Instalação e configuração do módulo AMP através do AnyConnect 4.x e do ativador AMP

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Implantação do AnyConnect para o AMP Enabler através do ASA Passo 1: Configurar o perfil do cliente do AnyConnect AMP Enabler Passo 2: Edite a política de grupo para baixar o AnyConnect AMP Enabler Passo 3: Baixe a política do FireAMP Passo 4: Baixe o perfil do cliente do Web Security Passo 5: Conecte-se com o AnyConnect e verifique a instalação do módulo Passo 6: Iniciar conexão VPN instalar o ativador AMP e o conector AMP Passo 7: Verifique o AnyConnect e se tudo está instalado Passo 8: Teste com uma string de Eicar contida em um arguivo PDF do Zombies Etapa 9: Resumo da implantação Etapa 10: Verificação de Detecção de Threads Additional Information Informações Relacionadas

Introduction

Este documento segue as etapas para instalar o conector Advanced Malware Protection (AMP) com AnyConnect.

O AnyConnect AMP Enabler é usado como um meio para implantar a AMP para endpoints. Ele mesmo não tem nenhuma capacidade de condenar a disposição do arquivo. Ele envia o software AMP para endpoints para um endpoint do ASA. Quando o AMP é instalado, ele usa a capacidade de nuvem para verificar a eliminação dos arquivos. Outro serviço AMP pode enviar arquivos para análise dinâmica chamada ThreatGrid, para pontuar comportamento de arquivos desconhecidos. Esses arquivos podem ser condenados como mal-intencionados se determinados artefatos forem atendidos. Isso é amplamente útil para ataques de dia zero.

Prerequisites

Requirements

- AnyConnect Secure Mobility Client versão 4.x
- FireAMP / AMP para endpoints
- Adaptive Security Device Manager (ASDM) versão 7.3.2 ou posterior

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Adaptive Security Appliance (ASA) 5525 com versão de software 9.5.1
- AnyConnect Secure Mobility Client 4.2.00096 no Microsoft Windows 7 Professional de 64 bits
- ASDM versão 7.5.1(112)

Implantação do AnyConnect para o AMP Enabler através do ASA

As etapas envolvidas na configuração são as seguintes:

- Configure o perfil do cliente do AnyConnect AMP Enabler.
- Edite a política de grupo do AnyConnect VPN e faça o download do Perfil de serviço do ativador AMP.
- Faça login no painel AMP para obter o link de download da URL do conector.
- Verifique a instalação na máquina do usuário.

Passo 1: Configurar o perfil do cliente do AnyConnect AMP Enabler

- Navegue até Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.
- Adicione o perfil de serviço do ativador AMP.

| ÷ | Add 🗹 Edit | 🔆 Change Group Policy 📋 Delete 🐺 Import 🖷 Export 🗃 Valida | te | |
|----------|--------------------------------------|--|--------------|----|
| a | Add AnyConne | ect Client Profile | L | 23 |
| | Profile Name | amp | | |
| | Profile Usage | AMP Enabler Service Profile 🔹 | | |
| | Enter a device f automatically cr | ile 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 | <unassigned></unassigned> | | |
| | | Enable 'Always On VPN' for selected group | | |
| | | | | |
| | | OK Cancel Help | | |

| 🛧 Add 🗹 Edit 🗱 Change Group Policy | 📋 Delete 🔁 Import 🗟 Export | S 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 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Passo 2: Edite a política de grupo para baixar o AnyConnect AMP Enabler

- Navegue até Configuration > Remove Access VPN > Group Policies > Edit (Configuração > Remover VPN de Acesso > Políticas de Grupo > Editar).
- Vá para Avançado > Cliente AnyConnect > Módulos de cliente opcionais para baixar.
- Escolha AnyConnect AMP Enabler.

