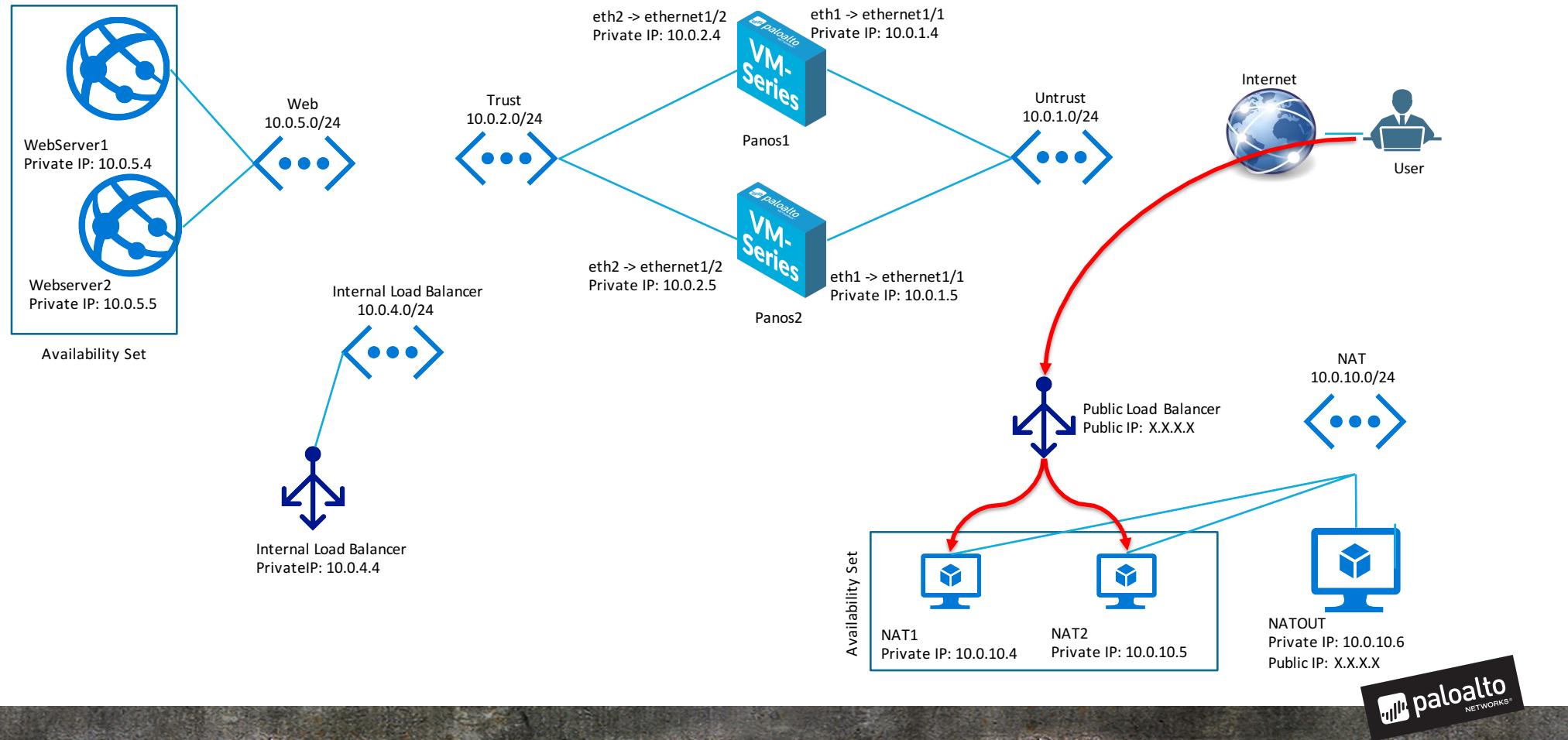




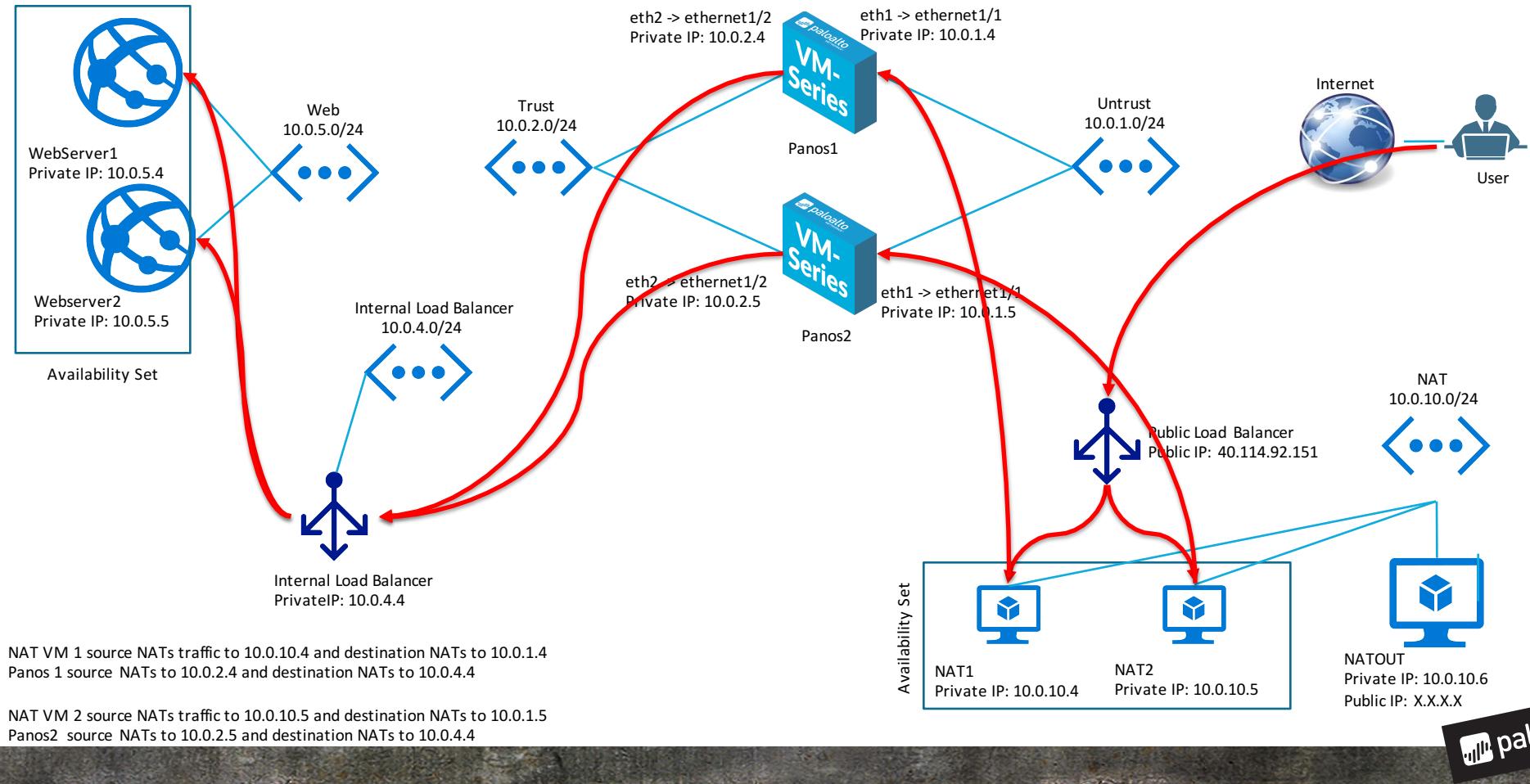
Load Balancer Sandwich Template Overview



Load Balancer “Sandwich” Template Logical Architecture



Load Balancer “Sandwich” Template Logical Architecture



Overview of the deployment in the Azure Portal

Microsoft Azure

Dashboard

Search resources

New

Resource groups

Virtual networks

All resources

Recent

App Services

Virtual machines (classic)

Virtual machines

SQL databases

Cloud services (classic)

Subscriptions

Azure Active Directory

Monitor

Security Center

Billing

Help + support

NAT1-Ubuntu-16

panos1

Stopped

NAT2-Ubuntu-16

panos2

Stopped

NATOUT-Ubuntu-16

Stopped

PublicLB

IbsandInternal

WebServer1

WebServer2

Stopped

NAT-UDR

Untrust-UDR

Trust-UDR

LB-UDR

WEB-UDR



This screenshot shows the Microsoft Azure portal dashboard with a grid of resources. The resources are categorized into several boxes:

- Top Left:** NAT1-Ubuntu-16 (panos1) and NAT2-Ubuntu-16 (panos2), both labeled "Stopped".
- Middle Left:** NATOUT-Ubuntu-16, also labeled "Stopped".
- Top Middle:** PublicLB.
- Top Right:** IbsandInternal, containing WebServer1 and WebServer2, both labeled "Stopped".
- Bottom Row:** NAT-UDR, Untrust-UDR, Trust-UDR, LB-UDR, and WEB-UDR, each with a small icon below it.

