

ARUBA CLEARPASS ONGUARD AND-FORTIGATE VPN INTEGRATION

Table of Contents

Context	2
Components Used	2
Workflow	2
Traffic Flow	3
ClearPass configuration	3
Clearpass Onguard Configuration	3
Posture Policy Configuration	4
OnGuard Service Configuration	5
Deployment and Success Criteria:	11
Dependencies	11

Context

This document describes about the Fortigate VPN integration with Clearpass OnGuard. The use case here is to check the system compliance with the third party VPN Solution which is already in place.

With OnGuard we get more granular checks on the Device health. The data we get from the OnGuard could be posted to the FortiGate Firewall using the Rest API's. The same model is supported by FortiGate.

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/912201/clearpass-integration-for-dynamic-address-objects>

API Format used:

```
curl -k -X POST https://<Ip-Address>/api/v2/monitor/firewall/clearpass-address/add -H "Authorization: Bearer7k0w33G4swstdGmGqcz175zH90ybwk" -H "accept: application/json" -H "Content-Type: application/x-www-form-urlencoded" -d '{"endpoint_ip' : ['10.10.10.2', '11.10.10.10', '12.16.8.203'], 'spt': 'healthy'}"
```

Based on the posture information FortiGate Firewall would allow or deny the VPN traffic.

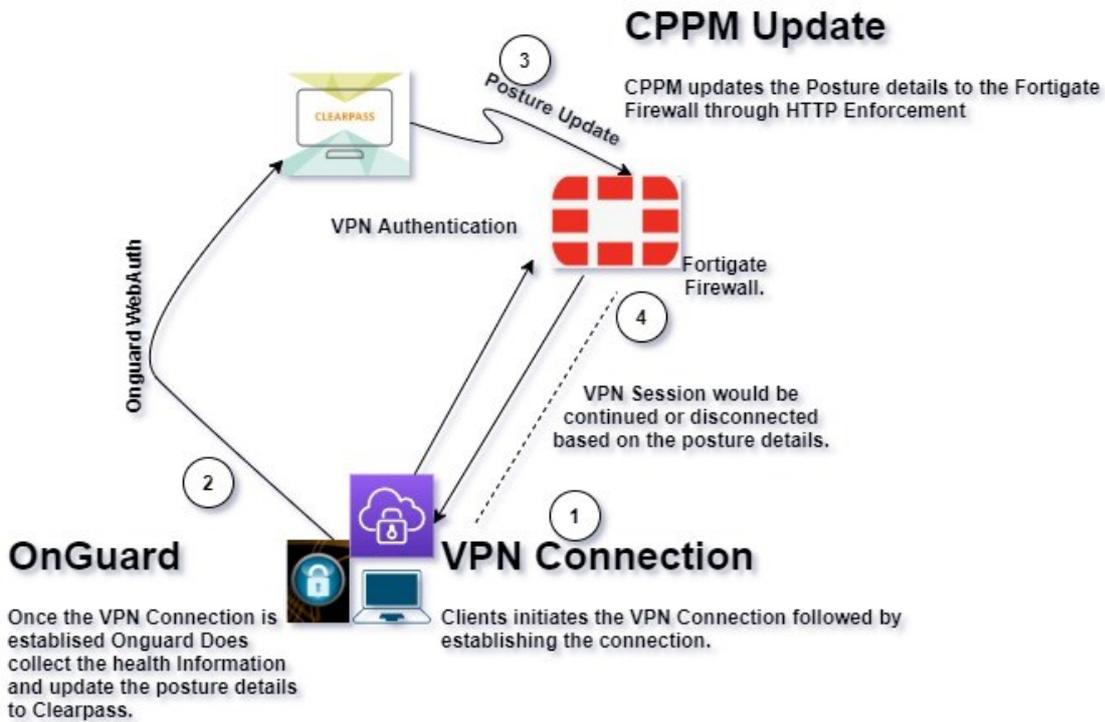
Components Used

1. Clearpass(6.7.0)
2. OnGuard
3. Fortigate Firewall.(6.2.3)
4. POSTMAN to check the CURL

Workflow

- User initiates SSL VPN connection using Fortigate VPN
- OnGuard sends a HTTPS request to ClearPass with the client posture detail
- CPPM Service: *OnGuard WEBAUTH* - (Posture=Healthy)
- ClearPass sends a HTTP Enforcement to the Fortigate Firewall about the User IP & Posture information.
- Based on the Posture Details Client traffic either can be Allowed or Denied on the Fortigate Firewall.

