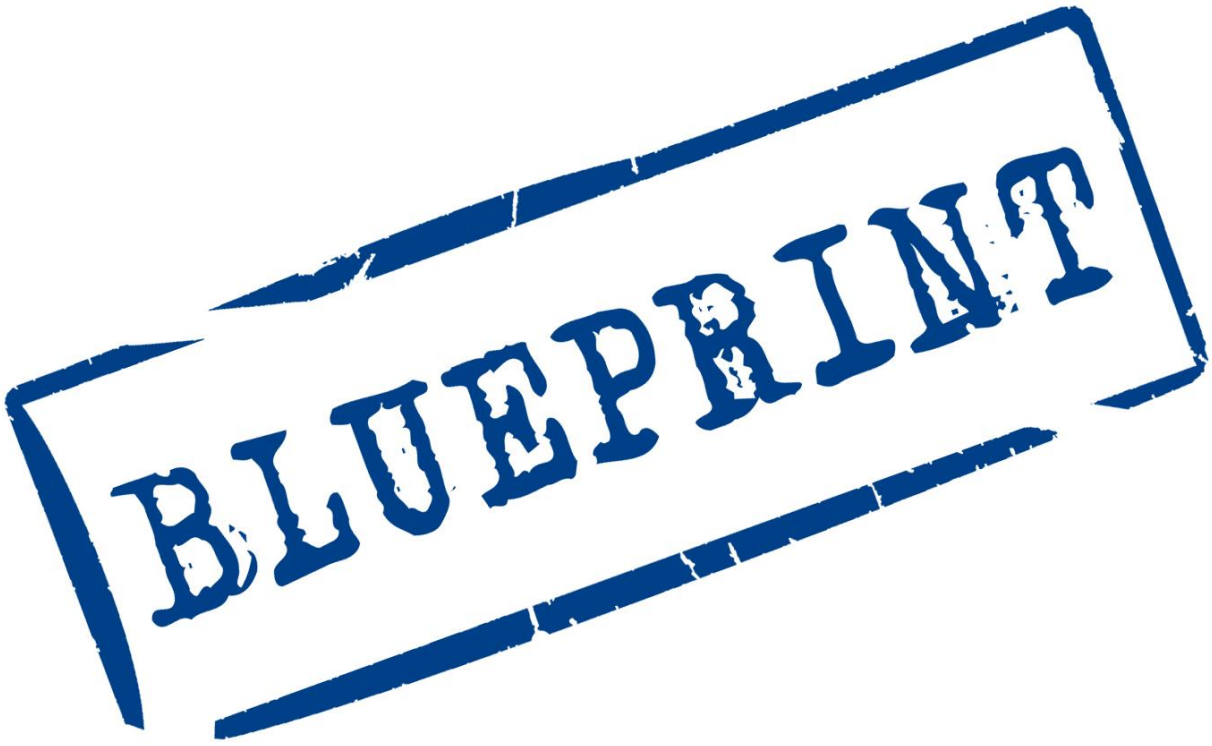
ukcloud

Pure commitment.

UKCloud Building a Multi-tier Application



UKC-GEN-112

INTRODUCTION

Government systems are increasingly digital, allowing for services to be shared across government organisations as well as enabling citizens to engage and transact with those systems online. In this context, systems are moving from being entirely isolated in closed communities to becoming citizen-facing and open to wider communities of users.

To maintain security in this new context, it is essential that systems implement 'defence in depth' (also known as deep or elastic defence) to ensure there are layers of controls between the untrusted Internet and the precious data assets.

One approach is to implement 'n-tier' architectures. For example, the system could have a web tier which is open to all users, a data tier which can never be accessed directly by users but is open to other application tiers to allow indirect access. There could also be a management tier which can only be accessed by trusted administrators.

This Blueprint will provide guidance as to how a three-tiered virtual environment can be built on the UKCloud Platform with advice on how a Bastion Host can be implemented – providing an additional layer of user authentication in scenarios where access and management is required over the Internet.

