Delay Before Password Prompt Appears while you Login via SSH/Telnet

Contents

Introduction

This document describes the delay before password prompt appears while you login via SSH/Telnet.

This issue is commonly observed when you attempt to login via SSH or Telnet to the mgmt0 interface on a Nexus 5K/6K.

After you enter the User ID, this text is shown and there is a longer delay as expected, before the password prompt appears.

```
login as: admin
<delay for several seconds before below text is appears>
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password:
```

Problem: Delay before Password Prompt Appears while you Login via SSH/Telnet

The problem happens because of Reverse DNS Lookup.

By default, ip domain-lookup is enabled on the Nexus and if a DNS server list (ip name-server) is configured under VRF Management then the switch will perform a reverse DNS lookup of the user's source IP address whenever they connect to the mgmt0 port via SSH or Telnet.

A reverse DNS lookup is intended for security purposes to verify that the source IP address is legitimate and to prevent IP spoofing.

Here is an example where we used a DNS server 10.67.84.45

The DNS server in this case does not have an entry for the source IP address of the client and it does not provide a response. This results in the Nexus switch performing multiple queries, as the server does not return a result hence this causes the delay.

```
ip domain-lookup
```

```
vrf context management
  ip name-server 10.67.84.45
```

From this output of **show hosts**, you can see that there is a DNS server configured for VRF Management and that IP domain lookup is enabled.

```
N5548P-2# show hosts
DNS lookup enabled

Name servers for vrf:management is  10.67.84.45

Host                    Address
```

These Ethanalzyer captures were taken after the username is entered and you wait for the password prompt to appear.

It shows that the Nexus switch performs two reverse DNS lookups against the user's source IP address, 62.84.137.10

SSH to the N5K mgmt0 interface

```
Username: admin
<delay for several seconds>

N5548P-2# ethanalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:11:44.105674  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2015-05-09 22:11:49.102673  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa

N5548P-2# 2 packets captured
The password prompt is then displayed for the user
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password
:
```

Similarly, when you login via Telnet, the switch first performs the above reverse DNS lookup on the user's source IP address and then displays the login prompt.

Telnet to the N5K mgmt0 interface

```
telnet to switch 10.67.84.56
N5548P-2# ethanalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:24:56.303878  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2015-05-09 22:25:01.302680  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2 packets captured
```

The login prompt is then displayed:

```
Nexus 5000 Switch
login: admin
Password:
```

Solution

Solution 1. Modify the list of DNS servers configured on the Nexus, so that the responsive DNS server is consulted before the non-responsive DNS server.

If the Nexus receives a valid DNS record from the local DNS server then it will not consult the second DNS server in the list. This reduces the delay.

Example:

```
vrf context management
no ip name-server 10.67.84.45
ip name-server  10.67.84.48 10.67.84.45
```

You can use these command to verify the current list of DNS servers where the local server appears first in the list:

```
N5548P-2# sh hosts
DNS lookup enabled

Name servers for vrf:management is  10.67.84.48 10.67.84.45

Host                    Address
```

From these Ethanalyzer capture, first the IP to name lookup is performed and a response is received.

This is followed by a name-to-IP address lookup where a response is received.

In this case, there was no noticeable delay observed when logging in via SSH or Telnet.

```
N5548P-2# ethanalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:55:46.037079  10.67.84.56 -> 10.67.84.48 DNS Standard query PTR
 20.196.104.64.in-addr.arpa
2015-05-09 22:55:46.037444 10.67.84.48 -> 10.67.84.56  DNS Standard query res
ponse PTR no-sense-1.cisco.com
2015-05-09 22:55:46.041907  10.67.84.56 -> 10.67.84.48 DNS Standard query A n
o-sense-1.cisco.com
2015-05-09 22:55:46.042295 10.67.84.48 -> 10.67.84.56  DNS Standard query res
ponse A 64.104.196.20
```

Solution 2. Remove the DNS list from the management VRF.

Example:

vrf context management

```
no ip name-server 10.67.84.48 10.67.84.45
```

- Disable IP domain lookup

```
no ip domain-lookup
```

> **Note**: There is an enhancement request open for disable reverse DNS lookup for SSh/Telnet.

CSCur27501 Disable r-DNS lookup for SSH/Telnet