ukcloud

Pure commitment.

BRING YOUR OWN FIREWALL TO UKCLOUD

version 2.0

CONTENTS

OVERVIEW

This blueprint discusses how you can install your own networking device in the cloud (effectively bringing your own firewall).

In this blueprint, we will focus on the deployment of two commercially available firewalls; Palo Alto next generation firewall appliance and a pfSense network firewall distribution built upon FreeBSD. However, you can utilise the steps outlined in this blueprint to deploy a technology of your choice.

One of the key components of any cloud solution is the capability of the networking components utilised by the cloud infrastructure.

Historically, UKCloud have required all users of its cloud platform to utilise the vCNS edge device provided as part of the initial deployment.

For some customers, their requirements exceed what is natively capable in the VCNS Edge device:

- The existing solutions do not scale neatly to accommodate to complex enterprise solutions now being hosted on the cloud.
- Increased capability available in commercially available alternatives, opening access to a range of advanced features, such as active content inspection, packet filtering, policy traffic management, centralised management and application whitelisting.
- Leveraging existing internal expertise in a 3rd party solutions – such as Palo Alto. Often customers have built up a capability in a technology that meets their requirements, and the retraining and redevelopment overhead can be quite high for new technologies.

Note! The use of Palo Alto and pfSense in this document should not be an endorsement or support capability for these technologies.

vCNS Edge Device

Before undertaking the steps to install your own firewalls, you should ensure that the vCNS network device cannot satisfy your requirements. For the majority of environments, this device performs well and is proven to be suitable for production workloads. This device is a virtual network appliance and can assist you with virtual networking and provide a networking gateway into and out of your environment, as well as basic networking. Utilising features including; IP firewalling, network address translation, VPN access/endpoint termination and IP load balancing.

If the vCNS Edge device is not appropriate, read on to discover how to install your own gateway device.

UKCloud deployment of a VDC without an vCNS device

To start the process, raise a new Support Call 'My Calls' section of the UKCloud Portal, selecting:

1. How can we help you? – *I am requesting information on/administration of my service*
2. Select Product – *Connectivity (N3/HSCN, PSN, IP Addresses)*
3. What is the nature of your query? – *Add a new service*
4. Request summary – *I would like an internet connection for my VDC (BYOF)*
5. Please provide any further details regarding your request - *Please can you provision a network to <insert VDC Name here> for me to attach my firewall to.*

Provision your VDC through the UKCloud portal as normal however do not select "Build Edge Gateway" and you are then free to deploy the chosen appliance in your new VDC connected to the network created in your Support Call.

Regardless of what technology is deployed, the same provisioning method will need to be used.

As detailed in figure 1, there are distinct areas of responsibility:

- We will provision 'external' transit networks to VDC from the UKCloud managed firewalls.
- You will be responsible for everything below the provisioned network. We cannot provide any support of the boundary area.

Further details can be found in the Bring Your Own Firewall service scope, available from the UKCloud knowledge centre.

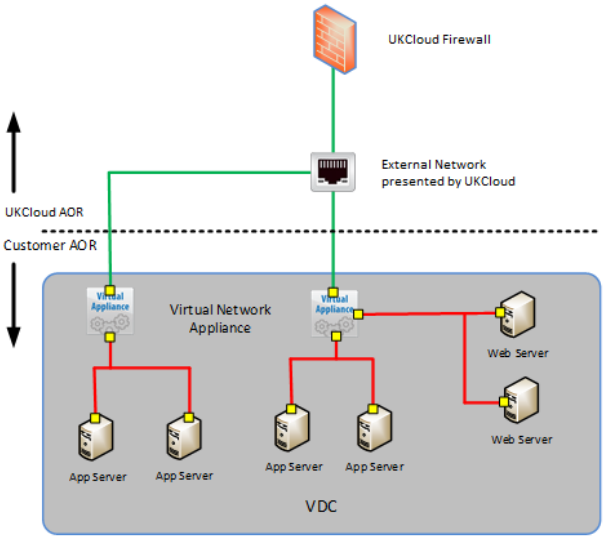

Figure 1. Network topology and areas of responsibility

Common amongst any deployment without a vShield edge is the provisioning of isolated organisation or vApp networks depending on your network design.

The inline UKCloud managed firewall will sit in front of your VDC as normal with the same rules and rulesets applied to them.

