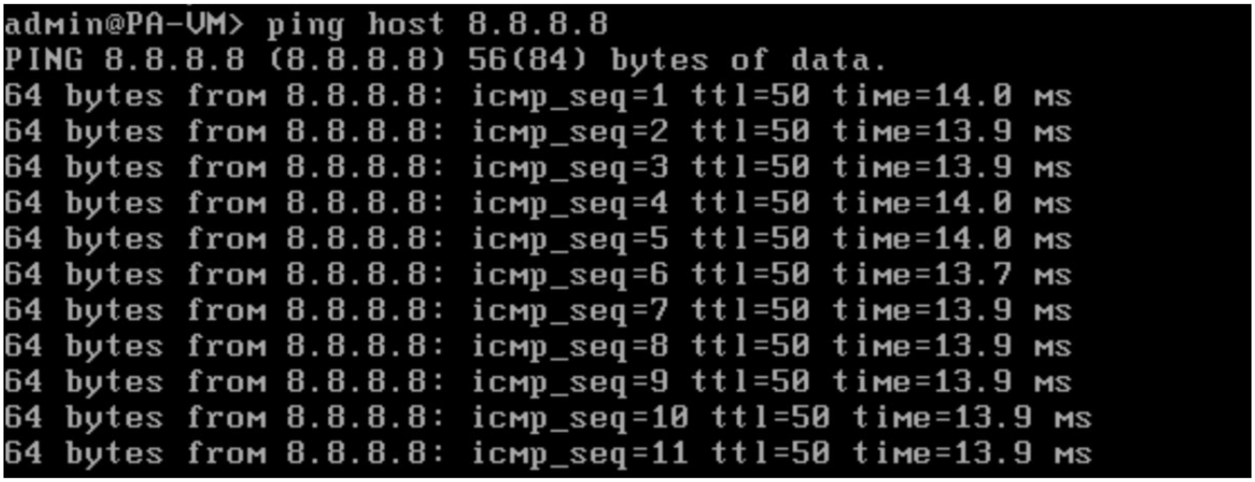
paloalto NETWORKS®
the enterprise security company™

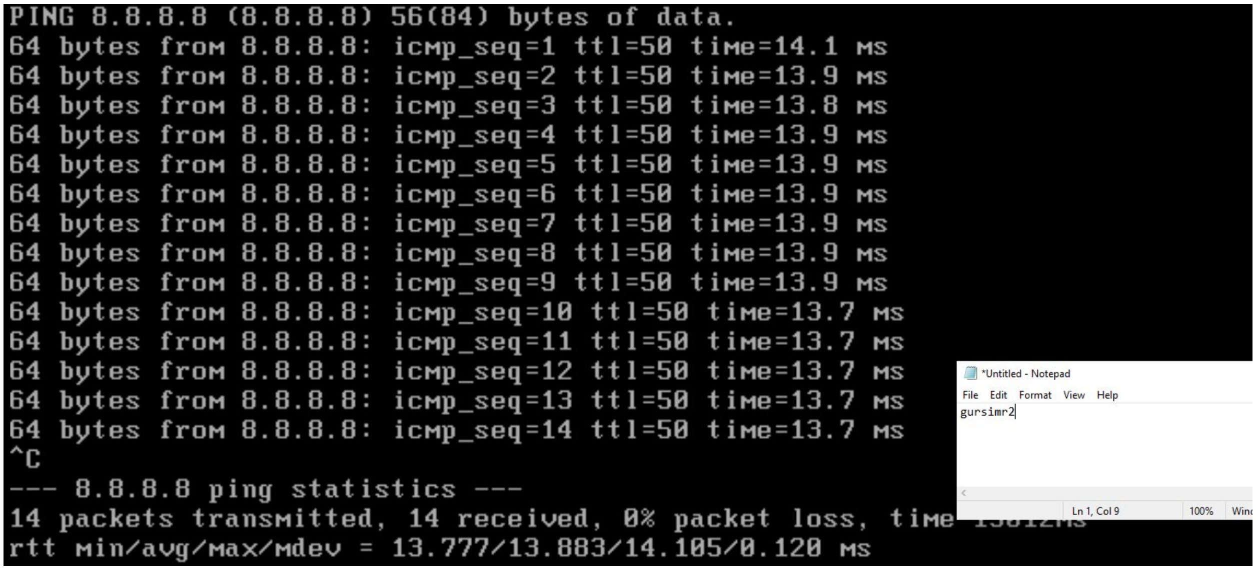
Palo Alto Firewall Homework

Contents

<u>Task1</u>



```
admin@PA-VM> ping host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=50 time=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=50 time=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=50 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=50 time=13.9 ms
```

