Installatie en configuratie van de AMP-module via AnyConnect 4.x en AMP-controller

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten AnyConnect-implementaties voor AMP-ondersteuning via ASA Stap 1: Clientprofiel met AnyConnect AMP Enabler configureren Stap 2: Bewerk het groepsbeleid om de AnyConnect-AMP-controller te downloaden Stap 3: FirePOWER-beleid downloaden Stap 4: Clientprofiel voor webbeveiliging downloaden Stap 5: Connect met AnyConnect en controleer de installatie van de module Stap 6: Start VPN Connection installatieautomaat van AMP en AMP-aansluiting Stap 7: Controleer AnyConnect en controleer of alles is geïnstalleerd Stap 8: Testen met een Eicar String in een PDF-bestand van Zombies Stap 9: Samenvatting van implementatie Stap 10: Detectie van bedreigingen Aanvullende informatie Gerelateerde informatie

Inleiding

Dit document gaat door stappen om de Advanced Malware Protection (AMP)-connector met AnyConnect te installeren.

AnyConnect AMP Enabler wordt gebruikt als medium om AMP voor endpoints te implementeren. Op zichzelf heeft het geen mogelijkheid om bestandsdispositie te veroordelen. Het duwt de AMP voor Endpoints software op een eindpunt van ASA. Nadat de Advanced Malware Protection is geïnstalleerd, gebruikt u de wolkencapaciteit om de verwerking van bestanden te controleren. Nadere AMP-service kan bestanden naar dynamische analyse, ThreatGrid, sturen om onbekend bestandsgedrag te scoren. Deze bestanden kunnen als kwaadaardig worden veroordeeld indien aan bepaalde artefacten is voldaan. Dit is zeer nuttig voor aanvallen met een dag op nul.

Voorwaarden

Vereisten

- AnyConnect Secure Mobility Client versie 4.x
- FirePOWER/AMP voor endpoints
- Adaptieve Security Adapter Manager (ASDM) versie 7.3.2 of hoger

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Adaptieve security applicatie (ASA) 5525 met software versie 9.5.1
- AnyConnect Secure Mobility Client 4.2.0096 op Microsoft Windows 7 Professional 64-bits
- ASDM versie 7.5.1(12)

AnyConnect-implementaties voor AMP-ondersteuning via ASA

De bij de configuratie betrokken stappen zijn als volgt:

- Configureer het clientprofiel van AnyConnect AMP Enabler.
- Bewerk het AnyConnect VPN-groepsbeleid en download het AMP Enabler-serviceprofiel.
- Meld u aan bij het AMP-dashboard om de URL-downloadlink van de connector te krijgen.
- Controleer de installatie op de gebruikersmachine.

Stap 1: Clientprofiel met AnyConnect AMP Enabler configureren

- navigeren naar Configuratie > Remote Access VPN > Netwerktoegang (client) > AnyConnectclientprofiel.
- Voeg het AMP-serviceprofiel toe.

🔂 Add 🗹 Edit	🔆 Change Group Policy 前 Delete 🌄 Import 🖶 Export 🎒 Valida	ate
add AnyConne	ect Client Profile	23
Profile Name	amp	
Profile Usage	AMP Enabler Service Profile 🔹 👻	
Enter a device fi automatically cre	le path for an xml file, ie. disk0:/ac_profile. The file will be eated if it does not exist.	
Profile Location	disk0:/amp.asp	Browse Flash
		Upload
Group Policy	<pre>Unassigned></pre>	
	Enable 'Always On VPN' for selected group	
	OK Cancel Help	

🕈 Add 🗹 Edit 🔀 Change (Group Policy 📋 Delete 🐺 Import 🗟 Exp	ort 🞒 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

Stap 2: Bewerk het groepsbeleid om de AnyConnect-AMP-controller te downloaden

- Navigeren in configuratie > Toegang VPN verwijderen > Groepsbeleid > Bewerken.
- Ga naar Geavanceerd > AnyConnect-client > optionele clientmodules voor downloads.
- Kies AnyConnect AMP Enabler.