The diagram below shows a green external network that will be provisioned via a service request, the yellow and red networks will be provisioned by you. These networks will attach to the virtual appliance and depend upon whether the configuration, rulesets, and policies will manage traffic and data flows.

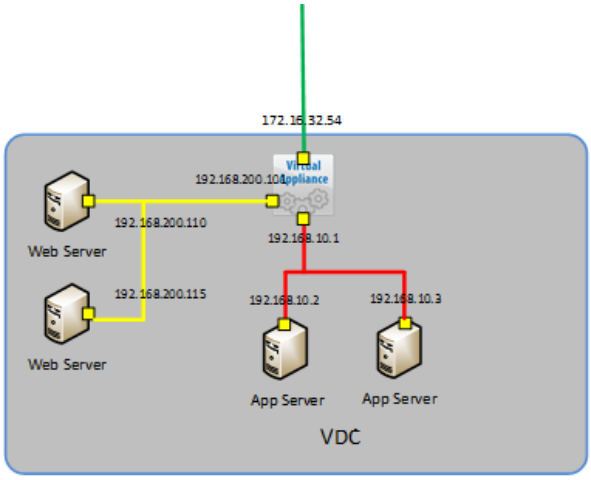

Figure 2. Network topology including the chosen networking virtual appliance

IMPORTANT! Please be aware that creating isolated networks via the vCloud GUI will **always** deploy a vShield in the back end until any edge gateway services on the network are disabled. This is because the GUI instinctilvely believes that a DHCP server is required.

Please note that if isolated networks are created via the API without explicitly defining that no DHCP service is required, then a new vCNS Edge will be deployed in the background leading to possible configuration issues.

When creating a new Org VDC Isolated network, ensure the DHCP option is unchecked. This can be done from **'Configure Services'** of the network you created.

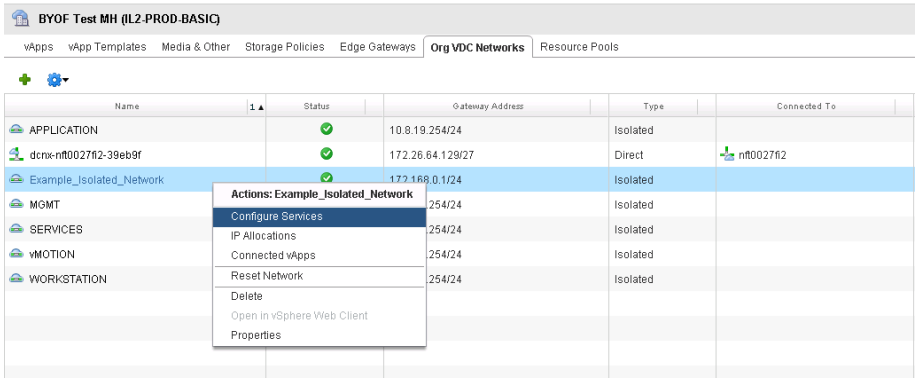

Figure 3. Configuring services on an external network in vCloud Director

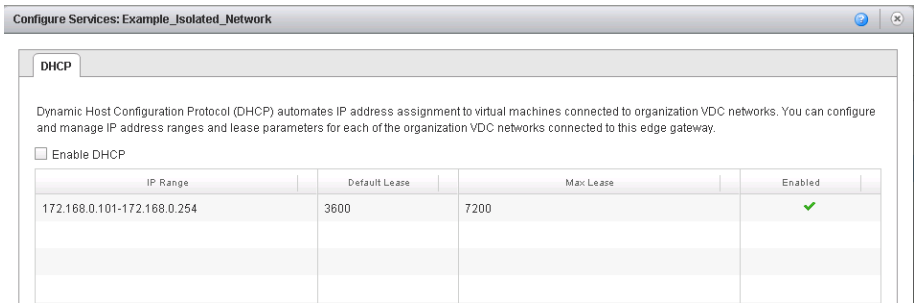

Figure 4. Disabling DHCP setting to avoid creation of vCNS devices

Checking which external IP addresses, you have assigned

Once you have installed a firewall of your own choice, you can check the details of available networks using the following method:

1. Go to the administration tab of your VDC
2. Select Org VDC Networks.
3. Locate External Network Object (highlighted in light blue in figure 5 below)
4. Right click, select properties

