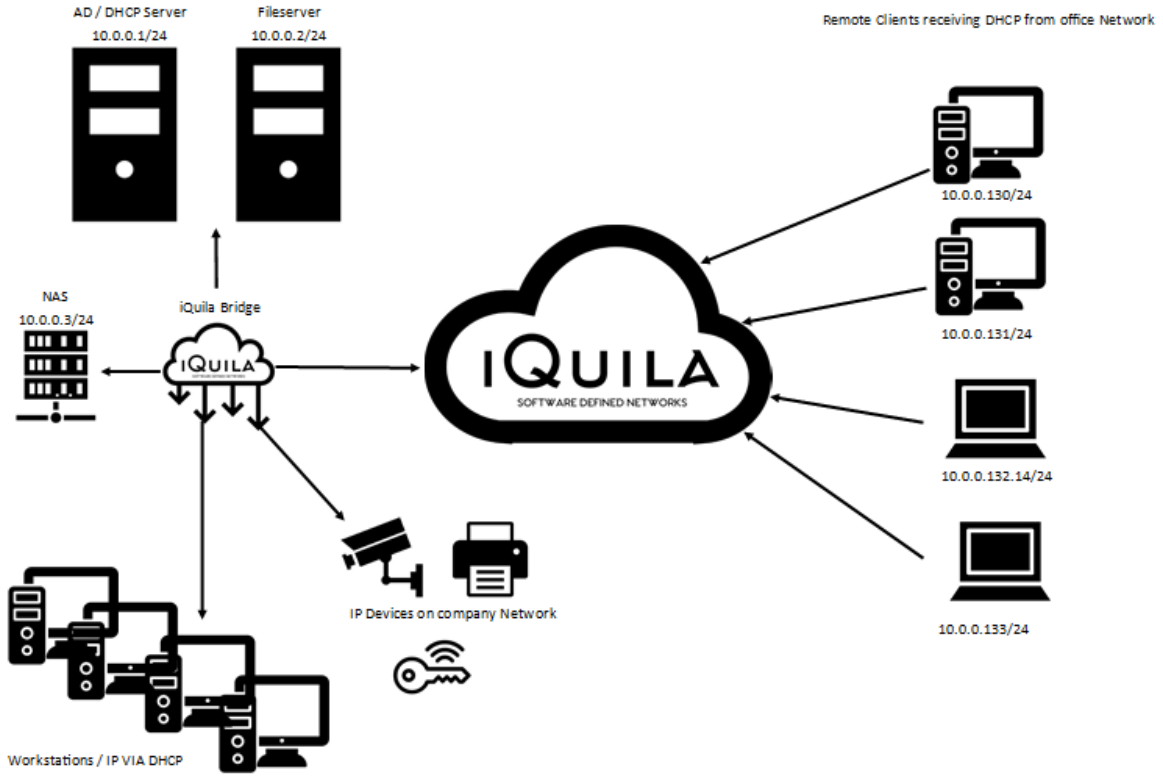


In this configuration, an Overlay network, NAT and Secure Gateway is enabled on the iQuila Cloud and the agent is deployed to company servers and remote client computers/laptops, the iQuila cloud will issue a 192.168.30.* address range as default to all iQuila clients and a Gateway of 192.168.30.1, the client software should be deployed to every active directory server and assigned with a static IP address in the same subnet as the iQuila Cloud clients, Network Metric configured on the server to a higher value, the DNS on the iQuila Cloud should be configured to the static IP address you set of you Active Directory servers, this configuration will route all traffic for Clients via the datacentre, company traffic will be directed to the server and internet traffic is router via the datacentre keeping all client connections safe and protected against rogue Wi-Fi access points. Also, the server traffic routing as not changed.

The client will now have full access to Active Directory login with full Group Policy just as they were located on the domain in the office.

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 software or an iQuila Hardware Bridge.