Servers Advanced	Keep Installer on Client System	2 Inherit C Tes C No	
Advanced			
The second se	Detagram Transport Layer Security (DTLS):	V Inherit C Bruble C Druble	
Growser Proxy	07LS Compressions	Exhert C Enable C Double	
Psec(REv1) Clent	552. Compression:	Ethert O Defaie O L25 O Dable	
	Ignore Don't Fragment(DF) Biti	Entert C trutte C trutte	
	Client Bypass Protocol:	😨 brieft 🕐 Drable 🕐 Drable	
PQDN of This Devices MTU: Keepalive Messages: Optional Clent Modules to Download: Always-On VPN:	FQDN of this Device:	V PQDN	
	MTU:	2 bheit	
	Keepalive Messages:	Etherit Deable Interval seconds	
	Ethert Secondar		
	Always-On VPN:	Inherit AnyConnect DART AnyConnect Network Access Manager	
	Client Profiles to Download:	Inherit AnyConnect Network Vability AnyConnect Sills	
		Add	
		Profile Name AnyConnect DE Posture AnyConnect Posture	
		SERVICE T	oc Cancel
		P9	International Associations and
* (0 mm		
er	grien grienn		

Stap 3: FirePOWER-beleid downloaden

Opmerking: Controleer voordat u verdergaat of uw systeem voldoet aan de vereisten voor de Advanced Malware Protection of Endpoints Windows Connector.

Systeemvereisten voor Advanced Malware Protection voor endpoints en Windows-connector

Dit zijn de minimum systeemvereisten voor de FireAMP-connector die op het Windowsbesturingssysteem is gebaseerd. De FireAMP-connector ondersteunt zowel 32-bits als 64-bits versies van deze besturingssystemen. De nieuwste AMP-documentatie is te vinden in de <u>AMP-implementatie</u>

Besturingssystee m	processor	Geheugen	Disc-ruimte, Alleen cloudmodus 150 MB	Schijf ruimte
Microsoft Windows 7	1 GHz of snellere processor	1 GB RAM	beschikbare vaste-schijfruimte - alleen cloudmodus	beschikbare vaste-schijfruimte - TETRA
Microsoft Windows 8 en 8.1 (hiervoor is FirePOWER- connector 5.1.3 of hoger nodia)	1 GHz of snellere processor	512 MB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows Server 2003	1 GHz of snellere processor	512 MB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows Server 2008	2 GHz of snellere processor	2 GB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA
Microsoft Windows Server 2012 (hiervoor is FireAMP- connector 5.1.3 of hoger nodig)	2 GHz of snellere processor	2 GB RAM	150 MB beschikbare vaste-schijfruimte - alleen cloudmodus	1 GB beschikbare vaste-schijfruimte - TETRA

Het meest gebruikelijk is om de installateur van AMP op de website van de onderneming te laten plaatsen.

Ga om de connector te downloaden naar **Management > Download connector**. Kies vervolgens type en **Download** FirePOWER (Windows, Android, Mac, Linux).

/ Dehboard x +	-			= 0 ×
🔶 🚊 https://conscis.amp.sourcefine.com/dishboard		v C Q Search	200	* * 4 @ • 9 = • 8 =
My Work Zone - Cons A Topic Search 🛐 Home - Tech Zone Q Ceselowery T	Loomeans Backlog Vie 🔛 Acce	ount Team Directory 🗌 Any connect Websecu	r 🗿 Cisce HTML5 Upleed 🎑	TZ 🔒 Misc 🎴 Bugs 🛕 Webmonitor
SOURCE		0 installs 1 detection (7 days) Achieve	ncements Chaport 7 Help	19 Ling Out
Dashboard Analysis - Outbreak Co	stol - Reports Management	Accounts •	15	2.3005102317
Dashboard	Quick Start Computers		Group Filter Selec	t Groups *
Overview Events Heat Map	Groups Policies			Refresh All O Auto-Refresh •
Indications of Compromise	Hosts Detectie Download Co	needer	Hosts Detecting Networ	k Threats (7 days)
Directory of Carrielly of Computer's with Addictions of Computerion	Computer Deployment	Summary and	Computer	Count
	Cloud Necal	_		
	Mahuare Threats (7 days)		Network Threats (7 days	9
	Detection Name	Count	Remote IP	Count
	W32.0CAR.36	-1	These are so intent with	
	Recent Malware Threats		Recent Network Threats	
	Computer	Detection Name	Computer	Detection Name Remote IP
	WCOBAQW7PN8DEMO	W32.EICAR.16g1		ort Deng Jebenbern D. Rigikay

