

Configure los módulos AnyConnect para VPN de acceso remoto en FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración](#)

[Configuración en Firepower Management Center \(FMC\)](#)

[Configuración en Firepower Device Manager \(FDM\)](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar los módulos AnyConnect para la configuración de VPN de acceso remoto (RA VPN) que ya existe en Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC) a través de Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica del funcionamiento de VPN de RA.
- Comprensión de la navegación a través del FMC/FDM.
- Conocimiento básico de la API REST y el Explorador de API Rest de FDM.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Management Center (FMC) versión 6.7.0
- Cisco Firepower Threat Defense (FTD) versión 6.7.0
- Cisco Firepower Device Manager (FDM) versión 6.7.0
- Cisco AnyConnect Secure Mobility Client, ejecución 4.9.0086
- Postman o cualquier otra herramienta de desarrollo API

Nota: FMC/FDM no tiene un Editor de perfiles integrado y el [Editor de perfiles de AnyConnect](#) para Windows se debe utilizar para crear un perfil.

Nota: La información de este documento se creó a partir de dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier cambio de configuración.

Antecedentes

Cisco AnyConnect Secure Mobility Client no se limita a su soporte como cliente VPN, sino que también cuenta con otras opciones que se pueden integrar como módulos. Anyconnect admite los siguientes módulos:

- Inicio antes de iniciar sesión (SBL): este módulo permite al usuario establecer una conexión VPN en la empresa antes de iniciar sesión en Windows.
- Herramienta de diagnóstico e informes (DART): este módulo se utiliza para realizar diagnósticos e informes sobre la instalación y conexión de AnyConnect. DART funciona ensamblando los registros, el estado y la información de diagnóstico para su análisis.
- Cisco Advanced Malware Protection (AMP): Este módulo proporciona una solución de última generación en la nube para detectar, prevenir y responder a diversas amenazas.
- Condición de ISE: Cisco Identity Services Engine (ISE) proporciona una política de control de acceso e identidad de última generación. Este módulo proporciona la capacidad de identificar el sistema operativo (OS), el antivirus, el AntiSpyware, etc. que están instalados actualmente en un host. Esta información se utiliza luego junto con una política para determinar si el host podrá conectarse a la red.
- Módulo de visibilidad de la red: El módulo de visibilidad de la red supervisa el uso de una aplicación de terminal para descubrir posibles anomalías de comportamiento y tomar decisiones de diseño de red más fundamentadas.
- Umbrella: Cisco Umbrella Roaming es un servicio de seguridad proporcionado en la nube que protege los dispositivos cuando están fuera de la red corporativa.
- Seguridad web: Cisco Web Security Appliance (WSA), con tecnología de Cisco Talos, protege el terminal bloqueando automáticamente sitios de riesgo y probando sitios desconocidos.
- Administrador de acceso de red: Network Access Manager proporciona una red de capa 2 segura de acuerdo con sus políticas. Detecta y selecciona la red de acceso de capa 2 óptima y realiza la autenticación de dispositivos para el acceso a las redes por cable e inalámbricas.
- Comentarios: Este módulo recopila la información y la envía periódicamente al servidor. Ayuda al equipo de productos a mejorar la calidad, fiabilidad, rendimiento y experiencia de usuario de AnyConnect.

En Firepower 6.7, se agrega la interfaz de usuario de FMC y la compatibilidad con la API FTD Device REST para permitir la implementación sin problemas de todos los módulos AnyConnect

mencionados.



Esta tabla enumera las Extensiones de perfiles y las Los tipos de módulos necesarios para implementar correctamente la funcionalidad del terminal.

Extensiones de perfil	Tipo de módulo
.fsp	COMENTARIOS
.asp o .xml	AMP_ENABLER
.sip o .xml	ISE_POSTURE
.nvmsp o .xml	NETWORK_VISIBILITY
.nsp o .xml	NETWORK_ACCESS_MANAGER
.json o .xml	UMBRELLA
.wsp o .xml	WEB_SECURITY

Nota: Los módulos DART y SBL no requieren ningún perfil.

Nota: No se requiere ninguna licencia adicional para el uso de esta función.

