# 通過AnyConnect 4.x和AMP Enabler安裝和配置 AMP模組

## 目錄

簡介 必要條件 需求 採用元件 通過ASA的AMP啟用程式的AnyConnect部署 第1步:配置AnyConnect AMP啟用程式客戶端配置檔案 第2步:編輯組策略下載AnyConnect AMP啟用程式 步驟3:下載FireAMP策略 第4步:下載網路安全客戶端配置檔案 第5步:使用AnvConnect連線並驗證模組的安裝 第6步:啟動VPN連線安裝AMP啟用程式和AMP聯結器 第7步:檢查AnvConnect並驗證是否已安裝所有裝置 第8步:使用殭屍PDF檔案中包含的Eicar字串進行測試 第9步:部署摘要 步驟10:執行緒檢測驗證 其他資訊 相關資訊

## 簡介

本文逐步完成使用AnyConnect安裝高級惡意軟體防護(AMP)聯結器的步驟。

AnyConnect AMP啟用程式用作部署面向終端的AMP的媒介。它本身沒有任何能力判定檔案的處置 情況。它將面向終端的AMP軟體從ASA推送到終端。安裝AMP後,它會使用雲容量檢查檔案性質。 進一步的AMP服務可以將檔案提交到名為ThreatGrid的動態分析中,以便對未知檔案行為進行評分 。如果符合某些專案,這些檔案可能被認定為惡意檔案。這在零日攻擊中非常有用。

## 必要條件

## 需求

- AnyConnect安全行動化使用者端版本4.x
- FireAMP/AMP端點版
- 自適應安全裝置管理器(ASDM)版本7.3.2或更高版本

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •採用軟體版本9.5.1的調適型安全裝置(ASA)5525
- Microsoft Windows 7 Professional 64位版AnyConnect安全00096動客戶端4.2.1
- ASDM版本7.5.1(12)

## 通過ASA的AMP啟用程式的AnyConnect部署

設定中涉及的步驟如下:

- 配置AnyConnect AMP Enabler客戶端配置檔案。
- 編輯AnyConnect VPN組策略並下載AMP啟用程式服務配置檔案。
- 登入到AMP儀表板以獲取聯結器URL下載連結。
- •驗證使用者電腦上的安裝。

## 第1步:配置AnyConnect AMP啟用程式客戶端配置檔案

- 導航到Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Client Profile。
- •新增AMP Enabler Service Profile。

ect Client Profile	2
amp	
AMP Enabler Service Profile	
le path for an xml file, ie. disk0:/ac_profile. The file will be eated if it does not exist.	
disk0:/amp.asp	Browse Flash
	Upload
<unassigned></unassigned>	
Enable 'Always On VPN' for selected group	
OK Cancel Help	
	ect Client Profile amp AMP Enabler Service Profile le path for an xml file, ie. disk0:/ac_profile. The file will be eated if it does not exist. disk0:/amp.asp <unassigned> <unassigned>   © Enable 'Always On VPN' for selected group</unassigned></unassigned>

🛧 Add 🗹 Edit 🔀 Change Group Policy	👕 Delete 🔁 Import 🖶 Expo	rt 🎒 Validate	
Profile Name	Profile Usage	Group Policy	Profile Location
PRIMARY	AnyConnect VPN Profile	GroupPolicy1	disk0:/primary.xml
amp	AMP Enabler Service Profile	GroupPolicy1	disk0:/amp.asp

## 第2步:編輯組策略下載AnyConnect AMP啟用程式

- 導航到Configuration > Remove Access VPN > Group Policies > Edit。
- •轉到Advanced > AnyConnect Client > Optional Client Modules to Download。
- 選擇AnyConnect AMP Enabler。

	a product and a state of the st	the state of the s				
Jeneral Servers	Keep Installer on Client System	[2] Inherit	OTE	C No		
dvanced Solt Turoning	Delagram Transport Layer Security (DTLS):	V Inherit	O Enable	C Duble		
Browser Proxy	07LS Compression:	2 Inherit	C Brable	() Double		
= Psec(XEv1) Clent	59. Compression:	10 Inherit	O Defete	0.125	C Diable	
	Ignore Don't Fragment(DF) Bit:	(2) Inherit	O buble	O Deable		
	Client Bypess Protocol:	[2] Inherit	() brable	() Double		
	PQDN of this Device:	PQ0N				
MTU: Keepalive M Optional Cit Always-On	MTU:	2 Inherit				
	Keepalive Messages:	[2] Inherit	Deable	Interviel [	seconds	
	Optional Client Modules to Download:	Elshert	rependen	-		-
	Always-On VPN:	2 Inherit	AnyCom	ect DART ect Network	Access Manager	
	Client Profiles to Download:	Divert	AnyCarr	ect Network ect SBL	Vsbity	
		4 ASS 1	AnyCom	wect Web Sec	unity Mer	
		Profile Name	AnyCarr	ect ISE Post ect Posture	n	
		FREMARY.				OK Cancel
		-				temperature of Approximation
de i	O Next O Previou					