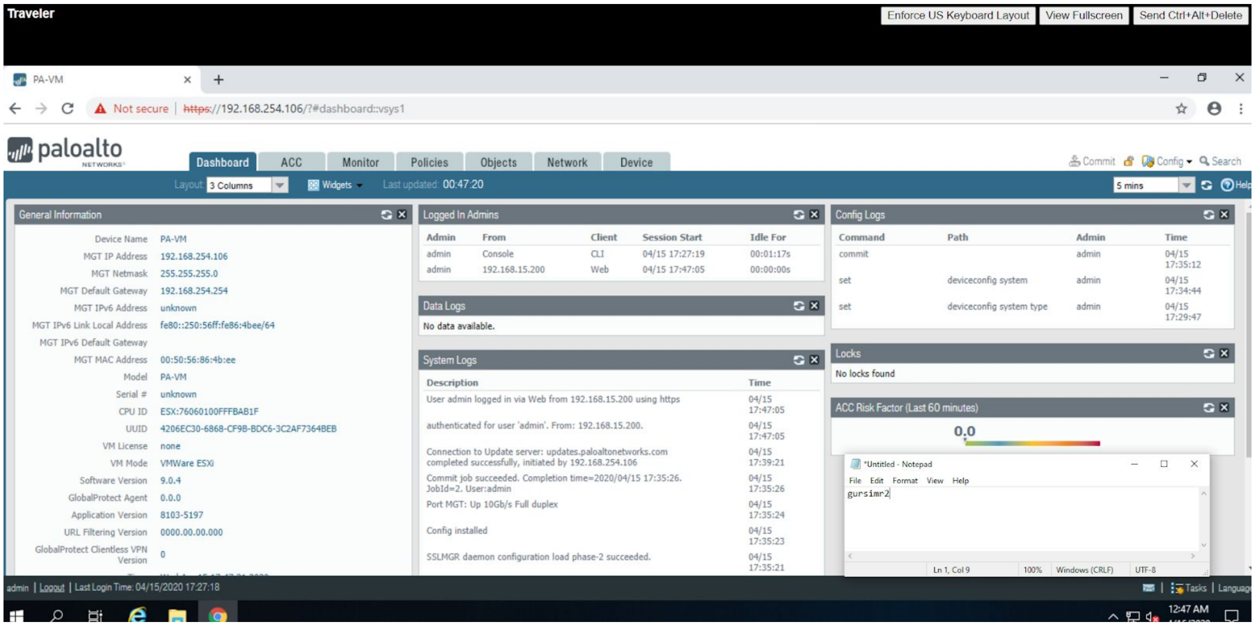


```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=14.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=13.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=50 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=50 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=50 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=50 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=50 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=50 time=13.7 ms
^C
--- 8.8.8.8 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13012ms
rtt min/avg/max/mdev = 13.777/13.883/14.105/0.120 ms
```

gursimr2

Proving Connection between Firewall and 8.8.8.8

Task2



~~https~~://192.168.254.106/?#dashboard::vsys1

Last updated: 00:47:20

General Information

Device Name	PA-VM
MGT IP Address	192.168.254.106
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.254.254
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::250:56ff:fe86:4bee/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:50:56:86:4b:ee
Model	PA-VM
Serial #	unknown
CPU ID	ESX:76060100FFFBAB1F
UUID	4206EC30-6868-CF9B-BDC6-3C2AF7364BEB
VM License	none
VM Mode	VMWare ESXi
Software Version	9.0.4
GlobalProtect Agent	0.0.0
Application Version	8103-5197
URL Filtering Version	0000.00.00.000
GlobalProtect Clientless VPN Version	0

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	Console	CLI	04/15 17:27:19	00:01:17s
admin	192.168.15.200	Web	04/15 17:47:05	00:00:00s

Data Logs

No data available.

System Logs

Description	Time
User admin logged in via Web from 192.168.15.200 using https	04/15 17:47:05
authenticated for user 'admin'. From: 192.168.15.200.	04/15 17:47:05
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.254.106	04/15 17:39:21
Commit job succeeded. Completion time=2020/04/15 17:35:26. JobId=2. User:admin	04/15 17:35:26
Port MGT: Up 10Gb/s Full duplex	04/15 17:35:24
Config installed	04/15 17:35:23
SSLMGR daemon configuration load phase-2 succeeded.	04/15 17:35:21

Config Logs

Command	Path	Admin	Time
commit		admin	04/15 17:35:12
set	deviceconfig system	admin	04/15 17:34:44
set	deviceconfig system type	admin	04/15 17:29:47

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

0.0

*Untitled - Notepad

```
gursimr2
```

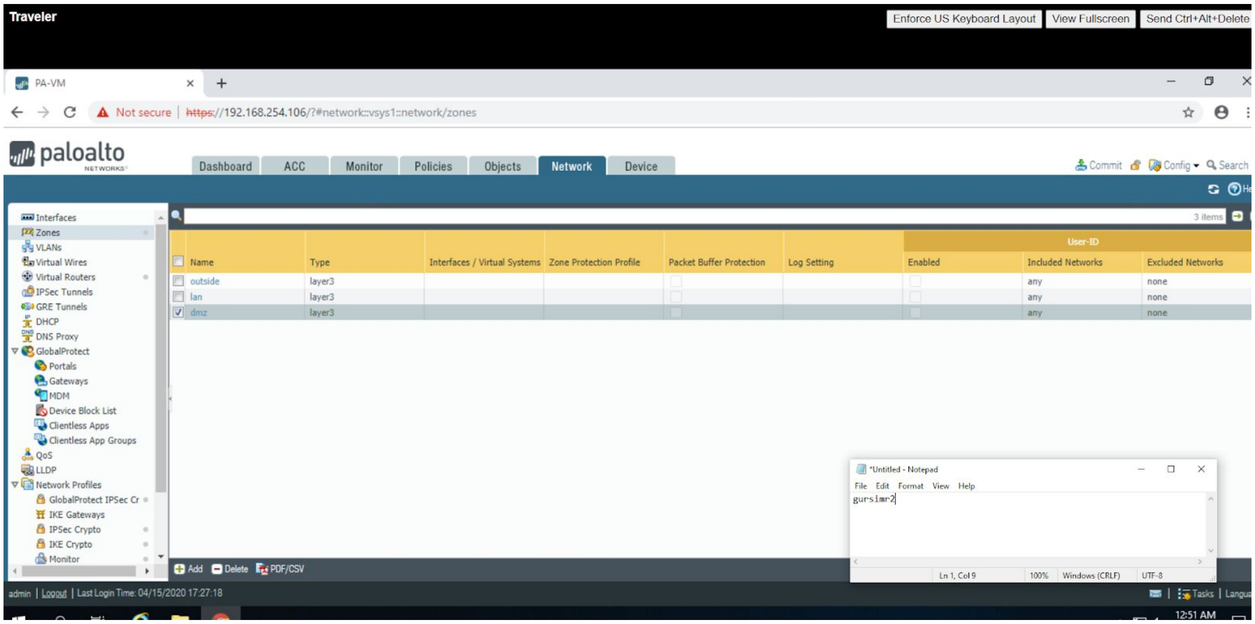
Ln 1, Col 9 | 100% | Windows (CRLF) | UTF-8