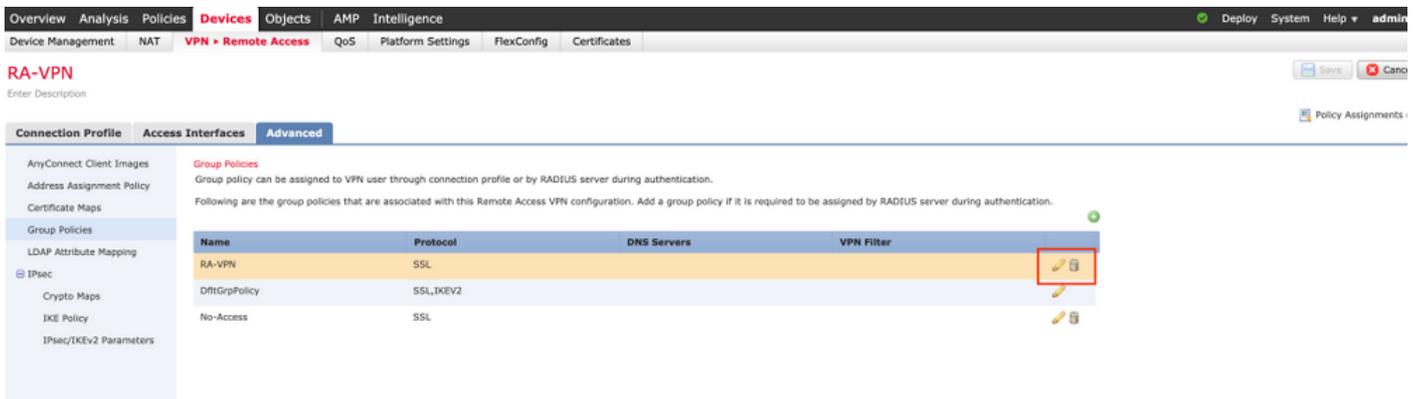
Configuración

Configuración en Firepower Management Center (FMC)

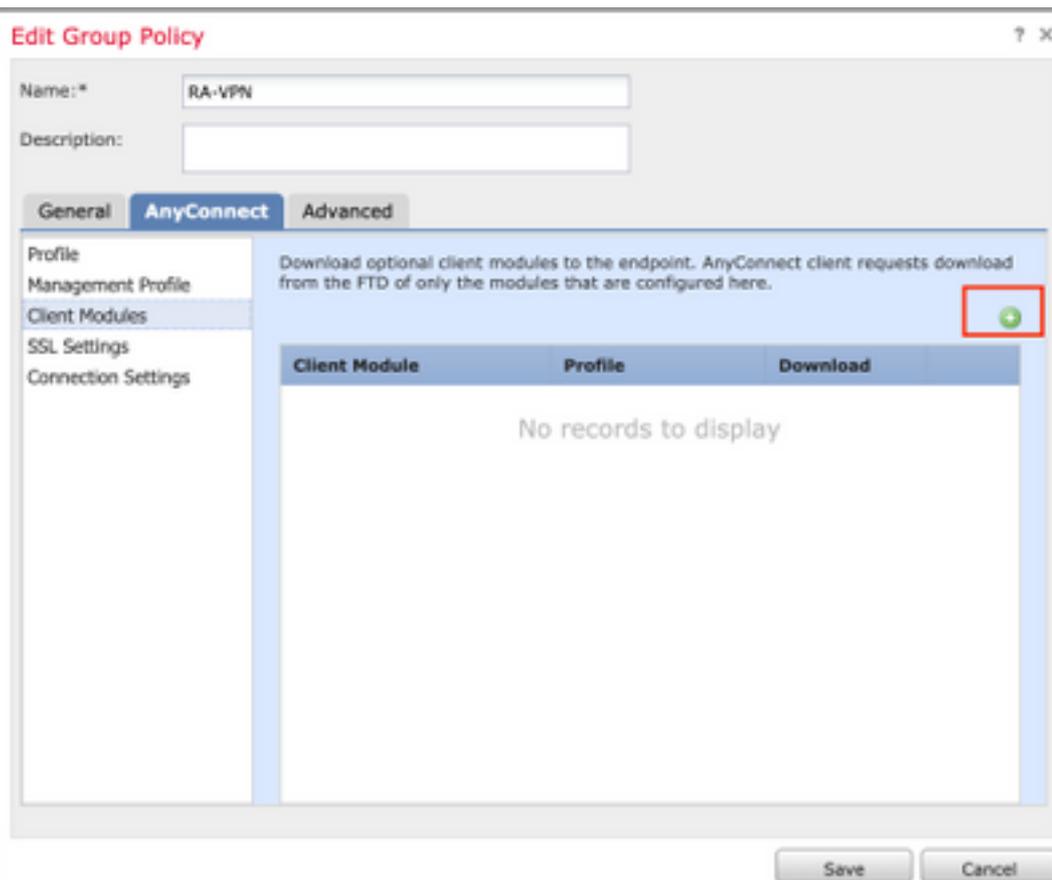
Paso 1. Navegue hasta **Device > VPN > Remote Access** y haga clic en **Edit** para la configuración de RA VPN.



Paso 2. Navegue hasta **Avanzadas > Políticas de Grupo** y haga clic en **Editar** para la política de Grupo correspondiente, como se muestra en esta imagen.



Paso 3. Navegue hasta **AnyConnect > Client Modules** y haga clic en **+** para agregar los módulos, como se muestra en esta imagen.



Para la demostración, se muestra la implementación de los módulos AMP, DART y SBL.

Paso 4. Seleccione el módulo **DART** y haga clic en **Agregar**, como se muestra en esta imagen.

Add Client Module ? X

Client Module: DART

Profile to download: [Empty] +

Enable module download:

Add Cancel

Paso 5. Haga clic en + para agregar otro módulo y seleccione el módulo **Inicio antes de iniciar sesión** , como se muestra en esta imagen.