IN THIS BLUEPRINT

HOW TO BUILD A THREE TIERED VIRTUAL ENVIRONMENT

When designing the environment for this scenario, the key requirement is to provide separation between the different tiers of the application. This is done by configuring the virtual firewall (vShield® Edge Gateway) to create virtual networks or tiers.

In the diagram below the four security tiers (virtual networks) can be seen, together with the UKCloud-managed physical firewall and the customer-managed vShield® Edge Gateway virtual appliance.

The first part of the environment to note is the Bastion Host, named “Jump Off”. This server is a Linux server that can be accessed from the Internet via SSH and, following successful authentication, administrators can access the various servers in the infrastructure. Alternatively, a Windows Jump Off server could be used, with users first establishing a VPN prior to using Microsoft Remote Desktop Protocol (RDP/MSTSC) to access the Windows server.

Fig 1. Four security zones with firewall

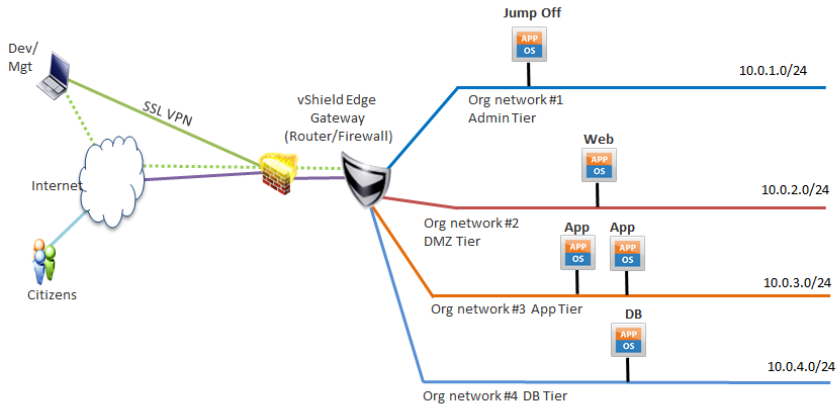


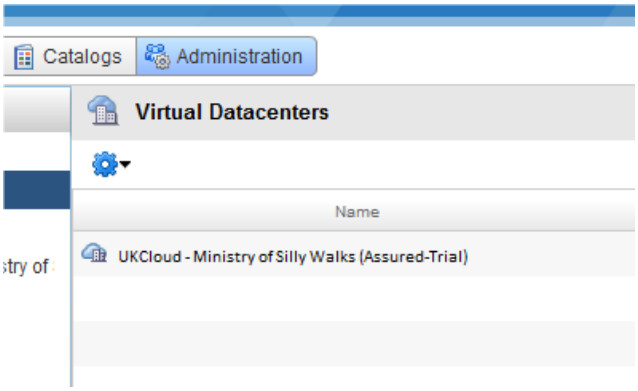
Figure 1 also shows servers for Web, Application (App) and Database (DB) roles which are each in segmented network tiers. Access to, from and between these network tiers is controlled by the customer-managed virtual firewall (vShield® Edge Gateway). By default, the virtual firewall is configured to block all access as part of a ‘Secure by Default’ security policy implemented by UKCloud. The remainder of this Blueprint describes how a customer should configure their virtual firewall to:

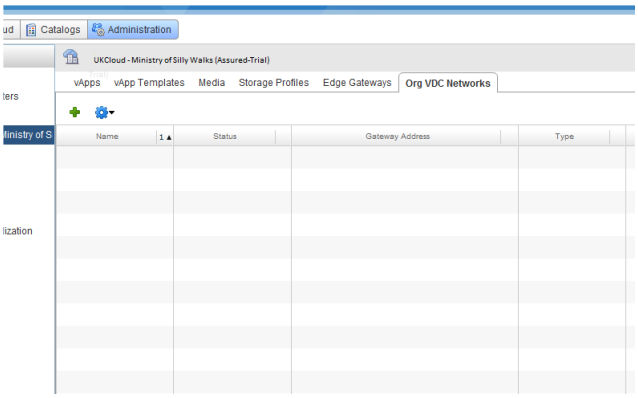
- Only allow inbound internet access into the web server (internet users cannot directly access the App or DB servers)
- Only allow access from the web server to the App servers (not directly to the DB server)
- Only allow access from the App server to the DB server

