

ARUBA CLEARPASS ONGUARD AND-FORTIGATE VPN INTEGRATION

Chaitanya DNSS



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 "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

Dashboard	0	Administration » Agents a	nd Software Upd	lates » OnGuard Settings -				
Monitoring	•	OnGuard Settings -						Global Agent Settings
Configuration	•	y-						Policy Manager Zones ClearPass EULA
Administration	0	Use the OnGuard Settings	page to configui	re the OnGuard agent deploy	ment packages for Windows, n	nacOS, and Linux.		0
— 🤌 ClearPass Portal	<u>^</u>	Settings Installers	Agentless OnG	uard				
Users and Privileges		Agent Version:	6.8.1.109777					
- Je Admin Users		Agent Library Version:	10.0.13.10077	17				
- 🥜 Admin Privileges		Agent Library version:	10.0.13.10977					
🖃 📶 Server Manager		Linux Installer Mode:	Do not install/en	nable Aruba VIA component V	form boolth checks for client m	ashinas. This setting will	not install the Arche 1/74 component. If also	adu installed, then the VIA
- 🥜 Server Configurat	tion		component will	I he disabled on the client ma	achine	denines. This setung with	not instan the Aruba via component. If alle	ady installed, then the VIA
- 🥜 Log Configuration			Note: This W	ILL remove any existing/i	nstalled Aruba VIA client			
- Jocal Shared Fold	lers	Agent Customization						
- 🥜 Licensing		Agent Custonnization						
🥜 Device Insight		Managed Interfaces:		🗏 Wired 💷 Wireless 🗹 V	PN U Other			
🖃 📲 External Servers		Mode:		Authenticate with health check	is 🔻			
- 🤌 SNMP Trap Receiv	vers			Authentication type:	Username & Password V			
- A Syslog Targets				Username Text:	Username			
🥜 Syslog Export Filt	ers			Password Text:	Password			
- 🥜 Messaging Setup		Agent action when an upo	late is available:	Download and Install	T			
- 🥜 Endpoint Context	Servers	rigent action men an ape		Dominious and motal				
File Backup Serve	ers	Agent Remediation Use	r Interface Cu	stomization				
- P External Accounts		Custom User Interface:	Configure					
🖃 🔒 Certificates		Nativo Diccolvablo Ago	nt Cuctomizati	0.0				
- Jectificate Store		Native Dissolvable Age						
- 🥜 Trust List		Managed Interfaces:	🗹 Wired 🗹 V	Wireless 🔍 VPN 🔍 Other				
Revocation Lists								
Dictionaries								
🖃 🗞 Agents and Software U	pdates							
- /P OnGuard Settings	s							
🥜 Software Updates	•							Cancel



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 a	nd Software Updates » OnGuard Settings -		
OnGuard Setting	5 -		 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.		0
Settings Installers	Agentless OnGuard		
Agent Installers updated a	at Apr 22, 2020 08:32:16 PDT		
都 Windows	https://10.67.10.110/agent/installer/windows/ClearPassOnGuardInstall.exe	(Full Install - EXE)	24MB
	https://10.67.10.110/agent/installer/windows/ClearPassOnGuardInstall.msi	(Full Install - MSI)	24MB
	https://10.67.10.110/agent/installer/windows/ClearPassOnGuardLibraryUpdate.exe	(Update Only)	8MB
💣 macOS	https://10.67.10.110/agent/installer/mac/ClearPassOnGuardInstall.dmg	(Full Install)	23MB
	https://10.67.10.110/agent/installer/mac/ClearPassOnGuardLibraryUpdate.pkg	(Update Only)	5MB
🥎 Ubuntu	https://10.67.10.110/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz	(Full Install)	30MB
	https://10.67.10.110/agent/installer/ubuntu/ClearPassOnGuardLibraryUpdate.tar.gz	(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 Age	ent Apps		
鸄 Windows	https://10.67.10.110/agent/webagent/windows/OnGuard Windows Health Checker.exe	(Full Install)	10MB
	https://10.67.10.110/agent/webagent/windows/OnGuard Windows Health Checker Library Update.exe	(Update Only)	4MB
💣 macOS	https://10.67.10.110/agent/webagent/mac/OnGuard Mac Health Checker.dmg	(Full Install)	11MB
	https://10.67.10.110/agent/webagent/mac/OnGuard Mac Health Checker Library Update.pkg	(Update Only)	5MB
 ✓ Ubuntu ☆ CentOS ● Red Hat ● SUSE ⑦ Fedora 	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker-x86.tar.gz	(Full Install 32-bit)	10MB
	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker.tar.gz	(Full Install 64-bit)	11MB
	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker Library Update-x86.tar.gz	(Update Only 32-bit)	9MB
	https://10.67.10.110/agent/webagent/linux/OnGuard Linux Health Checker Library Update.tar.gz	(Update Only 64-bit)	9MB

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 \rightarrow Posture \rightarrow Posture Polices.