admin | Logout | Last Login Time: 04/15/2020 17:27:18

12:47 AM

Palo Alto Firewall Landing Page upon first login

Task3

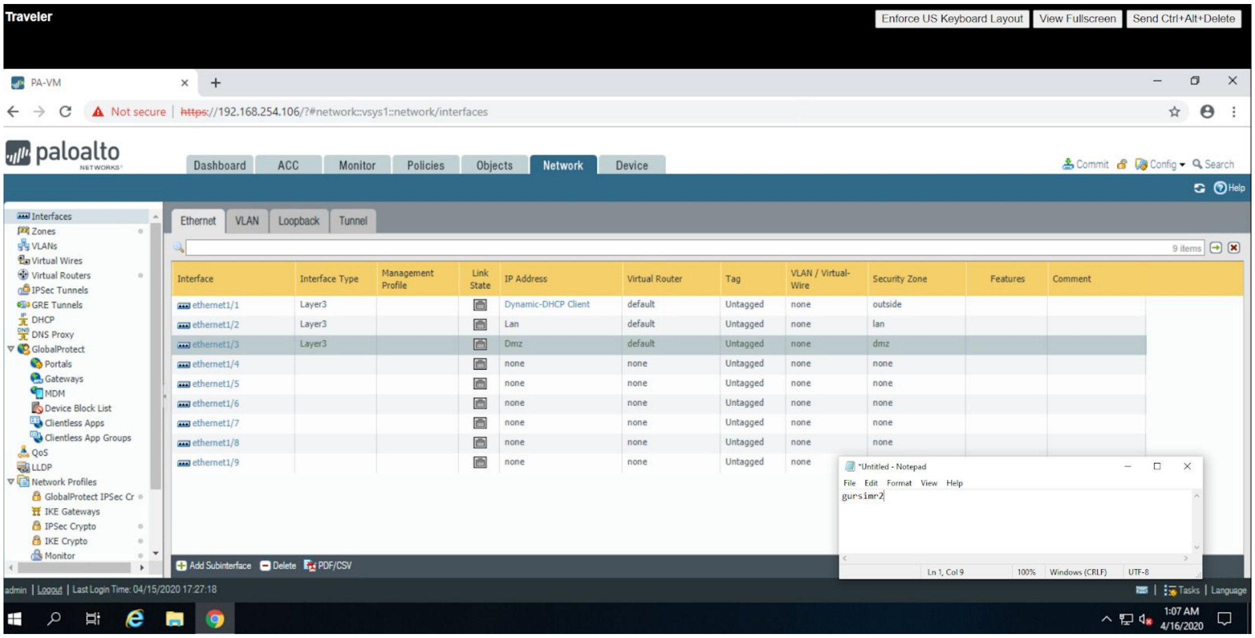


						User-ID		
Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	Included Networks	Excluded Networks
☐ outside	layer3			☐		☐	any	none
☐ lan	layer3			☐		☐	any	none
☑ dmz	layer3			☐		☐	any	none

```
gursimr2
```

Setting Up Zones

Task4



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3		▣	Dynamic-DHCP Client	default	Untagged	none	outside		
ethernet1/2	Layer3		▣	Lan	default	Untagged	none	lan		
ethernet1/3	Layer3		▣	Dmz	default	Untagged	none	dmz		
ethernet1/4			▣	none	none	Untagged	none	none		
ethernet1/5			▣	none	none	Untagged	none	none		
ethernet1/6			▣	none	none	Untagged	none	none		
ethernet1/7			▣	none	none	Untagged	none	none		
ethernet1/8			▣	none	none	Untagged	none	none		
ethernet1/9			▣	none	none	Untagged	none			

*Untitled - Notepad

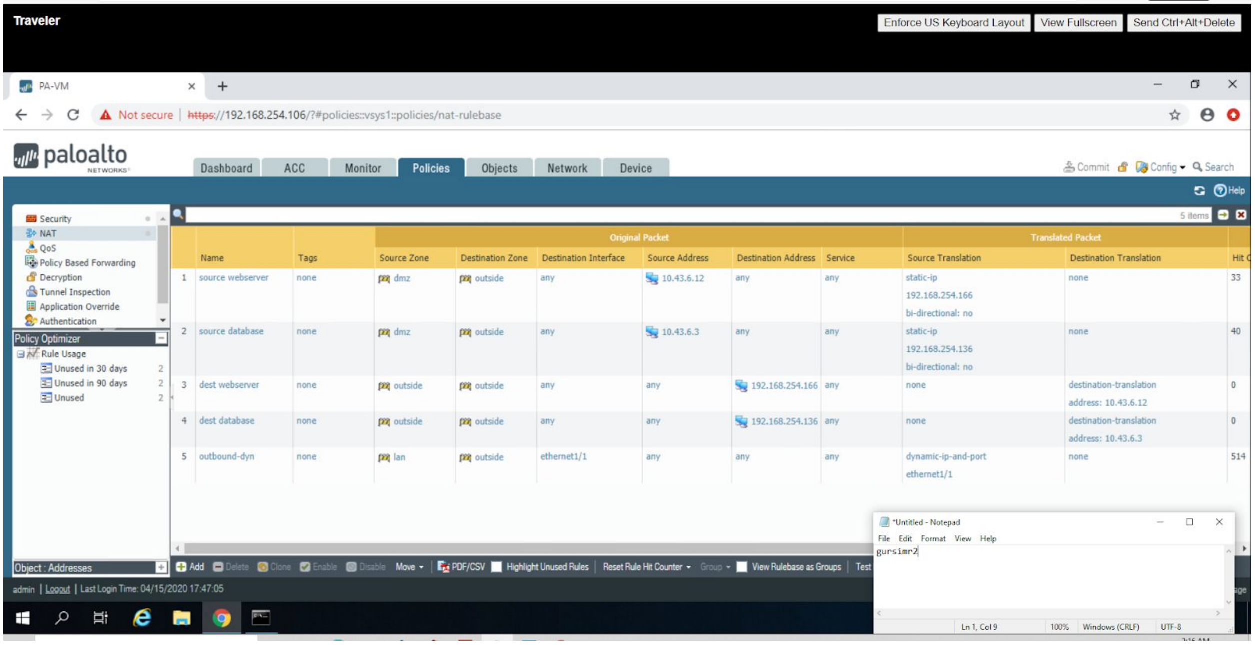
File Edit Format View Help

```
gursimr2
```

