

Palo Alto Firewall Homework



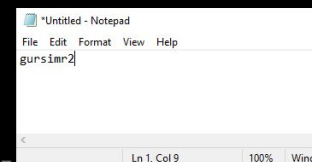
Contents

<i>Palo Alto Firewall Homework</i>	<i>1</i>
<i>Contents</i>	<i>1</i>
<i>Task1</i>	<i>3</i>
<i>Task2</i>	<i>4</i>
<i>Task3</i>	<i>4</i>
<i>Task4</i>	<i>5</i>
<i>Task5</i>	<i>5</i>
<i>Task6</i>	<i>6</i>
<i>Task7</i>	<i>6</i>
<i>Task8</i>	<i>7</i>
<i>Task9</i>	<i>8</i>
<i>Task10</i>	<i>9</i>
<i>Task11</i>	<i>10</i>

Task1

```
admin@PA-UM> 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 13612ms
rtt min/avg/max/mdev = 13.777/13.883/14.105/0.120 ms
```



Proving Connection between Firewall and 8.8.8.8

Task2

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM

Not secure | https://192.168.254.106/?#dashboard:sys1

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Layout 3 Columns Widgets Last updated: 00:47:20 5 mins

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:bbee/64
MGT IPv6 Default Gateway: unknown
MGT MAC Address: 00:50:56:b6:4b:ee
Model: PA-VM
Serial #: unknown
CPU ID: ESX:76060100FFB8B1F
UUID: 4206EC30-6868-CF9B-BDC6-3C2AF73648EB
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

File Edit Format View Help

gursier2

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

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM

Not secure | <https://192.168.254.106/?#networkcvsys1:network/zones>

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects **Network** Device

Commit Config Search

Interfaces

- Zones
- VLANs
- Virtual Wires
- Virtual Routers
- IPSec Tunnels
- GRE Tunnels
- DHCP
- DNS Proxy
- GlobalProtect
- Portals
- Gateways
- MDM
- Device Block List
- Clientless Apps
- Clientless App Groups
- QoS
- LLDP
- Network Profiles
- GlobalProtect IPSec Cr
- IKE Gateways
- IPSec Crypto
- IKE Crypto
- Monitor

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	User ID	Included Networks	Excluded Networks
<input type="checkbox"/> outside	layer3			<input type="checkbox"/>		<input type="checkbox"/>	any		none
<input type="checkbox"/> lan	layer3			<input type="checkbox"/>		<input type="checkbox"/>	any		none
<input checked="" type="checkbox"/> dmz	layer3			<input type="checkbox"/>		<input type="checkbox"/>	any		none

3 items

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

12:51 AM

Setting Up Zones

Task4

Traveler Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM x +

Not secure | https://192.168.254.106/?#network:vsys1:network/interfaces

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects **Network** Device

Commit Config Search Help

Interfaces

- Zones
- VLANs
- Virtual Wires
- Virtual Routers
- IPSec Tunnels
- GRE Tunnels
- DHCP
- DNS Proxy
- GlobalProtect
- Portals
- Gateways
- MDM
- Device Block List
- Clientless Apps
- Clientless App Groups
- QoS
- LLDP
- Network Profiles
- GlobalProtect IPSec Cr
- IKE Gateways
- IPSec Crypto
- IKE Crypto
- Monitor

Ethernet VLAN Loopback Tunnel

9 items

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	none		

Add Subinterface Delete PDF/CSV

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

1:07 AM 4/16/2020

Tasks | Language

Setting Up Interfaces

Task5

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM x +

Not secure https://192.168.254.106/?#policiescvsys1:policies/nat-rulebase

paloalto NETWORKS®

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection
- Application Override
- Authentication

Policy Optimizer

- Rule Usage
- Unused in 30 days
- Unused in 90 days
- Unused

			Original Packet					Translated Packet			
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count
1	source webserver	none	dmz	outside	any	10.43.6.12	any	any	static-ip 192.168.254.166	none	33
2	source database	none	dmz	outside	any	10.43.6.3	any	any	static-ip 192.168.254.136	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

