Implementación de políticas de acceso dinámico (DAP) ASA 9.X

Contenido

Introducción

Este documento describe la implementación, las características y el uso de las políticas de acceso dinámico (DAP) de ASA 9.x.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Gateways de red privada virtual (VPN)
- Políticas de acceso dinámicas (DAP)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

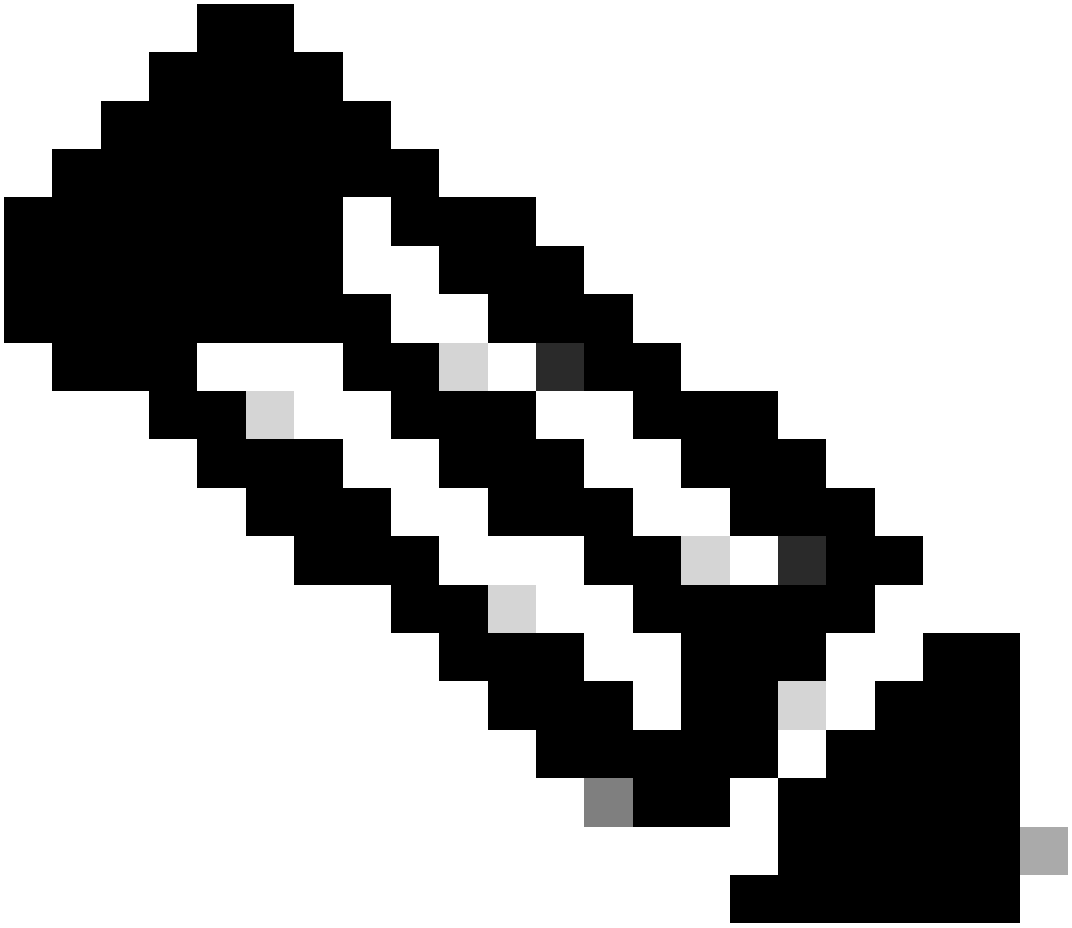
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