Ln 1, Col 9 100% Windows (CRLF) UTF-8

Setting Up Interfaces

Task5



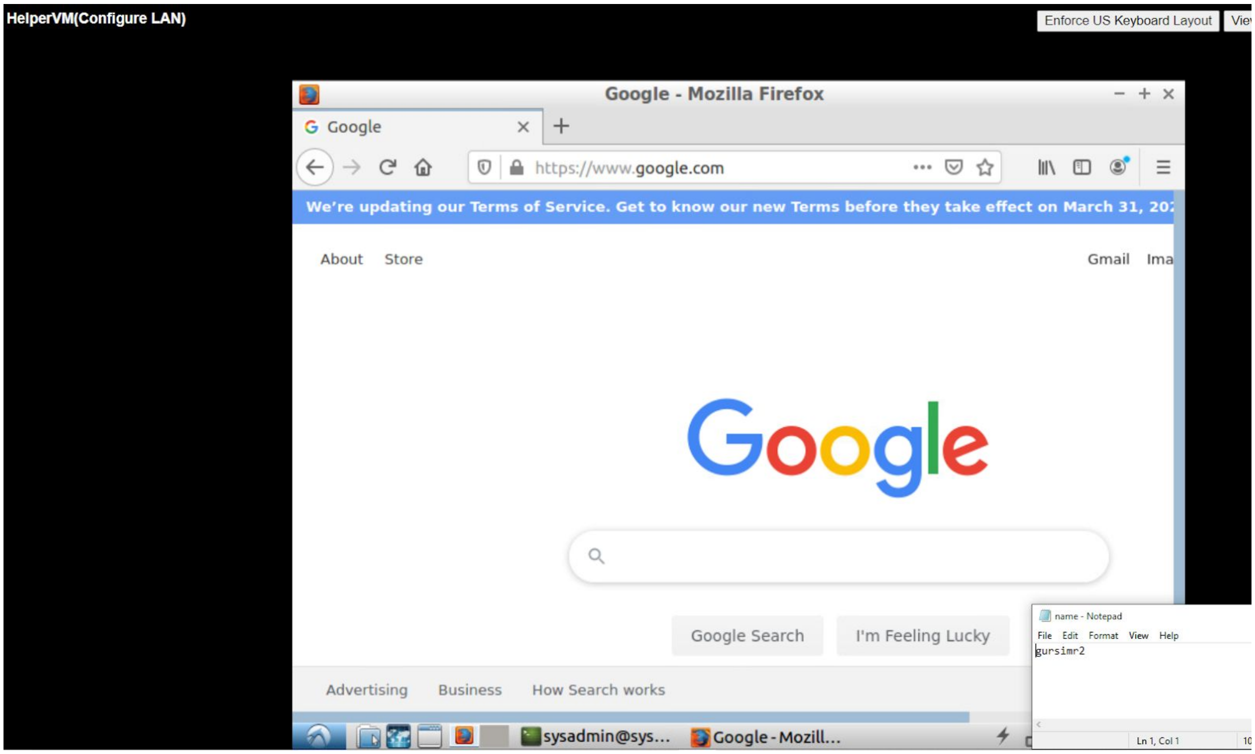
	Name	Tags	Original Packet						Translated Packet		Hit C
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
1	source webserver	none	dmz	outside	any	10.43.6.12	any	any	static-ip 192.168.254.166 bi-directional: no	none	33
2	source database	none	dmz	outside	any	10.43.6.3	any	any	static-ip 192.168.254.136 bi-directional: no	none	40
3	dest webserver	none	outside	outside	any	any	192.168.254.166	any	none	destination-translation address: 10.43.6.12	0
4	dest database	none	outside	outside	any	any	192.168.254.136	any	none	destination-translation address: 10.43.6.3	0
5	outbound-dyn	none	lan	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none	514

```
gursimr2
```