| | a second s | | | | | |
|--------------------|---|-------------|------------------|-------------------------------|-----------------|--|
| Seneral Servers | Keep Installer on Clerk System | [2] Inheit | C Tel | () No | | |
| wanced | Delagram Transport Layer Security (DTLS): | V Inherit | () Enable | Otable | | |
| Browser Proxy | 07LS Compression: | 2 Inherit | C Brable | () Doble | | |
| = Psec(XEv1) Clent | 59, Compression: | 2 Inherit | 🗇 Defete | 0.125 | () Daable | |
| | Ignore Don't Fragment(DF) Bit: | (2) Inherit | C Enable | () Doable | | |
| | Client Bypess Protocol: | [] Inheit | () brable | () Double | | |
| | FQDN of this Devices | PQ0N | | | | |
| | MTU: | [] Inherit | | | | |
| | Keepalive Messages: | Differit | Dealer | Intervali [| seconds | |
| | Optional Client Modules to Download: | Elshert | impenatio | | | • |
| | Always-On VPN: | 2 Inherit | AnyCon | ect DART ect Network | Access Manager | |
| | Client Profiles to Download: | Dheit | AnyCon AnyCon | vect Network vect SBL | Visibility | |
| | | 4 ASS 1 | AnyCon | nect Web Sec | curity class | |
| | | Profile Nam | AnyCan | lect ISE Post lect Posture | ure . | |
| | | SECONALY. | | | (| OK Cancel |
| | | 1 | | | | and the second s |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| d: | Next Previou | 4 | | | | |
| | | | | | | |

Passo 3: Baixe a política do FireAMP

Note: Antes de continuar, verifique se o sistema atende aos requisitos da AMP do conector do Windows do endpoint.

Requisitos do sistema para o AMP para endpoints Conector do Windows

Esses são os requisitos mínimos do sistema para o conector FireAMP baseado no sistema operacional Windows. O conector FireAMP suporta as versões de 32 e 64 bits desses sistemas operacionais. A documentação mais recente da AMP pode ser encontrada na <u>implantação da</u> <u>AMP</u>

| Sistema operacional | Processador | Memória | Espaço em disco, Modo somente nuvem | Espaço em disco |
|--|---|---------------|--|--|
| Microsoft Windows 7 | Processador de 1 GHz ou mais rápido | 1 GB de RAM | disponível no disco rígido - modo somente | 1 GB de espaço disponível no disco rígido - TETRA |
| Microsoft Windows 8 e 8.1 (requer FireAMP Connector 5.1.3 ou posterior) | Processador de 1 GHz ou mais rápido | 512 MB de RAM | 150 MB de espaço disponível no disco rígido - modo somente na nuvem | 1 GB de espaço disponível no disco rígido - TETRA |
| Microsoft Windows Server 2003 | Processador de 1 GHz ou mais rápido | 512 MB de RAM | 150 MB de espaço disponível no disco rígido - modo somente na nuvem | 1 GB de espaço disponível no disco rígido - TETRA |
| Microsoft Windows Server 2008 | Processador de 2 GHz ou mais rápido | 2 GB de RAM | 150 MB de espaço disponível no disco rígido - modo somente na nuvem | 1 GB de espaço disponível no disco rígido - TETRA |
| Microsoft Windows Server 2012 (requer o FireAMP Connector 5.1.3 ou posterior) | Processador de 2 GHz ou mais rápido | 2 GB de RAM | 150 MB de espaço disponível no disco rígido - modo somente na nuvem | 1 GB de espaço disponível no disco rígido - TETRA |

O mais comum é colocar o instalador da AMP no servidor web da empresa.

Para baixar o conector, navegue até **Management > Download Connector**. Em seguida, escolha o tipo e **Baixe o** FireAMP (Windows, Android, Mac, Linux).

| P Deshboard x + | | | | |
|--|-------------------------------|--|--------------------------|--|
| | | v C Q Associ | 0 0 ¢ | * * 4 0 . 9 8 = |
| My Work Zone - Cons | 🖡 Loomeans Backlog Vie 🎦 Acci | ount Team Directory 🗌 Anyconnect Websec | w 🔾 Cisco HTMLS Upload 🎑 | TZ 🔒 Micc 🎴 Bugs 🛕 Webmonitor |
| SOURCE | | () installs 1 detection (7 days) Anster | uncements Chaport Thelp | Pe Log Out |
| Dashboard Analysis - Outbreak Co | etrol - Reports Management | Accounts • | 15 | 2 3005102317 |
| Dashboard | Quick Start Computers | | Group Filter Selec | ct Groups = |
| Overview Events Heat Map | Geoups Policies | | | Refresh All 🔘 Auto-Refresh 🔹 |
| Indications of Compromise | Hosts Detection | meeter . | Hosts Detecting Networ | k Threats (7 days) |
| (there are converte of computer) with tobicitions of computation | Computer Deployment | Summary und | Computer | Count |
| | Courter | | | |
| | | | | |
| | Maharare Threats (7 days) | | Network Threats (7 days | 4 |
| | Detection Name | Count | Remote iP | Count |
| | WITH CARLINGS | | | of the distance of the distanc |
| | | | | |
| | Recent Malware Threats | Detection Name | Recent Network Threats | Outerflow Name Remote IP |
| | WCOBAQW7PNBOEMO | W32.6ICAR.16g1 | There are by carent data | ort (freq) intertient to illiping |
| | | | | |
| | | | | |

