AnyConnect 4.x および AMP イネーブラを介した AMP モジュールのインストールと設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> ASA を介した AMP イネーブラのための AnyConnect の導入 <u>ステップ1:AnyConnect AMPイネーブラクライアントプロファイルの設定</u> ステップ2:AnyConnect AMP イネーブラをダウンロードするためのグループ ポリシーの編集 ステップ3: FireAMP ポリシーのダウンロード ステップ4:Webセキュリティクライアントプロファイルのダウンロード ステップ5: AnyConnect への接続とモジュールのインストールの検証 ステップ6:VPN接続の開始AMPイネーブラとAMPコネクタのインストール 手順7:AnyConnectの確認とすべてのコンポーネントがインストールされているかどうかの検証 ステップ8: ゾンビPDFファイルに含まれるEicar文字列を使用したテスト 手順9:導入の概要 手順 10:スレッド検出の検証 追加情報 関連情報

概要

このドキュメントでは、高度なマルウェア防御(AMP)コネクタをAnyConnectとともにインストー ルする手順を説明します。

AnyConnect AMPイネーブラは、エンドポイント向けAMPを導入するためのメディアとして使用 されます。それ自体はファイルの性質を証明する能力を持っていません。AMP for Endpointsソフ トウェアをASAからエンドポイントにプッシュします。AMPがインストールされると、クラウド 容量を使用してファイルの性質を確認します。さらにAMPサービスは、ThreatGridと呼ばれる動 的な分析にファイルを送信して、未知のファイルの動作をスコア化できます。これらのファイル は、特定のアーティファクトが満たされると、悪意があると判断される可能性があります。これ は、ゼロデイ攻撃に広く使用されています。

前提条件

要件

- AnyConnectセキュアモビリティクライアントバージョン4.x
- FireAMP / エンドポイント向け AMP
- Adaptive Security Device Manager(ASDM)バージョン7.3.2以降

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- •ソフトウェアバージョン9.5.1が稼働する適応型セキュリティアプライアンス(ASA)5525
- Microsoft Windows 7 Professional 64ビット上のAnyConnectセキュアモビリティクライアン ト4.2.00096
- ASDM バージョン 7.5.1(112)

ASA を介した AMP イネーブラのための AnyConnect の導入

設定に含まれる手順は次のとおりです。

- AnyConnect AMPイネーブラクライアントプロファイルを設定します。
- AnyConnect VPNグループポリシーを編集し、AMPイネーブラサービスプロファイルをダウ ンロードします。
- AMPダッシュボードにログインして、コネクタURLダウンロードリンクを取得します。
- •ユーザマシンでインストールを検証します。

ステップ1: AnyConnect AMPイネーブラクライアントプロファイルの設定

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]に移動します。
- AMP Enablerサービス・プロファイルを追加します。

Add AnyConne	ect Client Profile	
Profile Name	amp	
Profile Usage	AMP Enabler Service Profile	
Enter a device f	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
-	<unassigned></unassigned>	
Group Policy		
Group Policy	Enable 'Always On VPN' for selected group	
Group Policy	Enable 'Always On VPN' for selected group	

🛧 Add 🗹 Edit 🗱 Change Group Policy	📋 Delete 🛃 Import 🖏 Export	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

ステップ 2:AnyConnect AMP イネーブラをダウンロードするためのグループ ポ リシーの編集

- [Configuration] > [Remove Access VPN] > [Group Policies] > [Edit] の順に移動します。
- [Advanced] > [AnyConnect Client] > [Optional Client Modules to Download]に移動します。
- [AnyConnect AMP Enabler]を選択します。

ステップ 3 : FireAMP ポリシーのダウンロード

注:続行する前に、システムがAMP of Endpoints Windows Connectorの要件を満たしているかどうかを確認してください。

AMP for Endpoints Windows Connector のシステム要件

これらは、Windowsオペレーティングシステムに基づくFireAMPコネクタの最小システム要件で す。FireAMP Connector は、次のオペレーティング システムの 32 ビット バージョンと 64 ビッ ト バージョンをサポートします。最新のAMPドキュメントは、AMPの導入で入手<u>できます</u>

