aruba
a Hewlett Packard
Enterprise company

ARUBA CLEARPASS ONGUARD AND-FORTIGATE VPN INTEGRATION

Chaitanya DNSS

aruba
a Hewlett Packard Enterprise company

Table of Contents

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 "Cotent-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.

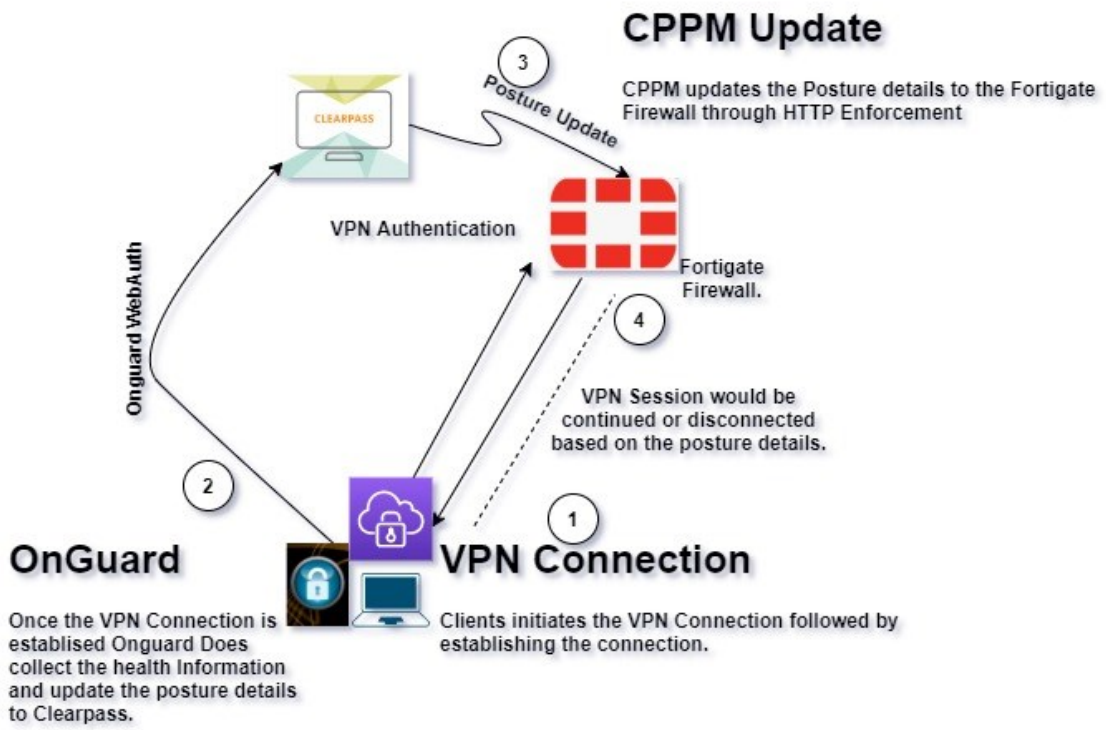
Components Used

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

Workflow

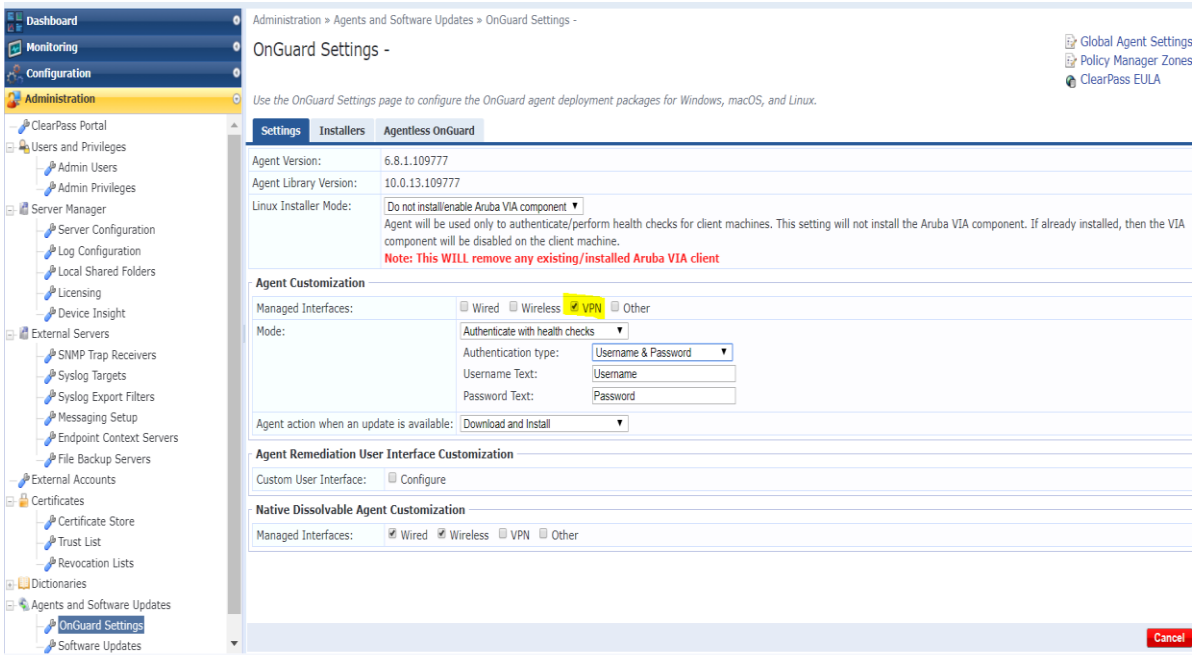
- User initiates SSL VPN connection using Fortigate VPN
- OnGuard sends a HTTPS request to ClearPass with the client posture detail
- CPPM Service: *OnGuard WEBAUTH* - (Posture=Healthy)
- ClearPass sends a HTTP Enforcement to the Fortigate Firewall about the User IP & Posture information.
- Based on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