aruba		ClearPass Policy Manager		Menu
Dashboard 0	Configuration » Posture »	Posture Policies » Edit - Windows Health Policy		
Monitoring 0	Posture Policies -	Windows Health Policy		
🖧 Configuration 💿	Summary Policy	Posture Plugins Rules		
-	Policy:			
Authentication	Policy Name:	Windows Health Policy		
🖃 🚨 Identity	Description:			
-\$\$ Single Sign-On (SSO)	Posture Agent:	Web Agent		
🎝 Local Users	Host Operating System:	WINDOWS		
- 🛱 Endpoints	Plugin Version:	2.0		
- 🎝 Static Host Lists	Restrict by Roles:			
- CR Koles	Posture Plugins:			
- A Role Happings	The list of selected pluging	c ·		
- Posture Policies	Plugin Name	o.	Plugin Configuration	Status
- D Audit Servers	1. ClearPass Windows	Universal System Health Validator	View	Configured
- 🛱 Agentless OnGuard				
B Enforcement	Rules:			
🎝 Policies	Rules Evaluation Algorithr	m: First applicable		
🛱 Profiles	Conditions			Posture Token
	1. Passes all SHV checks	 ClearPass Windows Universal System Health Validator 		HEALTHY
—.贷 Devices	2. Fails one or more SHV	checks - ClearPass Windows Universal System Health Validator		QUARANTINE
- Device Groups				
- Proxy Targets				
- Q Event Sources				
- Delicy Cimulation				

Define the Posture Plugin for respective OS.



aruba	ClearPass Policy Manager Menu	
Dashboard 0	Configuration » Posture » Posture Policies » Edit - Windows Health Policy	
Monitoring O	Posture Policies - Windows Health Policy	
Configuration	Stimmary Policy Posture Pholos Rules	
Configuration Continuential A Wizards Service Emplotes & Wizards Service Emplotes & Wizards Service Emplotes & Wizards Service Employee Configuration Configura	Stature Yie gringer Relation of the stature Yie gringer Idear Place Viscon Universal System Relath Validator Configured Viscon	
- Cent Sources	Enable User Notification: true	
	Allow any product: true Windows 8:	
Administration 0	Back to Posture Policies Can	el

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

aruba	ClearPass Policy Manager	Menu 🗮
Dashboard 0	Configuration » Posture » Posture Policies » Edit - Windows Health Policy	
Monitoring 0	Posture Policies - Windows Health Policy	
🖧 Configuration 📀	Summary Policy Posture Plugins Rules	
— Service Templates & Wizards — Services	Rules Evaluation Algorithm: First applicable	
🗈 🗣 Authentication	Conditions	Posture Token
🖃 🚨 Identity	1. Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
–🛱 Single Sign-On (SSO)	2. Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE
- 🛱 Local Users - 🎝 Endpoints	Add Rule	Move Up † Move Down ↓ Edit Rule Remove Rule
- 🛱 Static Host Lists		
- 🛱 Roles		
🛱 Role Mappings		

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.

Add Endpoint Context Serv	/er	8
Server		
Select Server Type:	Generic HTTP Context Server	
Server Name:	10.10.10	
Server Base URL:	https://10.10.10.10	
Authentication Method:	Basic •	
Username:		
Password:	Verify:	
Validate Server:	Enable to validate the server certificate	
Bypass Proxy:	Enable to bypass proxy server	
IP Version:	🖲 IPv4 🔍 IPv6 🔍 Both	



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

ndpoint Context Server D	etails			
Action Header Co	ontent	Attributes		
Server Type:	Gene	eric HTTP Conte	xt Server 🔻	
Server Name:	10.10	0.10.10	T	
Action Name:	Send	Healthy Token		
Description:			12	
HTTP Method:	POS	Т	V	
Authentication Method:	None	;	▼	
URL:	/api/	/v2/monitor/fi	rewall/clearpass-address/add	
			Save	ancel

Header :

End	point Co	ontext Serv	er Details			8
А	ction	Header	Content	Attributes	5	
Spe	cify the	key-value p	pairs to be in	ncluded in t	he HTTP Header -	
#	Head	er Name			Header Value	
1.	Autho	rization		=	Bearer7k0w33G4swstdGmGqcz175zH90ybwk	ŵ
2.	accep	t		=	application/json	亩
3.	Conte	ent-Type		=	application/x-www-form-urlencoded	Ť
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



Depending on the token desired this can be changed accordingly.

		ClearPass	Policy Manager	
0	Administration » Diction	naries » Context Server A	ctions	
0	Endpoint Context Serv	er Details		0
0	Action Header	Content Attributes		e that Clear
A	Content-Type:	JSON	T	
ges	Content:	{'endpoint_ip' : ['healthy'}	<pre>'%{Connection:Client-IP-Address}'], 'spt':</pre>	
S				
			C	Сору
namic Autł				
Services				
Attributes				
s				
erver Action			Save	
otfixes				

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:	НТТР	
Action:	Accept	
Device Group List:	-	
Attributes:		
Attribute Name		Attribute Value
1. Target Server		
2. Action		= Jena Healthy

OnGuard Service:

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



Image: Daskbaard Configuration > Services > Edit - OnGuard Health Check Image: Daskbaard Configuration > Services > Edit - OnGuard Health Check Image: Daskbaard Services - OnGuard Health Check Image: Daskbaard Description:	rd O ng O	 Configuration » Services » 			
Services - OnGuarding Services - OnGuarding Service Rotionard Service Rotionard Service OnGuard Health Check Service OnGuard Health Check Authentication Name: OnGuard Health Check on Authentication; Only Health Check for all Services Authentication Description: Web-Based Access - No Authentication; Only Health Check for all Services Disple Sign- On (SSO) Type: Enabled Disple Sign- On (SSO) Status: Enabled	ng o		Edit - OnGuard Health Check		
Stummary Service Roles Posture Enforcement - © Service Templates & Wizards - © Service - © Service Templates & Wizards - © Service - © Service - © Service Templates & Wizards - © Service - © Service Templates & Wizards - © Service - © Service Templates & Wizards - © Service - © Service Templates & Wizards - © Service - © Service Templates & Wizards - © Service - © Service Templates & Wizards - © Service Templates & Web-Based Access - No Authentication; Only Health Check for all Services - © Service Templates & Web-Based Access - No Authentication; Only Health Check for all Services - © Service Templates - © Service Templ		 Services - OnGua 	ard Health Check		
C Service Templates & Wizards C Service C Se	ation 💿	O Summary Service	Roles Posture Enforcement		
→ Converse Name: OnGuard Health Check → Authentication Description: Web-Based Access - No Authentication; Only Health Check for all Services → Display Single Sign-On (SSO) Type: Web-Based Access - No Authentication; Only Health Check for all Services → Display Single Sign-On (SSO) Type: Web-Based Health Check Only → Display Single Sign-On (SSO) Status: Enabled	Templates & Wizards	Service:			
Instrumentation Description: Web-Based Access - No Authentication; Only Health Check for all Services Identity Type: Web-based Health Check Only - Q Local Users Status: Enabled - Optimizer Maniper Median Discipling	s	Name:	OnGuard Health Check		
Defaulty Type: Web-based Health Check Only Default Single Sign-On (SSO) Type: Web-based Health Check Only Default Single Sign-On (SSO) Status: Enabled Default Single Sign-On (SSO) Status: Enabled	ication	Description:	Web-Based Access - No Authentication: Only H	lealth Check for all Services	
Approximation (abo) Status: Enabled Approximation (abo) Approximation (abo) Status: Enabled		Type:	Web-based Health Check Only		
A Endepiete Meniter Media Dirabled	cal Users	Status:	Enabled		
a crigopolitis monitor mode. Disabled	idpoints	Monitor Mode:	Disabled		
Static Host Lists More Options: Posture Compliance	atic Host Lists	More Options:	Posture Compliance		
Gales	bles	Hore options:	rostare compliance		
	le Mappings			Service Rule	
Posture Match ANY of the following conditions:		Match ANY of the following	g conditions:		
- ¹ Posture Policies Type Name Operator Value	sture Policies	Туре	Name	Operator	Value
- Audit Servers 1. Host CheckType MATCHES_EXACT Health	idit Servers	1. Host	CheckType	MATCHES_EXACT	Health
Agentless OnGuard Boles:	gentless OnGuard	Roles:			
Bendermannen Beierer	ment	Role Manning Policy:			
A Polices (voic Propping Policy)	ofiles	Role Happing Policy.			
- A Fromes Posture: Posture:	(Posture:			
Drivings Posture Policies:	vices	Posture Policies:			
- Device Groups Posture Policies: 1. MacOSX Health Policy 2. Windows Health Policy	evice Groups	Posture Policies:	1. MacOSX Health Policy 2. Windows Health Policy		
A Proxy largets Default Posture Token: UNKNOWN (100)	oxy largets	Default Posture Token:	UNKNOWN (100)		
Attent Sources Remediate End-Hosts: Disabled	Scan	Remediate End-Hosts:	Disabled		
Policy Simulation Remediation URL:	imulation	Remediation URL:			
Feferement		Enforcement			

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

aruba	ClearPass Policy Manager					
Dashboard	Request Details					
Monitoring	Summary Input	Output				
	Enforcement Profiles:	Firewall Healthy Update				
	System Posture Status:	HEALTHY (0)				
	RADIUS Response					
Analysis & Trendin	Posture Response					
Profiler and Network Sc	Posture Evaluation Results					
	Application Response					
	HTTP:Action 3 HTTP:TargetServer 3	005 [Send Healthy (Generic HTTP Context Server)]				
-						

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.



FortiGate 60E	DocsFG-6	50E	Q+ >_	0	? •	۵۵	👤 admin •
Dashboard	>	New REST API Admin					
🔆 Security Fabric	>						
EortiView	>	Username cp-api					
Network	>	Comments de la commente de la commen					
System	×	Administrator Pronie clearpass					
Administrators	4						
Admin Profiles		CORSTANDWORgin C					
Firmware		Restrict login to trusted hosts					
Settings		Trusted Hosts 10.1.100.0/24					
HA		0					
SNMP							
Replacement Mess	ages						
Replacement Mess	age	OK Cancel					

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

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.