admin | Logout | Last Login Time: 04/15/2020 17:47:05

Creating NAT Policies

Task6

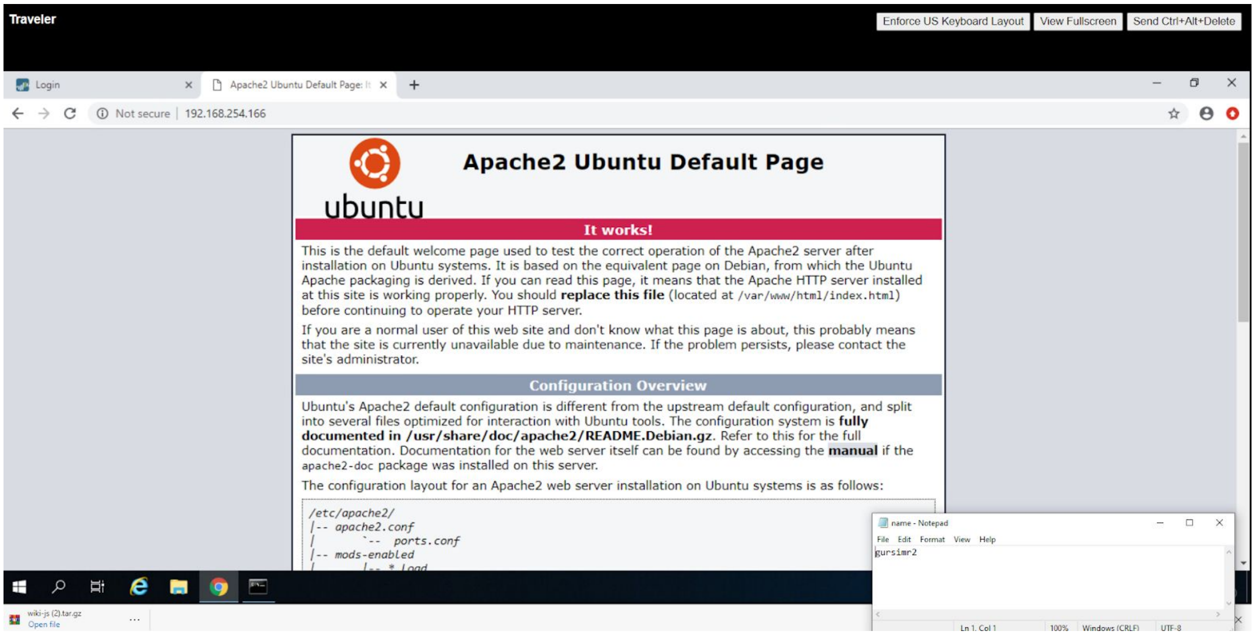


We're updating our Terms of Service. Get to know our new Terms before they take effect on March 31, 202

gursimr2

Checking Internet Connection

Task7



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

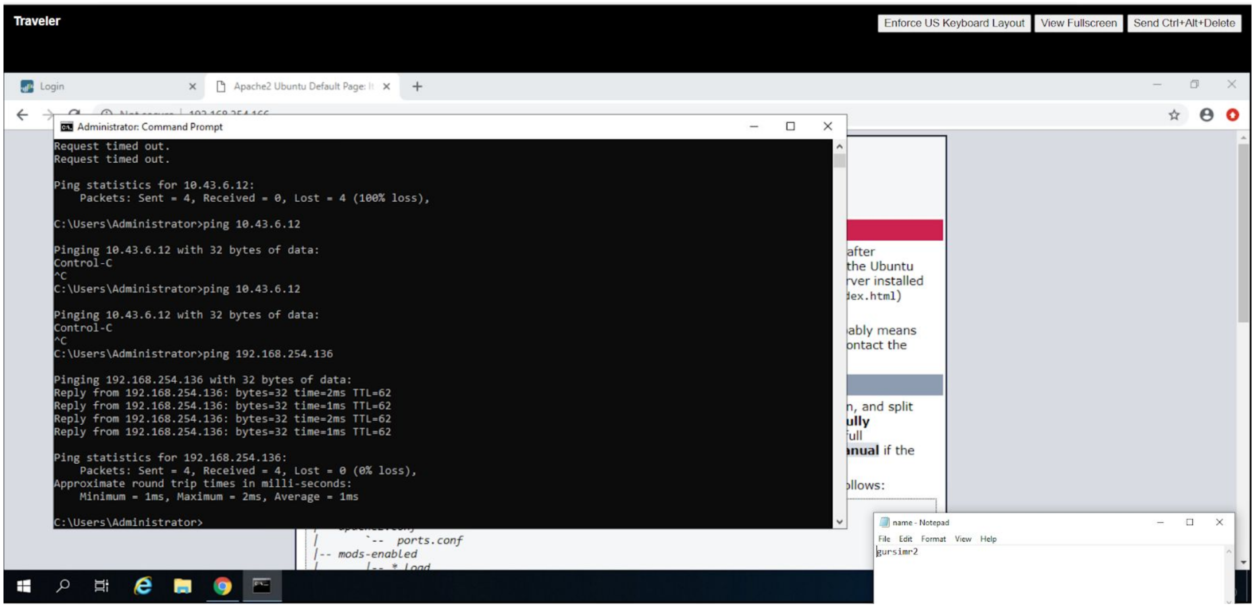
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
```

```
gursimr2
```

Connecting to webserver using publicIP from outside zone.

Task8



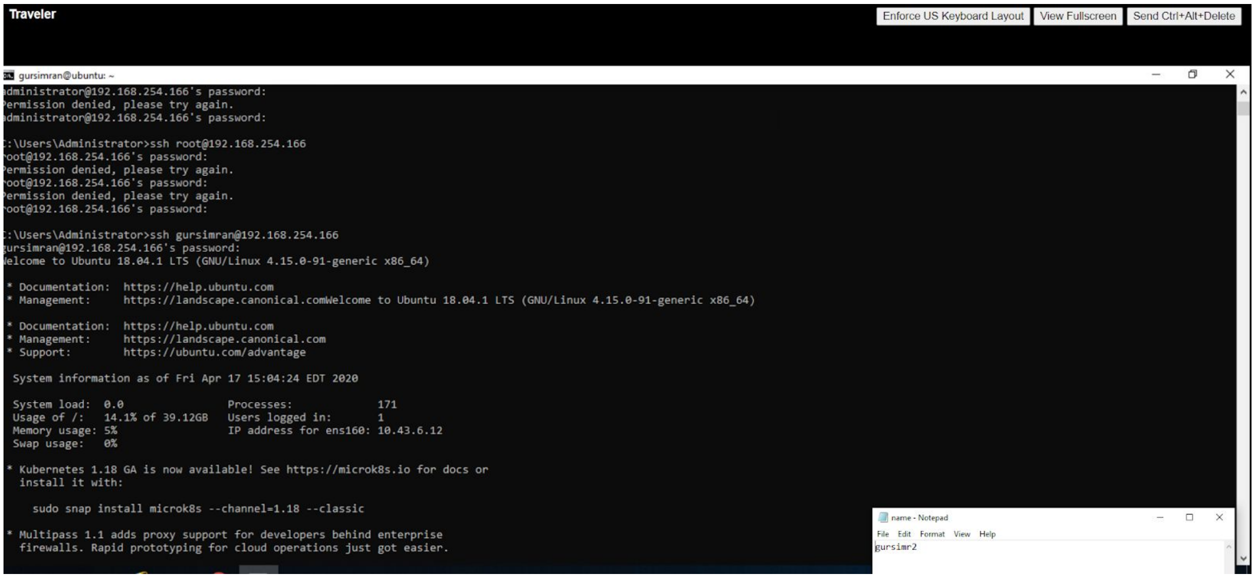
Traveler
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Login
Apache2 Ubuntu Default Page: It
Administrator: Command Prompt
name - Notepad
File Edit Format View Help

```
Request timed out.
Request timed out.

