

# HW09 - Firewall (Part 2)

UBNetDef Systems Security(SysSec)

November 04, 2021



UBNetDef

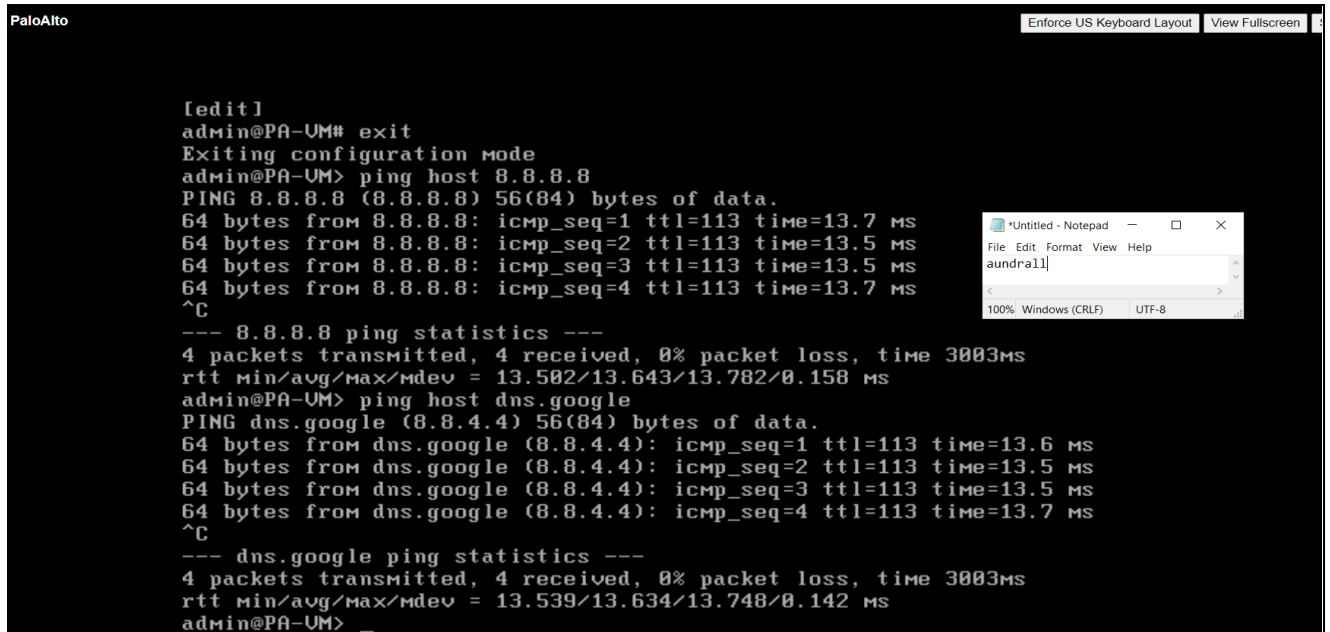
**SUBMITTED BY**

AKHILESH ANAND UNDRALLA

## TABLE OF CONTENTS

Task 1	3
Task 2	3
Task 3	4
Task 4	4
Task 5	5
Task 6	5
Task 7	6
Task 8	6
Task 9	7
Task 10	7
Task 11	7