Traffic Flow



ClearPass configuration

Clearpass Onguard Configuration

The screenshot shows the 'OnGuard Settings' configuration page in the ClearPass management console. The page is titled 'Administration > Agents and Software Updates > OnGuard Settings'.

Settings | **Installers** | **Agentless OnGuard**

Agent Version: 6.8.1.109777
Agent Library Version: 10.0.13.109777
Linux Installer Mode: Do not install/enable Aruba VIA component
Note: This WILL remove any existing/installed Aruba VIA client

Agent Customization

Managed Interfaces: Wired Wireless VPN Other
Mode: Authenticate with health checks
Authentication type: Username & Password
Username Text: Username
Password Text: Password
Agent action when an update is available: Download and Install

Agent Remediation User Interface Customization

Custom User Interface: Configure

Native Dissolvable Agent Customization

Managed Interfaces: Wired Wireless VPN Other

Navigation menu on the left includes: Dashboard, Monitoring, Configuration, Administration (ClearPass Portal, Users and Privileges, Server Manager, External Servers, External Accounts, Certificates, Dictionaries, Agents and Software Updates).

Make sure we enable Health Check for VPN Interface alone, this would help OnGuard to collect the health information only when there is a status change in the VPN interface of the User.

Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings -

[Global Agent Settings](#)
[Policy Manager Zones](#)
[ClearPass EULA](#)

Use the OnGuard Settings page to configure the OnGuard agent deployment packages for Windows, macOS, and Linux.

Settings	Installers	Agentless OnGuard
Agent Installers updated at Apr 22, 2020 08:32:16 PDT		
Windows	https://10.67.10.110/agent/installer/windows/ClearPassOnGuardInstall.exe https://10.67.10.110/agent/installer/windows/ClearPassOnGuardInstall.msi https://10.67.10.110/agent/installer/windows/ClearPassOnGuardLibraryUpdate.exe	(Full Install - EXE) 24MB (Full Install - MSI) 24MB (Update Only) 8MB
macOS	https://10.67.10.110/agent/installer/mac/ClearPassOnGuardInstall.dmg https://10.67.10.110/agent/installer/mac/ClearPassOnGuardLibraryUpdate.pkg	(Full Install) 23MB (Update Only) 5MB
Ubuntu	https://10.67.10.110/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz https://10.67.10.110/agent/installer/ubuntu/ClearPassOnGuardLibraryUpdate.tar.gz	(Full Install) 30MB (Update Only) 18MB
CentOS	https://10.67.10.110/agent/installer/rpm/ClearPassOnGuardInstall.tar.gz	(Full Install) 37MB
Red Hat	https://10.67.10.110/agent/installer/rpm/ClearPassOnGuardLibraryUpdate.tar.gz	(Update Only) 19MB
Native Dissolvable Agent Apps		
Windows	https://10.67.10.110/agent/webagent/windows/OnGuard Windows Health Checker.exe https://10.67.10.110/agent/webagent/windows/OnGuard Windows Health Checker Library Update.exe	(Full Install) 10MB (Update Only) 4MB
macOS	https://10.67.10.110/agent/webagent/mac/OnGuard Mac Health Checker.dmg https://10.67.10.110/agent/webagent/mac/OnGuard Mac Health Checker Library Update.pkg	(Full Install) 11MB (Update Only) 5MB
Ubuntu	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker-x86.tar.gz	(Full Install 32-bit) 10MB
CentOS	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker.tar.gz	(Full Install 64-bit) 11MB
Red Hat	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker Library Update-x86.tar.gz	(Update Only 32-bit) 9MB
SUSE	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker Library Update.tar.gz	(Update Only 64-bit) 9MB
Fedora		