Met de pagina Download Connector kunt u de installatiepakketten voor elk type van FireAMPconnector downloaden. Dit pakket kan op een netwerkaandeel worden geplaatst of via beheersoftware worden verspreid.

est a shoup			
FireAMP Windows	FireAMP Android	🔹 FireAMP Mac	∆ FireAMP Linux
Flash Scan on Install	Activation Codes	Flash Scan on Install	GPG Public Key
🛓 Download	🛓 Download	🛓 Download	🛓 Download
Show URL	Show URL	Show URL	Show URL

Een groep selecteren

- Alleen controle: Controle van het systeem op basis van SHA-256 berekend over elk bestand. Deze Controlemodus stelt de malware niet in quarantaine, maar stuurt een gebeurtenis als alarm.
- Beschermen: Beveiliging van modus met quarantainebestanden. Monitorbestand kopiëren en verplaatsen.
- Triage: Dit is voor gebruik op een reeds gecompromitteerde/geïnfecteerde computer.
- Server: Installatiesuite voor Windows server, waar de connector installeert zonder Tetra-motor en DFC-stuurprogramma. Deze groep is ontworpen door de naam ervan voor servers die niet op het domein vallen.

• **Domain Controller:** Het standaardbeleid voor deze groep wordt ingesteld op audit mode zoals in servergroep. Associeer al uw actieve directory servers in deze groep, dit betekent dat de connector op een Windows Domain Controller zal worden uitgevoerd.

De AMP heeft de functie TETRA, de volledige antivirusmotor. Deze optie is optioneel per beleid.

Functies

- Flash Scan op installatie: Scan het proces tijdens de installatie. Het is relatief snel om te starten en aanbevolen slechts één keer te draaien.
- Herverdelbaar: U dient één pakket te downloaden, dat 32-bits en 64-bits installatieprogramma's bevat. In plaats van een bootstrapper, die beschikbaar is om deze optie los te laten en de installatiebestanden te downloaden, zodra deze uitgevoerd is.

Opmerking: U kunt uw eigen groep maken en hieraan gekoppeld beleid configureren. Het doel is om alle actieve telefoongids servers in één groep te plaatsen, waar het beleid in de auditmodus staat.

De rapper en de herdistribueerbaar installateur bevatten ook allebei een bestand policy.xml dat wordt gebruikt als configuratiebestand voor de AMP-connector.

Stap 4: Clientprofiel voor webbeveiliging downloaden

Geef een webserver van het bedrijf of een netwerkaandeel op met de AMP-installateur. Dit wordt het meest gebruikt door bedrijven om bandbreedte op te slaan en vertrouwde installateurs op een gecentraliseerde locatie te plaatsen.

Zorg ervoor dat de HTTPS-link op de eindpunten kan worden bereikt zonder certificaatfout en dat het basiscertificaat in de machinewinkel is geïnstalleerd.

Ga terug naar het AMP-profiel dat voor de ASA is gemaakt (stap 1) en bewerk **AMP Enablerprofiel**:

- 1. Klik voor de AMP-modus op de radioknop Installeer AMP Enabler.
- 2. Voeg in het veld **Windows Installatieprogramma** de IP voor de webserver en het bestand voor FireAMP toe.
- 3. Windows-opties zijn optioneel.

Klik op **OK** en pas de wijzigingen toe.