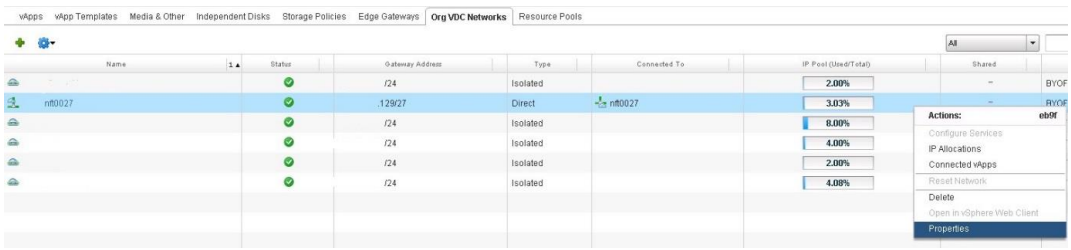

Figure 5. Selecting the External Network Object

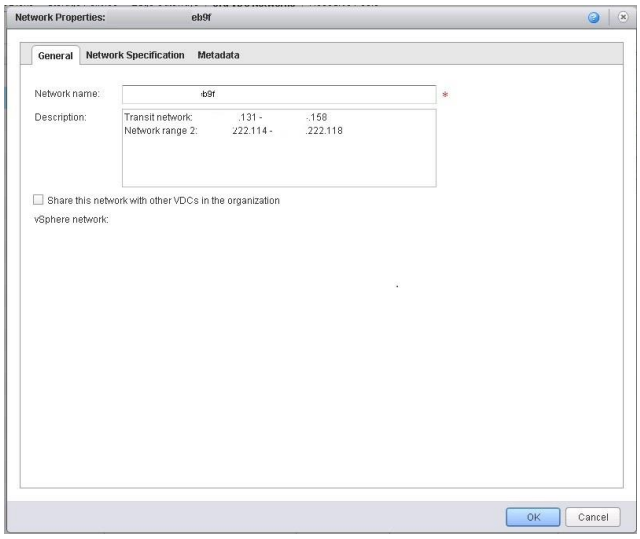

Figure 6. Retrieving external network information

Information from external networks is added to this section when the BYOF is initially configured.

Example 1: Virtual Networking Appliance Palo Alto

We will now look at the deployment of the Palo Alto device on our Cloud. In our demonstration we are using the following software version:

Palo Alto VM300 running PanOS 7.01

IMPORTANT! All commercial agreements, support and licensing will need to be procured through a Palo Alto reseller. We do not offer support for Palo Alto devices, or commercial mechanisms for purchasing the licencing.

1. Once the external network has been provisioned, you can deploy the Palo Alto appliance from within vCloud Director
2. Download the appliance from the Palo Alto website, redeem the activation code against the product and ensure you have the correct access to your company's online Palo Alto web portal
3. The package from Palo Alto will be in an OVF (Open Virtualisation Format) file type. The easiest way to deploy this will be from the vCloud director catalogue so you will need to upload the OVF via the Java Plugin – see end of the blueprint for details
4. The Palo Alto Appliance OVF is now stored in your private catalogue you can now deploy the appliance directly into a vApp. An onscreen wizard will guide you through deployment
5. Please refer to current Palo Alto documentation and guidelines before deployment found at (registration required): https://support.paloaltonetworks.com
6. Once the device is deployed successfully and powered on, you can manage the appliance from the console to configure

There are a couple of points of interest for users of the Palo Alto device:

- Firstly, Network Interface Controller (NIC) is used for management traffic
- NICs are discovered during boot so you can't 'hot add/remove' them to/from the device

- All virtual machines have a maximum NIC count of 10 in vSphere 5.5/6.0

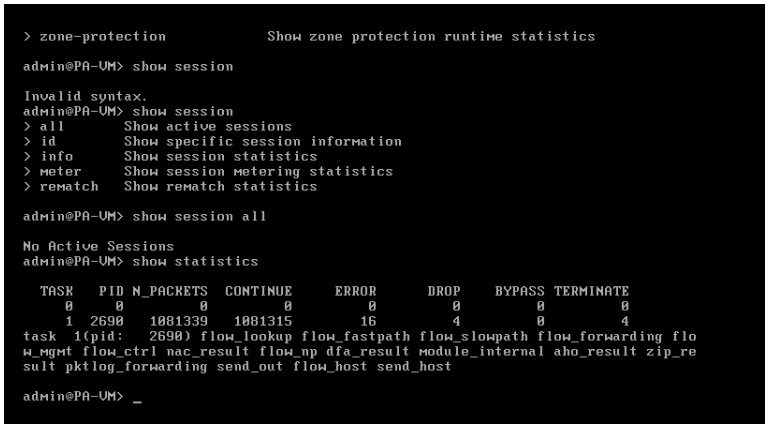

Figure 7. Palo Alto Console

7. Having the networks provisioned before you deploy the appliance will make configuration easier. As there is no vShield Edge device deployed, you must create isolated vOrg networks and attach them to the Palo Alto device as needed.