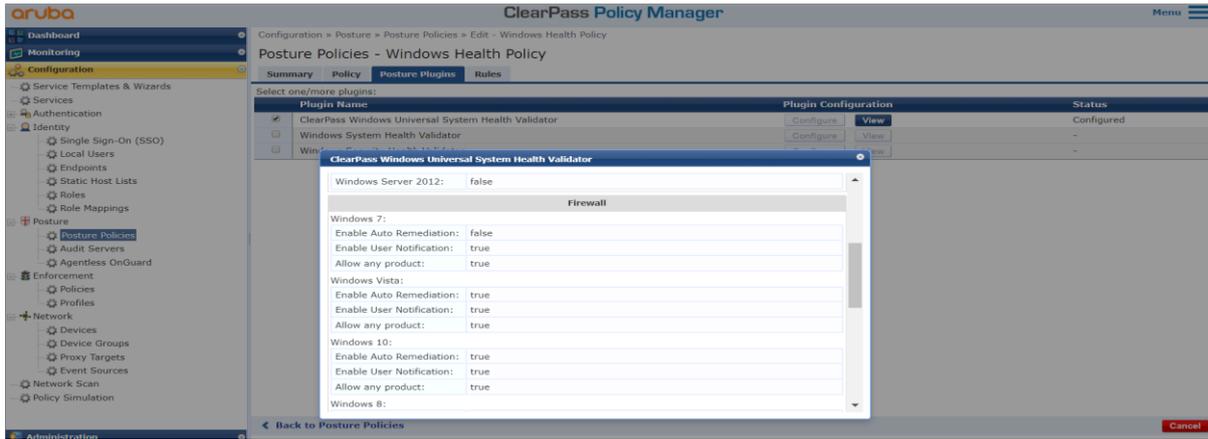
Install the OnGuard Package on the End User system through GPO/or any installation tool.

Posture Policy Configuration

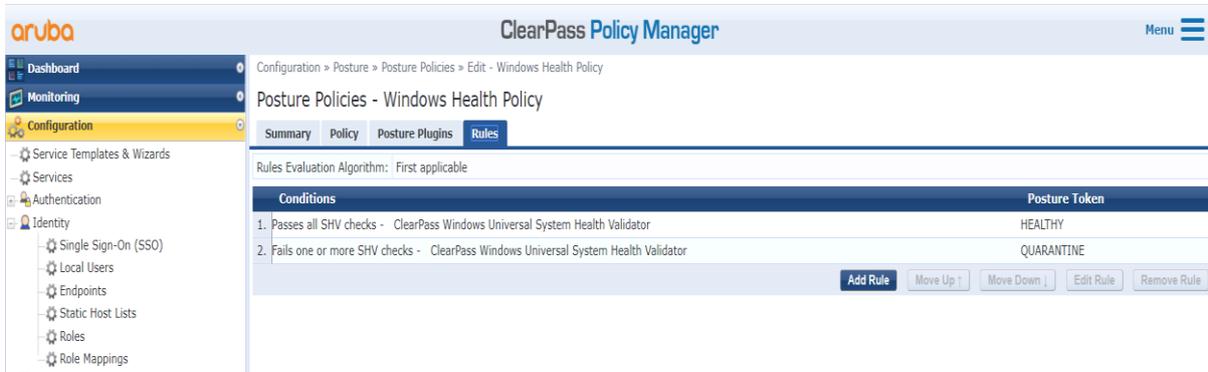
OnGuard Posture Policy needs to be defined in order to derive a system compliance. The configuration has to be done by navigating to Configuration → Posture → Posture Policies.