Add Client Module ? X

Client Module: Start Before Login

Profile to download: [Empty] +

Enable module download:

Add Cancel

Nota: Este paso le permite descargar el módulo SBL. SBL también debe habilitar en el perfil de cliente anyconnect, que se carga a medida que navega hasta **AnyConnect > Profile** en la Política de grupo.

Paso 6. Haga clic en + para agregar otro módulo y seleccione **AMP Enabler**. Haga clic en + para agregar un perfil de cliente, como se muestra en esta imagen.

Add Client Module ? X

Client Module: AMP Enabler

Profile to download: [Empty] +

Enable module download:

Add Cancel

Proporcione el **nombre** del perfil y cargue el **perfil de AMP**. Haga clic en **Guardar**, como se muestra en esta imagen.

Add AnyConnect File ? X

Name:* AMP

File Name:* Amp.asp Browse..

File Type:* AMP Enabler Service Profile

Description:

Save Cancel

Elija el perfil creado en el paso anterior y haga clic en la **casilla de verificación Habilitar descarga de módulo**, como se muestra en esta imagen.

Add Client Module ? X

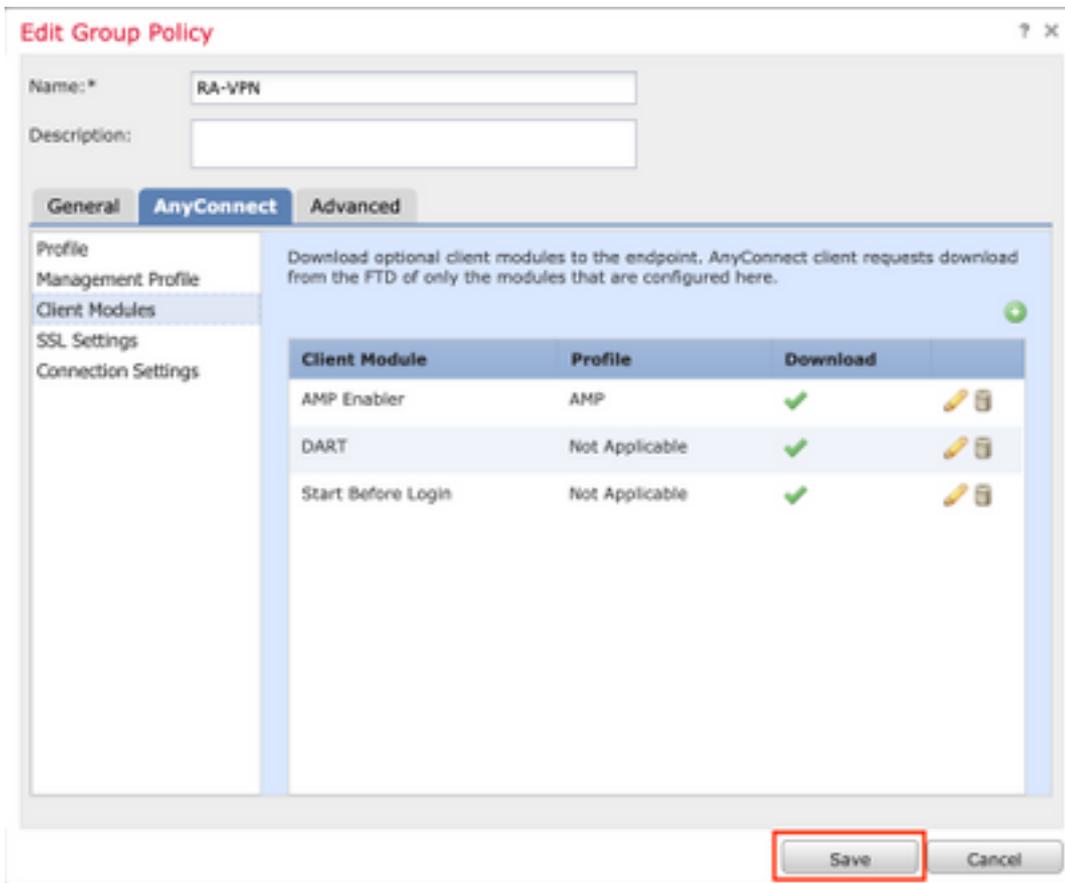
Client Module AMP Enabler

Profile to download AMP +

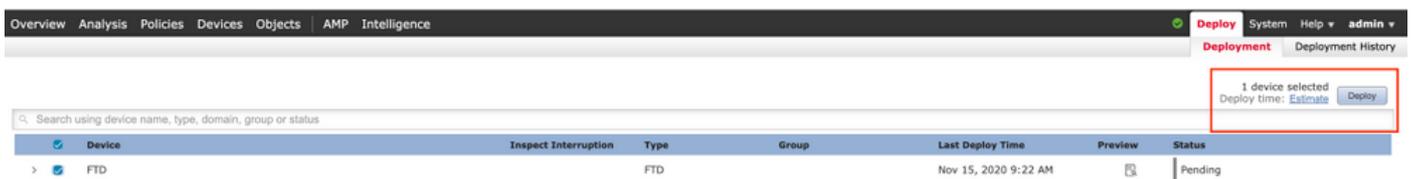
Enable module download

Add Cancel

Paso 7. Haga clic en **Guardar** una vez que se hayan agregado todos los módulos deseados.