CREATING THE VIRTUAL NETWORKS

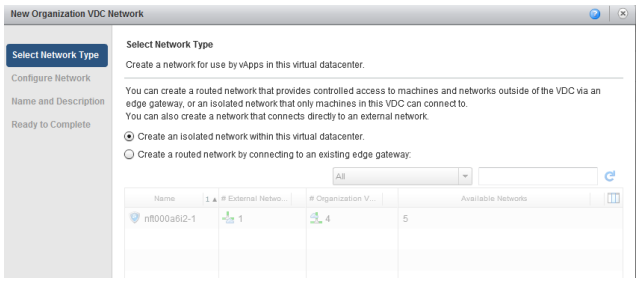
When setting up a cloud environment, it's important to have already decided how to segregate the various VMs from each other from a security perspective. This will help define the virtual networks that will either route via the vShield® Edge Gateway (and to each other), or be isolated from the vShield® Edge Gateway and use VMs to have two or more network interfaces and act as routers between the virtual networks. Just because a virtual network is routed via the vShield® Edge Gateway does not mean that it will have internet access – this will have to be specifically enabled through the use of a Source NAT (SNAT) rule (described later).

As part of UKCloud's 'Secure by Default' policy, all access is denied unless the customer allows it themselves. It is necessary to set up SNAT, Destination NAT (DNAT) and firewall rules to enable access. In order to create virtual networks, select the Administration tab in the UKCloud Portal, and then double-click on the Virtual Data Centre (VDC) that you want to work in.





Now click on the green '+' symbol to add a virtual network (circled above).

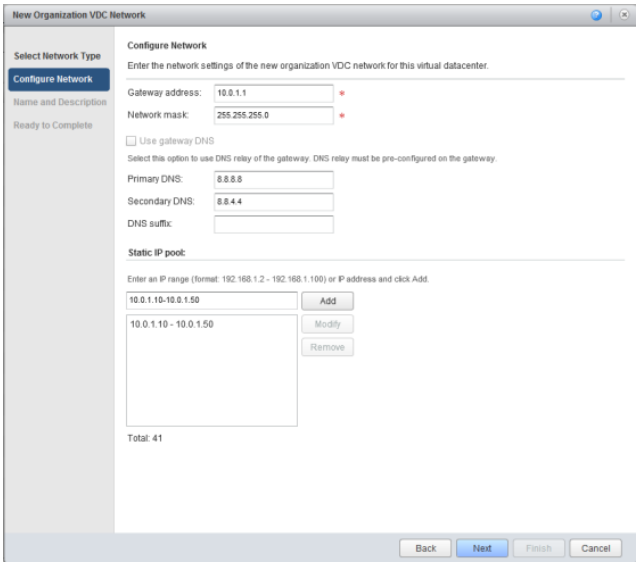


Two options are now presented.

- An isolated network is not connected to the vShield® Edge Gateway and so, by itself, cannot connect with any other virtual network. This can be used for certain use cases where VMs need to be kept isolated from other networks.

- When choosing the Routed Network option, you must also select the vShield® Edge Gateway to route via, otherwise you will see an error message.

For the rest of this example a Routed Network is used, with the first network as the Admin network. This will have a definition of 10.0.1.0/24 with a gateway address of 10.0.1.1.