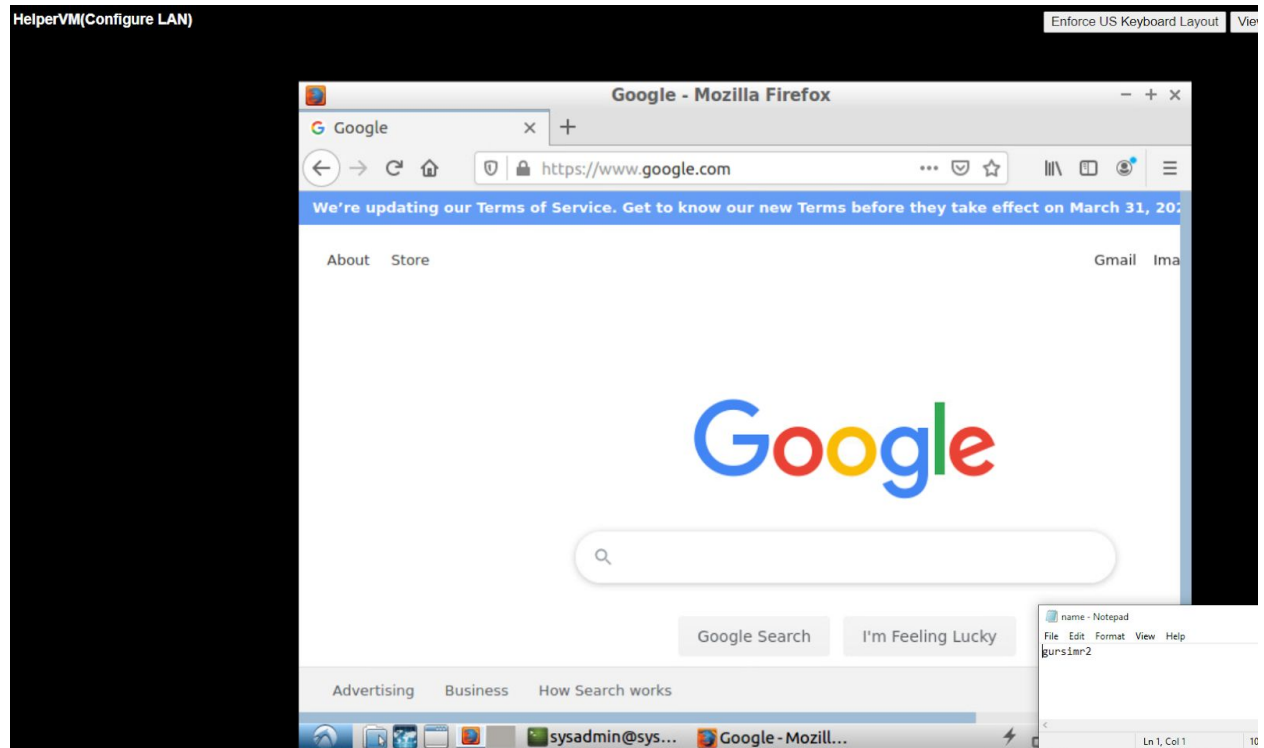
Object: Addresses

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

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