## Task 1

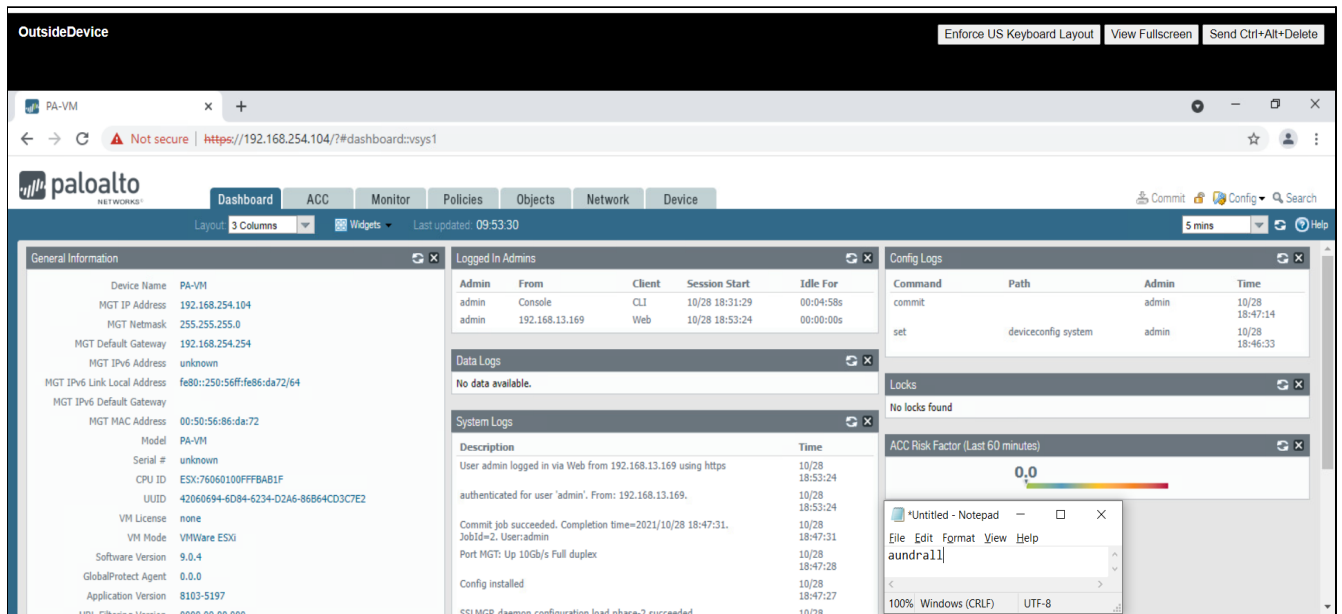


The screenshot shows a terminal window for a Palo Alto VM. The user has entered the command 'exit' to leave configuration mode and then 'ping host 8.8.8.8'. The output shows four successful ping requests with a time of 13.7 ms. Then, the user enters 'ping host dns.google', and the output shows four successful ping requests with a time of 13.6 ms. A Notepad window is open in the background with the text 'aundral1'.

```
[edit]
admin@PA-VM# exit
Exiting configuration mode
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=113 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=13.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=13.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=13.7 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 13.502/13.643/13.782/0.158 ms
admin@PA-VM> ping host dns.google
PING dns.google (8.8.4.4) 56(84) bytes of data.
64 bytes from dns.google (8.8.4.4): icmp_seq=1 ttl=113 time=13.6 ms
64 bytes from dns.google (8.8.4.4): icmp_seq=2 ttl=113 time=13.5 ms
64 bytes from dns.google (8.8.4.4): icmp_seq=3 ttl=113 time=13.5 ms
64 bytes from dns.google (8.8.4.4): icmp_seq=4 ttl=113 time=13.7 ms
^C
--- dns.google ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 13.539/13.634/13.748/0.142 ms
admin@PA-VM>
```

Figure 1: Ping dns.google.com via IP

## Task 2



The screenshot shows the Palo Alto Networks Web-GUI. The 'System Logs' tab is selected, showing a list of logs. The 'General Information' tab is also visible, showing details about the device. A Notepad window is open in the background with the text 'aundral1'.

**General Information**

Field	Value
Device Name	PA-VM
MGT IP Address	192.168.254.104
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:da72/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:50:56:86:da:72
Model	PA-VM
Serial #	unknown
CPU ID	ESX:76060100FFB81F
UUID	42060694-6D84-6234-D2A6-86B64CD3C7E2
VM License	none
VM Mode	VMWare ESXi
Software Version	9.0.4
GlobalProtect Agent	0.0.0
Application Version	8103-5197

**System Logs**

Description	Time
User admin logged in via Web from 192.168.13.169 using https	10/28 18:53:24
authenticated for user 'admin'. From: 192.168.13.169.	10/28 18:53:24
Commit job succeeded. Completion time=2021/10/28 18:47:31.	10/28 18:47:31
Port MGT: Up 10Gb/s Full duplex	10/28 18:47:28
Config installed	10/28 18:47:27
SQL MGT: daemon configuration load phase-2 succeeded	10/28 18:47:27

**Config Logs**

Command	Path	Admin	Time
commit		admin	10/28 18:47:14
set	deviceconfig system	admin	10/28 18:46:33