Paso 8. Navegue hasta **Implementar > Implementación** e implemente la configuración en el FTD.



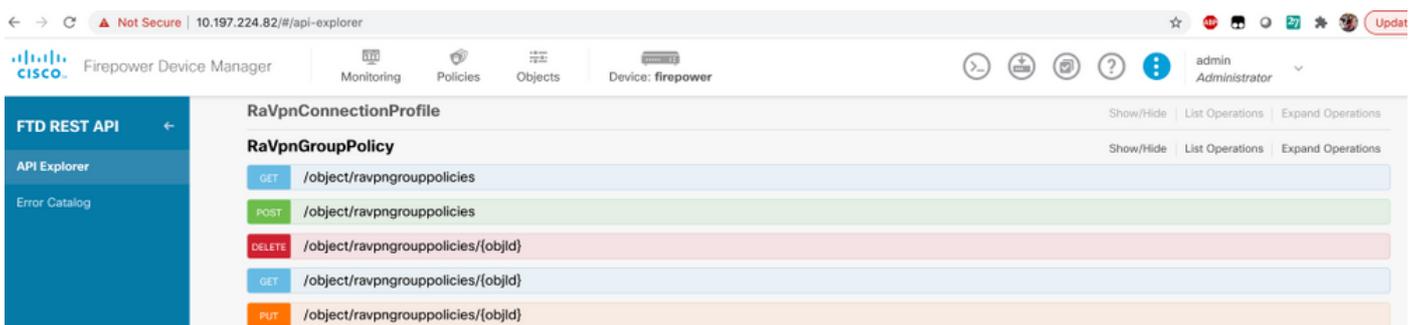
Configuración en Firepower Device Manager (FDM)

Paso 1. Inicie el Explorador de API del FTD en una ventana del explorador.

Vaya a <https://<FTD Management IP>/api-explorer>

Esto contiene la lista completa de API disponible en el FTD. Se divide en función de la función principal con varias solicitudes GET/POST/PUT/DELETE que admite el FDM.

RaVpnGroupPolicy es la API utilizada.



Paso 2. Agregue una colección Postman para los módulos AnyConnect. Proporcione un nombre para la colección. Haga clic en **Crear**.

CREATE A NEW COLLECTION

Name

AnyConnect Module

Description Authorization Pre-request Scripts Tests Variables

This description will show in your collection's documentation, along with the descriptions of its folders and requests.

AnyConnect Module

Descriptions support [Markdown](#)

Cancel Create

Paso 3. Agregar una nueva solicitud **Autenticación** para crear una solicitud POST de inicio de sesión en el FTD para obtener el token para autorizar cualquier solicitud POST/GET/PUT. Haga clic en **Guardar**.

AnyConnect Module ☆
0 requests

This collection
collection and

- ➔ Share Collection
- 🔒 Manage Roles
- A| Rename ⌘E
- ✎ Edit
- 🔗 Create a fork
- 🔗 Create Pull Request
- 🔗 Merge changes
- GET** Add Request
- 📁 Add Folder

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

Auth

Request description (Optional)

Make things easier for your teammates with a complete request description.

Descriptions support [Markdown](#)

Select a collection or folder to save to:

Search for a collection or folder

AnyConnect Module

+ Create Folder

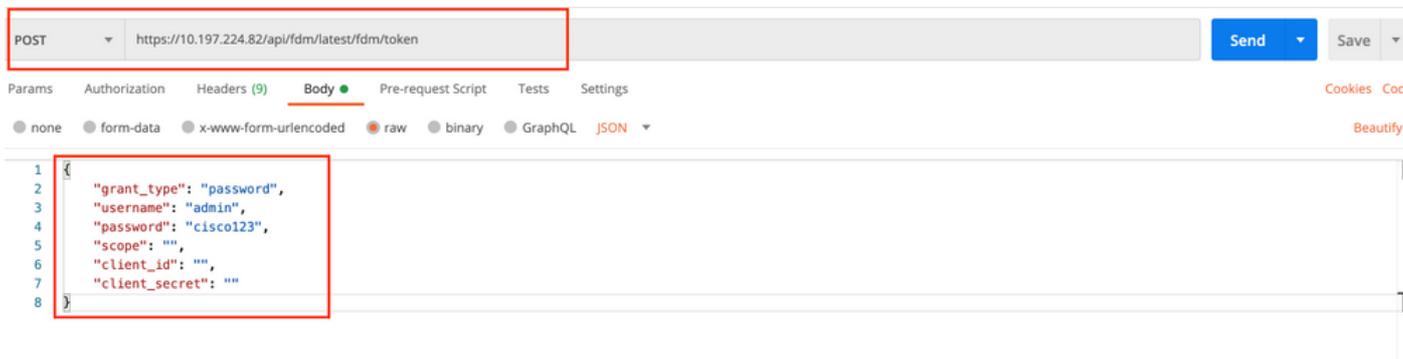
Cancel

Save to AnyConnect Module

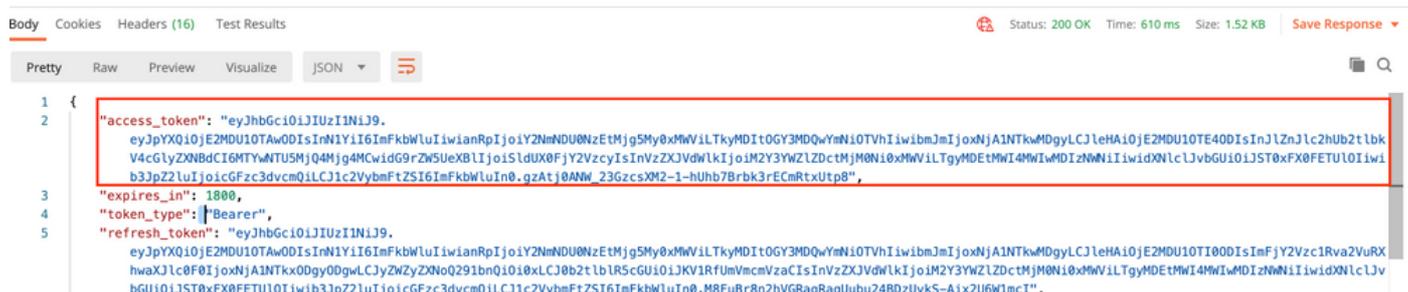
El cuerpo de la solicitud POST debe contener lo siguiente:

Tipo	raw - JSON (aplicación/json)
Grant_type	contraseña
Nombre de usuario	Nombre de usuario del administrador para iniciar sesión en el FTD
contraseña	La contraseña asociada a la cuenta de usuario administrador

Solicitud POST: <https://<FTD Management IP>/api/fdm/latter/fdm/token>



El cuerpo de la respuesta contiene el token de acceso que se utiliza para enviar cualquier solicitud PUT/GET/POST a/desde el FTD.



Paso 4. Cree una política **Get Group** para agregar detalles de las políticas de grupo existentes. Haga clic en **Guardar**, como se muestra en esta imagen.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).
[Learn more about creating collections](#)

Request name

Request description (Optional)

Descriptions support [Markdown](#)

Select a collection or folder to save to:

◀ AnyConnect Module [+ Create Folder](#)

POST Auth

La ficha Autorización debe contener esto para todas las solicitudes GET/POST subsiguientes:

Tipo Token portador

Token El token de acceso recibido al ejecutar la solicitud POST de autenticación

OBTENER SOLICITUD: <https://<FTD Management IP>/api/fdm/latest/object/ravpngrouppolicies>

Get Group Policy Comments 0 Examples 0

GET

Params **Authorization** Headers (8) Body Pre-request Script Tests Settings Cookies Code

TYPE
 Bearer Token

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Token

El cuerpo de la respuesta muestra todas las políticas de grupo configuradas en el dispositivo. **ID** de la política de grupo se utiliza para actualizar la política de grupo específica.

```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 218 ms Size: 4.72 KB Save Response
Pretty Raw Preview Visualize JSON
1
2 "items": [
3
4   {
5     "version": "ijtc7ii45gloz",
6     "name": "DfltGrpPolicy",
7     "banner": null,
8     "dnsServerGroup": null,
9     "defaultDomainName": null,
10    "simultaneousLoginPerUser": 3,
11    "maxConnectionTimeout": null,
12    "maxConnectionTimeAlertInterval": 1,
13    "vpnIdleTimeout": 30,
14    "vpnIdleTimeoutAlertInterval": 1,
15    "ipv4LocalAddressPool": [],
16    "ipv6LocalAddressPool": [],
17    "dhcpScope": null,
18    "ipv4SplitTunnelSetting": "TUNNEL_ALL",
19    "ipv6SplitTunnelSetting": "TUNNEL_ALL",
20    "ipv4SplitTunnelNetworks": [],
21    "ipv6SplitTunnelNetworks": [],
22    "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
23    "splitDNSDomainList": "",
24    "scepForwardingUrl": null,
25    "periodicClientCertAuthenticationInterval": 1,
26    "enableDTLS": false,
27    "enableDTLSCompression": false,
28    "sslCompression": "DISABLED",
29    "enableSSIRekey": false.
30  }
31 ]
32 }
```

```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 218 ms Size: 4.72 KB Save Response
Pretty Raw Preview Visualize JSON
59
60   {
61     "version": "lc2t2sspzbfy7",
62     "name": "RA-VPN",
63     "banner": null,
64     "dnsServerGroup": null,
65     "defaultDomainName": null,
66     "simultaneousLoginPerUser": 3,
67     "maxConnectionTimeout": null,
68     "maxConnectionTimeAlertInterval": 1,
69     "vpnIdleTimeout": 30,
70     "vpnIdleTimeoutAlertInterval": 1,
71     "ipv4LocalAddressPool": [],
72     "ipv6LocalAddressPool": [],
73     "dhcpScope": null,
74     "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
75     "ipv6SplitTunnelSetting": "TUNNEL_ALL",
76     "ipv4SplitTunnelNetworks": [
77       {
78         "version": "ne3zzud5spztm",
79         "name": "Split-acl",
80         "id": "71b85ceb-27ba-11eb-9202-a5a0daf9088c",
81         "type": "networkobject"
82       }
83     ],
84     "ipv6SplitTunnelNetworks": [],
85     "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
86     "splitDNSDomainList": "",
87     "scepForwardingUrl": null.
88   }
89 ]
90 }
```

```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 218 ms Size: 4.72 KB Save Response
Pretty Raw Preview Visualize JSON
108
109   "restrictVPNViewLANID": null,
110   "clientFirewallPrivateNetworkRules": null,
111   "clientFirewallPublicNetworkRules": null,
112   "browserProxyType": "NO_MODIFY",
113   "proxy": {
114     "serverHost": null,
115     "port": null,
116     "type": "serverhostandport"
117   },
118   "proxyExceptions": [],
119   "enabledAnyConnectModules": [],
120   "isEnabledPeriodicClientCertAuthentication": false,
121   "id": "74b60c8e-27ba-11eb-9202-594cb5cbaldf",
122   "type": "ravpngrouppolicy",
123   "links": {
124     "self": "https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cbaldf"
125   }
126 },
127 "paging": {
128   "prev": [],
129   "next": [],
130   "limit": 10,
131   "offset": 0,
132   "count": 2,
133   "pages": 0
134 }
135 }
```