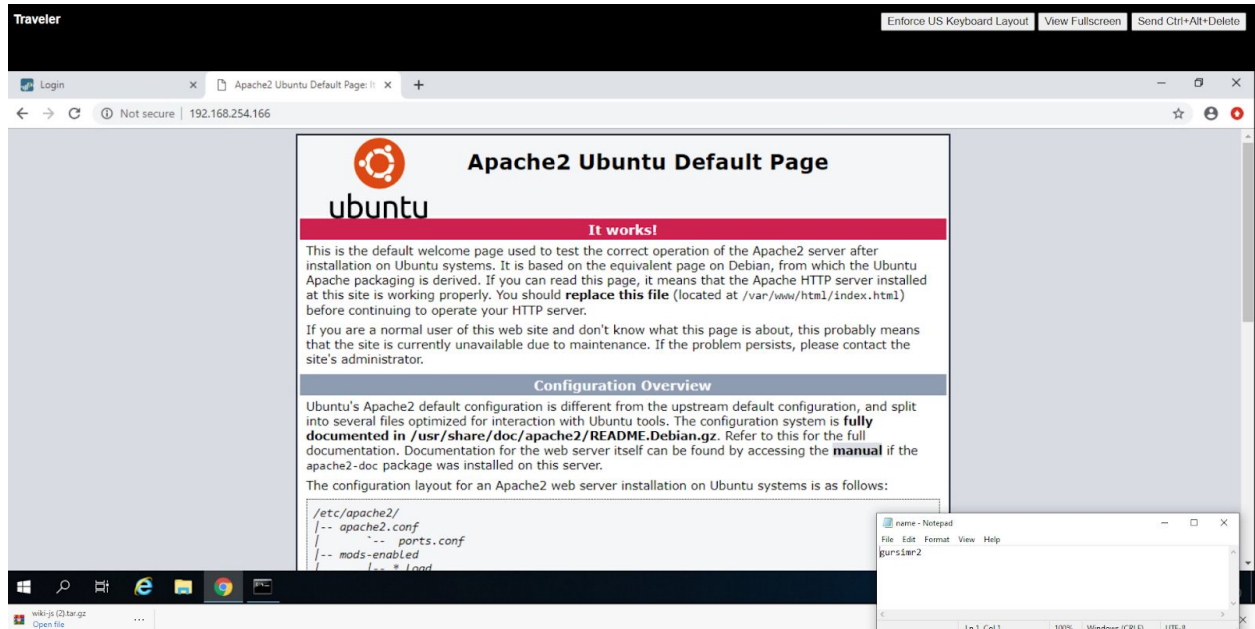
Creating NAT Policies

Task6



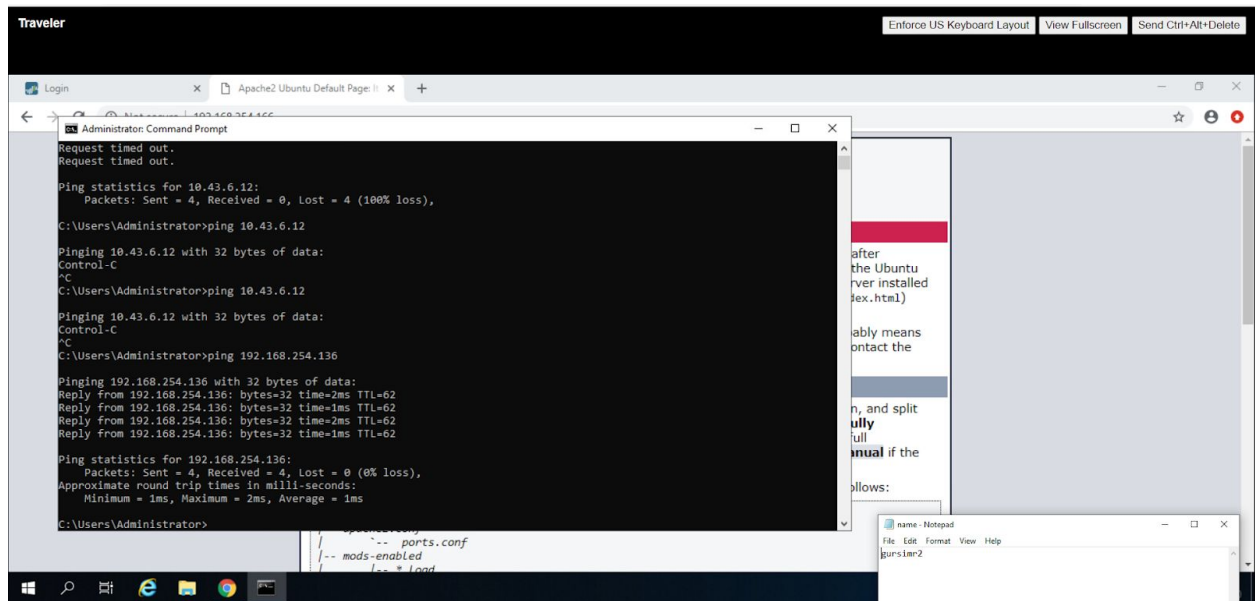
Checking Internet Connection

Task7