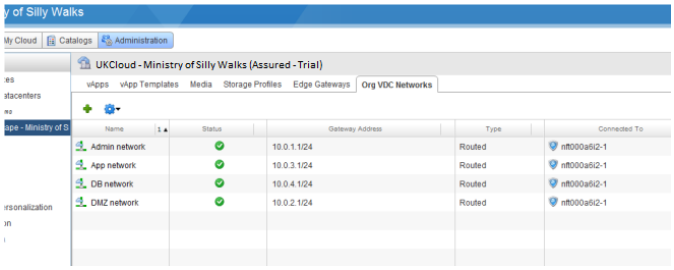
UKCloud does not provide DNS services, and so for this example is using Google DNS services on 8.8.8.8/8.8.4.4.

A static IP pool has been created with a range of 10.0.1.10-10.0.1.50. This is similar to DHCP – IP addresses will be allocated to VMs from that pool depending on how the IP allocation method is chosen (Static IP Pool, Static IP Manual or DHCP). A DHCP pool can also be defined on the Org Network if required.

When provisioning the VM, VMware Tools will inject the correct networking configuration into the VM. If Static IP Pool is chosen, then the VM will be allocated and injected with a static IP address; whereas if DHCP is chosen, the VMs operating system will have DHCP enabled.

Finally, a network name must be provided, for this example ‘Admin Network’ was used. Then click ‘OK’ to complete the operation.

Having created the other three networks, the networks will be visible in the interface.



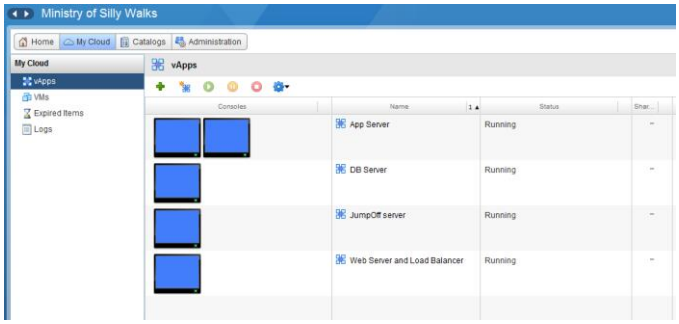
POPULATING THE ENVIRONMENT

Having created the networks, users can create or upload the various VMs that will make up the environment. In this example, a typical Java test application called Travel App is used which comprises:

- An Apache server acting as a simple load balancer
- Two Tomcat application servers
- A MySQL database server

Figure 2. VM environment as seen on home page

Figure 3. VM environment as seen on MyCloud



Note: A Linux server will be provisioned to act as a Jump Off or Bastion Host and all the VMs are running Centos Linux. The Travel App servers were imported into UKCloud as an OVF bundle, while the Jump Off server was deployed from the UKCloud public catalog.

In the screenshots below, the VMs are either on the Home page or the My Cloud page. For most, each vApp contains just one VM, but in the case of the App Server it contains two.

CREATING FIREWALL RULES BETWEEN ZONES

The various tiers of the application will need to communicate with each other over specific protocols and ports, and all other traffic will be blocked, in-line with the secure by default policy.

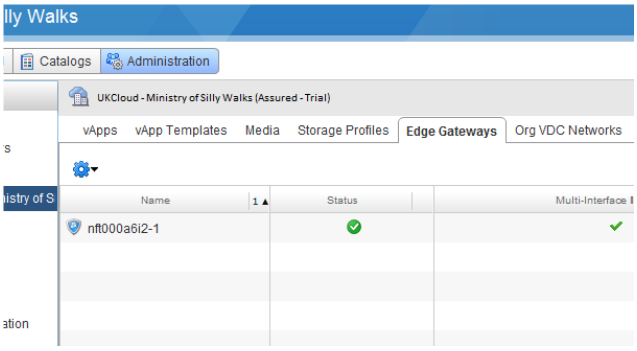
Data flow	Port/protocol
Inbound web requests from internet	80/TCP
Inbound Jump Off server access from internet	22/TCP
Cloud servers access to the internet	*/TCP
Web server to App server	8009/TCP
App Server to DB server	3306/TCP
Jump Off to all servers	22/TCP

To configure these rules, it will be necessary to access the vShield® Edge Gateway via the UKCloud Portal and set up some DNAT/SNAT and firewall rules.