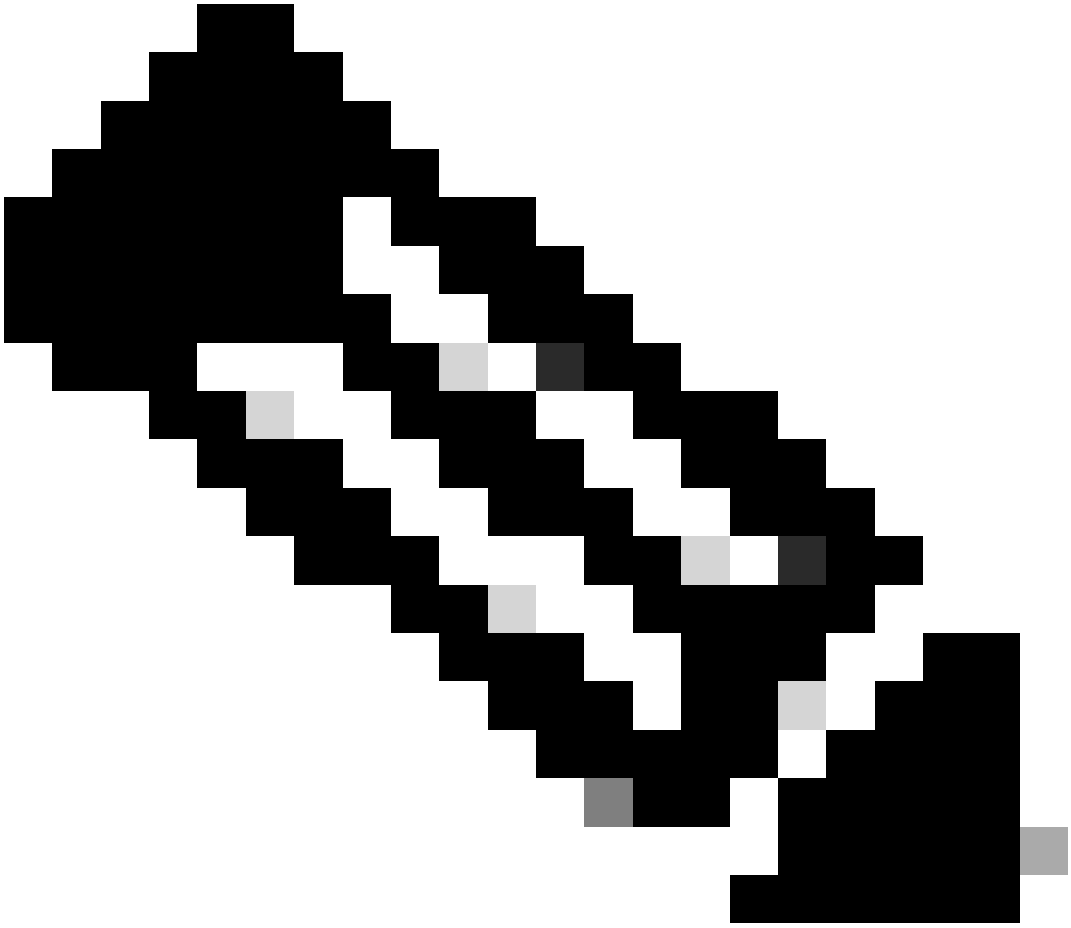
Los gateways de red privada virtual (VPN) funcionan en entornos dinámicos. Varias variables pueden afectar a cada conexión VPN; por ejemplo, las configuraciones de intranet que cambian con frecuencia, las distintas funciones que cada usuario puede tener en una organización y los inicios de sesión de sitios de acceso remoto con diferentes configuraciones y niveles de seguridad. La tarea de autorizar usuarios es mucho más complicada en un entorno de VPN dinámico que en una red con una configuración estática.

Las políticas de acceso dinámicas (DAP) son una función que le permite configurar la autorización que se ocupa de la dinámica de los entornos VPN. Una directiva de acceso dinámico se crea estableciendo una colección de atributos de control de acceso que se asocian a un túnel o una sesión de usuario específicos. Estos atributos abordan problemas de pertenencia a varios grupos y seguridad de terminales.

Por ejemplo, el dispositivo de seguridad concede acceso a un usuario concreto para una sesión concreta en función de las políticas que defina. Genera un DAP a través de la autenticación de usuario seleccionando o agregando atributos de uno o más registros DAP. Selecciona estos registros DAP basándose en la información de seguridad del terminal del dispositivo remoto y/o la información de autorización AAA para el usuario autenticado. A continuación, aplica el registro DAP al túnel o la sesión del usuario.



Nota: El archivo dap.xml, que contiene los atributos de selección de políticas DAP, se almacena en la memoria flash ASA. Aunque puede exportar el archivo dap.xml fuera de la caja, editarlo (si conoce la sintaxis XML) y volver a importarlo, tenga mucho cuidado porque puede hacer que ASDM deje de procesar los registros DAP si ha configurado algo erróneamente. No hay CLI para manipular esta parte de la configuración.