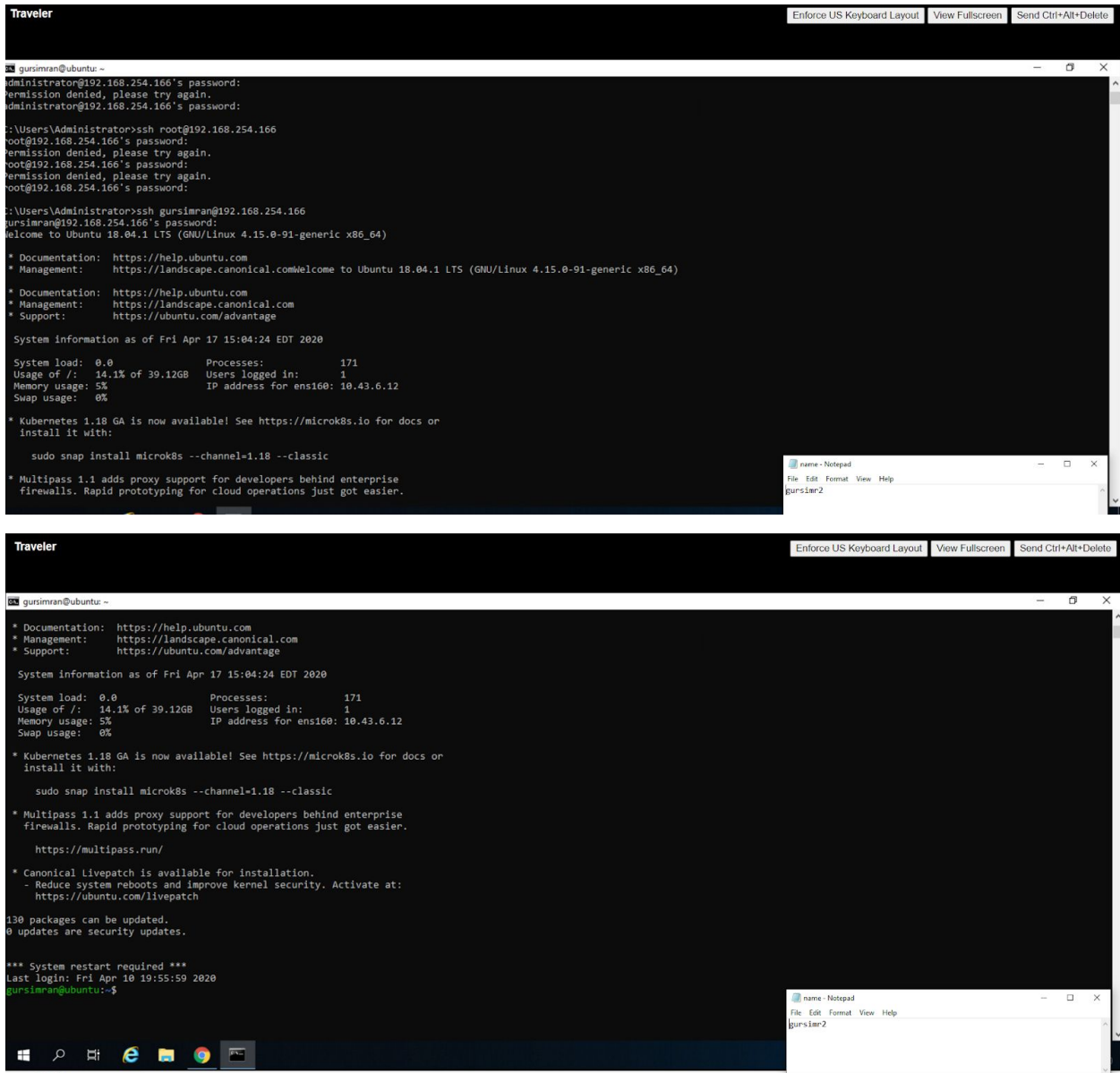
Connecting to webserver using publicIP from outside zone.

Task8



Pinging to Database Server to check Connectivity.

