pfSense - Feature #6457

Allow ability to configure AWS EC2 AMI via userdata

06/06/2016 08:50 PM - Danny Schuh

Status:	New	**Start date:**	06/06/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Installer	**Estimated time:**	0.00 hour
Target version:	Future		

Description

Most AWS EC2 AMIs allow you to configure many aspects of the instances that you are launching via the 'userdata'. Currently the pfSense AMI supplied by NetGate only allows us to configure the management network and the default admin user password. Having the ability to configure the instance with values supplied via the instance 'userdata' allows end-users to be able to launch instances configured in a manner that they are ready for use. Some examples that would be nice to have, but certainly can be expanded upon:
Management UI Port(1) - Allow the end-user to supply a port that sets $config[system][webui][port], and also automatically adds an appropriate rule to allow traffic
Management SSH Port(1) - Allow the end-user to supply a port that sets $config[system][ssh][port], and also automatically adds an appropriate rule to allow traffic
Enable SSH Management(1) - Allow the end-user to supply a boolean that sets $config[system][enablesshd]
Enable default VPN Configuration(2) - Allow the end-user to supply a boolean that tells the system to configure all of the openVPN/IPSec VPN configuration that currently comes with the AMI
Packages to Install - Allow the end-user to supply a list of package names to install (examples: haproxy,snort)
Package Configuration Array - Allow the end-user to supply an array to configure all packages given in above list that will set $config[installedpackages][$packagename]
NAT Configuration Array - Allow the end-user to supply an array to set $config[nat]
Rules Configuration Array - Allow the end-user to supply an array to set $config[filter][rule]

Notes:
1) Allowing the user to configure the default management ports (for SSH as well as WebUI) enables the user to set the correct security groups when launching the instance. If you have the WebUI and SSH listening on their current defaults (80/443/22), and production traffic for the end-user application listens on these ports, extra measures have to be taken while the instance is reconfigured to keep the newly created instance secure and also to not cause application service interruptions. Allowing SSH enabled during launch allows for automation tools like ansible to run against this instance once the instance is in the running state.
2) The current AMI ships with a lot of default configuration to make the pfSense appliance a VPN-based appliance. This is a great feature, but it would be great if it was able to be enabled by request. For end-users that wish to use the pfSense only for its firewall filtering and forwarding capabilities, this causes manual configuration (or de-configuration) before it can be put into production.

History

#1 - 06/06/2016 09:43 PM - Danny Schuh

Missed a pretty important one:
Interfaces - Allow the end-user to supply an array to configure the interfaces

#2 - 06/08/2016 10:53 PM - Danny Schuh

Thinking through this, it may be easier to supply a userdata dictionary who's value is an S3 object that is a recorded session to be automatically played back like what is mentioned here: https://doc.pfsense.org/index.php/Using_the_PHP_pfSense_Shell#Playing_back_a_session

This would allow ansible-tooled (or whatever the end-user uses) deployments to template out an S3-stored configuration during instance launch, eliminating any need to have hands on the unit.

#3 - 06/08/2016 11:18 PM - Jim Thompson

- Assignee changed from Jeremy Porter to Matthew Smith

#4 - 09/20/2017 09:46 AM - Clinton Cory

Internal redmine ticket related to one of the user data options:
https://redmine.netgate.com/issues/162

#5 - 03/14/2018 12:08 PM - John Burwell

A means of running a shell script in some manner as root at first launch would be helpful, a la `fetch -o - $USER_SCRIPT_URL | sh -s`

#6 - 09/21/2020 02:54 PM - Renato Botelho

- Assignee deleted (Matthew Smith)