Traffic Flow

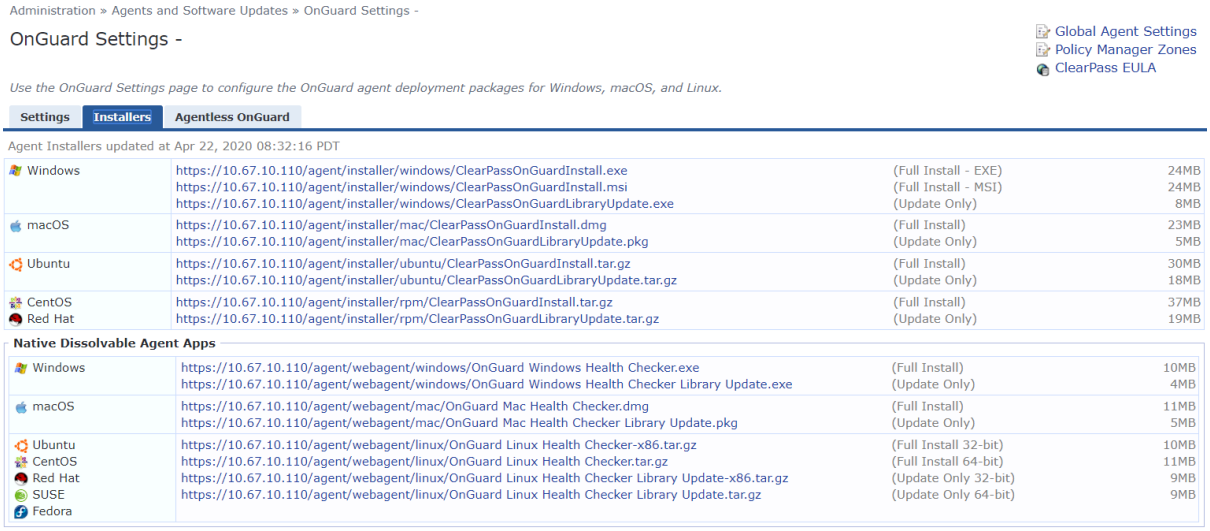


ClearPass configuration

Clearpass Onguard Configuration



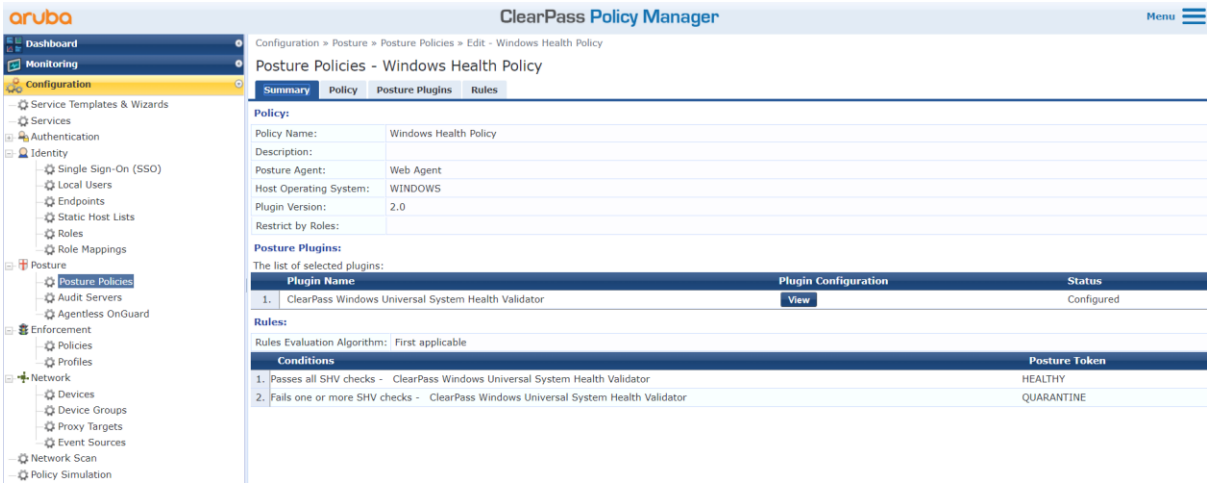
Make sure we enable Health Check for VPN Interface alone, this would help OnGuard to collect the health information only when there is a status change in the VPN interface of the User.