AnyConnect Client Profile Editor Profile: vpn	- vpn	About
AMP Enabler Profile		
AMP Mode	Install AMP Enabler O Uninstall AMP Enabler	
Windows Installer	https:// webserver.cisco.com/Audit_FireAMPSetup.exe Check	
Mac Installer	https:// Check	
Windows Options	 Add To Start Menu Add To Desktop Add To Context Menu Save Reset	
	OK Cancel Help	

Stap 5: Connect met AnyConnect en controleer de installatie van de module

Wanneer een VPN-gebruiker AnyConnect aansluit, drukt ASA de AnyConnect AMP Enablermodule door VPN. Voor reeds ingelogde gebruikers, wordt het aanbevolen om uit te loggen en dan terug in te loggen zodat de functionaliteit wordt ingeschakeld.

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

Stap 6: Start VPN Connection installatieautomaat van AMP en AMP-aansluiting

Zodra u op de knop drukt om de VPN te starten, wordt de nieuwe downloader-module gedownload. Dit zal AMP in staat stellen en het AMP pakket van het URL pad hebben gedownload dat u een paar stappen eerder hebt opgegeven.

S Cisco AnyCo	onnect Secure Mobility Client		
	VPN: Connected to 10.168.109.18.	_	
00:00:07	10.168.109.18		Disconnect IPv4
	AMP Enabler: Installing AMP for Endpoints		
\$			alialia cisco

If you look at the event viewer:

AMP enabler install: Date : 04/24/2017 Time : 10:08:34 Type : Information Source : acvpndownloader Description : Cisco AnyConnect Secur

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

Stap 7: Controleer AnyConnect en controleer of alles is geïnstalleerd

Controleer AnyConnect en controleer of alles correct geïnstalleerd is nadat de VPN is aangesloten en de configuratie van de webserver is geïnstalleerd.

In services.msc kunt u een nieuwe dienst vinden die CiscoAMP_5.1.3 wordt genoemd. In de opdracht PowerShell zien we:

PS C:\Use	ers\winUser348>	Get-Service -name "*CiscoAMP*"	
Status	Name	DisplayName	
Running	CiscoAMP_5.1.3	Cisco AMP for Endpoints Connector 5	5



Met het installatieprogramma van AMP worden nieuwe stuurprogramma's aan het Windowsbesturingssysteem toegevoegd. U kunt de driverquery-opdracht gebruiken om een lijst van de stuurprogramma's op te geven.

C:\Windo	ws\System32	>driverquer	y /v	findstr immunet			
ImmunetP	rote Immune	etProtectDri	ver	ImmunetProtectDriver	File System	System	Running
OK	TRUE	FA					
LSE	4,096	69,632	0	3/17/2017 5:04:20	PM		
/;;/C:/M	INDOWS\Syst	em32\Driver	s∖imm	unetprotect.s 8,192			
ImmunetS	elfP Immune	etSelfProtec	tDriv	ImmunetSelfProtectDriv	v File System	System	Running
OK	TRUE	FA					
LSE	4,096	28,672	0	3/17/2017 5:04:08	PM		
\??\C:\W	INDOWS\Syst	em32\Driver	s∖imm	unetselfprote 8,192			

Stap 8: Testen met een Eicar String in een PDF-bestand van Zombies

Test met een Eicar string in een PDF-bestand van Zombies in een testcomputer om te controleren of het kwaadaardige bestand in quarantaine staat.



Zombies.pdf bevat oorlogen als touwtje

Stap 9: Samenvatting van implementatie

Deze pagina toont u een lijst van succesvolle en mislukte installaties van de connector van FireAMP evenals de installaties die momenteel in bedrijf zijn. U kunt naar **Management > Deployment Summary** gaan.



Stap 10: Detectie van bedreigingen

Zombies.pdf zorgde voor een quarantaine-event en stuurde naar het AMP-dashboard.