The left sidebar lists various Azure services like Resource groups, Virtual networks, and App Services. The top right corner shows the user's email (david@wi.rr.com) and profile picture.

Overview of the deployment

This template deploys:

- Two BYOL Palo Alto Networks firewalls- Panos1 and Panos2
- One internal Load Balancer
- One public Load Balancer
- Two Ubuntu NAT Servers for Inbound traffic– NAT1 and NAT2
- One Ubuntu NAT Server for Outbound traffic- NATOUT
- Two internal Web Servers with Apache – WebServer1 and WebServer2
- UDRs to direct traffic through the firewalls
- At this point the template deploys to the US Central Region

Post deployment tasks that need to be done to complete the setup:

- The firewalls need to be licensed and configured.





To start the deployment

To start the deployment click on the Deploy to Azure from the README.md

README.md

2 VM-Series Firewalls in a load balancer sandwich along with two webservers

NOTE---DO NOT USE!!! THIS IS STILL UNDER CONSTRUCTION AND DOES NOT YET WORK AS INTENDED!

The intent of this ARM template is to deploy a firewall sandwich environment that includes:

- One Public Load Balancer
- Two Palo Alto Networks Firewalls
- One Internal Load Balancer
- Two Web Servers with apache webserver
- VNET 10.0.0.0/16
- Multiple Subnets and UDRs to support the traffic flow

This template creates all the infrastructure and appropriate UDRs. It does not currently license or configure the firewall. That will need to be done afterwards.

 Deploy to Azure  Visualize





Everything will deploy into a single Resource Group. I usually create a new group to make it easier to delete later.

Select “Central US” as this is where all the individual resources will get deployed.

The Storage account must be globally unique so this must be changed or the deployment will fail.

The Pub Firewall DNS records are the DNS names for the firewall MGMT interfaces and must also be globally unique.

Fill out the template parameters

The screenshot shows the Microsoft Azure portal's "Custom deployment" page. On the left, there's a sidebar with icons for different resource types like storage, databases, and networks. The main area has a dark header bar with the title "Custom deployment" and a sub-header "Deploy from a custom template". Below the header, there's a "TEMPLATE" section showing a "Customized template" with 47 resources, with "Edit" and "Learn more" buttons. The "BASICS" section contains fields for "Subscription" (set to "AzureSEConsulting"), "Resource group" (radio buttons for "Create new" and "Use existing" are visible), and "Location" (set to "Central US"). The "SETTINGS" section lists several variables with their values: "Virtual Machines_Admin_password" (empty field), "Virtual Machines_Admin_username" (value "fwadmin"), "Storage Accounts_lbsandwich_name" (value "lbsandwich"), "Pub Firewall2dnsrecord" (value "lbsandfw20"), and "Pub Firewall1dnsrecord" (value "lbsandfw10"). At the bottom, there's a "TERMS AND CONDITIONS" section with a checkbox for "Pin to dashboard" and a blue "Purchase" button.





Fill out the template parameters

Scroll down and check the agreement terms. I also check the Pin to dashboard.

Click on the Purchase button.

Screenshot of the Microsoft Azure 'Custom deployment' page. The page shows a list of parameters for a custom deployment:

- Resource group:** Create new (selected) or Use existing (unchecked). Value: spears
- Location:** Central US
- SETTINGS:** Virtual Machines_Admin_password, Virtual Machines_Admin_username, Storage Accounts_lbsandwich_name, Pub Firewall2dnsrecord, Pub Firewall1dnsrecord
- TERMS AND CONDITIONS:** A box containing the Azure Marketplace Terms and Azure Marketplace terms. It includes a note about third-party templates and a checkbox for agreeing to terms and conditions.

Two red arrows point to the checkboxes at the bottom of the page:

- I agree to the terms and conditions stated above
- Pin to dashboard

A blue 'Purchase' button is located at the bottom of the page.





Everything will deploy into a single Resource Group. I usually create a new group to make it easier to delete later.