A página Baixar conector permite que você faça o download dos pacotes de instalação para cada tipo de conector FireAMP. Este pacote pode ser colocado em um compartilhamento de rede ou distribuído por meio de software de gerenciamento.

| lect a Group T | | | |
|-------------------------|------------------|-------------------------|-----------------|
| FireAMP Windows | FireAMP Android | SireAMP Mac | ∆ FireAMP Linux |
| ☑ 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 |

Selecionar um grupo

- Somente auditoria: Monitorando o sistema com base no SHA-256 calculado sobre cada arquivo. Este modo de Auditoria apenas não coloca o malware em quarentena, mas envia um evento como um alerta.
- **Proteger:** Modo de proteção com arquivos mal-intencionados em quarentena. Monitorar cópia e movimentação de arquivos.
- Triagem: Destina-se ao uso em computadores já comprometidos/infectados.
- Servidor: Conjunto de instalação para servidor Windows, onde o conector é instalado sem o mecanismo Tetra e o driver DFC. Esse grupo é projetado por seu nome para servidores de controladores que não são de domínio.

 Controlador de domínio: A política padrão para esse grupo é definida para o modo de auditoria como no grupo Servidor. Associe todos os servidores do Ative Diretory neste grupo, o que significa que o conector estará em execução em um Controlador de Domínio do Windows.

O AMP tem o recurso chamado TETRA, que é um mecanismo antivírus completo. Essa opção é opcional por política.

Recursos

- Flash Scan na instalação: O processo de verificação é executado durante a instalação. É relativamente rápido e recomendado executar apenas uma vez.
- **Redistribuível:** Você deve fazer o download de um único pacote, que contém instaladores de 32 e 64 bits. Em vez de um bootstrapper, que está disponível, deixando essa opção sem marca e fazendo o download dos arquivos do instalador, uma vez executados.

Note: Você pode criar seu próprio grupo e configurar a política associada para ele. O objetivo é colocar todos, por exemplo, os servidores Ative Diretory em um grupo, onde a política está no modo de auditoria.

O instalador bootstrapper e redistribuível também contém um arquivo policy.xml usado como um arquivo de configuração para o conector AMP.

Passo 4: Baixe o perfil do cliente do Web Security

Especifique o servidor Web da empresa ou um compartilhamento de rede com o instalador da AMP. Isso é mais comumente usado em empresas para economizar largura de banda e colocar instaladores confiáveis em locais centralizados.

Certifique-se de que o link HTTPS pode ser alcançado nos endpoints sem nenhum erro de certificado e de que o certificado raiz está instalado no armazenamento da máquina.

Volte para o perfil da AMP criado antes no ASA (etapa 1) e edite o perfil do ativador da AMP:

- 1. No AMP Mode (Modo AMP), clique no botão de opção **Install AMP Enabler (Instalar o AMP Enabler)**.
- 2. No campo Windows Installer, adicione o IP para o servidor Web e o arquivo para o FireAMP.
- 3. As Opções do Windows são opcionais.

Clique em OK e aplique as alterações.

| 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 | V Add To Start Menu | |
| | Add To Desktop | |
| | V Add To Context Menu | |
| | Save Reset | |
| | | |
| | | |
| | | |
| | | |
| | OK Cancel Help | |

Passo 5: Conecte-se com o AnyConnect e verifique a instalação do módulo

Quando os usuários do AnyConnect VPN se conectam, o ASA envia o módulo do AnyConnect AMP Enabler pela VPN. Para usuários já conectados, é recomendável fazer logoff e, em seguida, fazer logon novamente para que a funcionalidade seja habilitada.