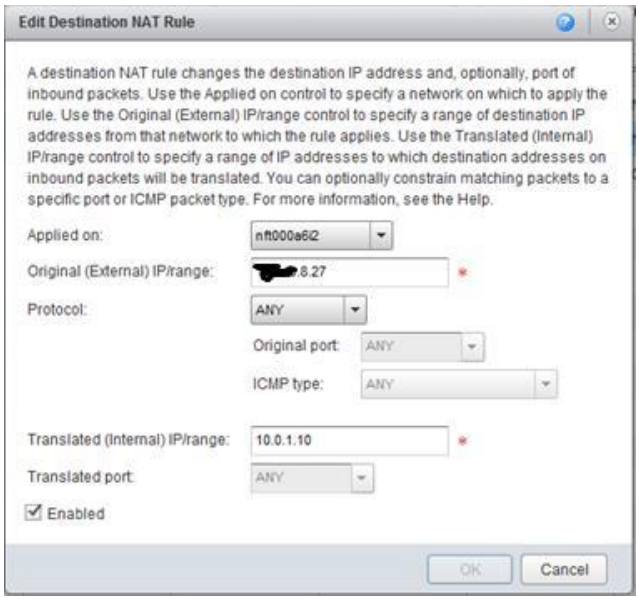
Source and Destination NAT rules

In order to allow traffic through the vShield® Edge Gateway from the Internet, a DNAT rule or rules will need to be configured.

First, browse to the vShield® Edge Gateway, and right-click on it, then ‘Configure Services’.



Here a DNAT rule is being configured to map any traffic hitting the Public IP address x.y.8.27 to an internal address 10.0.1.10 with any port or protocol (secured with a firewall rule later). This rule is to map a Public IP to the Jump Off server.



Similarly, a rule to map a Public IP to the Web server is being defined.

Note that it is possible with DNAT rules to use a Public IP address several times, and to redirect according to port or protocol. For example, port 22 could be mapped from to the Public IP address to the Jump Off server, but if the port is 80, map to the Web server. This is recommended when trying to minimise the number of Public IP addresses being used. This is sometimes called Port Address Translation (PAT).

Having defined the DNAT rules, it's important to add another layer of security by adding some firewall rules. By default, even though the DNAT rules have been defined, the firewall is set to block all traffic inbound.

Firewall rules

In the same way as with DNAT, right-click the vShield® Edge Gateway, and select 'Configure Services', and then the Firewall tab.

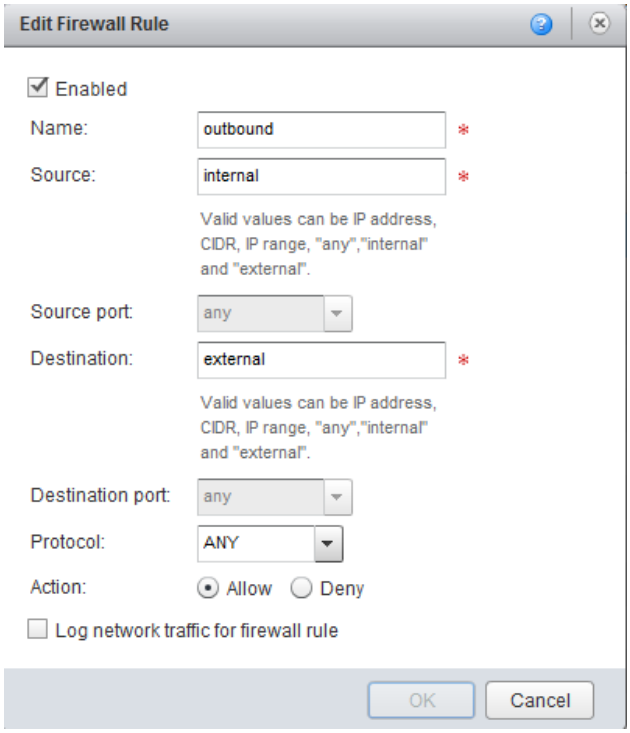
The example above shows the user creating a rule that will allow traffic from 'external' (the Internet side of the Edge) to access the Public IP address x.y.8.27 on port 22 and protocol TCP.