Ping statistics for 10.43.6.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 10.43.6.12

Pinging 10.43.6.12 with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>ping 10.43.6.12

Pinging 10.43.6.12 with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>ping 192.168.254.136

Pinging 192.168.254.136 with 32 bytes of data:
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62
Reply from 192.168.254.136: bytes=32 time=1ms TTL=62
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62
Reply from 192.168.254.136: bytes=32 time=1ms TTL=62

Ping statistics for 192.168.254.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Administrator>
```

```
gursimr2
```

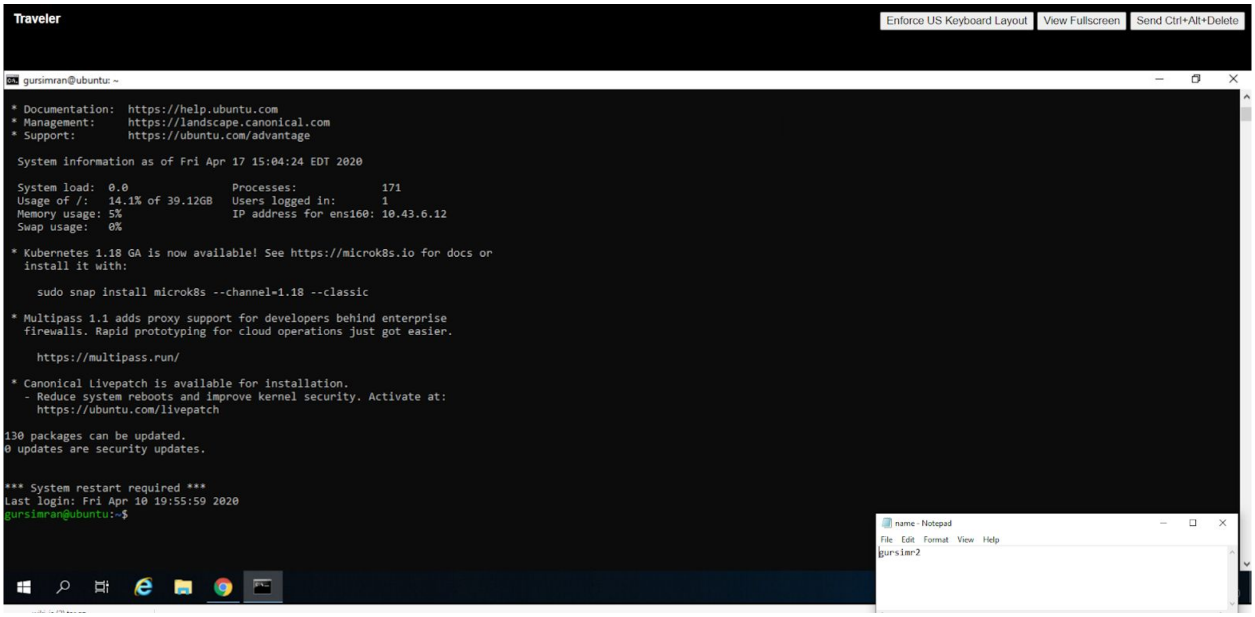
Pinging to Database Server to check Connectivity.

Task9



```
dministrator@192.168.254.166's password:
ermission denied, please try again.
dministrator@192.168.254.166's password:

:\Users\Administrator>ssh root@192.168.254.166
oot@192.168.254.166's password:
ermission denied, please try again.
oot@192.168.254.166's password:
ermission denied, please try again.
oot@192.168.254.166's password:

:\Users\Administrator>ssh gursimran@192.168.254.166
ursimran@192.168.254.166's password:
elcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.comWelcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Apr 17 15:04:24 EDT 2020

  System load:  0.0               Processes:             171
  Usage of /:   14.1% of 39.12GB   Users logged in:       1
  Memory usage: 5%                IP address for ens160: 10.43.6.12
  Swap usage:   0%

 * Kubernetes 1.18 GA is now available! See https://microk8s.io for docs or
   install it with:

     sudo snap install microk8s --channel=1.18 --classic

 * Multipass 1.1 adds proxy support for developers behind enterprise
   firewalls. Rapid prototyping for cloud operations just got easier.
```

