pfSense - Todo #8245

use delayed compression for sshd

12/29/2017 08:08 PM - Art Manion

Status:	Resolved	**Start date:**	12/29/2017
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	2.4.3		

Description

FreeBSD default sshd config is "compression delayed". [1] This defends against vulnerabilities like CVE-2016-10012 [2]. This also came up in a PCI compliance scan FWIW. I'm not aware of any reason not to use "compression delayed".

My pfSense and sshd version info:
2.4.2-RELEASE-p1 (amd64)
built on Tue Dec 12 13:14:55 CST 2017
FreeBSD 11.1-RELEASE-p6

OpenSSH_7.2p2, OpenSSL 1.0.2m-freebsd 2 Nov 2017

Simple patch:

```
[2.4.2-RELEASE][foo@bar]/root: diff ~~u /etc/sshd.0 /etc/sshd~~
-- /etc/sshd.0    2017-12-29 18:19:10.642116000 -0500
+++ /etc/sshd    2017-12-29 18:20:31.265030000 -0500
@ -81,7 +81,7 @
foreach ($keys as $key) {
$sshconf .= "HostKey {$sshConfigDir}/ssh_host_{$key['suffix']}key\n";
}
-$sshconf .= "Compression yes\n";
+$sshconf .= "Compression delayed\n";
$sshconf .= "ClientAliveInterval 30\n";
$sshconf .= "PermitRootLogin yes\n";
if (isset($config['system']['ssh']['sshdkeyonly'])) {
```

[1] https://www.freebsd.org/cgi/man.cgi?sshd_config(5)
[2] https://nvd.nist.gov/vuln/detail/CVE-2016-10012

Associated revisions

Revision 4cad9a5b - 01/16/2018 01:15 PM - Jim Pingle

Change sshd compression to 'delayed' to match current FreeBSD default. Fixes #8245

Revision 08bdeb89 - 01/16/2018 01:15 PM - Jim Pingle

Change sshd compression to 'delayed' to match current FreeBSD default. Fixes #8245

(cherry picked from commit 4cad9a5bd1666c9bd5ce32b82f9b897dbbe5a5bf)

Revision 3c73e81d - 01/16/2018 01:15 PM - Jim Pingle

Change sshd compression to 'delayed' to match current FreeBSD default. Fixes #8245

(cherry picked from commit 4cad9a5bd1666c9bd5ce32b82f9b897dbbe5a5bf)

Revision 8d403391 - 01/16/2018 01:15 PM - Jim Pingle

Change sshd compression to 'delayed' to match current FreeBSD default. Fixes #8245

(cherry picked from commit 4cad9a5bd1666c9bd5ce32b82f9b897dbbe5a5bf)

History

#1 - 12/29/2017 08:11 PM - Art Manion

```
[2.4.2-RELEASE][foo@bar]/root: diff -u /etc/sshd.0 /etc/sshd
-- /etc/sshd.0 2017-12-29 18:19:10.642116000 -0500
+++ /etc/sshd 2017-12-29 18:20:31.265030000 -0500
@ -81,7 +81,7 @@
foreach ($keys as $key) {
$sshconf .= "HostKey {$sshConfigDir}/ssh_host_{$key['suffix']}key\n";
}
-$sshconf .= "Compression yes\n";
+$sshconf .= "Compression delayed\n";
$sshconf .= "ClientAliveInterval 30\n";
$sshconf .= "PermitRootLogin yes\n";
if (isset($config['system']['ssh']['sshdkeyonly'])) {
```

#2 - 01/16/2018 01:30 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 4cad9a5bd1666c9bd5ce32b82f9b897dbbe5a5bf.

#3 - 02/15/2018 01:39 PM - Jim Pingle

- Status changed from Feedback to Resolved

Delayed compression is in sshd_config on current snaps.