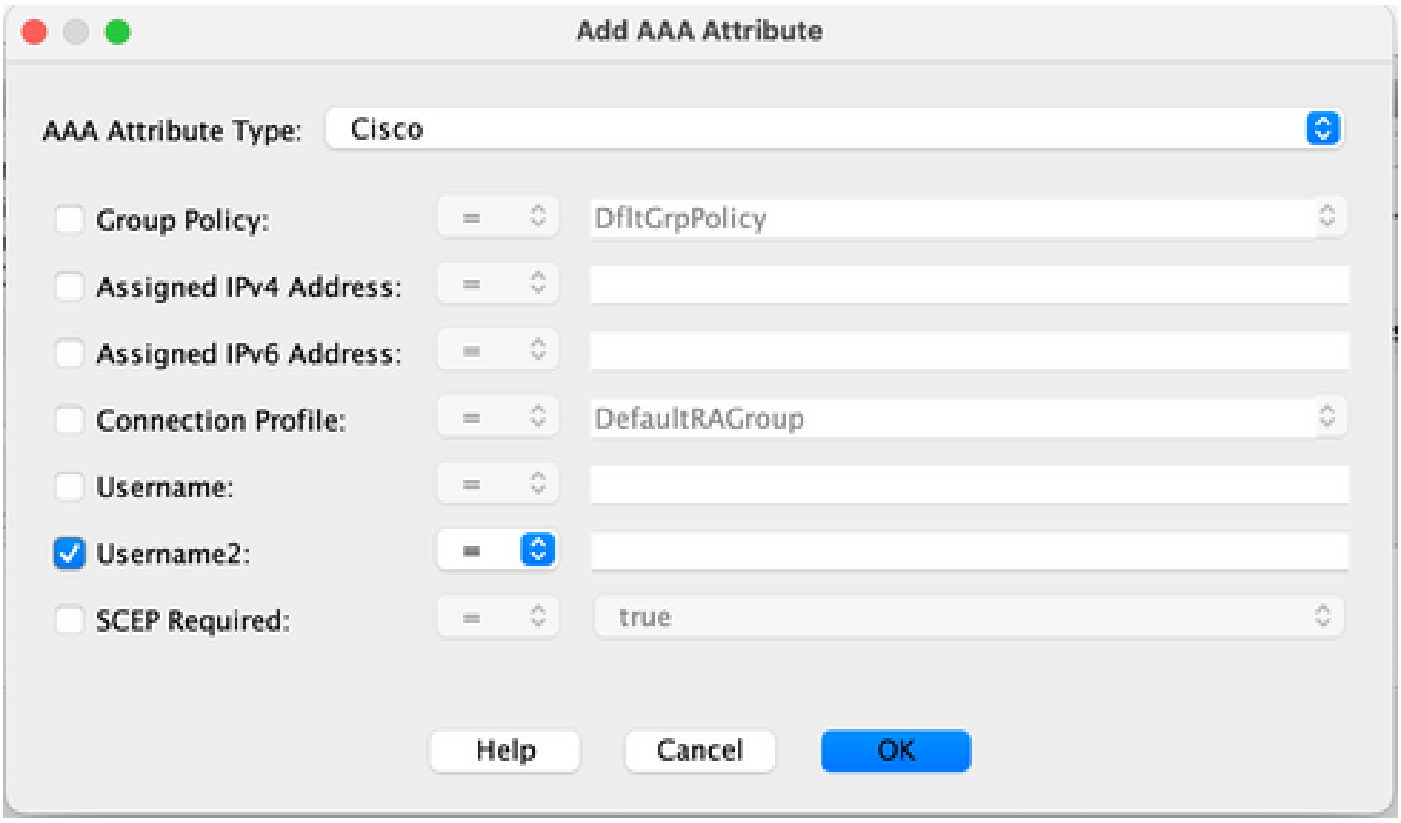
Nota: Intentar configurar los parámetros de acceso al registro de políticas de acceso dinámico a través de la CLI puede hacer que DAP deje de funcionar aunque ASDM administraría correctamente el mismo. Evite la CLI y utilice siempre ASDM para administrar las políticas DAP.

Atributos DAP y AAA

DAP complementa los servicios AAA y proporciona un conjunto limitado de atributos de autorización que pueden sustituir a los atributos que proporciona AAA. El dispositivo de seguridad puede seleccionar registros DAP en función de la información de autorización AAA para el usuario. El dispositivo de seguridad puede seleccionar varios registros DAP en función de esta información, que luego agrega para asignar atributos de autorización DAP.

Puede especificar atributos AAA desde la jerarquía de atributos AAA de Cisco o desde el conjunto completo de atributos de respuesta que el dispositivo de seguridad recibe de un servidor RADIUS o LDAP, como se muestra en la Figura 1.