The screenshot shows the ClearPass Policy Manager interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Posture Policies - Windows Health Policy' and shows the configuration for a specific policy. The 'Policy' tab is active, displaying details such as Policy Name (Windows Health Policy), Description, Posture Agent (Web Agent), Host Operating System (WINDOWS), and Plugin Version (2.0). Below this, there is a section for 'Posture Plugins' with a table listing the selected plugins. The table has columns for Plugin Name, Plugin Configuration, and Status. One plugin, 'ClearPass Windows Universal System Health Validator', is listed with a 'View' button and a status of 'Configured'. At the bottom, the 'Rules' section shows the evaluation algorithm as 'First applicable' and a table of conditions. The conditions table has columns for Conditions and Posture Token. Two conditions are listed: 'Passes all SHV checks - ClearPass Windows Universal System Health Validator' with a 'HEALTHY' token, and 'Fails one or more SHV checks - ClearPass Windows Universal System Health Validator' with a 'QUARANTINE' token.

Define the Posture Plugin for respective OS.



Define the Posture's based on the passed SHV checks.

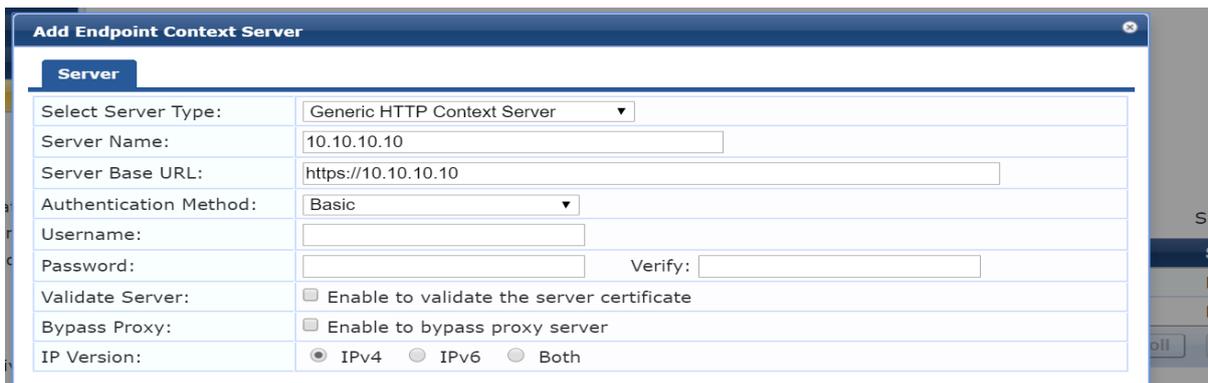


OnGuard Service Configuration

Context Server and Enforcement Profile Creation:

We need to first create the Enforcement Profiles that would push the Posture details to the Fortinet.

Create the Http Context Server followed by create the context server actions associated to it.



Firewall by navigating to Administration → Dictionaries → Context Server Actions and click Add and enter the following URL followed by Header & Content.

Endpoint Context Server Details

Action | Header | Content | Attributes

Server Type: Generic HTTP Context Server

Server Name: 10.10.10.10

Action Name: Send Healthy Token

Description:

HTTP Method: POST

Authentication Method: None

URL: /api/v2/monitor/firewall/clearpass-address/add

Save Cancel

Header :

Endpoint Context Server Details

Action | **Header** | Content | Attributes

Specify the key-value pairs to be included in the HTTP Header -

#	Header Name	Header Value	
1.	Authorization	= Bearer7k0w33G4swstdGmGqcz175zH90ybwk	🗑️
2.	accept	= application/json	🗑️
3.	Content-Type	= application/x-www-form-urlencoded	🗑️
4.	Click to add...		