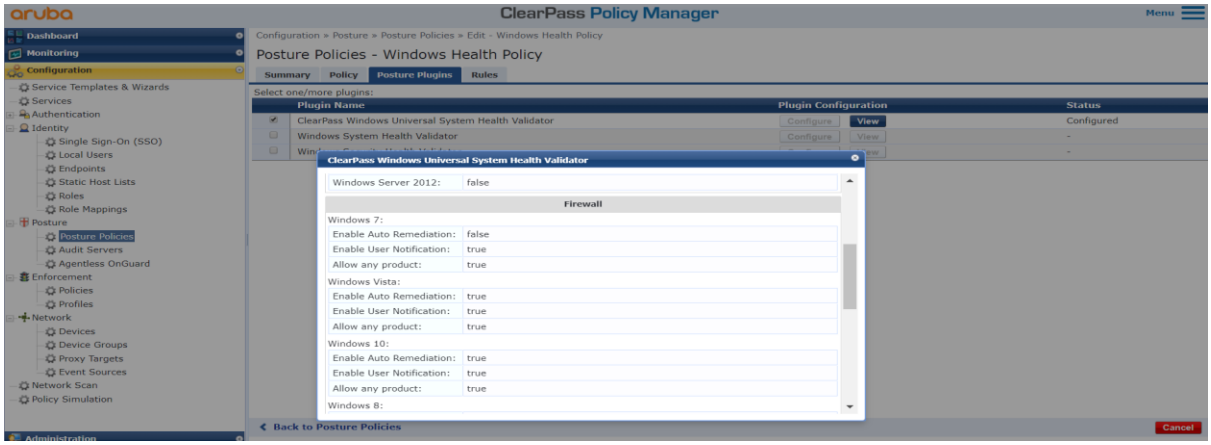
Install the OnGuard Package on the End User system through GPO/or any installation tool.

Posture Policy Configuration

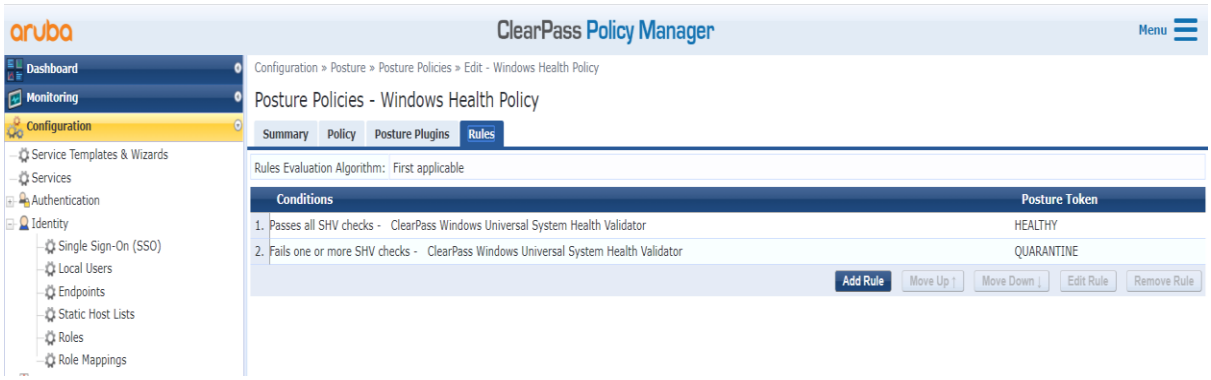
OnGuard Posture Policy needs to defined in order to derive a system compliance. The configuration has to be done by navigating to Configuration ➔ Posture ➔ Posture Polices.