| 10:08:29 AM 10:08:29 AM 10:08:29 AM 10:08:29 AM 10:08:31 AM 10:08:32 AM | Establishing VPN session The AnyConnect Downloader is performing update checks Checking for profile updates Checking for product updates Downloading AnyConnect AMP Enabler 4.4.01054 - 48% Downloading AnyConnect AMP Enabler 4.4.01054 - 91% |
|--|---|
| 10:08:33 AM | Downloading AnyConnect AMP Enabler 4.4.01054 - 100% |
| AnyConnec | t Secure Mobility Client Downloader |
| | The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.00096. Please wait |
| | |
| | |

Passo 6: Iniciar conexão VPN instalar o ativador AMP e o conector AMP

Quando você pressiona o botão conectar para iniciar a VPN, ela faz o download do novo módulo do downloader. Isso terá o ativador do AMP e fará o download do pacote do AMP do caminho do URL que você especificou algumas etapas antes.

| 🔇 Cisco AnyCo | onnect Secure Mobility Client | | |
|---------------|--|---|----------------|
| | YPN: Connected to 10.168.109.18. | | |
| | 10.168.109.18 | ~ | Disconnect |
| 00:00:07 | | | IPv4 |
| | AMP Enabler: Installing AMP for Endpoints | | |
| \$ () | | | altab 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]
```

Passo 7: Verifique o AnyConnect e se tudo está instalado

Depois que a VPN estiver conectada e a configuração do servidor Web estiver instalada, verifique o AnyConnect e verifique se tudo está instalado corretamente.

No services.msc, você pode encontrar um novo serviço chamado CiscoAMP_5.1.3. No comando Powershell vemos:

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

Status Name DisplayName

------

Running CiscoAMP_5.1.3 Cisco AMP for Endpoints Connector 5...
```



O Instalador do AMP adiciona novos drivers ao sistema operacional Windows. Você pode usar o comando driverquery para listar os drivers.

| C:\Window | ws\System32 | >driverquery | y/v | findstr immunet | | | |
|-----------|-------------|---------------|-------|------------------------|---------------|--------|---------|
| ImmunetPi | rote Immune | tProtectDriv | ver | ImmunetProtectDriver | File System | System | Running |
| OK | TRUE | FA | | | | | |
| LSE | 4,096 | 69,632 | 0 | 3/17/2017 5:04:20 | PM | | |
| /??/C:/WI | INDOWS\Syst | em32\Drivers | s∖imm | unetprotect.s 8,192 | | | |
| ImmunetSe | elfP Immune | tSelfProtect | 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\Drivers | s∖imm | unetselfprote 8,192 | | | |

Passo 8: Teste com uma string de Eicar contida em um arquivo PDF do Zombies

Teste com uma string Eicar contida em um arquivo PDF do Zombies em um computador de teste para verificar se o arquivo mal-intencionado está em quarentena.



Zombies.pdf contém uma string Eicar

Etapa 9: Resumo da implantação

Esta página mostra uma lista das instalações bem-sucedidas e com falha do conector FireAMP, bem como das que estão em andamento no momento. Você pode ir para **Gerenciamento > Resumo da implantação**.



Etapa 10: Verificação de Detecção de Threads

O Zombies.pdf acionou um evento de quarentena, envie para o painel do AMP.