Note that the vShield® Edge Gateway processes firewall rules before NAT rules. With the firewall rule going through the Edge (rather than internal networks) the user is defining a rule from the external side to the Public IP, rather than external side or Public IP to internal network or address. The same applies for the Web server.

In order for servers within the cloud to access services on the Internet, it will be necessary to create a SNAT rules on the vShield® Edge Gateway. This rule will map internal IP addresses to a Public IP address. A firewall rule must also be created to allow traffic outbound.

In the example, the Admin network (10.0.1.0/24) has been mapped to a Public IP address.

This is the corresponding firewall rule to allow all traffic from 'internal' network to the 'external' interface. This could be locked down further if required.



Note that ICMP/Ping is blocked on the UKCloud physical firewalls, so it will not be possible to 'ping' a server somewhere else on the Internet.

To check Internet connectivity, using nslookup is a good test.

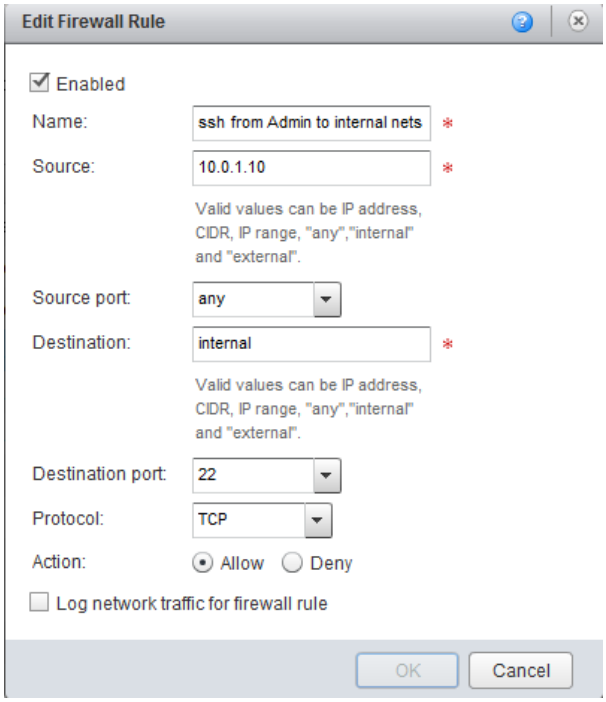
```
[root@JumpOff ~]# nslookup www.google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 173.194.35.49
Name:   www.google.com
Address: 173.194.35.50
Name:   www.google.com
Address: 173.194.35.52
Name:   www.google.com
Address: 173.194.35.51
Name:   www.google.com
Address: 173.194.35.48
```

Security between tiers

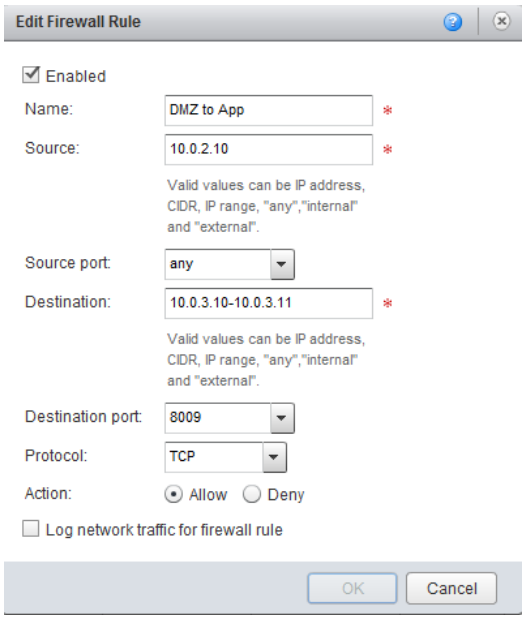
In a similar way to the previous section, the firewall rules need to be configured to allow the various tiers of servers and software to communicate with each other.