步驟3:下載FireAMP策略

附註:繼續之前,請檢查系統是否滿足終端AMP Windows聯結器的要求。

#### 面向終端的AMP Windows聯結器的系統要求

這些是基於Windows作業系統的FireAMP聯結器的最低系統要求。FireAMP聯結器支援這些作業系統的32位和64位版本。最新的AMP文檔可在AMP部署<u>中找到</u>

作業系統	處理器	記憶體	咝咮空间、 僅雲模式	磁碟空間
Microsoft Windows 7 Microsoft	1 GHz或更快的 處理器	1 GB RAM	150 MB可用硬碟 空間 — 僅雲模式	1GB可用硬碟空 間 — TETRA
Windows 8和 8.1(需要 FireAMP聯結器 5.1.3或更高版本 )	1 GHz或更快的 處理器	512 MB記憶體	150 MB可用硬碟 空間 — 僅雲模式	1GB可用硬碟空 間 — TETRA
Microsoft Windows Server 2003	1 GHz或更快的 處理器	512 MB記憶體	150 MB可用硬碟 空間 — 僅雲模式	1GB可用硬碟空 間 — TETRA
Microsoft Windows Server 2008	2 GHz或更快的 處理器	2 GB RAM	150 MB可用硬碟 空間 — 僅雲模式	1GB可用硬碟空 間 — TETRA
Microsoft Windows Server 2012(需要 FireAMP聯結器 5.1.3或更高版本 )	2 GHz或更快的 處理器	2 GB RAM	150 MB可用硬碟 空間 — 僅雲模式	1 GB可用硬碟空 間 — TETRA

最常見的是將AMP安裝程式放在企業Web伺服器上。

若要下載聯結器,請導覽至**管理>下載聯結器**。然後依次選擇type和**Download** FireAMP(Windows、 Android、Mac、Linux)。

/ Dehboard x +				= 0 ×
🔹 🗿 (https://conscis.org/acurcefice.com/dishboard		v C Q Asset	2 8 V	* * 4 @ • @ = • = =
My Work Zone - Cons	🖡 Loomeans Backlog Vie 🔛 Accos	et Team Directory 🗌 Anyconnect Websec	a 🗿 Cace HTMLS Upleed 🎑 1	TZ 🔒 Misc 🎴 Bugs 🛕 Webmonitor
SOURCE		0 installs 1 detection (7 days) Advise	ncements Chapport Thelp	The Log Out
Dashboard Analysis - Outbreak Co	etrol - Reports Management +	Accounts +		3005102317
Dashboard	Quick Stat Computers		Group Filter Select	Groups *
Overview Events Heat Map	Groups Policies			Refresh All 🔘 Auto-Refresh 🔹
Indications of Compromise	Hosts Detection		Hosts Detecting Network	Threats (7 days)
(there are carriedly to computer) with indication of computation	Computer Deployment S	ummary unt	Computer	Count
	WCDBAQW7P Cloud Recall		Cherry are no record early of	A first abelies to during
	Mahuare Threats (7 days)		Network Threats (7 days)	
	Detection Name	Coant	Remote iP	Count
	W32-DCAR.35	1	There are in intent without	et divent debentuur für alsgeleg.
	Recent Malware Threats		Recent Network Threats	
	Computer	Detection Name	Computer I	Detection Name Remote IP
	WCOBAQW/7PN80EMO	W32.6ICAR.16g1		A Dest Alberten D. Alpin
				*

Download Connector頁面允許您下載每種型別的FireAMP聯結器的安裝程式包。此包可以放置在網路共用上或通過管理軟體分發。

ect a droup			
FireAMP Windows	FireAMP Android	🔹 FireAMP Mac	∆ FireAMP Linux
Flash Scan on Install	Activation Codes	Flash Scan on Install Ø	SFlash Scan on Install O GPG Public Key
🛓 Download	🛓 Download	🛓 Download	🛓 Download
Show URL	Show URL	Show URL	Show URL

#### 選擇組

- 僅稽核: 根據通過每個檔案計算的SHA-256監視系統。此「僅稽核」模式不會隔離惡意軟體 , 但會傳送事件作為警報。
- •保護:使用隔離惡意檔案保護模式。監視檔案複製和移動。
- •分類:這用於已受感染/感染的電腦上。
- **伺服器**:用於Windows伺服器的安裝套件,其中聯結器的安裝不帶Tetra引擎和DFC驅動程式。 此組根據其名稱為非域控制器伺服器設計。
- **域控制器:**此組的預設策略設定為稽核模式,與伺服器組中一樣。關聯此組中的所有Active Directory伺服器,這意味著聯結器將在Windows域控制器上運行。