Figure 2: Web-GUI

## Task 3

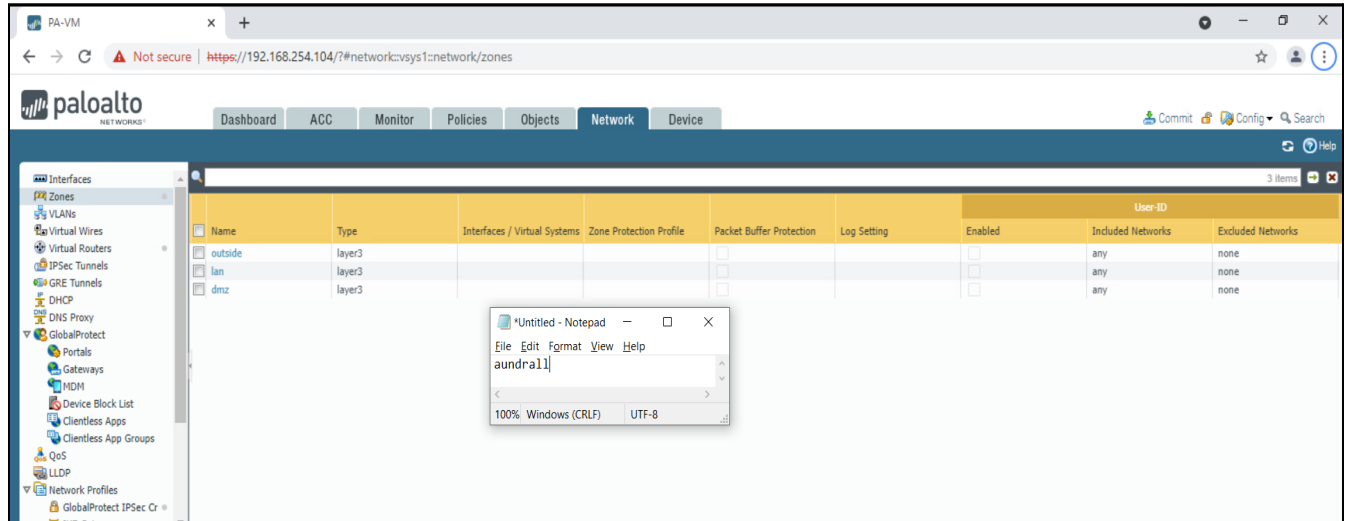


Figure 3: Zone configuration

## Task 4

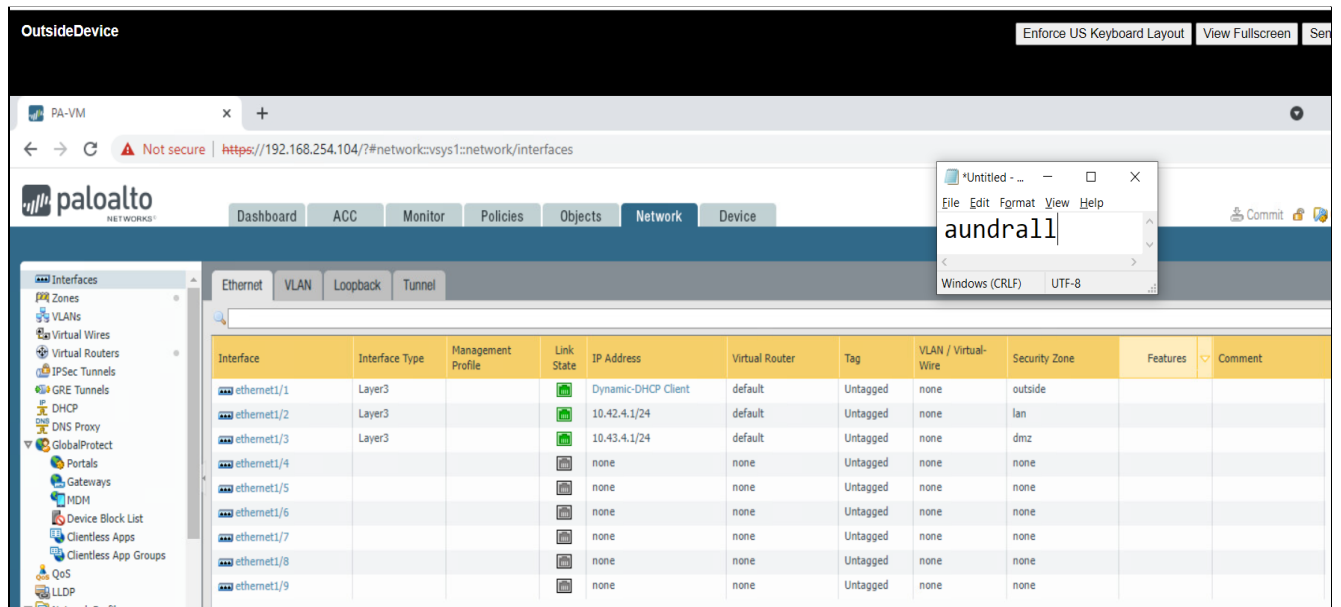
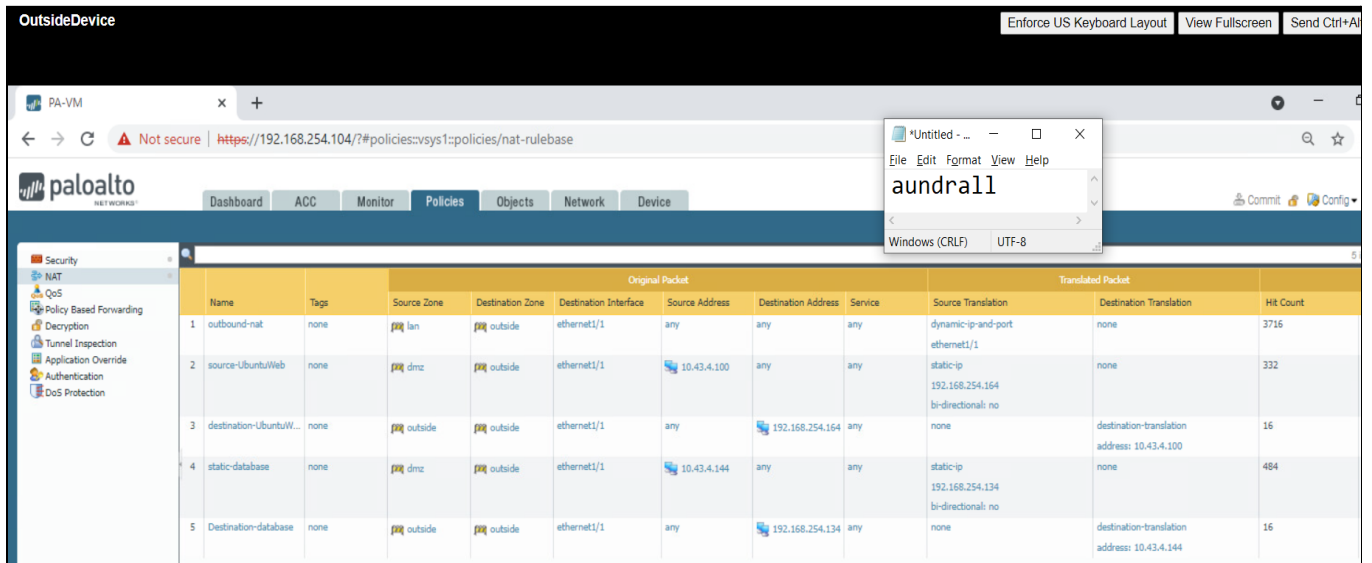


Figure 4: Interfaces configuration

## Task 5



The screenshot shows the Palo Alto Networks PA-VM interface. The 'Policies' tab is selected, displaying a list of NAT policies. A text editor window is open in the foreground with the word 'aundrall'.

	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count
1	outbound-nat	none	lan	outside	ethernet1/1	any	any	any	dynamic-ip-and-port	none	3716
2	source-UbuntuWeb	none	dmz	outside	ethernet1/1	10.43.4.100	any	any	static-ip 192.168.254.164	none	332
3	destination-UbuntuW...	none	outside	outside	ethernet1/1	any	192.168.254.164	any	none	destination-translation address: 10.43.4.100	16
4	static-database	none	dmz	outside	ethernet1/1	10.43.4.144	any	any	static-ip 192.168.254.134	none	484
5	Destination-database	none	outside	outside	ethernet1/1	any	192.168.254.134	any	none	destination-translation address: 10.43.4.144	16