Para la demostración, se muestra la implementación de los módulos AMP, DART y SBL.

Paso 5. Cree una solicitud para **Cargar un perfil**. Este paso sólo es necesario para los módulos

que requieren un perfil. Cargue el **perfil** en la sección **FileUpload**. Haga clic en **Guardar**.

SOLICITUD POST: <https://<FTD Management IP>/api/fdm/current/action/uploadDiskfile>

El cuerpo de la solicitud debe contener el archivo Profile agregado en Body en formato de datos de formulario. El perfil debe crearse mediante [el Editor de perfiles de AnyConnect para Windows](#)

El tipo de clave debe ser **FileToUpload**.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).
[Learn more about creating collections](#)

Request name

Request description (Optional)

Descriptions support [Markdown](#)

Select a collection or folder to save to:

◀ AnyConnect Module [+ Create Folder](#)
POST Auth
GET Get Group Policy

KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/> fileToUpload	File ▾ .Amp.asp X			
Key	Text Value	Description		
	File			

El cuerpo de la respuesta proporciona un id/nombre de archivo que se utiliza para hacer

referencia al perfil con el módulo correspondiente.



```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 325 ms Size: 911 B Save Response
Pretty Raw Preview Visualize JSON
1 {
2   "version": null,
3   "name": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
4   "fileName": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
5   "id": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
6   "type": "fileuploadstatus",
7   "links": {
8     "self": "https://10.197.224.82/api/fdm/latest/action/uploaddiskfile/69cc2046-2897-11eb-9202-b71d409c1cf2.asp"
9   }
10 }
```

Paso 6. Cree una solicitud para actualizar el **perfil de AnyConnect**. Este paso sólo es necesario para los módulos que requieren un perfil. Haga clic en **Guardar.**, como se muestra en esta imagen.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

AnyConnect Profile

Request description (Optional)

Make things easier for your teammates with a complete request description.

Descriptions support [Markdown](#)

Select a collection or folder to save to:

Search for a collection or folder

AnyConnect Module

+ Create Folder

POST Auth

GET Get Group Policy

GET Upload Profile

Cancel

Save to AnyConnect Module

SOLICITUD POST: <https://<FDM IP>/api/fdm/update/object/anyconnectclientprofiles>

El cuerpo de la solicitud contiene esta información:

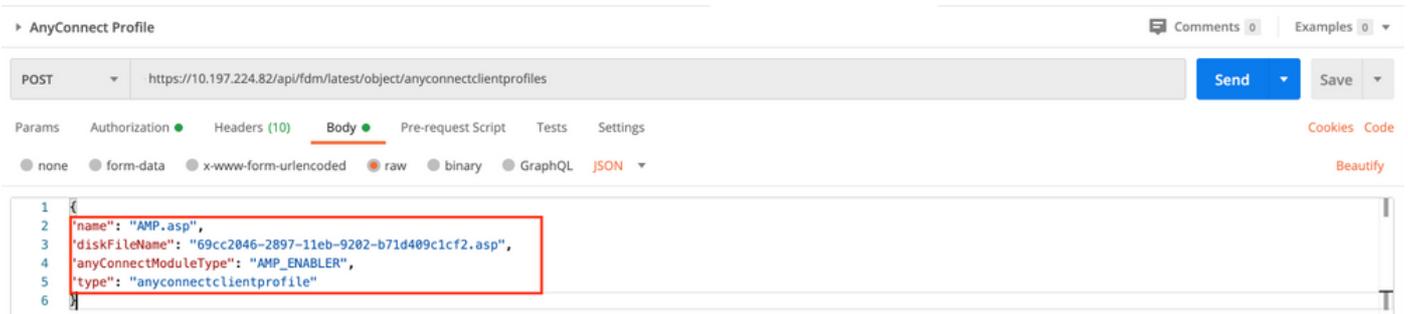
nombre

Nombre lógico al que llamaría el archivo

diskFileName

Necesita coincidir con el nombre de archivo recibido en la respuesta POST d

perfil de carga
AnyConnectModuleType Métodos para que coincidan con el módulo apropiado que se muestra en la T
de Tipos de [Módulo](#)
tipo anyconnectclientprofile



```
1 {
2   "name": "AMP.asp",
3   "diskFileName": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
4   "anyConnectModuleType": "AMP_ENABLER",
5   "type": "anyconnectclientprofile"
6 }
```

