SSH/Telnet経由でログインすると、パスワードプロンプトが表示される

内容

概要

このドキュメントでは、SSH/Telnet経由でログインする際に、パスワードプロンプトが表示される前の遅延について説明します。

この問題は、Nexus 5K/6K上のmgmt0インターフェイスにSSHまたはTelnetでログインしようとすると、一般に発生します。

ユーザIDを入力すると、次のテキストが表示され、パスワードプロンプトが表示される前に、予想よりも長い遅延が発生します。

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

問題：SSH/Telnet経由でログインしている間にパスワードプロンプトが表示される前の遅延

この問題は、逆DNSルックアップが原因で発生します。

デフォルトでは、Nexusでip domain-lookupが有効になっており、VRF ManagementでDNSサーバリスト(ip name-server)が設定されている場合、スイッチはSSHまたはTelnet経由でmgmt0ポートに接続するたびに、ユーザの送信元IPアドレスの逆DNSルックアップをを実行します。

リバースDNSルックアップは、送信元IPアドレスが正当であることを確認し、IPスプーフィングを防止するためのセキュリティ目的に使用されます。

DNSサーバ10.67.84.45を使用した例を次に示します

この場合、DNSサーバにはクライアントの送信元IPアドレスのエントリがなく、応答がありません。この結果、Nexusスイッチは複数のクエリを実行します。サーバが結果を返さないため、遅延が発生します。

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

show hostsのこの出力から、VRF管理用に設定されたDNSサーバがあり、IPドメインルックアップが有効になっていることがわかります。

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

Name servers for vrf:management is  10.67.84.45

Host                    Address
```

これらのEthanalzyerキャプチャは、ユーザ名が入力され、パスワードプロンプトが表示されるまで待ってから取得されたものです。

これは、Nexusスイッチが、ユーザの送信元IPアドレス62.84.137.10に対して2つの逆DNSルックアップを実行することを示しています

N5K mgmt0インターフェイスへのSSH

```
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
:
```

同様に、Telnet経由でログインすると、スイッチはまずユーザの送信元IPアドレスで上記の逆DNSルックアップを実行し、ログインプロンプトを表示します。

N5K mgmt0インターフェイスへのTelnet

```
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
```

ログインプロンプトが表示されます。

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

解決方法

解決策1. Nexusで設定したDNSサーバのリストを変更し、応答しないDNSサーバの前に応答するDNSサーバを調べます。

Nexusがローカルサーバから有効なDNSレコードを受信した場合、リスト内の2番目のDNSサーバを参照しません。これにより、遅延が減少します。

例：

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

ローカルサーバがリストの最初に表示されるDNSサーバの現在のリストを確認するには、次のコマンドを使用できます。

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

Name servers for vrf:management is  10.67.84.48 10.67.84.45

Host                    Address
```

これらのEthanalyzerキャプチャから、最初に名前検索のIPが実行され、応答が受信されます。

次に、応答を受信する名前からIPアドレスへのルックアップを行います。

この場合、SSHまたはTelnetを介してログインする際に顕著な遅延は発生しませんでした。

```
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
```

解決策2：管理VRFからDNSリストを削除します。

例：

VRFコンテキスト管理

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

- IPドメインルックアップを無効にする

```
no ip domain-lookup
```

注：SSh/Telnetの逆DNSルックアップを無効にする拡張要求が開いています。

CSCur27501 SSH/Telnetのr-DNSルックアップを無効にする