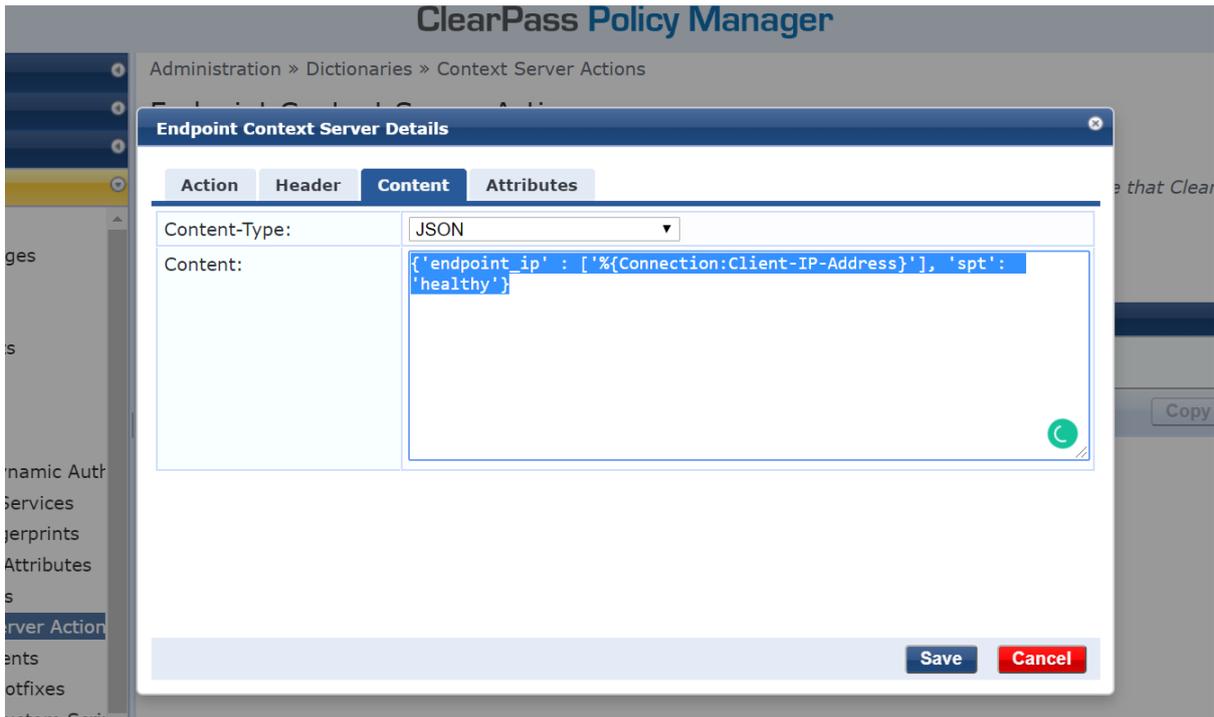
Save Cancel

Content would contain the Posture information along with Username and IP details.

{'endpoint_ip' : ['%{Connection:Client-IP-Address}'], 'spt': 'healthy'} → For Healthy Client

{'endpoint_ip' : ['%{Connection:Client-IP-Address}'], 'spt': 'infected'} → For Infected Client

Depending on the token desired this can be changed accordingly.



The above Context Server Actions are to be included in the HTTP Enforcement profiles in the respective WebAuth Enforcement Policies.

Enforcement Profiles - Firewall Healthy Update

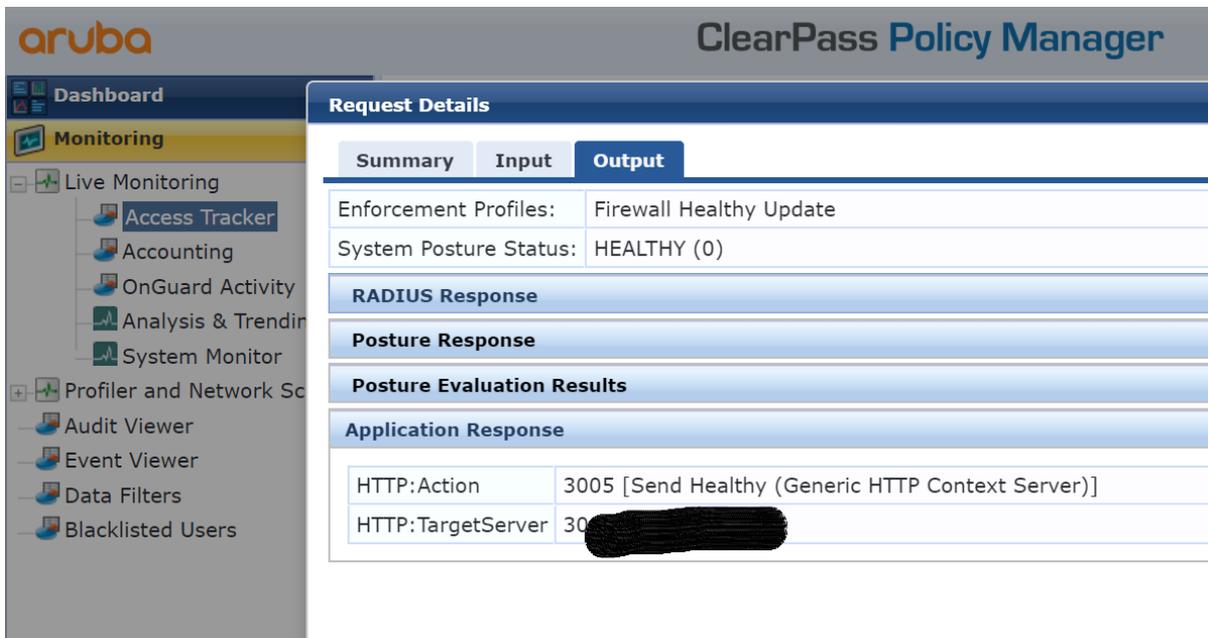
Summary		Profile	Attributes
Profile:			
Name:	Firewall Healthy Update		
Description:			
Type:	HTTP		
Action:	Accept		
Device Group List:	-		
Attributes:			
Attribute Name	Attribute Value		
1. Target Server	[Redacted]		
2. Action	Send Healthy		