Select “Central US” as this is where all the individual resources will get deployed.

The Storage account must be globally unique so this must be changed or the deployment will fail.

The Pub Firewall DNS records are the DNS names for the firewall MGMT interfaces and must also be globally unique.

Fill out the template parameters

The screenshot shows the Microsoft Azure portal's "Custom deployment" page. On the left, a sidebar lists various resource types like Virtual Machines, Storage Accounts, and Network Interfaces. The main area displays a "Customized template" with 47 resources. The "BASICS" section includes fields for "Subscription" (set to "AzureSEConsulting"), "Resource group" (radio button selected for "Create new"), and "Location" (set to "Central US"). The "SETTINGS" section contains several input fields: "Virtual Machines_Admin_password" (empty), "Virtual Machines_Admin_username" (set to "fwadmin"), "Storage Accounts_lbsandwich_name" (set to "lbsandwich"), "Pub Firewall2dnsrecord" (set to "lbsandfw20"), and "Pub Firewall1dnsrecord" (set to "lbsandfw10"). At the bottom, there are "TERMS AND CONDITIONS" and a "Purchase" button.





If the validation completes successfully you will be redirected to the dashboard.

Click on the Deploying Template tile to monitor the deployment process.

Monitor the deployment

A screenshot of the Microsoft Azure dashboard titled "Spears Dashboard". The left sidebar lists various services: Resource groups, Recent, App Services, Virtual machines, SQL databases, Cloud services (classic), Security Center (highlighted with a red arrow), Route tables, Azure Active Directory, Monitor, and Virtual networks. The main area shows a single tile titled "Deploying Template deployment" with a progress bar and three dots at the top right. The top right corner of the dashboard shows the user's email (dspears@paloaltonet...) and name (PALO ALTO NETWORKS).





You can click on the Refresh button to get an update.

Monitor the deployment

The screenshot shows the Microsoft Azure portal interface for monitoring a deployment. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons for notifications, settings, and help. The main title is "Microsoft.Template Deployment". A red arrow points to the "Refresh" button, which is highlighted in blue. The status message "Deploying" is displayed below the title. The "Summary" section provides details: DEPLOYMENT DATE: 11/11/2016, 9:31:02 AM; STATUS: Deploying; DURATION: PT0.8386736S; RESOURCE GROUP: spearsfwsand; RELATED: Events; TEMPLATE LINK: <https://raw.githubusercontent.com/djspears/PaloAlto...>. The "Outputs" section shows "NO DEPLOYMENT OUTPUTS". The "Inputs" section lists several variables with their values: VIRTUALMACHINES_ADMIN_P... (redacted), VIRTUALMACHINES_ADMIN_U... (davidspears), STORAGEACCOUNTS_LBSAND... (spearslsbandwich), PUBFIREWALL2DNSRECORD (spearslsbandfw20), and PUBFIREWALL1DNSRECORD (spearslsbandfw10). The "Operation details" section is partially visible at the bottom.





Scrolling down shows more specifics about what is being built.

Monitor the deployment

A screenshot of the Microsoft Azure portal showing the deployment status for a template named "Microsoft.Template". The interface includes a left sidebar with various icons for different service types. The main area displays a table titled "Operation details" with columns for RESOURCE, TYPE, STATUS, and TIMESTAMP. The table lists numerous resources, mostly of type "Microsoft.Compute" (Compute VMs), with statuses ranging from "OK" to "Created". A red arrow points to the timestamp for the last entry, which is "2016-11-11T15:11:11Z".

RESOURCE	TYPE	STA...	TIMESTAMP
NATOUT-Ubuntu-16/installcustomscript	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
WebServer2/installcustomscript	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
NAT1-Ubuntu-16/installcustomscript	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
NAT2-Ubuntu-16/installcustomscript	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
WebServer1/installcustomscript	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
panos2	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
panos1	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
NATOUT-Ubuntu-16	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
WebServer1	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
NAT1-Ubuntu-16	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
WebServer2	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
NAT2-Ubuntu-16	Microsoft.Compute...	OK	2016-11-11T15:11:11Z
webserver1	Microsoft.Network...	Created	2016-11-11T15:11:11Z
webserver2	Microsoft.Network...	Created	2016-11-11T15:11:11Z
panos1_eth2	Microsoft.Network...	Created	2016-11-11T15:11:11Z
natout_ubuntu	Microsoft.Network...	Created	2016-11-11T15:11:11Z
panos2_eth3	Microsoft.Network...	Created	2016-11-11T15:11:11Z
panos1_eth0	Microsoft.Network...	Created	2016-11-11T15:11:11Z





Once the deployment is done
the status will change to
Succeeded. This one too
5min 33 seconds to deploy.