and the second se	.amp.cisco.com/dashboard#/events/show	/0		ela	Hedat			N E	• •	0		
st Visited 🧕 Most Visite	ed 🧕 Most Visited 🧕 Most Visited 🧕	Nejnavštěvovanější 🛞 Getting Started 🐋 Latest Hea	adlines 📙 Mozilla Fire	efox 🤌 Most Visite	d 🤮 Mos	: Visited 闭	Getting Started	🛞 Jak začít 🧾 N	Most Visited	Nejr	avštěvovanějš	\$1
	cisco AM	P for Endpoints	Ø	Announcements	Support	? Help	Account	😝 Log Out				
	Dashboard Analy	ysis ~ Outbreak Control ~ Reports Managem	nent ~ Accounts ~		Search			Q				
	New AM Version 1.3,	AP for Endpoints Linux Connector 1.416 is now available. Learn more in the <u>Official Rel</u>	ease Notes	×								
ashboard	Overview Events Heat Map	0 Cr	ognitive Incidents	C								
🖯 Filter: (New) 🖗									Select a Fi	ilter		
Event Type All	l Event Types		+	Group All Grou	ps							+
Filters Ad	dd filters by clicking on the $oldsymbol{ au}$ icon in the	e event details										
Time Range W	leek ~ Sort	Time ~ 🗢						Not Subscri	ibed ~ R	Reset	Save Filter A	s
DJANULIK-HYYPD.	cisco.com detected 4XpJCE_X.pdf.part	as W32.Zombies.NotAVirus				P)	עק <mark>ום</mark> עק	uarantine: Success	ful 20	17-07-27	13:32:08 UT	С
DJANULIK-HYYPD. File Detection	cisco.com detected 4XpJCE_X.pdf.part Detection	as W32.Zombies.NotAVirus				P C		uarantine: Successi	ful 20)17-07-27	13:32:08 UT	с
DJANULIK-HYYPD. File Detection Connector Info	cisco.com detected 4XpJCE_X.pdf.part Detection Fingerprint (SHA-256)	as W32.Zombles.NotAVirus TW32.Zombles.NotAVirus T 00b32c34989bb002				PP C	29 (13) 9	uarantine: Successi	ful 20)17-07-27	' 13:32:08 UT(c
DJANULIK-HYYPD. File Detection Connector Info Comments	cisco.com detected 4XpjCE_X.pdf.part Detection Fingerprint (SHA-256) Filename	as W32.Zombles.NotAVirus TW32.Zombles.NotVirus T 00b32c34989bb002 T 4XpICE.X.pdf.part				Ph C	₽¥ (2) q	uarantine: Success	ful 20)17-07-27	' 13:32:08 UT(c
DJANULIK-HYYPD. File Detection Connector Info Comments	cisco.com detected 4XpJCE_X.pdf.part Detection Fingerprint (SHA-256) Filename Filepath	as W32.Zombies.NotAVirus TW32.Zombies.NotAVirus T 00b32c34989bb002 T4XpJCE.X.pdf.part C\Users\djanulik\AppData\Local\Temp\4Xp	JCE_X.pdf.part			P p (₽₽ (8)	uarantine: Successi	ful 20)17-07-27	7 13:32:08 UT(°C
DJANULIK-HYYPD. File Detection Connector Info Comments	cisco.com detected 4XpJCE_X.pdf.part Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes)	as W32.Zombies.NotAVirus	JCE_X.pdf.part			∎µ [9 (D) 9	uarantine: Successl	ful 20	017-07-25	7 13:32:08 UTu	c
DJANULIK-HYYPD. File Detection Connector Info Comments	Leisco.com detected 4XpJCE_X.pdf.part Detection Filepartint (SHA-256) Filepath FileSize (bytes) Parent Fingerprint (SHA-256)	as W32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus Twosters Columnation C:\Users\djanulik\AppData\Local\Temp\4Xp; 309500 Tofffob175fdf32be O	JCE_X.pdf.part			₽v [<u>, 12</u> , 0	uarantine: Successi	ful 20	017-07-27	7 13:32:08 UT	C.
DJANULIK-HYYPD. File Detection Connector Info Comments	Leisco.com detected 4XpJCE_X.pdf.part Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes) Parent Fingerprint (SHA-256) Parent Filename	as W32.Zombies.NotAVirus	JCE_X.pdf.part			1	9 10 1 49	uarantine: Successi	ful 20	017-07-27	7 13:32:08 UT	C.

Quarantine Event

Aanvullende informatie

Om je AMP account te krijgen, kun je je inschrijven bij de ATS-universiteit. Dit geeft een overzicht van AMP-functionaliteit in LAB.

Gerelateerde informatie

- AMP-functie configureren
- Technische ondersteuning en documentatie Cisco Systems