Figure 5: NAT Policies

## Task 6

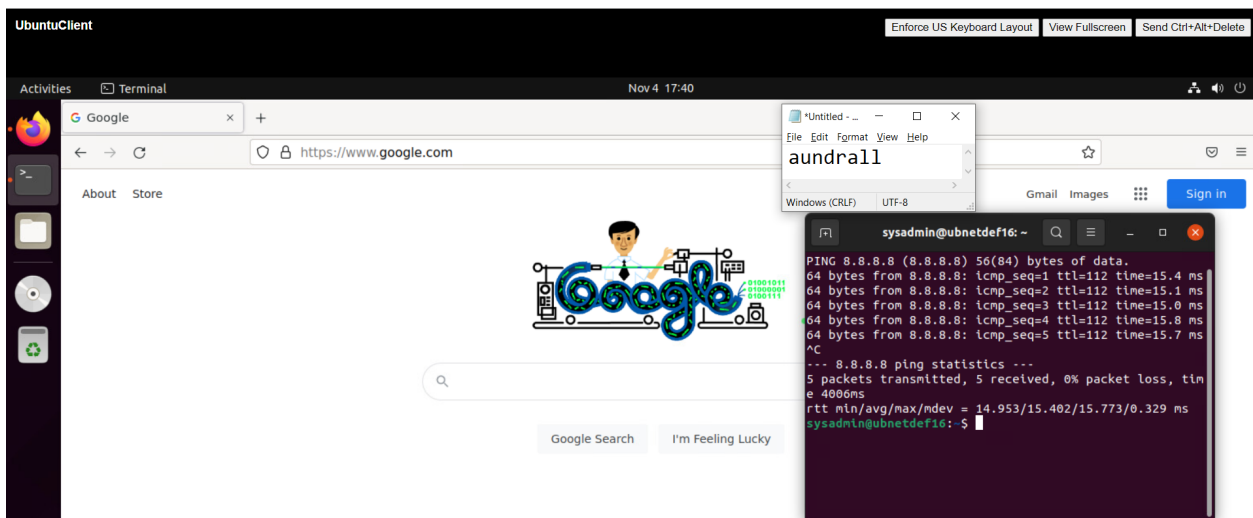


Figure 6: Connection to *outside*(Google)

## Task 7

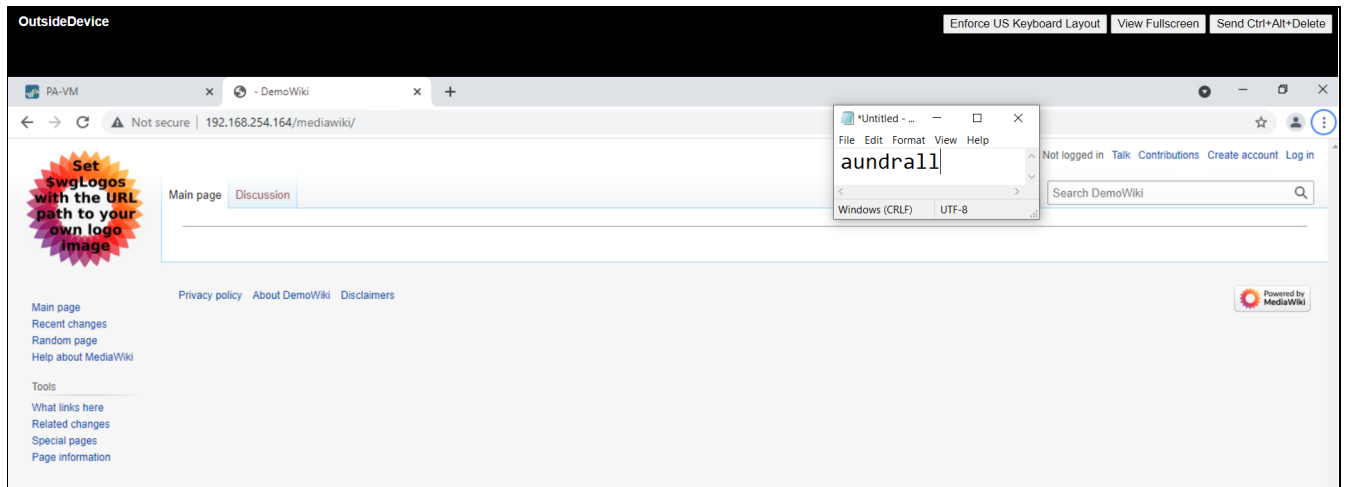


Figure 7: Navigate to Mediawiki (UbuntuWeb)