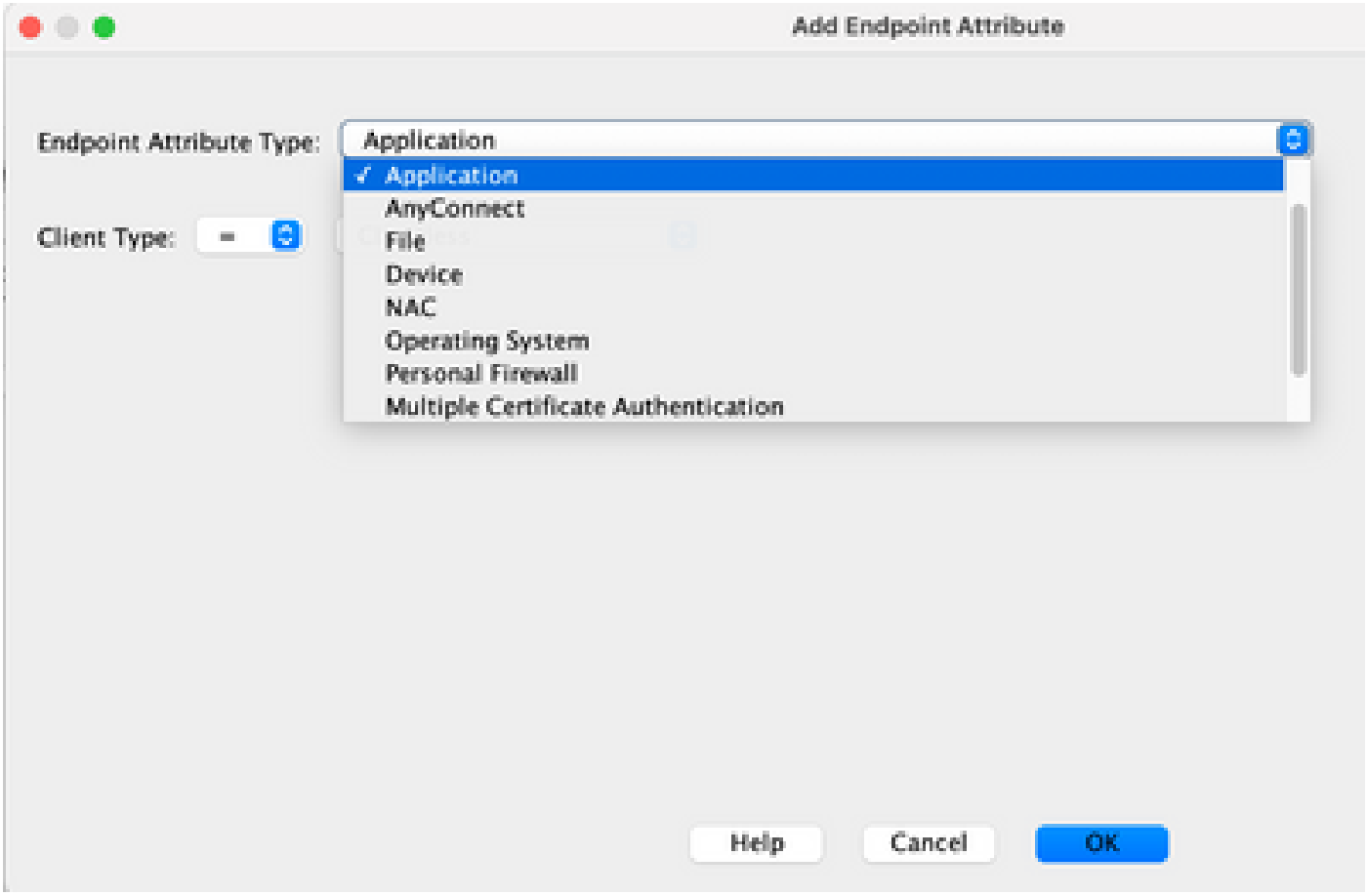
Figura 1. GUI de atributo AAA de DAP



Atributos de seguridad de DAP y terminales

Además de los atributos AAA, el dispositivo de seguridad también puede obtener atributos de seguridad de terminales mediante los métodos de evaluación de estado que configure. Entre ellos, se incluyen el análisis básico de host, Secure Desktop, la evaluación de terminales estándar/avanzada y NAC, como se muestra en la figura 2. Los atributos de evaluación de terminales se obtienen y se envían al dispositivo de seguridad antes de la autenticación del usuario. Sin embargo, los atributos AAA, incluido el registro DAP general, se validan durante la autenticación de usuario.