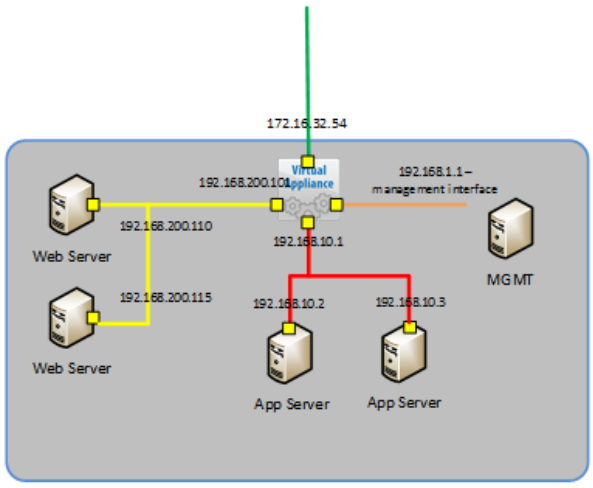

Figure 8. Topology of networks connected to a Palo Alto device

8. You are now ready to go. Management of the device can be via:
   - Command Line Interface (CLI)
   - PALO Alto RESTful API
   - Web interface

You can opt for centralised management with Palo Alto Panorama software. More information is available here.

Example 2: pfSense Networking Firewall Appliance

pfSense is a freely available open source firewall which is available to download from the pfSense community: https://www.pfsense.org. You should download and extract the GZ (GNU Zip) to obtain an ISO disk image for deployment.

In our demonstration, we are using the following software version:

pfSense v2.2.4 i386. Use the Java Plugin – see end of the blueprint for details. To upload the ISO to your vCloud Director catalogue.

1. You will need to create a VM from scratch and mount the pfSense ISO and boot to it. This initial deployment provides you with more customisation options and control over the scale and resources allocated to the device.

Note! This VM will be billed by UKCloud under its current G-Cloud pricing structure

2. When building a VM there are a few options that you will need to configure – please see current information at the pfSense community:
   - Select FreeBSD (32/64bit) from the other OS option
   - Size CPU and RAM based on your use case
   - Provision the NICs needed for the device - selecting the VMXNET3 adaptor type. This modern adaptor will perform better than the e1000 type

Note! On older packages em0 will always be allocated to the 'WAN' side of the device.

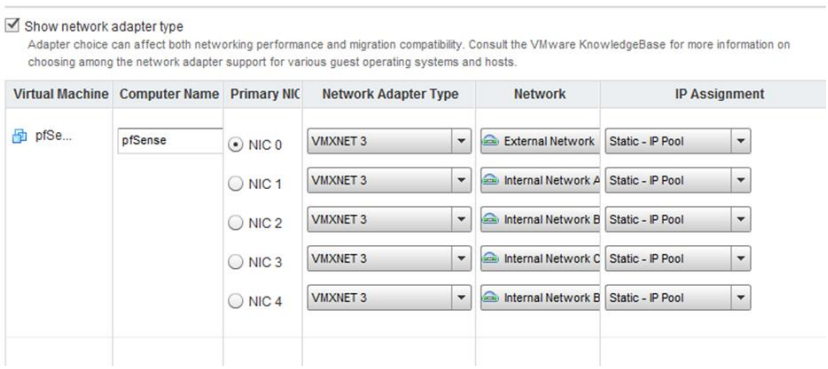

Figure 9. Configuring NICs on your pfSense virtual machine

3. Under SCSI controller select the LSI Logic Parallel. Select the amount of disk space required for the device – 1GiB is minimum but 8GiB is set as the default.

Note! The configuration presented above is a guideline and the pfSense online community are very active and will help with any sizing or configuration issues you may have.

4. Once the VM is built, attach the software ISO and boot the machine to the CD-ROM drive.

Right click from the console and select 'attach CD-ROM from catalogue'. Open the console once powered on and follow the configuration GUI under documentation consultation from: https://doc.pfsense.org.

