Enable Service Gateway forward proxy

1.登入 Vision One > Inventory Management > Service Gateway Inventory,在您的 Service Gateway 的

Action 欄位上點擊「亞」圖示

Trend Micro Vision One™ s	ervice Gateway Inventory				ତ	2022-06-12 10:19 (UTC+08:00)	🜲 🕄 TWTS_XDR	8
+ Download Virtual Appliance						Period: Last 24 hours 🗸	🌣 Manage API Key	0
Service Gateway \downarrow	Connection status	Connected endpoints	Uploaded	Downloaded	Last connected		Action	
	Healthy	4	141.98 MB	192.09 MB	Just now (2022-06-	12 10:39:11)	¢ 🖻	
SG-Bruce (172.16.250.246)	Healthy	4	117.17 MB	59.63 MB	Just now (2022-06-	12 10:39:09)	🌣 û	

2. Enable Service Gateway forward proxy service,如下圖:

Trend Micro V	ision One™ Service Gateway Inventory → localho	ost.localdomain	() 2022-04-21 01:55 (UTC+00:00)
< Back			Service Gateway Settings
Endpoint name:			localhost.localdomain
IPv4 address:			Services
IPv6 address:			ActiveUpdate ④
Connection status:			Smart Protection Services (i)
Last connected:			Suspicious Object List synchronization (i)
Version:			Third-party intelligence synchronization () Log forwarding ()
Storage:			Forward proxy (i)
System Resource Usag	423.5 GB free (Total:459 GB) e History		Active Directory connection ① Product Component Update

說明:若您在 Enable Forward proxy 出現以下訊息(圖一),表示您的 Service Gateway 版本尚未支 Forward proxy 功能,請升級您的 Service Gateway 版本,如(圖二)



3.步驟 2 執行完畢之後,請確認 Forward proxy 圖示呈現已打勾狀態☑,如下圖:



4.透過以下方式,確認您既有的 Vision One agent 是否已透過 forward proxy 自動回報回 Vision One:
a. 登入 Vision One > Inventory Management > Service Gateway Inventory > 點選您的 Service Gateway, 如下圖:

Trend Micro Vision One™	Service Gateway Inventory		
+ Download Virtual Appliance			
Service Gateway	Connection status	Connected endpoints	Uploaded
	 Healthy 	4	138.61 MB
SG-Bruce (172.16.250.246)	 Healthy 	4	114.75 MB

b. 從您的 Service Gateway > Connected Endpoints > Last proxy connection,確認您既有的 Vision One agent 有顯示 forward proxy 最後一次的連線時間,即表示 agent 與 forward proxy 連線正常,如下圖:

Connected Endpoints					
Period: Last 24 hours v	Product: All ~	Connected service: All 🗸	Q Endpoint name, IP address, GUID		
Endpoint	Product	Smart Protection queries Last qu	uery () Last synchronize	rd (i) Last log upload (i)	Last proxy connection ()↓
W10_bruce_XDR (172.16.20.140)	Trend Micro Vision One agent				Sm (2022-06-12 11:57:26)
W2016_Bruce_XBC (172.16.20.1.	. Trend Micro Vision One a				Sm (2022-06-12 11:56:59)

- 5.若您希望之後新安裝的 Vision One agent 都能透過 forward proxy 的方式回報回 Vision One,則安裝步 驟如下:
 - a. 登入 Vision One > Inventory Management > Endpoint Inventory > Agent Installer,如下圖:



b. 透過 copy download link 方式或 Download 方式下載 Endpoint Basecamp.exe 檔案,如下圖:



c. 下載 Service Gateway forward proxy deployment script,如下圖:



點擊 Download



d. 將下載的 Install.bat 與剛剛下載的 Endpoint Basecamp.exe 檔案放在同一個資料中,如下圖:

名稱	修改日期	類型	大小
🛃 EndpointBasecamp.exe	2022/6/12 下午 01:26	應用程式	2,826 KB
🐁 install.bat	2022/6/12 下午 01:38	Windows 批次檔案	2 KB

e. 點擊聲來複製 Script command 內容,如下圖:



f. 在 DOS 模式下,將路徑切換到與 Install.bat & Endpoint Basecamp.exe 的同一個資料夾底下,然後執 行步驟 e 的 Script command,開始執行安裝,如下圖:



g. 登入 Vision One > Inventory Management > Endpoint Inventory, 確認剛剛安裝的 agent 是否回報 到 Vision One,如下圖:

Tre	nd Micro Visior	n One [™] Endpoint Inventory				O 2022-06-12 12:58 (UT	C+08:00) 🌲
Endp	oint List Endpoint Gro	ups Agent Installer					
- C	P All	35	场 No features enabled	2	G Action required	0	
٩	Endpoint name						
	Endpoint name	IP address	Group	Operating system	Last connected	Features enabled	
	W10_Bruce_XBC	172.16.20.158	Bruce	Windows 10	2d (2022-06-09 16:40:09)	XDR Endpoint Sense	or, Vulnerabi
	W2016_Bruce_XBC	172.16.20.104	Bruce	Windows Server 2016	Just now (2022-06-12 14:10:33)	XDR Endpoint Sense	or, Vulnerabi
	₽ W10_bruce_XDR	172.16.20.140	Bruce	Windows 10	Just now (2022-06-12 14:09:10)	XDR Endpoint Sense	or, Vulnerabi

A. 登入 Vision One > Inventory Management > Service Gateway Inventory > 點選您的 Service Gateway
 > Connected Endpoints > Last proxy connection。確認您剛剛安裝的 agent 有顯示 forward proxy
 最後一次的連線時間,即表示 agent 與 forward proxy 連線正常,如下圖:

Connected Endpoints					
Period: Last 24 hours 🗸	Product: All 🗸	Connected service: Forward proxy V Q Endpoint	name, IP address, GUID		
Endpoint	Product	Smart Protection queries Last query 🔅	Last synchronized (i)	Last log upload (j)	Last proxy connection (j)
W10_bruce_XDR (172.16.20.140)) Trend Micro Vision One a				Just now (2022-06-12 14:17:26)
W2016_Bruce_XBC (172.16.20.1	Trend Micro Vision One a				Just now (2022-06-12 14:17:21)

6.可以在 agent 端透過檢查以下 proxy_server 機碼值,確認 agent 是否透過正確的 forward proxy 回報 到 Vision One,如下圖:

>	TrendMicro	^	Name	Type	Data		
>	Windows		ab) (Default)	REG SZ	(value not set)		
~	WOW6432Node		ab device id	REG SZ	f90e5e82-6a0d-41a8-8b81-6a5e7d73a15d		
>	Amazon		ab frequence	REG SZ	default		
>	Classes		is frequence ch	REG DWORD	0x00000001 (1)		
>	Clients		ab proxy bypass	REG SZ	0.0000000000000000000000000000000000000		
>	Google		10 proxy lastundat	REG OWORD	0x6260e314 (1650516756)		
>	Intel		ab proxy server	REG SZ	10.107.8.154:8080		
2	Microsoft		no proxy source	REG DWORD	0x00000001 (1)		
2	Delicies		ungrade actions	REG DWORD	0x00001068 (4200)		
2	Policies		10 upgrade actions	REG DWORD	0x00000bb8 (3000)		
1	RegisteredApplications		ab xdr device id	REG SZ	f90e5e82-6a0d-41a8-8b81-6a5e7d73a15d		
4	TrendMicro						
	> cep						
	OfficeScan						
	SecurityKeys						
	 TMSecurityService 						
	>action_records_v3						
	- ActProgress						
	- CETA						
	> finished_default_t	0					
	> monitor						
	> persistent						