オペレーティン グ システム	プロセッサ	メモリ	ディスク領域、 クラウド専用モ ード	ディスク領域
Microsoft Windows 7	1 GHz 以上のプ ロセッサ	メモリ 1 GB	150 MB の使用可 能なハード ディ スク領域 - クラ ウド専用モード	1 GB の使用可能 なハード ディス ク領域 - TETRA
Microsoft Windows 8 およ び 8.1 (FireAMP Connector 5.1.3 以降が必要)	1 GHz 以上のプ ロセッサ	メモリ 512 MB	150 MB の使用可 能なハード ディ スク領域 - クラ ウド専用モード	1 GBのハードデ ィスク空き容量 – TETRA
Microsoft Windows Server 2003	1 GHz 以上のプ ロセッサ	メモリ 512 MB	150 MB の使用可 能なハード ディ スク領域 - クラ ウド専用モード	1 GB の使用可能 なハード ディス ク領域 - TETRA
Microsoft Windows Server 2008	2 GHz 以上のプ ロセッサ	メモリ 2 GB	150 MB の使用可 能なハード ディ スク領域 - クラ ウド専用モード	1 GBのハードデ ィスク空き容量 – TETRA
Microsoft Windows Server 2012(FireAMP Connector 5.1.3 以降が必要)	2 GHz 以上のプ ロセッサ	メモリ 2 GB	150 MB の使用可 能なハード ディ スク領域 - クラ ウド専用モード	1 GBのハードデ ィスク空き容量 – TETRA

最も一般的なのは、AMPインストーラをエンタープライズWebサーバに配置することです。

コネクタをダウンロードするには、[Management] > [Download Connector] に移動します。次に 、[type]を選択し、[**Download** FireAMP (Windows、Android、Mac、Linux)]を選択します。

P Dehboard x +				
🔶 🚊 https://conscis.amp.sourcefine.com/dishboard		v C Q feach	0 0 ¢	* * 4 @ • @ = • = =
My Work Zone - Cons A Topic Search 🛐 Home - Tech Zone Q Casekwery	🗣 Learnearre Backlog Vie 🎦 Account T	sam Directory 🗔 Anyconnect Websec	ur 🔾 Cisce HTMLS Upleed 🎑 1	72 🔒 Micc 🎴 Bugs 🛕 Webmonitor
SOURCE		-0 installs 1 detection (7 days) - Anhles	incentents Chapport Thelp	1% Log Out
Dashboard Analysis - Outbreak (Control - Reports Management +	ccounts •	95.2	3005102317
Dashboard	Quick Start Computers		Group Filter Select	Groups -
Overview Events Healt Map	Groups Policies	_		Refresh All O Auto-Refresh •
Indications of Compromise	Hosts Detectir Download Connect		Hosts Detecting Network	Threats (7 days)
There are converte of computers with indications of prospectation	Computer Deployment Summ	ary ant	Computer	Count
	Cloud Recall	-		
	Mahuare Threats (7 days)		Network Threats (7 days)	
	Detection Name	Coant	Remote iP	Count
	W32.0CAR.19	1	There are in intent holigo	
	Recent Malware Threats		Recent Network Threats	
	Computer	Detection Name	Computer 0	Detection Name Remote IP
	WCOBAQW7PN80EM0	W32.6ICAR.16g1		A Deep Johnsteen Duitsping

[Download Connector]ページでは、FireAMPコネクタのタイプごとにインストールパッケージを ダウンロードできます。このパッケージは、ネットワーク共有に配置することも、管理ソフトウ ェアを介して配布することもできます。