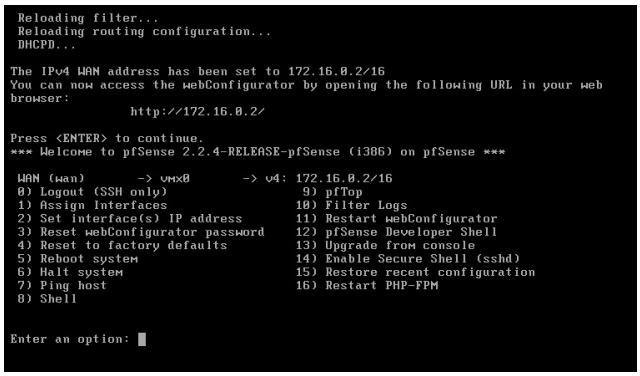

Figure 10. pfSense console

Once the image has been installed to the disk and the appliance has rebooted, your device load is complete and you can configure the device via the following mechanisms:

- The CLI
- The webConfigurator tool
- Navigating the 'WAN' IP.

Once configuration has been completed, you are ready to use the pfSense firewall on the UKCloud platform.

Uploading to the vCloud Catalogue using the Java Applet

Populating the vCloud Director Catalogue with version controlled source software allows you to be able to store a variety of images (vApp Template, VM Template, OVF/OFA, ISO and FLP) for future configuration controlled release. You can transfer existing vApp or VM images to the catalogue, however to get external images you must use the Java catalogue applet.

In your private organisation catalogue, select the upload icon and the applet will be launched (dependency on JRE installed on your client). Select the image type to upload and wait, depending on connection speed and image size.

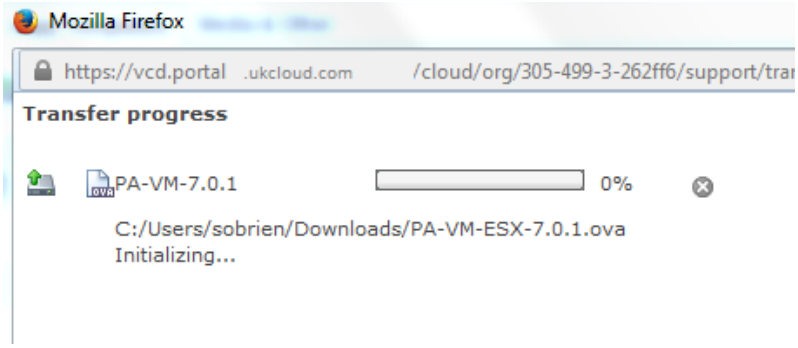

Figure 11. The Java applet presented by Firefox

Once the image is uploaded it can be copied and sorted into folder structures and have relevant permissions applied on them.

Reference

Customers that are deploying alternatives to the vShield Edge (either the ones listed above or others) are encouraged to provide feedback and engagement with UKCloud so we can make amendments to blueprints and keep these documents as current as possible.

Any customer benchmarking or performance testing results would be really appreciated to help gather information about the utilisation of the platform.

Documentation used is available from:

https://support.paloaltonetworks.com

https://www.pfsense.org/get-support/

MORE INFORMATION

For further information about UKCloud and how we can help you, please email us at info@ukcloud.com.

ABOUT UKCLOUD

UKCloud is dedicated to the UK Public Sector. We provide assured, agile and value-based true public cloud that enable our customers to deliver enhanced performance through technology.

- We're focused on cloud. Delivering a true cloud platform that is scalable, flexible, assured and cost-effective.
- We're open. You are never locked in. Using industry standards and open source software we enable flexibility and choice across multiple cloud solutions.
- Dedicated to the UK Public Sector. Our business is designed specifically to serve and understand the needs of public sector organisations.
- We develop communities. We bring together communities of users that are able to share datasets, reuse code, test ideas and solve problems.
- Customer engagement. We will only be successful if our customers are successful. We embody this in the promise: Easy to adopt. Easy to use. Easy to leave.

Additional information about UKCloud can be found at www.ukcloud.com or by following us on Twitter at @ukcloudltd.

UKCloud. The power behind public sector technology.

UKCloud Ltd

A8 Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX

T 01252 303300
E info@ukcloud.com

www.ukcloud.com

@ukcloudltd
ukcloudltd
ukcloud-ltd

UKC-GEN-310 • 09/2017 • version 2.0