OnGuard Service:

We need to map the Posture Policy & HTTP Enforcement created earlier into a Service.

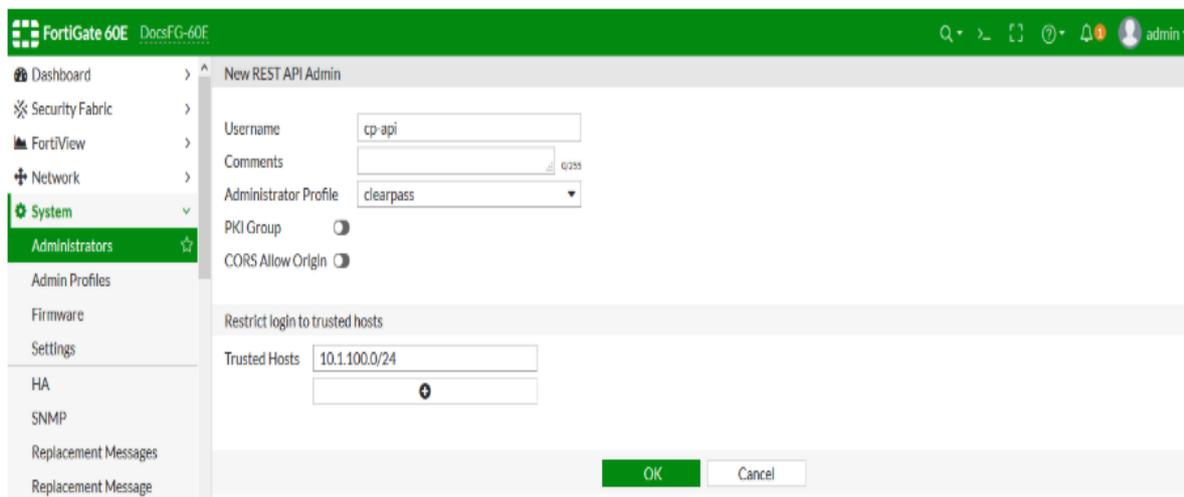


When Onguard sends the WebAuth information, the WebAuth would update the Firewall using the HTTP Enforcement.