```
gursimr2
```

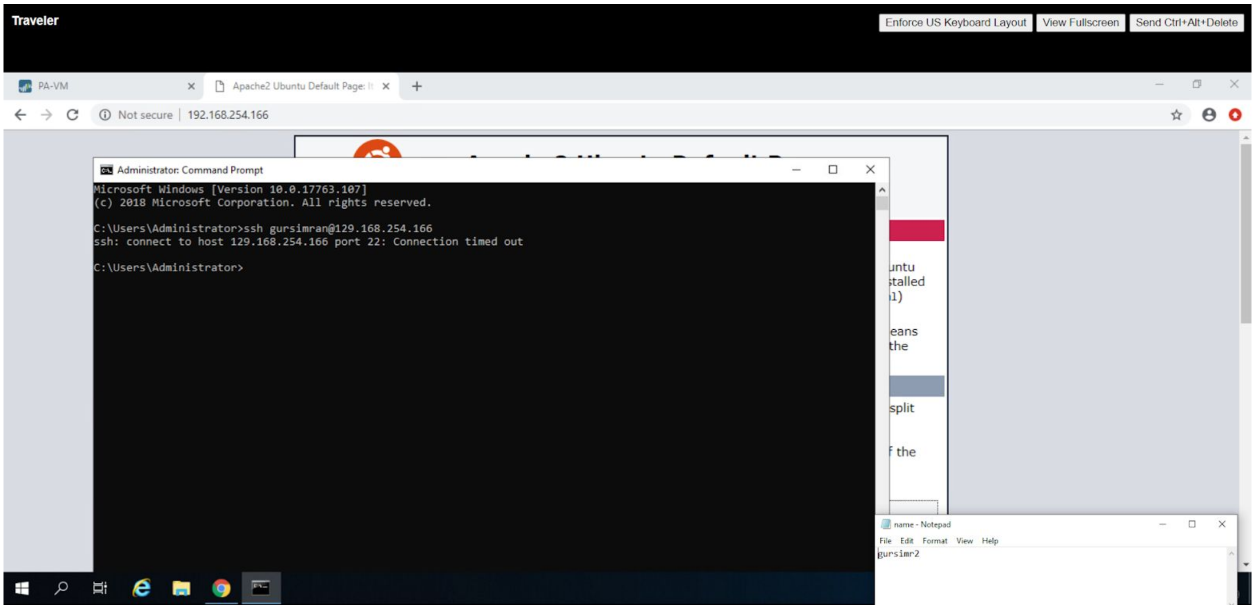


```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Apr 17 15:04:24 EDT 2020

  System load:  0.0               Processes:             171
  Usage of /:   14.1% of 39.12GB   Users logged in:       1
  Memory usage: 5%                IP address for ens160: 10.43.6.12
  Swap usage:   0%

 * Kubernetes 1.18 GA is now available! See https://microk8s.io for docs or
   install it with:

     sudo snap install microk8s --channel=1.18 --classic

 * Multipass 1.1 adds proxy support for developers behind enterprise
   firewalls. Rapid prototyping for cloud operations just got easier.

     https://multipass.run/

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

130 packages can be updated.
0 updates are security updates.


*** System restart required ***
Last login: Fri Apr 10 19:55:59 2020
gursimran@ubuntu:~$
```

```
gursimr2
```

SSH into Webserver with a user(or root if permitted) and getting the remote shell to check ssh working.

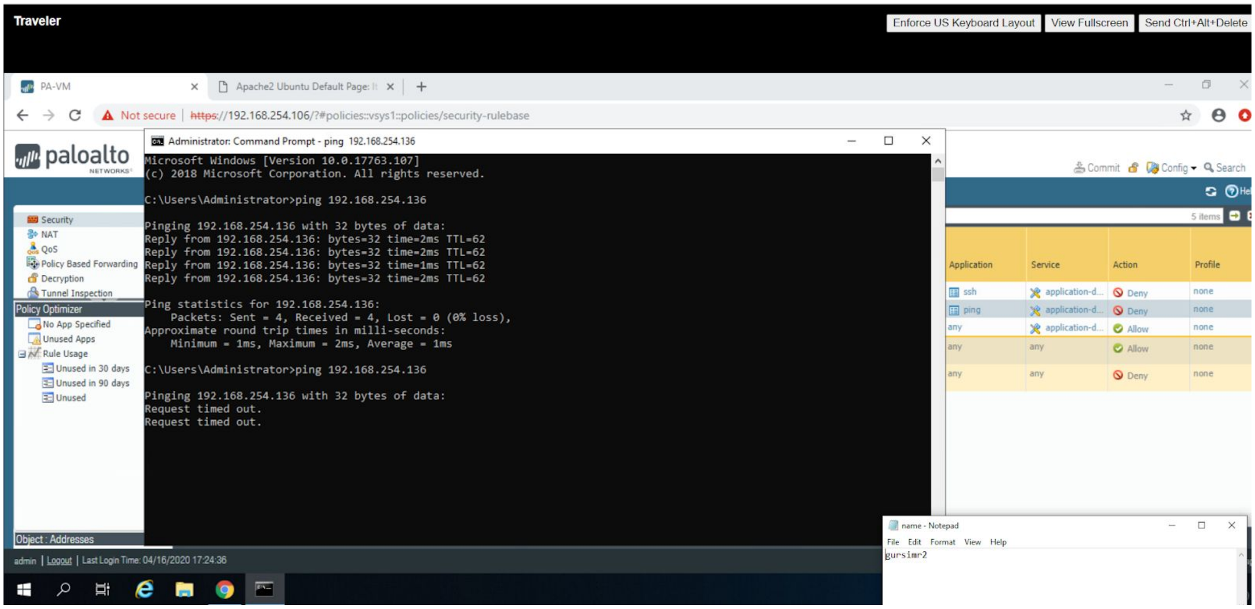
Task10



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ssh gursimran@129.168.254.166
ssh: connect to host 129.168.254.166 port 22: Connection timed out

C:\Users\Administrator>
```