FireAMP Windows	FireAMP Android	📽 FireAMP Mac	
Flash Scan on Install @	Activation Codes	Flash Scan on Install Ø	GPG Public Key
🛓 Download	🛓 Download	🛓 Download	🛓 Download
Show URL	Show URL	Show URL	Show URL

[Select a Group]

- [Audit Only]:各ファイルで計算されたSHA-256に基づいてシステムを監視します。この監査のみのモードでは、マルウェアは検疫されず、アラートとしてイベントが送信されます。
- [Protect]:悪意のあるファイルを隔離する保護モード。ファイルのコピーと移動を監視します。
- [Triage]:これは、すでに感染または感染しているコンピュータで使用されます。
- [Server]: Windowsサーバ用のインストールスイート。コネクタはTetraエンジンとDFCドラ イバなしでインストールされます。このグループは、非ドメインコントローラサーバの名前 で設計されています。
- [Domain Controller]: このグループのデフォルトポリシーは、サーバグループのように監査モ

ードに設定されます。このグループ内のすべてのActive Directoryサーバを関連付けます。これは、コネクタがWindowsドメインコントローラで実行されることを意味します。

AMPには、完全なウイルス対策エンジンであるTETRAという機能があります。このオプションは、ポリシーごとにオプションです。

機能

- [Flash Scan on Install]:インストール中にスキャンプロセスが実行されます。比較的迅速に 実行でき、1回だけ実行することを推奨します。
- [Redistributable]: 32ビットおよび64ビットのインストーラを含む1つのパッケージをダウン ロードする必要があります。このオプションをオフのままにして、インストーラのファイル をダウンロードするブートストラッパは実行されません。

注:独自のグループを作成し、それに関連付けられたポリシーを設定できます。この目的は 、ポリシーが監査モードになっている1つのグループにすべてのActive Directoryサーバを配 置することです。

ブートストラッパと再頒布可能インストーラの両方にpolicy.xmlファイルが含まれ、AMPコ ネクタの設定ファイルとして使用されます。

ステップ 4: Webセキュリティクライアントプロファイルのダウンロード

AMPインストーラで会社のWebサーバまたはネットワーク共有を指定します。これは、帯域幅を 節約し、信頼できるインストーラを一元化された場所に配置するために、企業で最も一般的に使 用されます。

エンドポイントで証明書エラーなしでHTTPSリンクに到達でき、ルート証明書がマシンストアに インストールされていることを確認してください。

ASAで以前に作成したAMPプロファイルに戻り(ステップ1)、AMPイネーブラプロファイルを **編集します**。

- 1. AMPモードの場合は、[AMPイネーブラのインストール]**ラジオ・ボタン**をクリックします。
- 2. [Windows Installer]フィールドに、WebサーバのIPとFireAMPのファイルを追加します。
- 3. [Windows Options] はオプションです。

[OK] をクリックし、変更を適用します。

Profile: 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://	
Windows Options	🗹 Add To Start Menu	
	Add To Desktop	
	Save Reset	
	OK Cancel Help	

ステップ 5: AnyConnect への接続とモジュールのインストールの検証

Anyconnect VPNユーザが接続すると、ASAはAnyConnect AMPイネーブラモジュールをVPN経由 でプッシュします。すでにログインしているユーザの場合は、機能を有効にするために、ログオ フしてから再度ログインすることをお勧めします。

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					

ステップ 6: VPN接続の開始AMPイネーブラとAMPコネクタのインストール

ボタン[connect]を押してVPNを開始すると、新しいダウンローダモジュールがダウンロードされ ます。これにより、AMPイネーブラが作成され、以前に指定したURLパスからAMPパッケージが ダウンロードされます。

🕥 Cisco AnyCo	onnect Secure Mobility Client		_ 🗆 🗙
	VPN: Connected to 10.168.109.18.		
_	10.168.109.18	*	Disconnect
00:00:07			IPv4
	AMP Enabler: Installing AMP for Endpoints		
¢ ()			ajialo 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 Secure Mobility Client Downloader (2) exiting, version 4.4.01054 , return code 0 [0x00000000]