Monitor the deployment

The screenshot shows the Microsoft Azure portal interface for monitoring a deployment. The title bar says "Microsoft Azure" and "Microsoft.Template Deployment". The top navigation bar includes "Delete", "Cancel", "Refresh", "Redeploy", and "View template". The main content area displays deployment details:

Summary
DEPLOYMENT DATE: 11/11/2016, 9:36:35 AM
STATUS: Succeeded
DURATION: 5 minutes 33 seconds
RESOURCE GROUP: spearsfwsand
RELATED: Events
TEMPLATE LINK: https://raw.githubusercontent.com/djspears/PaloAlto...

Below the summary, there are sections for "Outputs" (No deployment outputs) and "Inputs" (Virtual machine names and storage account names). A red arrow points to the "DURATION" field in the summary section.





License the firewall through the support site. There are two basic config files in the github directory that can be used as a starting point.

Those files are called panos1-config.xml and panos2-config.xml.

Navigate to the Device/setup/operations tab to the partial config file. Select import and copy the appropriate file to the corresponding firewall.

License and configure the firewall

The screenshot shows the Palo Alto Networks Management interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. Below the navigation bar, there are several sub-tabs: Management, Operations, Services, Content-ID, WildFire, and Session. The main content area is titled "Configuration Management". It lists various configuration management actions: Revert, Save, Load, Export, and Import. A red arrow points to the "Import named configuration snapshot" option under the Import section. The left sidebar contains a tree view of configuration categories: Setup (High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources), Certificate Management (Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP).



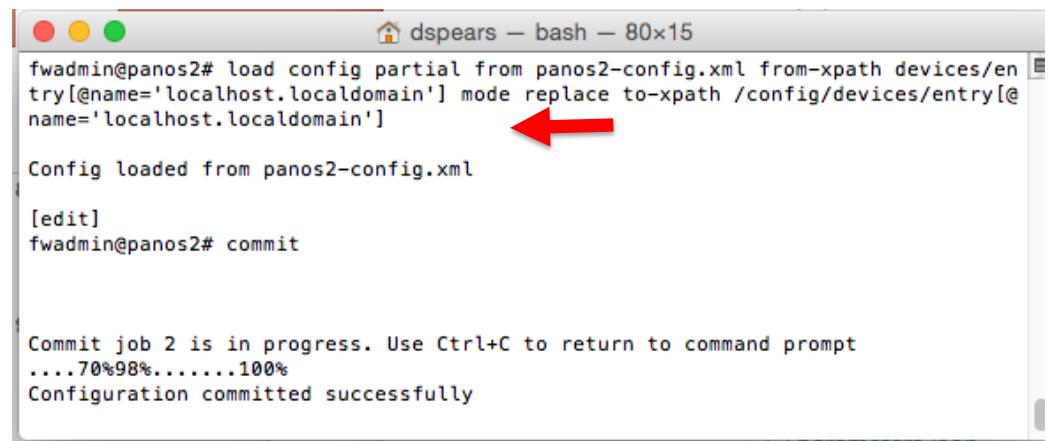
Load the configuration into the firewall

Ssh into the firewall and go into the configure mode.

To load the partial configuration type:

```
load config partial from panos2-config.xml from-xpath  
devices/entry[@name='localhost.localdomain'] mode  
replace to-xpath  
/config/devices/entry[@name='localhost.localdomain']
```

Commit the configuration



The screenshot shows a terminal window titled "dspears - bash - 80x15". The command entered is:

```
fwadmin@panos2# load config partial from panos2-config.xml from-xpath devices/en  
try[@name='localhost.localdomain'] mode replace to-xpath /config/devices/entry[@  
name='localhost.localdomain']
```

A red arrow points to the "replace" keyword in the command. The output shows:

```
Config loaded from panos2-config.xml  
[edit]  
fwadmin@panos2# commit
```

Commit job 2 is in progress. Use Ctrl+C to return to command prompt
....70%98%.....100%
Configuration committed successfully





Test

Navigate to the public address of the public load balancer to identify the ip address that can be used to access the web servers through the two panos firewalls.