Define the Posture Plugin for respective OS.



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

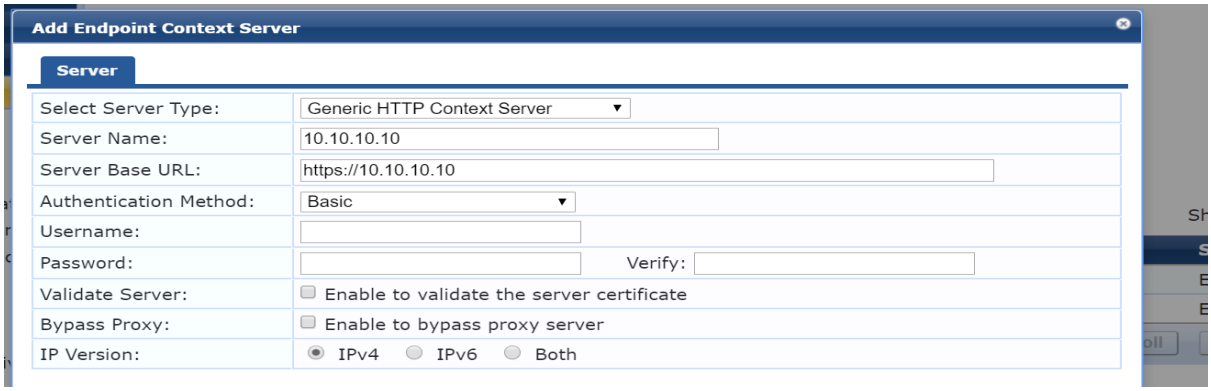


OnGuard Service Configuration

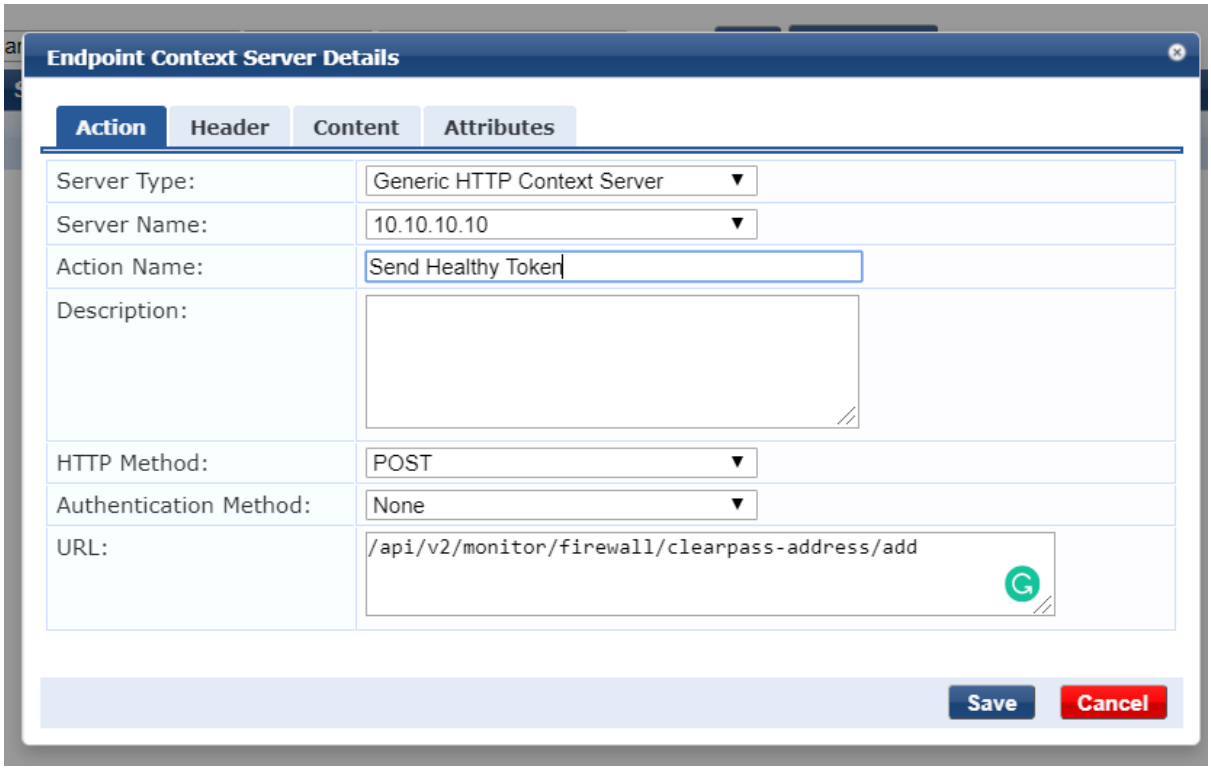
Context Server and Enforcement Profile Creation:

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

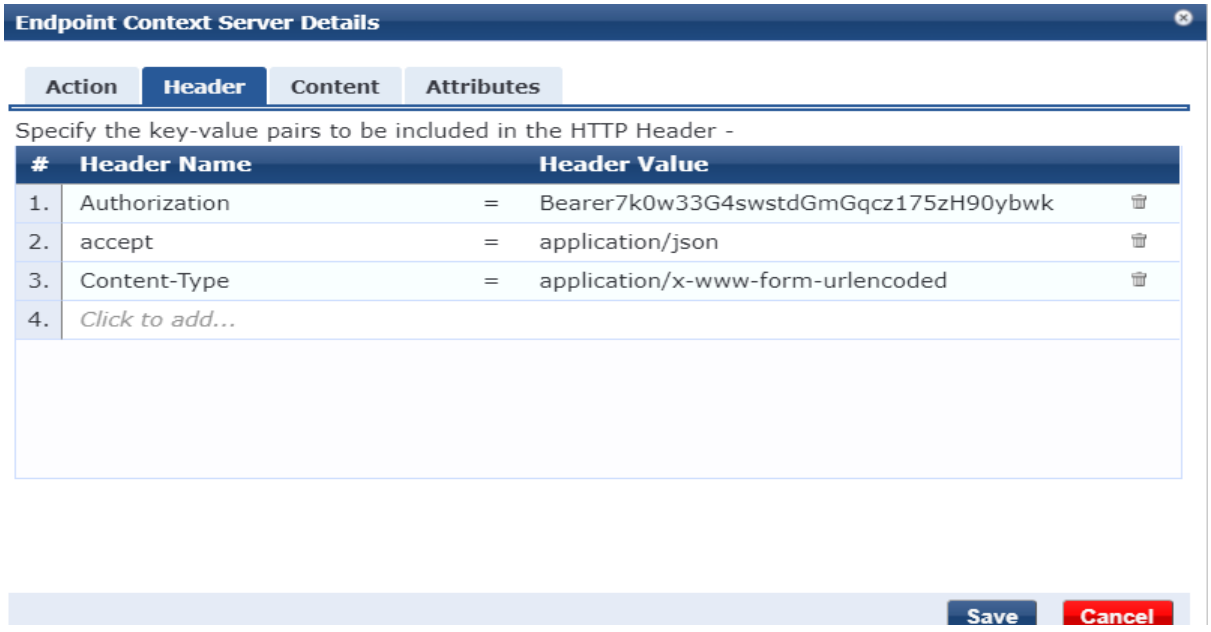
Create the Http Context Server followed by create the context server actions associated to it.



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



Header :