Figura 2 GUI de atributo de terminal

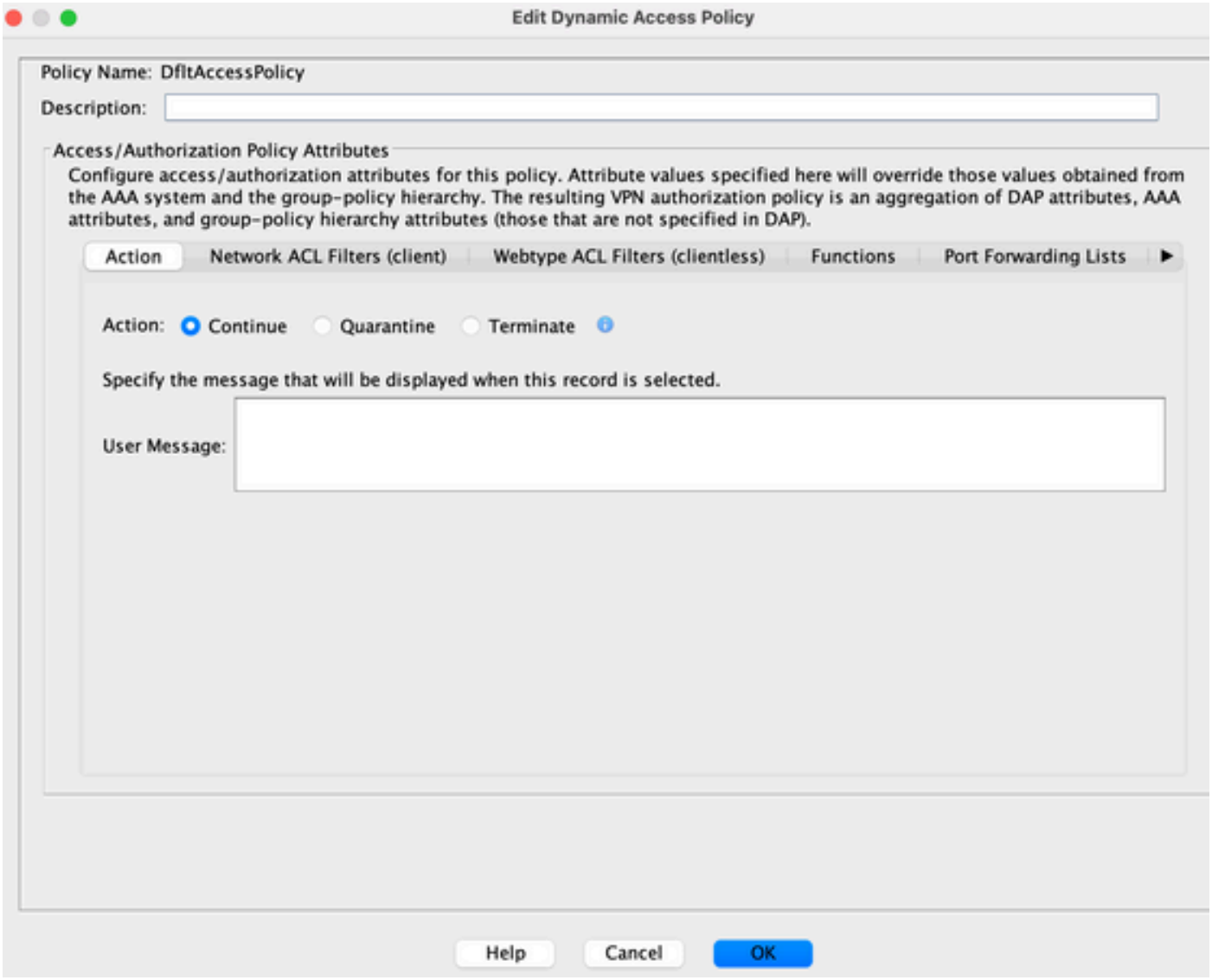


Política de acceso dinámica predeterminada

Antes de la introducción e implementación de DAP, los pares de valor/atributo de política de acceso que estaban asociados con un túnel o sesión de usuario específico se definían localmente en ASA (es decir, grupos de túnel y políticas de grupo) o se asignaban a través de servidores AAA externos.

DAP siempre se aplica de forma predeterminada. Por ejemplo, la aplicación del control de acceso a través de grupos de túnel, políticas de grupo y AAA sin la aplicación explícita de DAP puede seguir obteniendo este comportamiento. Para el comportamiento heredado, no se requieren cambios de configuración en la función DAP, incluido el registro DAP predeterminado, DfltAccessPolicy, como se muestra en la Figura 3.