AMP具有名為TETRA的功能,該功能是完整的防病毒引擎。此選項是每個策略的可選選項。

- **安裝時進行快閃記憶體掃描:**掃描進程在安裝期間運行。執行速度相對較快,建議只運行一次 。
- **可再分發:**您應下載一個軟體包,其中包含32位和64位安裝程式。而不是載入程式,該載入程 式可以在執行後保持此選項未勾選狀態並下載安裝程式檔案。

**附註**:您可以建立自己的組並配置與其關聯的策略。其目的是將所有伺服器(例如Active Directory伺服器)置於一個組中,其中策略處於稽核模式。 載入程式和可再發行安裝程式還都包含一個policy.xml檔案,該檔案用作AMP聯結器的配置檔 案。

### 第4步:下載網路安全客戶端配置檔案

使用AMP安裝程式指定公司Web伺服器或網路共用。這在各公司中最為常用,用於節省頻寬並將受 信任的安裝程式集中到位置。

請確保在端點上可以訪問HTTPS連結並且沒有任何證書錯誤,並且根證書已安裝在電腦儲存中。

返回之前在ASA上建立的AMP配置檔案(步驟1),然後編輯AMP啟用程式配置檔案:

- 1. 對於AMP模式,按一下**安裝AMP啟用程式**單選按鈕。
- 2. 在Windows Installer欄位中,為Web伺服器新增IP,為FireAMP新增檔案。
- 3. Windows選項是可選的。

	业会历发文。	
AnyConnect Client Profile Editor	- vpn	
Profile: vpn		About
AMP Enabler Profile		
AMD Made		
AMP Mode		
Windows Installer	https:// webserver.cisco.com/Audit_FireAMPSetup.exe Check	
Mac Installer	https://	
Windows Options	☑ Add To Start Menu	
	Add To Desktop	
	Add To Context Menu	
	Save Reset	
	OK Cancel Help	

## 第5步:使用AnyConnect連線並驗證模組的安裝

當Anyconnect VPN使用者連線時,ASA會通過VPN推送AnyConnect AMP啟用程式模組。對於已登入的使用者,建議先註銷,然後重新登入以啟用該功能。

10:08:29	AM	Establishing VPN session
10:08:29	AM	The AnyConnect Downloader is performing update checks
10:08:29	AM	Checking for profile updates
10:08:29	AM	Checking for product updates
10:08:31	AM	Downloading AnyConnect AMP Enabler 4.4.01054 - 48%
10:08:32	AM	Downloading AnyConnect AMP Enabler 4.4.01054 - 91%
10:08:33	AM	Downloading AnyConnect AMP Enabler 4.4.01054 - 100%
AnyCon	nect 9	Secure Mobility Client Downloader
inity con	incee .	Jecare i lobility client bomniodael
-		

The AnyConnect Downloader is installing AnyConnect Secure AnyConnect Secure Mobility Client 4.2.00096. Please wait...

## 第6步: 啟動VPN連線安裝AMP啟用程式和AMP聯結器

按下connect按鈕啟動VPN後,下載新的下載模組。這將具有AMP啟用程式,並從之前指定的幾步 中的URL路徑下載AMP包。

🔇 Cisco AnyCo	onnect Secure Mobility Client		
	<b>YPN:</b> Connected to 10.168.109.18. 10.168.109.18	<b>T</b>	Disconnect
00:00:07			IPv4
	AMP Enabler: Installing AMP for Endpoints		
¢			altato cisco

If you look at the event viewer:

AMP enabler install: Date : 04/24/2017 Time: 10:08:34Type: InformationSource: acvpndownloader

Description : Cisco AnyConnect Secure Mobility Client Downloader (2) exiting, version 4.4.01054 , return code 0 [0x00000000]

### 第7步:檢查AnyConnect並驗證是否已安裝所有裝置

連線VPN並安裝Web伺服器配置後,請檢查AnyConnect並驗證是否正確安裝了所有裝置。

在services.msc中,您可以找到名為CiscoAMP\_5.1.3的新服務。在Powershell命令中,我們可以看 到:

PS C:\Us	ers\winUse	er348> Get-Service -name "*CiscoAMP*"	
Status	Name	DisplayName	
Running	CiscoAMP_	5.1.3 Cisco AMP for Endpoints Connector 5  nect Secure Mobility Client  YPN: Connected to 10.168.109.18.	×
00:	01:22	10.168.109.18 Disconnect IPv4	l
	<b>S</b>	AMP Enabler: AMP for Endpoints installed.	1
<b>\</b>	i	ulta cisc	. :0