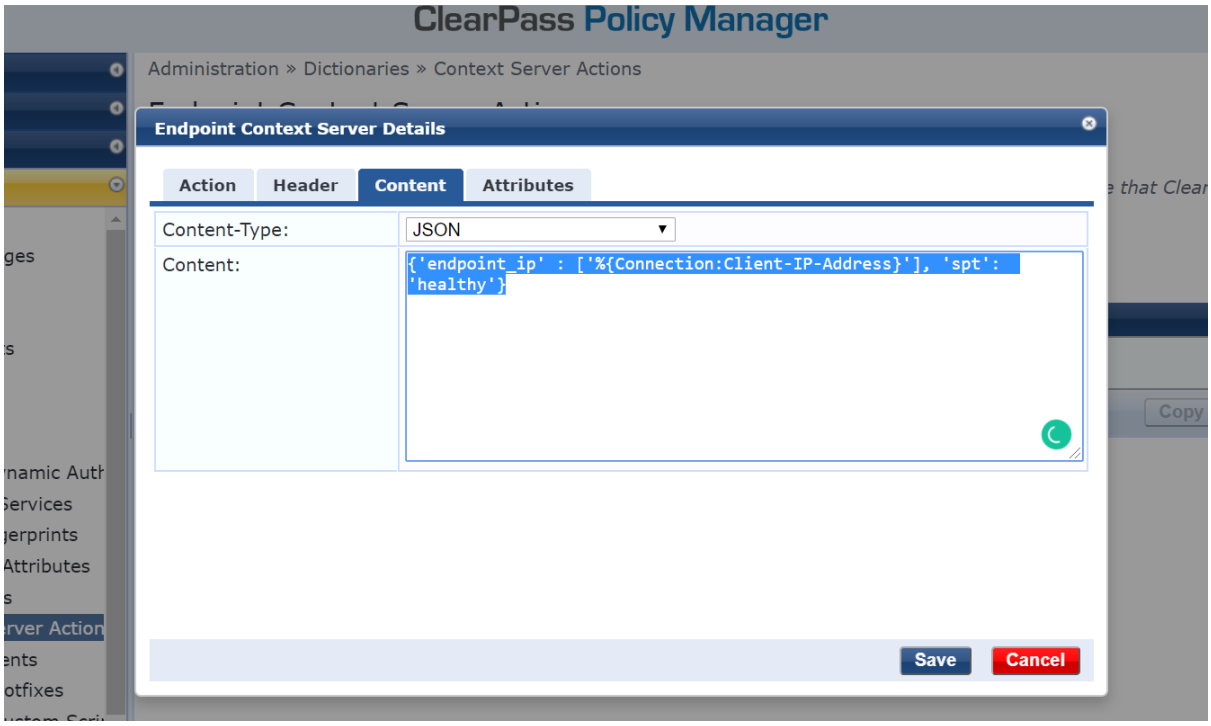


Content would contain the Posture information along with Username and IP details.

{'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:	-

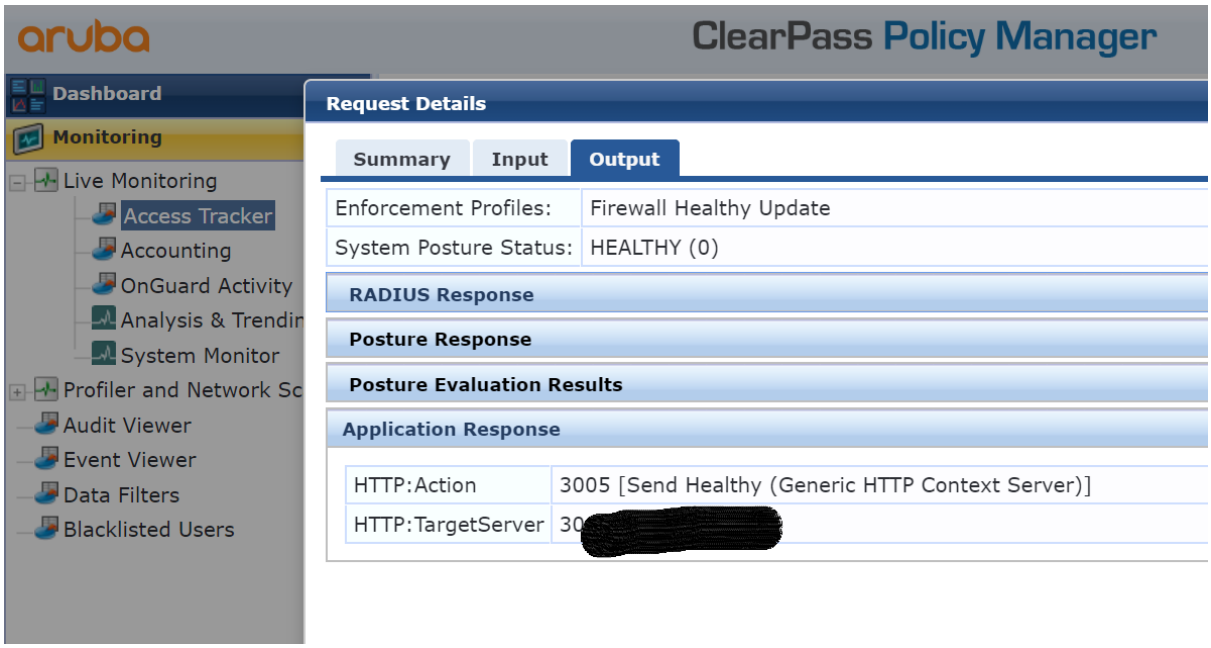
Attributes:

	Attribute Name	Attribute Value
1.	Target Server	= [redacted]
2.	Action	= Send Healthy

OnGuard Service:

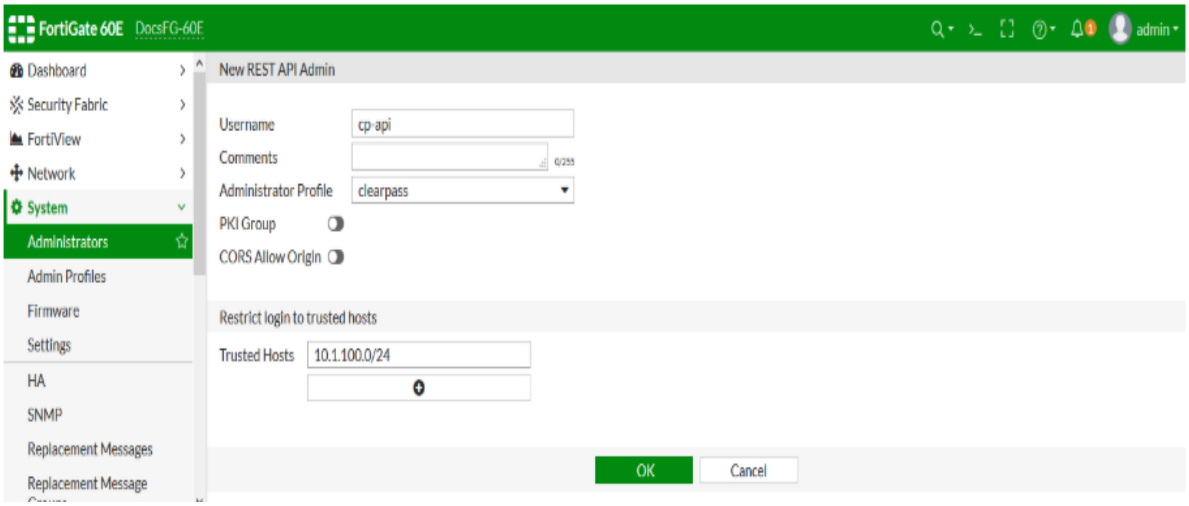
We need to map the Posture Policy & HTTP Enforcement created earlier into a Service.

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

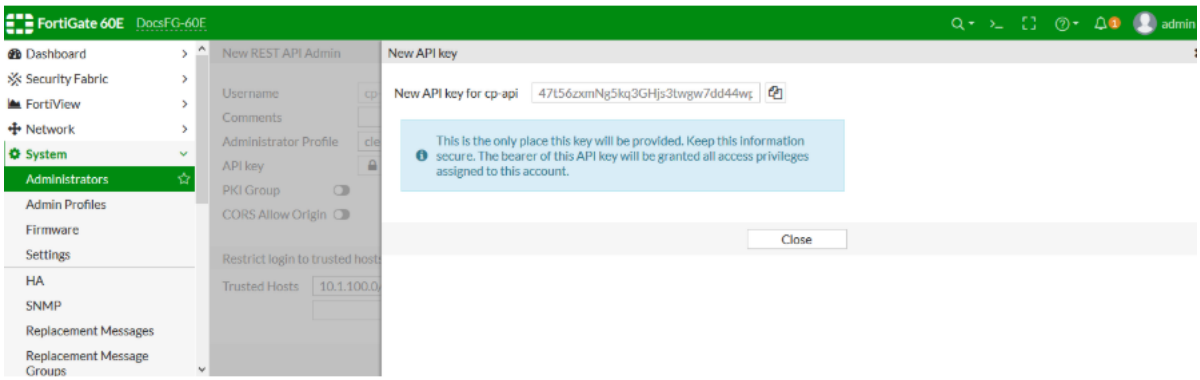


Configuration from FortiGate:

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 if 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**********