- The Jump Off server will need to communicate with all servers using SSH on port 22.
- The Web server will talk to the App servers using port 8009, and the App servers will talk to the database server using port 3306.
- There is no need for DNAT rules in this context, the vShield® Edge Gateway is acting as a router between the internal networks so we simply need to define firewall rules, as traffic is blocked by default.

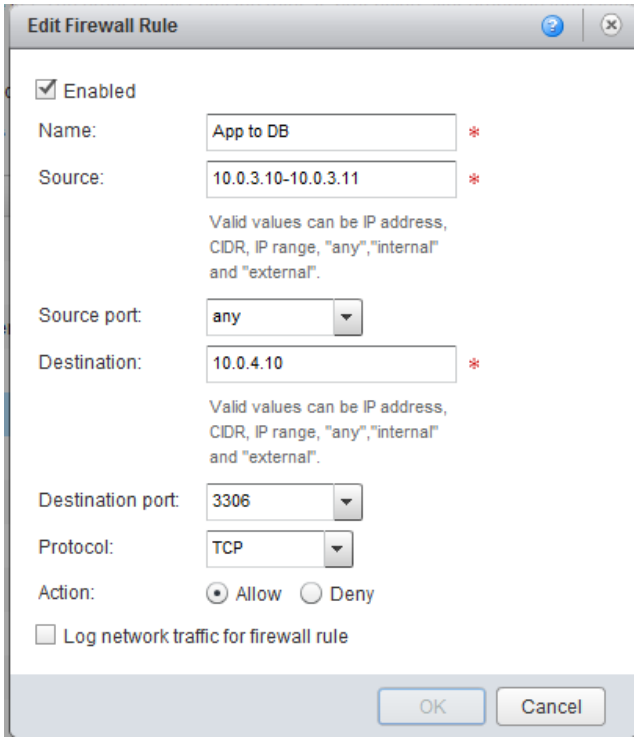
As in the previous section, navigate to the vShield® Edge Gateway, right-click on the 'Edge Gateway', and 'Configure Services'.



This rule allows SSH traffic from the Jump Off server to any other internal networks on port 22/TCP.



This rule allows traffic from the Web server to talk to the two App servers using port 8009/TCP.

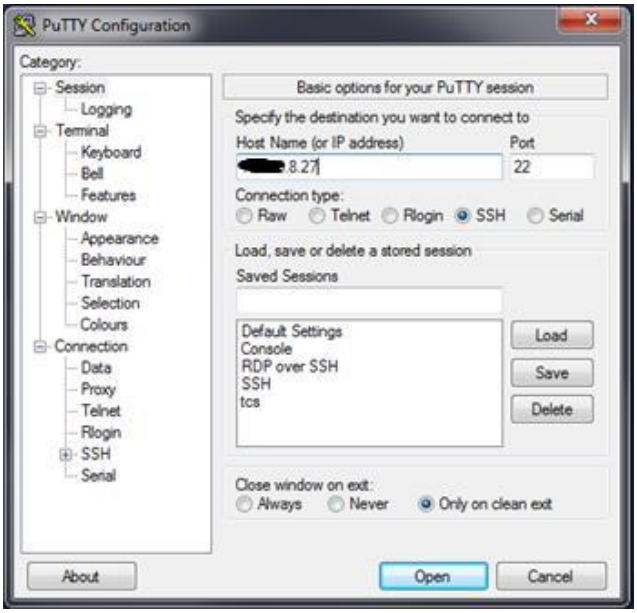


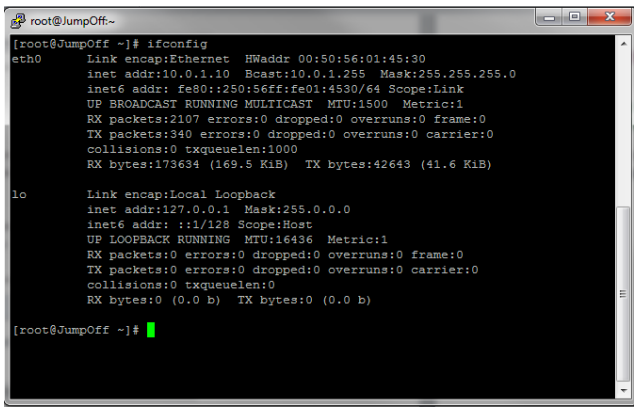
Lastly, this rule allows the App servers to talk to the DB server on port 3306/TCP.