Figura 3. Política de acceso dinámica predeterminada



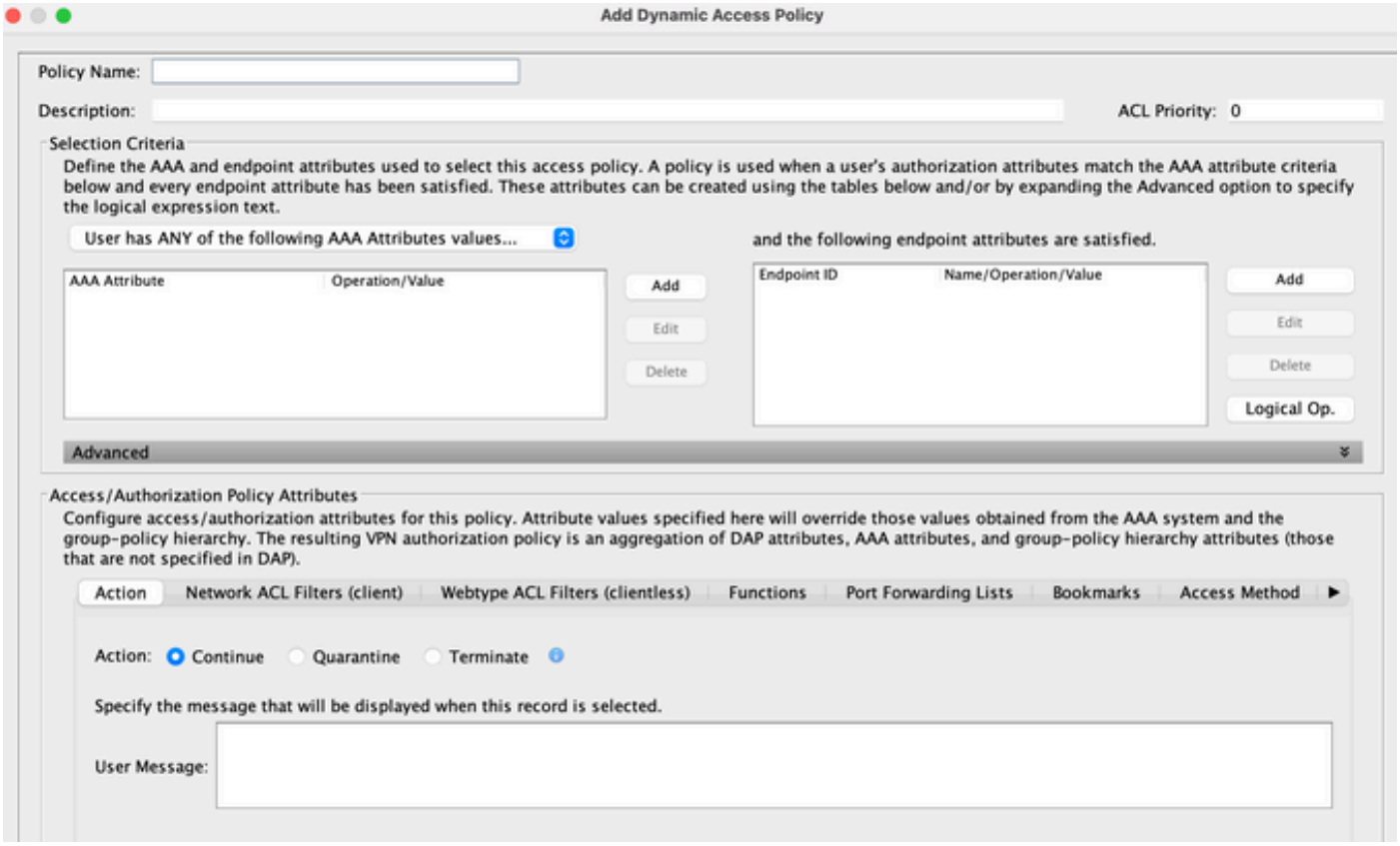
No obstante, si se cambia cualquiera de los valores predeterminados de un registro DAP, por ejemplo, el parámetro Action: en DfltAccessPolicy se cambia de su valor predeterminado a Terminate y no se configuran registros DAP adicionales, los usuarios autenticados pueden, de forma predeterminada, coincidir con el registro DAP DfltAccessPolicy y se les puede denegar el acceso VPN.

En consecuencia, es necesario crear y configurar uno o más registros DAP para autorizar la conectividad VPN y definir a qué recursos de red puede acceder un usuario autenticado. Por lo tanto, si se configura, el DAP puede tener prioridad sobre la aplicación de políticas heredadas.

Configuración de políticas de acceso dinámicas

Cuando utiliza DAP para definir a qué recursos de red tiene acceso un usuario, hay muchos parámetros que se deben tener en cuenta. Por ejemplo, si identifica si el terminal de conexión procede de un entorno administrado, no administrado o no fiable, determine los criterios de selección necesarios para identificar el terminal de conexión y, en función de la evaluación del terminal o las credenciales AAA, los recursos de red a los que puede acceder el usuario que se conecta. Para ello, primero debe familiarizarse con las funciones y características de DAP, como se muestra en la Figura 4.

Figura 4 Política de acceso dinámica



Al configurar un registro DAP, hay que tener en cuenta dos componentes principales:

- Criterios de selección, incluidas las opciones avanzadas
- Atributos de política de acceso

La sección Criterios de selección es donde un administrador configuraría los atributos AAA y de punto final utilizados para seleccionar un registro DAP específico. Se utiliza un registro DAP cuando los atributos de autorización de un usuario coinciden con los criterios del atributo AAA y se han satisfecho todos los atributos de terminal.

Por ejemplo, si se selecciona LDAP (Active Directory) de tipo de atributo AAA, la cadena de nombre de atributo es memberOf y la cadena de valor es Contractors, como se muestra en la figura 5a, el usuario autenticador debe ser miembro del grupo de Active Directory Contractors para coincidir con los criterios del atributo AAA.

Además de satisfacer los criterios de atributo AAA, también se puede requerir al usuario autenticador que satisfaga los criterios de atributo de punto final. Por ejemplo, si el administrador configuró para determinar la postura del terminal de conexión y basándose en esa evaluación de postura, el administrador podría utilizar esta información de evaluación como criterios de selección para el atributo de terminal que se muestra en la figura 5b.