El cuerpo de la respuesta muestra el perfil listo para ser enviado al dispositivo. El nombre, la versión, el id y el tipo recibidos en respuesta se utilizan en el paso siguiente para enlazar el perfil a la política de grupo.



```
1 {
2   "version": "c3woqajhvqxr",
3   "name": "AMP.asp",
4   "md5Checksum": "8697131026dbaf6a67e1191e8abe122",
5   "description": null,
6   "diskFileName": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
7   "anyConnectModuleType": "AMP_ENABLER",
8   "id": "eef22c7-2898-11eb-9202-77e0b953fcd0",
9   "type": "anyconnectclientprofile",
10  "links": {
11    "self": "https://10.197.224.82/api/fdm/latest/object/anyconnectclientprofiles/eef22c7-2898-11eb-9202-77e0b953fcd0"
```

Paso 6. Cree una solicitud **PUT** para agregar **Perfil y Módulo de Cliente** a la **Política de Grupo** existente. Haga clic en **Guardar**, como se muestra en esta imagen.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

Client Profile and Module

Request description (Optional)

Make things easier for your teammates with a complete request description.

Descriptions support [Markdown](#)

Select a collection or folder to save to:

Search for a collection or folder

AnyConnect Module [+ Create Folder](#)

- POST Auth
- GET Get Group Policy
- GET Upload Profile

Cancel

Save to AnyConnect Module

SOLICITUD PUT: <https://<FDM IP>/api/fdm/latter/object/ravpngrouppolicies/{objId}>

ObjId es la ID obtenida en el [Paso 4](#). Copie el contenido de la política de grupo correspondiente obtenida en el paso 4 al cuerpo de la solicitud y añada lo siguiente:

Perfil del cliente

Nombre, versión, id y tipo de perfil recibidos en el paso anterior.

Módulos de cliente

El nombre del Módulo que debe habilitarse debe coincidir exactamente como se indica en la Tabla [de Módulo](#).

Client Profile and Module

PUT <https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cba1df> Send

Params Authorization Headers (10) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {
2   "version": "lc2t2sspzbfy7",
3   "name": "RA-VPN",
4   "banner": null,
5   "dnsServerGroup": null,
6   "defaultDomainName": null,
7   "simultaneousLoginPerUser": 3,
8   "maxConnectionTimeout": null,
9   "maxConnectionTimeAlertInterval": 1,
10  "vpnIdleTimeout": 30,
11  "vpnIdleTimeoutAlertInterval": 1,
12  "ipv4LocalAddressPool": [],
13  "ipv6LocalAddressPool": [],
14  "dhcpScope": null,
15  "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
16  "ipv6SplitTunnelSetting": "TUNNEL_ALL",
17  "ipv4SplitTunnelNetworks": [
18    {
19      "version": "ne3zzud5spztm",
20      "name": "Split-acl",
21      "id": "71b85ceb-27ba-11eb-9202-a5a0daf9088c",
22      "type": "networkobject"
23    }
24  ],
25  "ipv6SplitTunnelNetworks": [],
26  "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
27  "splitDNSDomainList": "",
28  "scepForwardingUrl": null,
29  "periodicClientCertAuthenticationInterval": 1,
30  "enableDTLS": false,
31  "enableDTLSCompression": false,
32  "enableDTLSCompression": false
33 }
```

Client Profile and Module

PUT <https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cba1df> Send Save

Params Authorization Headers (10) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
44  "enableClientDPD": false,
45  "clientDPDInterval": 30,
46  "clientProfiles": [
47    {
48      "version": "c3woqajhvvqxr",
49      "name": "AMP.asp",
50      "id": "eeff22c7-2898-11eb-9202-77e0b953fcd0",
51      "type": "anyconnectclientprofile"
52    }
53  ],
54  "keepInstallerOnClient": false,
55  "vpnTrafficFilterACL": null,
56  "enableRestrictVPNTtoVLAN": false,
57  "restrictVPNTtoVLANid": null,
58  "clientFirewallPrivateNetworkRules": null,
59  "clientFirewallPublicNetworkRules": null,
60  "browserProxyType": "NO_MODIFY",
61  "proxy": {
62    "serverHost": null,
63    "port": null,
64    "type": "serverhostandport"
65  },
66  "proxyExceptions": [],
67  "enabledAnyConnectModules": ["START_BEFORE_LOGIN", "DART", "AMP_ENABLER"],
68  "isEnablePeriodicClientCertAuthentication": false,
69  "id": "74b60c8e-27ba-11eb-9202-594cb5cba1df",
70  "type": "ravpngrouppolicy",
71  "links": {
72    "self": "https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cba1df"
73  }
74 }
```