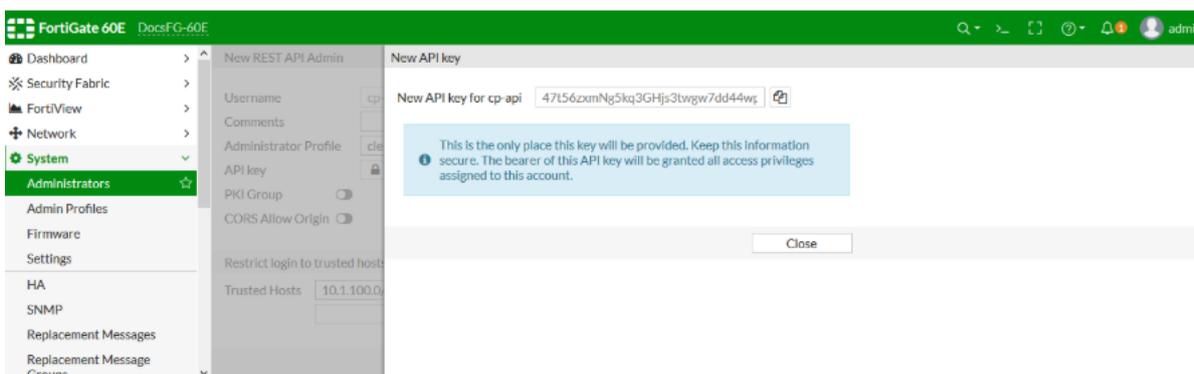


Configuration from FortiGate:

Please create a Rest API Administrator with Read Write access, and please make sure you allow the Clearpass IP Addresses from which the post will be triggered.



Once the Account is created it will provide you the Authorization Bearer Token as below.



Create the Policies on the FortiGate that would accept the Spt Token from Clearpass and decide to allow/deny/partially allow the VPN traffic. In this Example we are creating two policies one is to CPPM & the other one CPPM-Deny, please make sure that Onguard Communication to Clearpass is allowed when CPPM-Deny Policy is applied this is if the client turns to be Healthy OnGuard needs that Information to be sent to Clearpass, which in turn gets updated to Fortigate.

Customers can have multiple policies accordingly, as a backup solution we can have a backup policy in case the any of the policy doesn't fit which means if Spt token from clearpass is not updated/ some issue with policies vpn user traffic would be classified to backup policy and will still be allowed which will be redundant.

Policies can be created from GUI/CLI of Fortigate

config firewall address

```
edit "cppm" !! This policy looks for Token healthy
set uuid 62a180c0-cb36-51e9-6e70-4a2034d82179
set type dynamic
set sub-type clearpass-spt
```

```
set clearpass-spt healthy
set comment ''
set visibility enable
set associated-interface ''
set color 0
next
edit "cppm-deny" !! This policy looks for Token infected
set uuid b318e962-cb36-51e9-7a34-74a34cf3bf0b
set type dynamic
set sub-type clearpass-spt
set clearpass-spt infected
set comment ''
set visibility enable
set associated-interface ''
set color 0
next
end
```

Note : When the policy gets created it is expected that you might see a warning saying **Unresolved Dynamic Objects** or **Error with respect to Fabric Connector's** and this is expected as there

traffic tagged to the Spt tokens. Once Clearpass post the data to the Fortigate the warnings we see on the Policies would be gone.

We can check if the tags are getting applied to the VPN traffic by verifying the policies using CLI

```
diagnose firewall dynamic list
```

List all dynamic addresses:

```
cppm-deny: ID(141)
          ADDR(10.1.100.188)
```

```
cppm: ID(176)
      ADDR(10.1.100.185)
      ADDR(10.1.100.186)
```

Deployment and Success Criteria:

1. We will be installing the OnGuard agent on the identified endpoint device/s or in case of existing deployments you can enable OnGuard to monitor the VPN Interface.
2. Post the VPN session got established BY FortiGate , Aruba ClearPass's Onguard would check the health of the endpoint (Posture Check).
3. Define the posture guidelines on ClearPass
4. Post the Health Status of the Client with IP & token to the Fortigate.
5. Fortigate would apply the policy based on the Spt token.

Dependencies:

1. API account needs to be created on the Fortigate Firewall with Read-Write Access & policies are to be created accordingly.
2. Clearpass Server Ip's are to be allowed in the trust list for the API account created.
3. You might notice Warning with respect to the tags on the Fortigate Firewall which will be eventually gone after the posture tag gets updated.
4. In case you are performing the API check on the POSTMAN please make sure you disable the Certificate Check option in POSTMAN.

*****end of the document*****