## Task 8

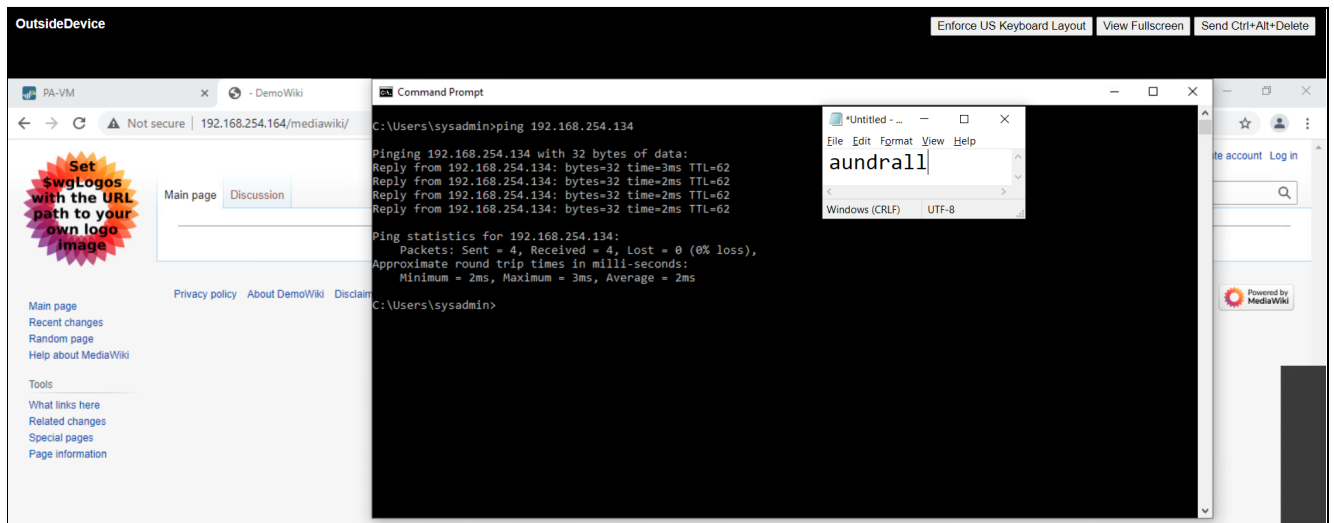


Figure 8: Ping OutsideDevice - RockyDB

## Task 9

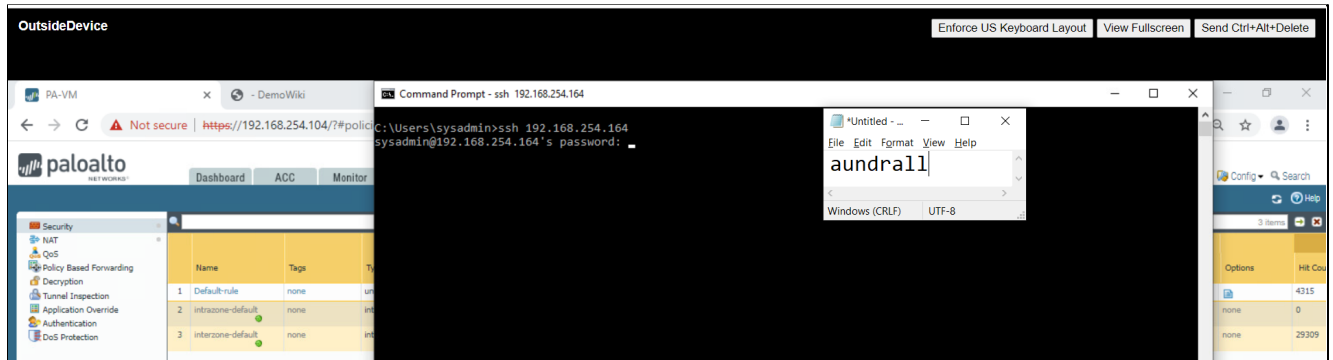


Figure 9: SSH OutsideDevice - UbuntuWeb

