Armada Data Solutions

Configuring Tripwire for Palo Alto Networks firewalls

Utilizing Tripwire to track changes to a Palo Alto Network firewall

James Costello
1/20/2012

Configuring Tripwire for Palo Alto Networks firewalls

Description

Tripwire® Enterprise is the market-leading solution for IT configuration control: a single source for assessing IT configurations and detecting, analyzing and reporting on change activity across the breadth of the IT infrastructure. Tripwire Enterprise monitors everything from servers and desktops to directory servers, hypervisors, databases, middleware applications and network devices.

The following configuration document is intended to assist with setting up a Tripwire Enterprise solution to monitor the configurations of Palo Alto Networks firewalls. Certain portions of this document are left general while others are more specific to the Palo Alto Networks firewall**.** This documentation is based on TripWire Enterprise 8.1.

Assumptions

- Familiarity with TripWire Enterprise
- Familiarity with Administrator configuration for Palo Alto Networks firewalls

Requirements

- IP address of the Palo Alto Firewall
- Username and password for login - a read only superuser account would be appropriate. It is also possible to use certificate based logon.

Process

Create a new Node object

As this is the first Palo Alto Network firewall object you are creating, it is a good practice to create a new node group

1. Click on the NODES tab of the Manager bar
    a. If there is an existing node group that will hold the new node group, select it. Otherwise select the top of the tree
2. Click Manage
    a. Select New Group
    b. Enter a name and optionally a description for the group being created.

A Linux based object with SSH connection will now need to be created next.

3. Select the node group create above or the appropriate node group
4. Click Manage
    a. Select New Node
    b. From the Network Device - Custom folder menu item select a custom node type of Linux and click OK
    c. Using the IP address or assigned DNS name and the password or certificate to connect
    d. Complete the remainder of New Node Wizard

Repeat this process for any other firewalls in the environment

Create a new Rule for the Palo Alto Networks firewall

As this will be the first Palo Alto Networks firewall rule, it is good practice to create a new rule group to associate the new rule.

1. Click on the RULES tab of the Manager bar

a. If there is an existing rule group that will hold the new rule group, select it. Otherwise select the top of the tree

2. Click Manage
    a. Select New Group
    b. Enter a name and optionally a description for the group being created

A new Command Output Validation Rule will need to be created.

3. Select the rule group create above or the appropriate rule group
    a. Click New Rule
    b. Select Network Device - Common - Command Output Validation Rule and click OK
        i. Name the new rule using the appropriate conventions
        ii. Enter the following commands in the New Rule Wizard
        iii. pre
            1. set cli terminal type vt100
            2. set cli config-output-format set
            3. set cli pager off
            4. configure
        iv. command to capture
            1. show
        v. post
            1. exit
    c. Complete the New Rule Wizard

Create or assign the rule for the Palo Alto Networks firewall to the firewall

4. Link the rule to the firewall.
    a. In the policy manager, open the property sheet for the newly create rule.
    b. Select the "Nodes" tab, click the "Add" button and select any individual node or group of nodes the policy applies to.

Create a new schedule for the Palo Alto Networks firewall task

Create a schedule for the Task created above for the Palo Alto Networks Firewall
The necessary schedule may already exist for the checks for the firewall. If not, create a new schedule for the

Create a new Task for the Palo Alto Networks firewall and baseline

Create a Task for the Palo Alto Networks firewall

5. Navigate to the task manager.
6. Click the "New Task" button.
    a. Select the node, rules and schedule for the task as part of the wizard
7. When selections are complete, select the option to perform a baseline of the firewall.