TESTING THAT IT WORKS

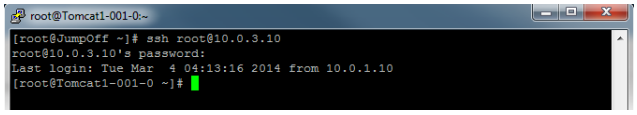
Using Putty/SSH to access the Jump Off server from the Internet

To test this aspect, Putty is used to access the Jump Off server using its Public IP address.

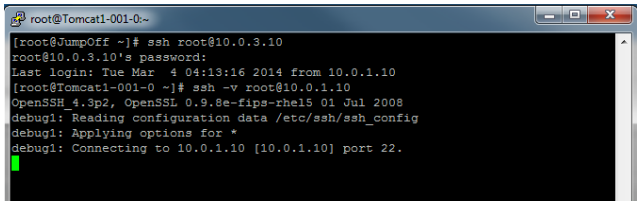




Once on the Jump Off server we can hop to each of the Travel App servers.



Note that it is not possible to go back the other way.



CAUTION: As this service will be available to anyone on the Internet, you should use strong authentication (such as complex passwords and two-factor authentication) and keep this Jump Off server regularly patched (to limit the impact of bugs such as the most recent HeartBleed vulnerability).

Testing the web application

To test that it's possible to access the web application via its Public IP address, customers should launch a web browser from an endpoint and attempt to connect to the public IP of the Web server (x.y.8.28).

ABOUT UKCLOUD

UKCloud has developed a range of cloud services designed specifically for the UK public sector, to help increase efficiencies, reduce costs, significantly improve procurement times and increase transparency. Our services are *easy to adopt, easy to use and easy to leave* to ensure that our customers remain in complete control with minimum risk. We were one of the first G-Cloud providers to achieve Pan Government Accreditation (PGA) up to Elevated OFFICIAL, and our services continue to achieve formal UK Government accreditations which make them suitable for all data at OFFICIAL (including OFFICIAL-SENSITIVE).

UKCloud's full offering consists of:

1. Infrastructure as a Service (IaaS) – seven offerings around Compute and Storage on demand

2. Software as a Service (SaaS) – offerings for email and collaboration

3. Platform as a Service (PaaS) – based upon Open Source Digital Application Platform and Hadoop which provides organisations the benefits of using a commodity cloud platform without the added management overheads

All of UKCloud's UK sovereign cloud computing services are hosted in one (or both) of our highly resilient tier 3 UK data centres in Farnborough and Corsham. UKCloud services are delivered with leading technologies from UKCloud Alliance Partners: QinetiQ, VMware, Cisco, EMC and Ark Data Centres. The Cloud Alliance also provides a collaborative resource which drives innovation and technical product development, helping to continually improve UKCloud's offering to meet the needs of the UK public sector.

UKCloud is focused on providing cloud services in a more agile, secure and cost effective manner. We strive to deliver solutions that harness technology as a way to facilitate the changes that are needed to streamline processes and reduce costs to support the UK public sector and, ultimately, UK citizens and taxpayers.

MORE INFORMATION

For further information about UKCloud and how we can help you, please send an email to info@ukcloud.com

UKCloud Ltd

A8 Cody Technology Park
Ively Road
Farnborough
Hampshire
GU14 0LX

+44 (0)1252 303300

info@ukcloud.com

www.ukcloud.com

UKC-GEN-112 • 07/2016