El cuerpo de la respuesta muestra el perfil y el módulo enlazados correctamente a la política de grupo.

```

Body Cookies Headers (17) Test Results
Status: 200 OK Time: 2.71 s Size: 2.75 KB Save Response
Pretty Raw Preview Visualize JSON
45 "clientDPDInterval": 30,
46 "clientProfiles": [
47   {
48     "version": "c3woqajhvvqxr",
49     "name": "AMP.asp",
50     "id": "eef22c7-2898-11eb-9202-77e0b953fcd0",
51     "type": "anyconnectclientprofile"
52   }
53 ],
54 "keepInstallerOnClient": false,
55 "vpnTrafficFilterACL": null,
56 "enableRestrictVPNTovLAN": false,
57 "restrictVPNTovLANid": null,
58 "clientFirewallPrivateNetworkRules": null,
59 "clientFirewallPublicNetworkRules": null,
60 "browserProxyType": "NO_MODIFY",
61 "proxy": {
62   "serverHost": null,
63   "port": null,
64   "type": "serverhostandport"
65 },
66 "proxyExceptions": [],
67 "enabledAnyConnectModules": [
68   "START_BEFORE_LOGIN",
69   "DART",
70   "AMP_ENABLER"
71 ],
72 "isEnabledPeriodicClientCertAuthentication": false.

```

Nota: Este paso permite descargar el módulo SBL. El SBL también tiene que habilitar en el perfil de cliente anyconnect que se puede cargar mientras navega a **Devices > Remote Access VPN > Group Policies > Edit Group Policy > General > AnyConnect Client Profile**.

Paso 7. Implemente la configuración en el dispositivo a través de FDM. Los cambios pendientes muestran el perfil del cliente y los módulos que se van a enviar.

Pending Changes
? ×

✔ Last Deployment Completed Successfully
17 Nov 2020 07:42 AM. [See Deployment History](#)

Deployed Version (17 Nov 2020 07:42 AM)	Pending Version ⏪ LEGEND
⚙ AnyConnect Group Edited: RA-VPN <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">clientProfiles:</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div>	<div style="border: 1px solid red; padding: 5px; margin-bottom: 5px;"> enabledAnyConnectModules[0]: DART enabledAnyConnectModules[1]: AMP_ENABLER enabledAnyConnectModules[2]: START_BEFORE_LOGIN </div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">AMP.asp</div>
+ AnyConnect Client Profile Added: AMP.asp <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">-</div>	<div style="border: 1px solid red; padding: 5px; margin-bottom: 5px;"> anyConnectModuleType: AMP_ENABLER md5Checksum: 8697131026bdbaf6a67e1191e8abe122 diskFileName: 69cc2046-2897-11eb-9202-b71d409c1cf2 ⋮ </div> <div style="background-color: #e0f0e0; padding: 2px; margin-bottom: 2px;">name: AMP.asp</div>

MORE ACTIONS ▾
CANCEL

DEPLOY NOW
▾

Configuración enviada a la CLI de FTD después de una implementación correcta:

```
!--- RA VPN Configuration ---!
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.9.00086-webdeploy-k9.pkg 2
  anyconnect profiles AMP.asp disk0:/anyconnprofs/AMP.asp
  anyconnect profiles defaultClientProfile disk0:/anyconnprofs/defaultClientProfile.xml
anyconnect enable
tunnel-group-list enable
```

!--- Group Policy Configuration ---!

```
group-policy RA-VPN internal
group-policy RA-VPN attributes
webvpn
  anyconnect modules value ampenabler,dart,vpngina
  anyconnect profiles value AMP.asp type ampenabler
```

Verificación

Establezca una conexión correcta con el FTD.

Navegue hasta **Settings > VPN > Message History** para ver los detalles sobre los módulos que se descargaron.



The screenshot shows the Cisco AnyConnect Secure Mobility Client interface. The left sidebar contains navigation options: Status Overview, VPN (selected), Network, Web Security, System Scan, and Roaming Security. The main content area is titled 'Virtual Private Network (VPN)' and has tabs for Preferences, Statistics, Route Details, Firewall, and Message History. The Message History tab is active, displaying a log of events for 15-11-2020. A red box highlights the following messages:

- 21:49:55 The AnyConnect Downloader is performing update checks...
- 21:49:55 Checking for profile updates...
- 21:49:57 Downloading AMP Enabler Service Profile - 100%
- 21:49:57 Checking for product updates...
- 21:49:58 Downloading AnyConnect DART 4.9.00086 - 100%
- 21:49:58 Downloading AnyConnect SBL 4.9.00086 - 100%
- 21:49:59 Downloading AnyConnect AMP Enabler 4.9.00086 - 100%

Troubleshoot

[Recopile DART](#) [para](#) resolver problemas con la instalación de módulos cliente.