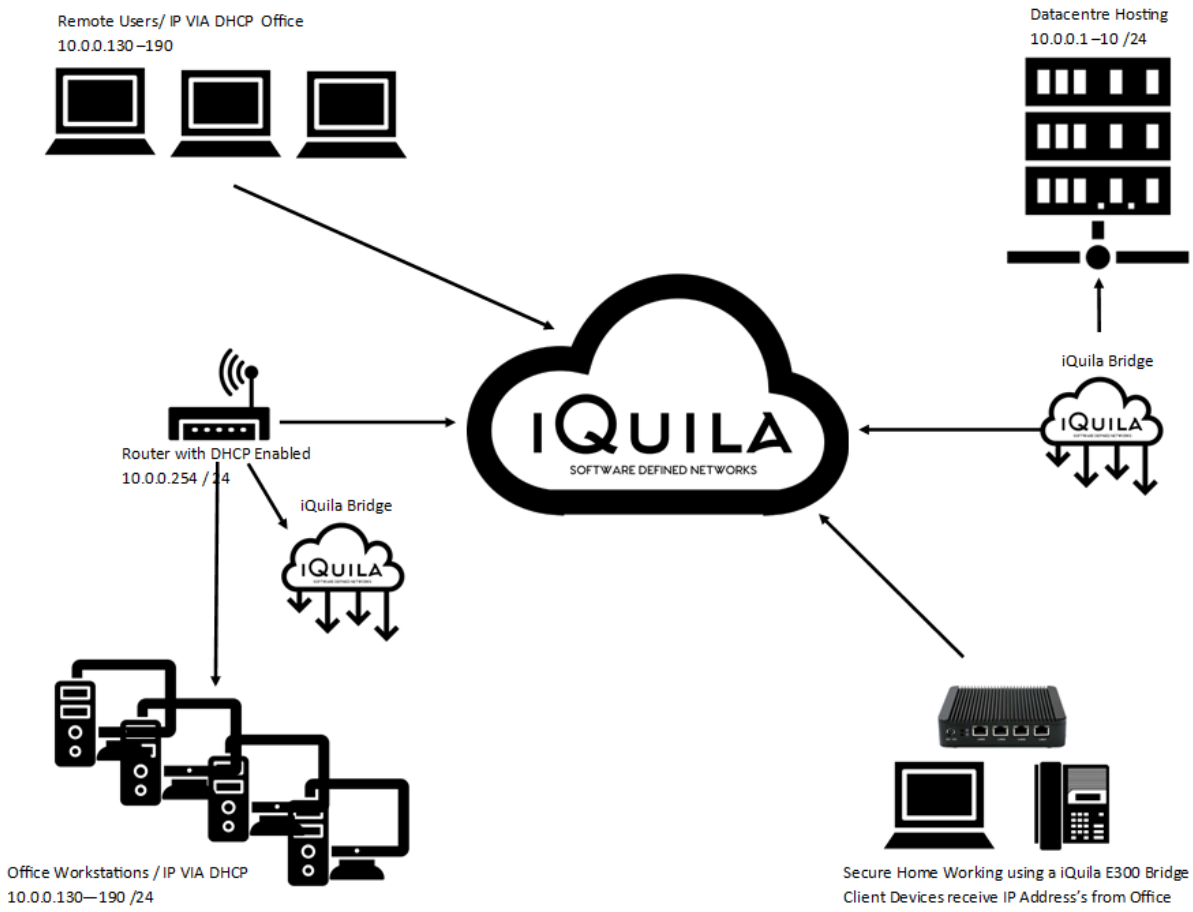


The iQuila Cloud is configured with NAT Disabled and a Bridge device created allowing DHCP on the Tunnel, all client will receive a DHCP address from the Office DHCP server and will have the same functionality as the client is located in the office, all traffic for Internet if routed via the office gateway, all remote clients will have access to any IP device on the internal office network.

To enable split tunnelling, simply change the matric on the iQuila Virtual network adaptor to a higher value. Internet traffic will now route from the remote device locally.

iQuila Cloud Bridging extending your Cloud network to 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.



The Bridge connection from the iQuila Cloud to the Datacentre has DHCP disabled, and the Bridge connection, from the iQuila Cloud to the Companies Office, DHCP is enabled on the connection, an iQuila Bridge is located behind the Router / Firewall, this device also has Local DHCP running (although this could be run from the datacentre) app Workstations Printers at the company office reside on the same subnet as the hosting environment, remote users access the network via the iQuila Cloud and revive and IP address front the company network, also joined is a secure home worker accessing very confidential information, this 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.