Published on *Cloud Hosting and Virtual Data Centre help* (http://cloudhelp.claranet.com)

Securing your appliance

As with any IT infrastructure, you should take steps to secure your Virtual Appliance against security risks, both internal and external. This help page is not intended to replace any best practise used in your organisation, but covers specific steps you may choose to take to mitigate the risks you feel are important to your organisation and which are appripriate to the application you are running in the Virtual Appliance.

Remember, unless you've configured multiple private VLANs, your Appliances will be connected using the default network. This means you *should* only need one firewall for all your Appliances on the default network, but do ensure you consider all your connectivity before you connect an Appliance to any internet access network.

Shared Internet Access (SIA)

The Claranet Cloud Shared Internet Access network provides a range of IP addresses across all customer environments in a physical datacenter. It is important to understand that this is a public network which extends the internet to your Virtual Appliance. You should treat this as with any other internet connection and take suitable security measures, such as implementing a virtual firewall appliance, hardening your operating systems and monitoring logs for intrusion attempts.

If you would like Claranet to provide you with a managed firewall service, please contact your account manager. With such a service you will have a dedicated connection from your Appliance to the managed firewall, and would not use the Shared Internet Access network.

Dedicated Internet Access (DIA)

If you have purchased Dedicated Internet Access connectivity, you will get a dedicated range of IP addresses registered to your company. Please understand that the same security risks apply to DIA as with SIA - you should consider a firewall, either virtual or as a managed service.

Passwords

When a Virtual Machine is deployed from an image, it uses the default username and password from the image. Please ensure that you change this password to match your organisation's security standards.

You should also ensure that you set a remote access password for all Virtual Machines. This

is done in the configuration page for each VM.

Denial of Service (DoS) attacks

Claranet protects the Cloud platform from denial of service attacks by blackholing traffic to machines under attack. This protects other machines at the expense of the machine which is being attacked by throwing away the attack traffic along with other traffic to that machine. If you would like a more sophisticated approach which offers a higher level of protection, please contact your account manager.