SSH Blocked from outside to Public IP of Webserver by Firewall

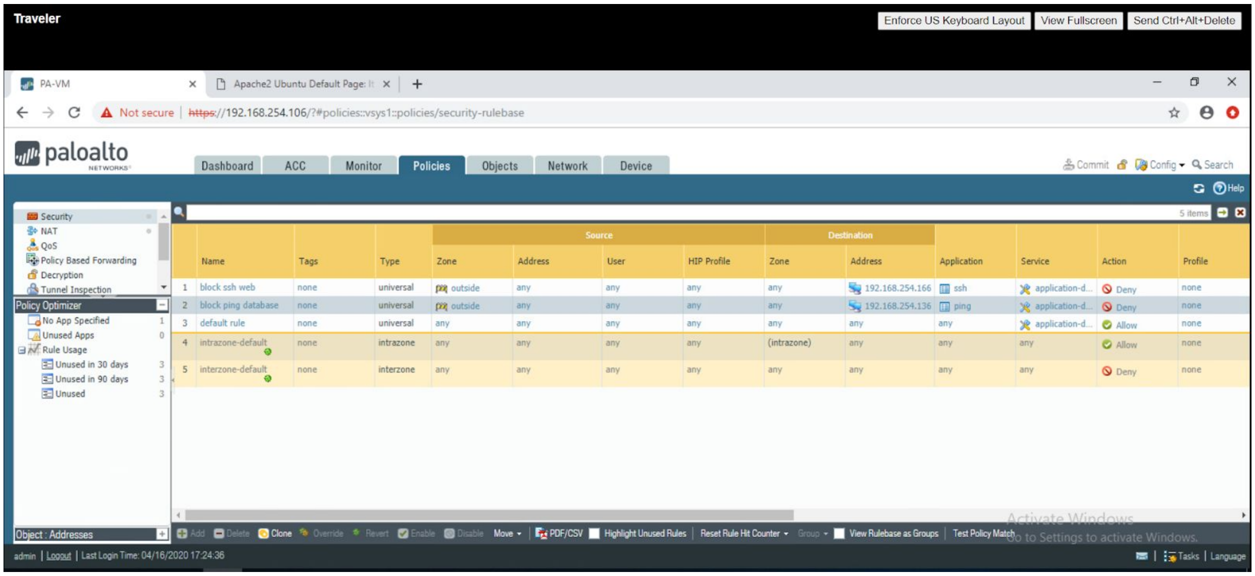
Task11



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.254.136

Pinging 192.168.254.136 with 32 bytes of data:
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62
Reply from 192.168.254.136: bytes=32 time=1ms TTL=62
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62

Ping statistics for 192.168.254.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Administrator>ping 192.168.254.136

Pinging 192.168.254.136 with 32 bytes of data:
Request timed out.
Request timed out.
```

```
gursimr2
```

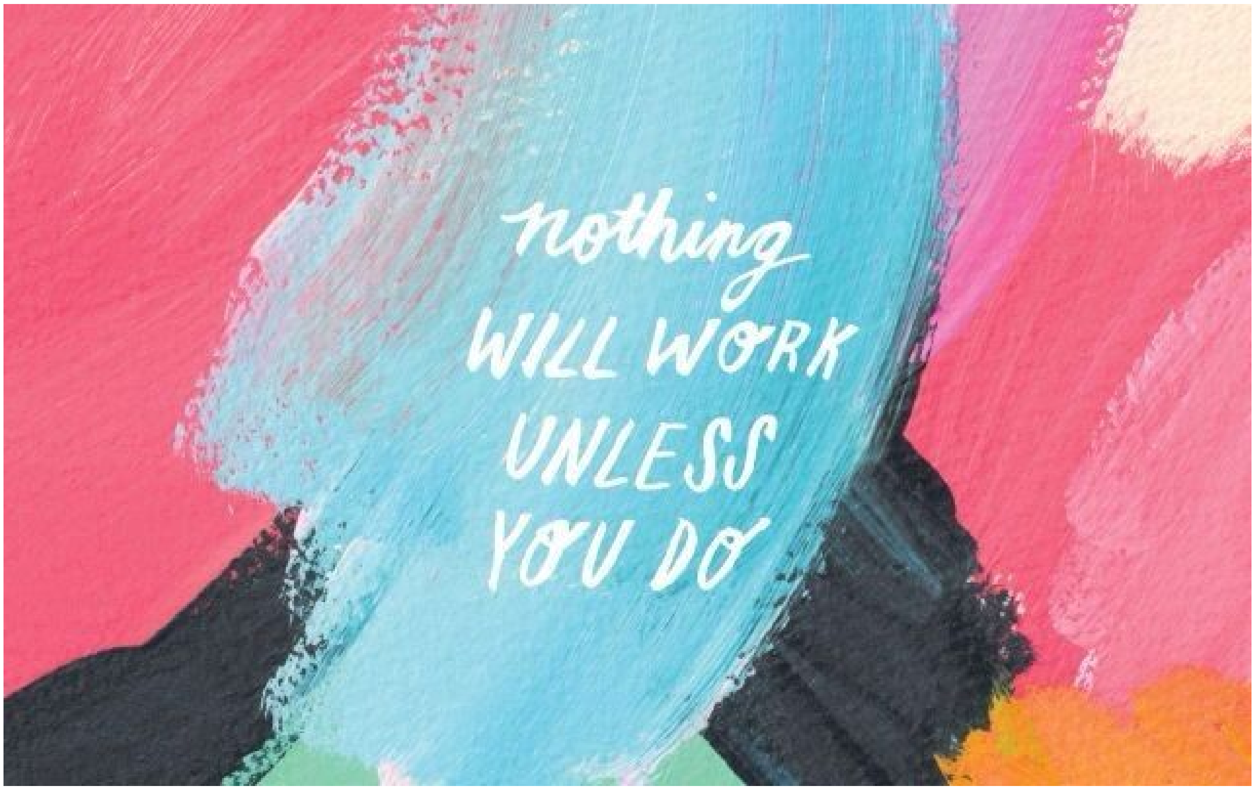
Blocked Ping to Database Server from Outside



				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	block ssh web	none	universal	outside	any	any	any	any	192.168.254.166	ssh	application-d...	Deny	none
2	block ping database	none	universal	outside	any	any	any	any	192.168.254.136	ping	application-d...	Deny	none
3	default rule	none	universal	any	any	any	any	any	any	any	application-d...	Allow	none
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none

Security Policies

paloalto NETWORKS®
the enterprise security company™



Interested in Learning more…