## Task 10

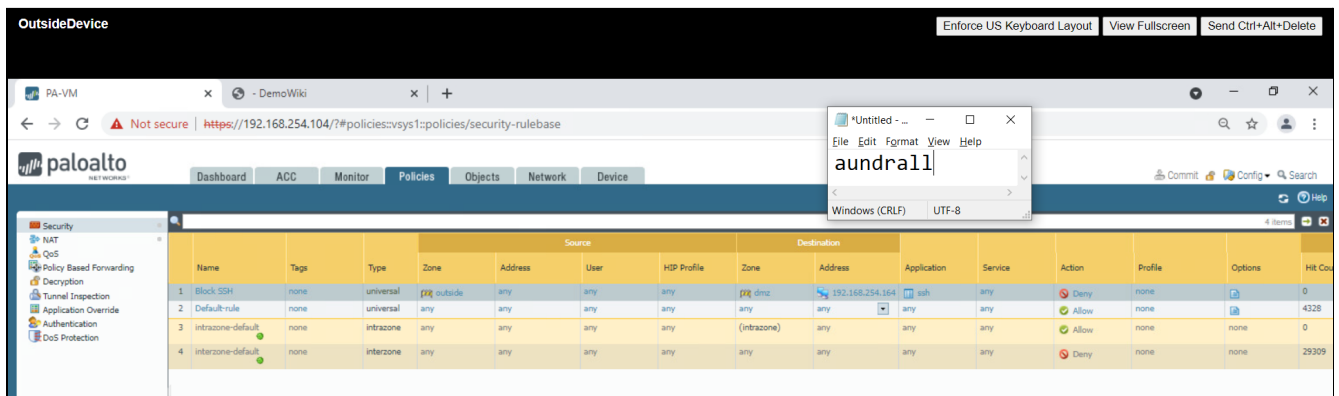


Figure 10: NGFW Security Policy to block SSH connections

## Task 11

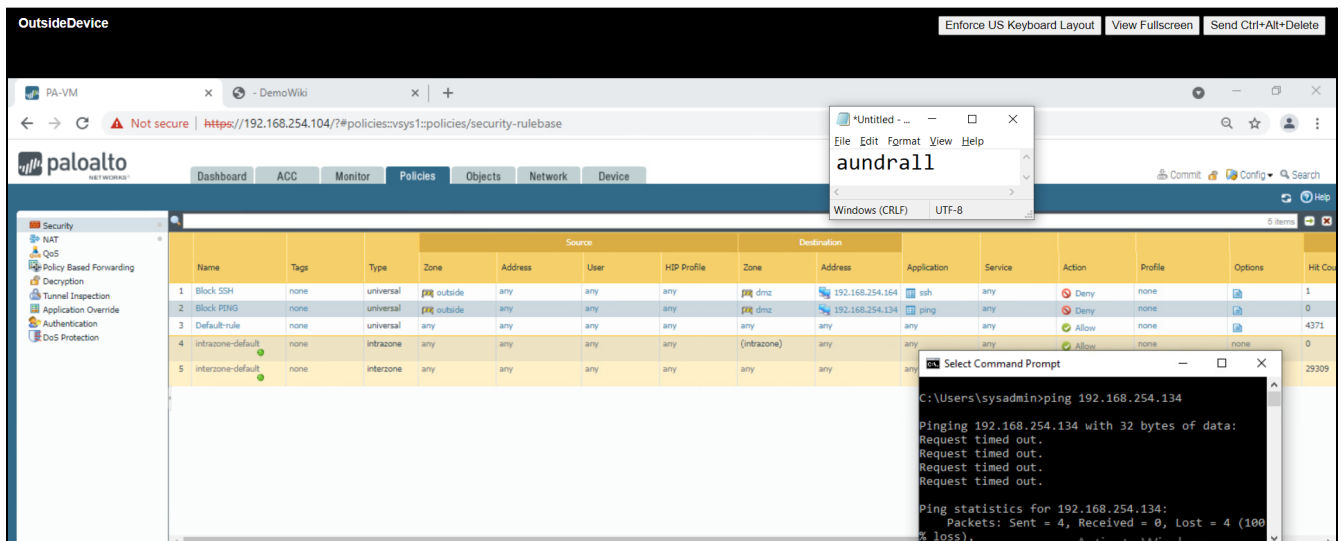


Figure 11: Security Policy to block ping to RockyDB