手順 7 : AnyConnect の確認とすべてのコンポーネントがインストールされている かどうかの検証

VPNが接続され、Webサーバの設定がインストールされたら、AnyConnectをチェックして、すべてが正しくインストールされていることを確認します。

services.mscには、CiscoAMP_5.1.3という名前の新しいサービスがあります。Powershellコマン ドには次のように表示されます。

PS C:\Users\winUser348> Get-Service -name "*CiscoAMP*"

Status	Name	DisplayName		
Running	CiscoAMP_5.1.3	Cisco AMP for Endpoints Connector 5.	•••	

0	Cisco AnyCo	nnect Secure Mobility Client		
		<u>VPN:</u> Connected to 10.168.109.18. 10.168.109.18	Y	Disconnect
	00:01:22			IPv4
		AMP Enabler: AMP for Endpoints installed.		
	\$ (i)			athatha cisco

AMPインストーラは、Windows OSに新しいドライバを追加します。driverqueryコマンドを使用 してドライバをリストできます。

C:\Windows\System32>driverquery /v | findstr immunet

ImmunetProte ImmunetProtectDriver ImmunetProtectDriver File System System Running OK TRUE FA 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 LSE 4,096 28,672 0 3/17/2017 5:04:08 PM \??\C:\WINDOWS\System32\Drivers\immunetselfprote 8,192

ステップ8:ゾンビPDFファイルに含まれるEicar文字列を使用したテスト

テストコンピュータのZombies PDFファイルに含まれるEicar文字列を使用してテストを行い、悪意のあるファイルが検疫されていることを確認します。



Zombies.pdfにはEicar文字列が含まれています

手順9:導入の概要

このページには、FireAMPコネクタのインストールの成功と失敗、および現在進行中のインスト ールのリストが表示されます。[Management] > [Deployment Summary] に移動できます。