| | u.amp.cisco.com/dashboard#/events/show/() | | equ | Hledat | | | \[\] □ ↓ | * 0 | | • ± |
|---|--|--|---------------------------------------|-----------------|---------------------|------------------|---|--|-------------------|--------|
| it Visited 🧧 Most Visite | ed 📓 Most Visited 📓 Most Visited 📓 N | lejnavštěvovanější 🛞 Getting Started 遍 Latest He | adlines 🔒 Mozilla Firefox 🧾 Most Visi | ed \lVert 🙆 Mos | Visited 🛞 G | etting Started | 🛞 Jak začít 📓 Most V | 'isited 🧕 N | lejnavštěvovanějš | H . |
| | cisco AMP | o for Endpoints | Announcements | Support | 7 Help 🛔 | My Account | (+ Log Out | | | |
| | Dashboard Analysi | s 🗸 Outbreak Control 🗸 Reports Managen | nent ~ Accounts ~ | Search | | | Q | | | |
| | New AMI Version 1.3.1.4 | P for Endpoints Linux Connector 116 is now available. Learn more in the <u>Official Rel</u> | ease Notes | | | | | | | |
| ashboard ashboard Inbox | Overview Events Heat Map | 0 C | ognitive Incidents 🗷 | | | | | | | |
| Filter: (New) 🛛 | | | | | | | Sel | ect a Filter | | |
| Event Type All | ll Event Types | | + Group All Gro | ups | | | | | | + |
| Filters Ac | dd filters by clicking on the ${\mathbb T}$ icon in the e | vent details | | | | | | | | |
| Filters Ac | dd filters by clicking on the T icon in the e /eek Sort T | vent details Time ~ + | | | | | Not Subscribed | Reset | Save Filter A | S |
| Filters Ac Time Range W | dd fliters by clicking on the T icon in the e reek ~ Sort T .cisco.com detected 4XpJCE _X.pdf.part as | ime v + | | | | 2 126 Qu | Not Subscribed v uarantine: Successful | 2017-07 | Save Filter A | s |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection | dd filters by clicking on the T icon in the e feek ~ Sort T .cisco.com detected 4XpJCE_X.pdf.part as Detection | wati details ime v ÷ W32.Zombies.NotAVirus TW32.Zombies.NotAVirus | | | Ph C | 2 126 Q | Not Subscribed v uarantine: Successful | Reset 2017-07 | Save Filter A | s |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection Connector Info | dd filters by clicking on the T icon in the e feek ~ Sort T .clisco.com detected 4XpJCE_X.pdf,part a: Detection Fingerprint (SHA-256) | W32.Zombles.NotAVirus W32.Zombles.NotAVirus TW32.Zombles.NotAVirus T 00b32c34989bb002 | | | Pr Q | 2 12 0 Q | Not Subscribed | 2017-07 | Save Filter A | s |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection Connector Info Comments | dd filters by clicking on the T icon in the e teek Sort T Control Co | W32.Zombies.NotAVirus W32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus | | | | 2 🖾 Qı | Not Subscribed v | 2017-07 | Save Filter A: | s |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection Connector Info Comments | dd filters by clicking on the T icon in the e teek Sort T Control Co | W32.Zombies.NotAVirus W32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus TW32.Zombies.NotAVirus CUb32234989bb002 T4XpjCE_X.pdf.part C:\Users\djanulik\AppData\Local\Temp\4Xp | JCE_X.pdf.part | | Pr Q | 2 12 6 Qi | Not Subscribed v | 2017-07 | Save Filter A | s |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection Connector Info Comments | dd filters by clicking on the T icon in the e teek Sort T L L L L L L L L L L L L L L L L L L L | went details ime v v W32.Zombles.NotAVirus TW32.Zombles.NotAVirus TW32.Zombles.NotAVirus COb32c34989bb002 V T4XpJCE_X.pdf.part C:\Users\djanulik\AppData\Local\Temp\4Xp 309500 | JCE_X.pdf.part | | P Y Q | 2 (2) Q | Not Subscribed v | 2017-07 | Save Filter A | s C |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection Connector Info Comments | dd filters by clicking on the T icon in the e teek Sort T ccisco.com detected 4XpJCE_X.pdf.part as Detection Fingerprint (SHA-256) Filename Filepath File Size (bytes) Parent Fingerprint (SHA-256) | vent details ime v v W32.Zombles.NotAVirus VW32.Zombles.NotAVirus T 00b32c34989bb002 v T 4XpJCE_X.pdf.part C:\Users\djanulik\AppData\Local\Temp\4Xp 309500 T offf6b175fdf32be v | JCE_X.pdf.part | | | 2 🖾 २४ | Not Subscribed | 2017-07 | Save Filter A | c |
| Filters Ac Time Range W DJANULIK-HYYPD. File Detection Connector Info Comments | dd filters by clicking on the T icon in the e teek Sort T Leckso.com detected 4XpJCE X.pdf.part as Leckso.com detected | vent details ime | JCE_X.pdf.part | | | 2 🖾 २ | Not Subscribed | 2017-07 | Save Filter A | s c |

evento de quarentena

Additional Information

Para obter sua conta AMP, você pode se inscrever na ATS University. Isso oferece uma visão geral da funcionalidade do AMP no LAB.

Informações Relacionadas

- Configurar o ativador da AMP
- Suporte Técnico e Documentação Cisco Systems