Task9



The screenshot shows a remote session titled "Traveler" with a terminal window and a Notepad window. The terminal window displays the following content:

```
gursimran@ubuntu:~$ ssh root@192.168.254.166
Permission denied, please try again.
gursimran@192.168.254.166:~$ ssh root@192.168.254.166
Permission denied, please try again.
gursimran@192.168.254.166:~$ ssh root@192.168.254.166
Permission denied, please try again.
gursimran@192.168.254.166:~$ ssh gursimran@192.168.254.166
gursimran@192.168.254.166:~$
Welcome 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.
     https://multipass.run/

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

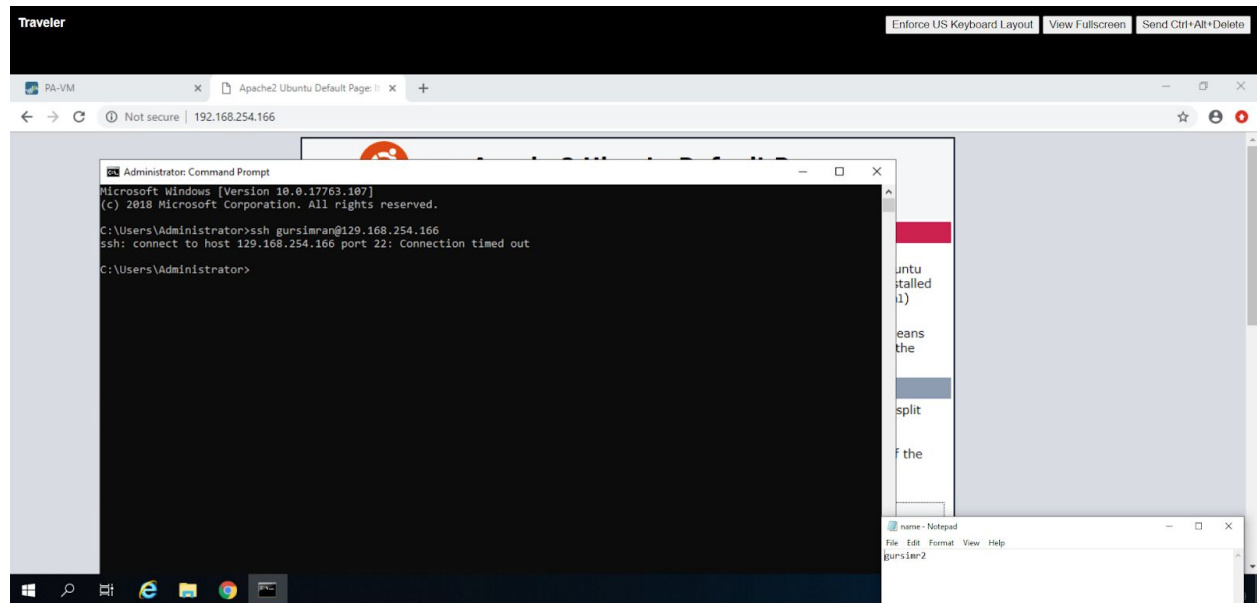
130 packages can be updated.
0 updates are security updates.

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

The Notepad window contains the text "gursimr2".

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

Task10



SSH Blocked from outside to Public IP of Webserver by Firewall

Task11

The screenshot shows the Palo Alto Networks Traveler interface. A web browser window displays the URL `https://192.168.254.106/?#policies:vsys1:policies/security-rulebase`. The interface shows a list of security rules. The rule `block ping database` is highlighted, showing its configuration: Source Zone `outside`, Source Address `any`, Destination Zone `any`, Destination Address `192.168.254.136`, Application `ping`, Service `application-d...`, Action `Deny`, and Profile `none`.

In the background, a Windows Command Prompt window shows the results of a ping command to `192.168.254.136`:

```

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.
  
```

Blocked Ping to Database Server from Outside

The screenshot shows the Palo Alto Networks Traveler interface, specifically the `Security Policies` configuration page. The page displays a list of security rules with columns for Name, Tags, Type, Zone, Address, User, HDP Profile, Zone, Address, Application, Service, Action, and Profile.

Name	Tags	Type	Zone	Address	User	HDP Profile	Zone	Address	Application	Service	Action	Profile
1 block ssh web	none	universal	px outside	any	any	any	any	192.168.254.166	ssh	application-d...	Deny	none
2 block ping database	none	universal	px 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

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM Apache2 Ubuntu Default Page: | x +

Not secure | https://192.168.254.106/?#policies:cvsys1:policies/nat-rulebase

paloalto Web Services

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection
- Policy Optimizer
- Rule Usage
 - Unused in 30 days 0
 - Unused in 90 days 0
 - Unused 0

Name	Tags	Original Packet							Translated Packet		Hit Count
		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	40	
2 source database	none	dmz	outside	any	10.43.6.3	any	any	static-ip 192.168.254.136 bi-directional: no	none	15	
3 dest webserver	none	lan	outside	any	any	192.168.254.166	any	none	destination-translation address: 10.43.6.12	69	
4 dest database	none	outside	outside	any	any	192.168.254.136	any	none	destination-translation address: 10.43.6.3	20	
5 outbound-dyn	none	lan	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none	60	

Object: Addresses

Add Delete Clone Enable Disable Move PDF/CSV Highlight Unused Rules Reset Rule Hit Counter View Rulebase as Groups Test Policy Match

Activate Windows. Go to Settings to activate Windows.

admin | Logout | Last Login Time: 04/17/2020 12:08:12

Able to access webserver using public IP in LAN