手順 10:スレッド検出の検証

Zombies.pdfは検疫イベントをトリガーし、AMPダッシュボードに送信します。

	u.amp.cisco.com/dashooarc	a ference and a ference of the			C Q	negat			N E			• ^ ·	- 3
Visited 🧕 Most Visite	ed 📓 Most Visited 📓 M	lost Visited 🧕 Ne	ejnavštěvovanější 🛞 Getting Started 📓 Li	atest Headlines Mozilla Fi	refox 🤰 Most Visite	d 川 🛃 Most	Visited 🛞	Getting Started	🛞 Jak začít 🧕	Most Visite	ed 🧕 Ne	ejnavštěvovan	ejší
	cis	Co AMP	for Endpoints	•	2 Announcements	Support	? Help	My Account	🕞 Log Out				
	Dashl	board Analysis	 Outbreak Control - Reports M 	lanagement ~ Accounts ~		Search			Q				
		New AMP Version 1.3.1.41	for Endpoints Linux Conn 16 is now available. Learn more in the Offi	ector cial Release Notes	×								
ishboard	Overview Events	Heat Map		0 Cognitive Incidents	s 🕑								
∃Filter: (New) ⊚									Select a Filter				
Event Type All Filters Ad	ll Event Types dd filters by clicking on th	e T icon in the ev	ent details	+	Group All Grou	ps							+
Event Type All Filters Ad Time Range We	Il Event Types dd filters by clicking on th Veek ~	e 🍸 icon in the evo Sort Tit	ent details me ~ \$	+	Group All Grou	ps			Not Subso	cribed ~	Reset	Save Filter	+ r As
Event Type All Filters Ad Time Range We	Il Event Types dd filters by clicking on th week ~ .cisco.com detected 4XpJ	e T icon in the ev Sort Tit	ent details me v v	*	Group All Grou	ps	P C	ס מט	Not Subsc	cribed ~	Reset	Save Filter 27 13:32:08 U	+ r As JTC
Event Type All Filters Ad Time Range W DJANULIK-HYYPD.	Il Event Types dd filters by clicking on th reek ~ .cisco.com detected 4Xpj Detection	e T icon in the ev Sort Ti CE_X.pdf.part as 1	ent details me v v W32.Zombies.NotAVirus TW32.Zombies.NotAVirus	*	Group All Grou	ps	PP G	ס ובו ענ	Not Subsc uarantine: Succes	cribed ~	Reset 2017-07-	Save Filter 27 13:32:08 U	+ r As UTC
Event Type All Filters Ad Time Range W DJANULIK-HYYPD.c File Detection	Il Event Types dd filters by clicking on th keek ~ .cisco.com detected 4Xpj Detection Fingerprint (SHA-	e ▼ icon in the ew Sort Tin CE,X.pdf.part as 1 256)	ent details me v ¢ W32.Zombles.NotAVirus TW32.Zombles.NotAVirus TW32.Zombles.NotAVirus V0b32c34989bb002	•	Group All Grou	p5	(B P) (9 (1) 9	Not Subsc	cribed ~	Reset	Save Filter 27 13:32:08 U	н AS JTC
Event Type All Filters Ad Time Range W DJANULIK-HYYPD. Connector Info Comments	Il Event Types dd filters by clicking on th veek ~ .cisco.com detected 4Xpj Detection Fingerprint (SHA- Filename	e ▼ icon in the ev Sort Tii CE_X.pdf.part as 1 256)	ent details me	•	Group All Grou	p5	P P C	ہ رہا برد	Not Subsc	cribed ~	Reset 2017-07-	Save Filter 27 13:32:08 U	+ rAs ллс
Event Type All Filters Ad Time Range Wi DJANULIK-HYYPD. File Detection Connector Info Comments	Il Event Types dd filters by clicking on th veek v v v v v v v v v v v v v v v v v v v	e ▼ icon in the ev Sort Ti CE X.pdf.part as 1 256)	ent details me	* mp\4XpJCE_X.pdf.part	Group All Grou	ps	PP C	9 (11) 9	Not Subsc	cribed v	Reset 2017-07-	Save Filter	+ r As JJTC
Event Type All Filters Ad Time Range Wi DJANULIK-HYYPD. File Detection Connector Info Comments	Il Event Types dd fliters by clicking on th keek ~ .ccscc.com detected 4XpJ Detection Fingerprint (SHA- Filename Filepath File Size (bytes)	e ♥ icon in the ev Sort Ti CE X.pdf.part as 1 256)	ent details me	+ mp\4XpJCE_X.pdf.part	Group All Grou	ps	Pr C	Q (D) 9	Not Subsc	cribed ~	Reset	Save Filter 27 13:32:08 U	+ r As JJTC
Event Type All Filters Ao Time Range Wi DJANULIK-HYYPD. File Detection Connector Info Comments	Il Event Types dd fliters by clicking on th keek kcisco-com detected 4Xpj Detection Filepartnt (SHA- Filepath Filepath File Size (bytes) Parent Fingerprint	e ♥ icon in the ev Sort Ti CE_X.pdf.part as 1 256) at (SHA-256)	ent details me	+ mp\4XpJCE_X.pdf.part	Group All Grou	ps	PP C	Q (C)	Not Subsc	cribed v	Reset	Save Filter	+ r As JJTC
Event Type All Filters Ac Time Range Wi DJANULIK-HYYPD. File Detection Connector Info Comments	Il Event Types dd fliters by clicking on th feek	e ♥ icon in the ev Sort Ti CE_X.pdf.part as 1 2256) at (SHA-256)	ent details me	+ rmp\4XpjCE_X.pdf.part	Group All Grou	ps	۲ ۳	9 10 9	Not Subsc	cribed v	Reset	Save Filter	+ r As

検疫イベント

追加情報

AMPアカウントを取得するには、ATS大学にサインアップできます。これにより、ラボのAMP機能の概要が示されます。

関連情報

- <u>AMP イネーブラの設定</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>