AMP安裝程式將新驅動程式新增到Windows作業系統。您可以使用driverquery命令列出驅動程式。

C:\Windows\System32>driverquery /v | findstr immunet ImmunetProte ImmunetProtectDriver ImmunetProtectDriver File System System Running OK TRUE FΑ LSE 4,096 69,632 0 3/17/2017 5:04:20 PM \??\C:\WINDOWS\System32\Drivers\immunetprotect.s 8,192 ImmunetSelfP ImmunetSelfProtectDriv ImmunetSelfProtectDriv File System System Running OK TRUE FA 28,672 0 3/17/2017 5:04:08 PM LSE 4,096 \??\C:\WINDOWS\System32\Drivers\immunetselfprote 8,192

### 第8步:使用殭屍PDF檔案中包含的Eicar字串進行測試

在測試電腦中使用殭屍PDF檔案中包含的Eicar字串進行測試,以驗證是否已隔離惡意檔案。



Zombies.pdf包含Eicar字串

### 第9步:部署摘要

此頁顯示成功和失敗的FireAMP聯結器安裝以及當前正在進行的安裝清單。您可以轉到**管理>部署摘** 要。



步驟10:執行緒檢測驗證

### Zombies.pdf觸發隔離事件,傳送到AMP控制面板。

	u.amp.cisco.com/dashboard#/events/show/[		CQ	Hledat			- W E	• 🕯		• × =	*
ist Visited 🤌 Most Visite	ed 🧕 Most Visited 🧕 Most Visited 🤌 N	ejnavštěvovanější   Getting Started 🌛 Latest Hea	dlines 📋 Mozilla Firefox 🏼 Most Visite	ed     🧾 Mos	Visited 😗	Getting Started	d 😗 Jak začít 🧾 M	lost Visited	🤌 Nejna	vštěvovanějš	
	cisco AMP	for Endpoints	2 Announcements	Support	? Help	Account	🕞 Log Out				
	Dashboard Analysi	s ~ Outbreak Control ~ Reports Managem	ent ~ Accounts ~	Search			Q)				
	New AM Version 1.3.1.	P for Endpoints Linux Connector 16 is now available. Learn more in the Official Rele	X ase Notes								
ashboard	Overview Events Heat Map	0 Cc	ognitive Incidents 🧭								
											_
Eilter: (New) 🖗								Select a Fil	lter		•
Event Type All	Il Event Types		+ Group All Grou	ups							+
Filters Ac	dd filters by clicking on the $\Upsilon$ icon in the e	vent details					-				
Time Range	Veek ~ Sort 1	ime 🗸 🗘					Not Subscrib	bed ~ Re	eset	ave Filter As	
	.cisco.com detected 4XpJCE_X.pdf.part a:	W32.Zombies.NotAVirus			P S	P ID 9	Quarantine: Successf	ful 201	17-07-27 1	3:32:08 UT(	
B DJANULIK-HYYPD.		▼W32.Zombies.NotAVirus									
File Detection	Detection										
File Detection	Fingerprint (SHA-256)	▼ 00b32c34989bb002									
DJANULIK-HYYPD.     File Detection     Connector Info     Comments	Detection Fingerprint (SHA-256) Filename	▼ 00b32c34989bb002									
Connector Info	Fingerprint (SHA-256) Filename Filepath	▼ 00b32c34989bb002	CE_X.pdf.part								
File Detection Connector Info Comments	Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes)	T 00b32c34989bb002         ~           T 4Xp)CE_X.pdf.part         C:\Users\djanulik\AppData\Local\Temp\4XpJ           309500         309500	CE_X.pdf.part								
JJANULIK-HYYPD     File Detection     Connector Info     Comments	Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes) Parent Fingerprint (SHA-256)	▼ 00b32c34989bb002 ● ~           ▼ 4XpjCE_X.pdf.part           C:\Users\djanulik\AppData\Local\Temp\4XpJ           309500           ▼ 0ff6b175fdf32be ● ~	CE_X.pdf.part								
OJANULIK-HYYPD     File Detection     Connector Info     Comments	Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes) Parent Fingerprint (SHA-256) Parent Filename	▼ 00b32c34989bb002 ● ~           ▼ 4Xp)CE_X.pdf.part           C:\Users\djanulik\AppData\Local\Temp\4XpJ           309500           ▼ 0fff6b175fdf32be ● ~           ▼ firefox.exe	CE_X.pdf.part								4

隔離事件

## 其他資訊

要獲取AMP帳戶,您可以註冊ATS大學。這為您提供了實驗室中的AMP功能的概述。

## 相關資訊

- 配置AMP啟用程式
- 技術支援與文件 Cisco Systems