Figura 5a. Criterios de atributos AAA

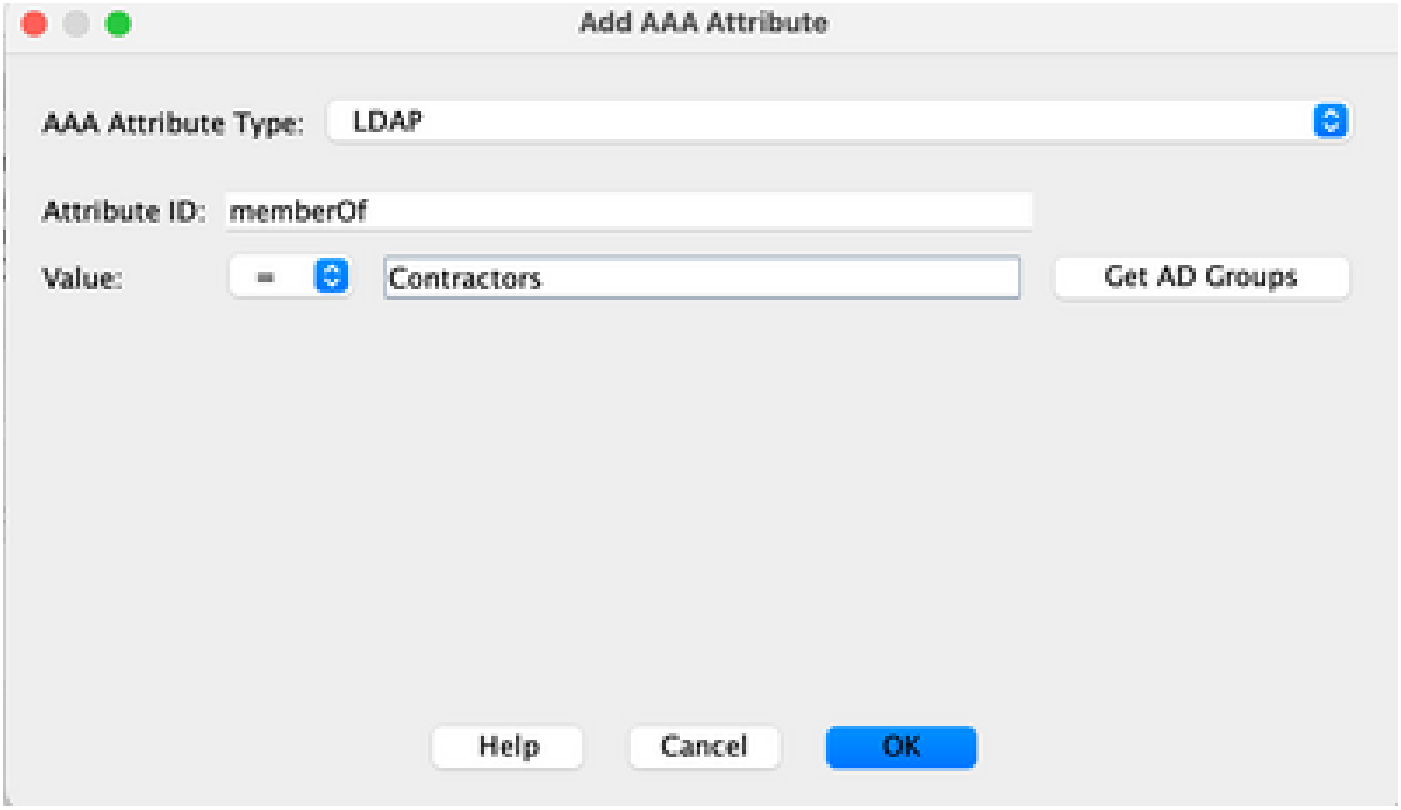


Figura 5b. Criterios de atributos de terminales

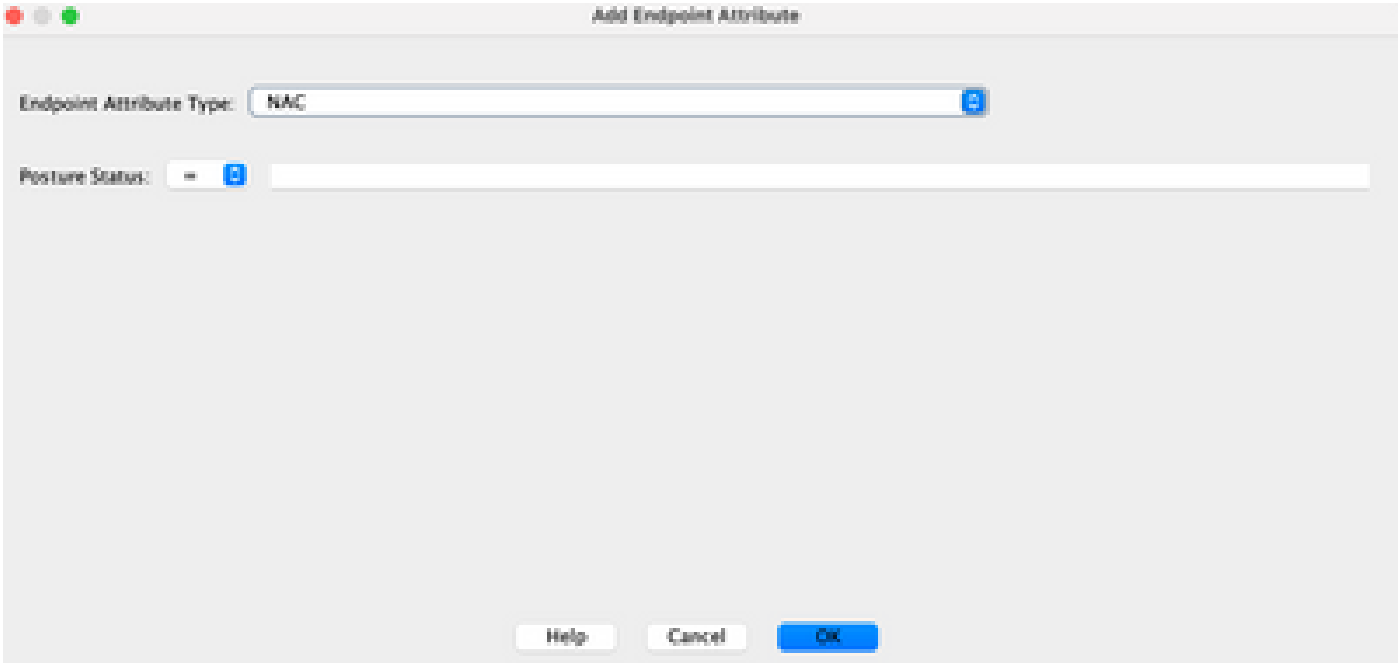
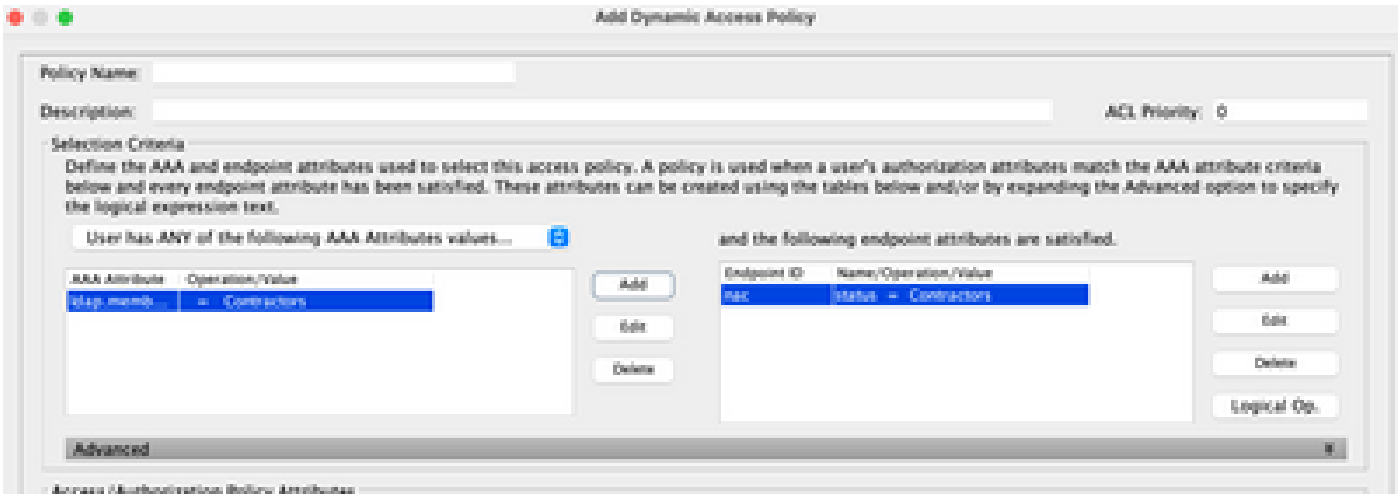


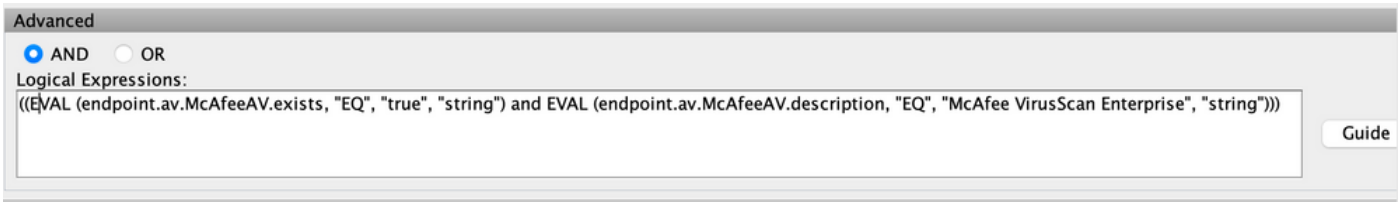
Figura 6. Coincidencia de criterios de atributos de AAA y terminales



Los atributos AAA y Endpoint se pueden crear utilizando las tablas descritas en la figura 6 y/o expandiendo la opción Advanced para especificar una expresión lógica como se muestra en la figura 7. En la actualidad, la expresión lógica se crea con funciones EVAL, por ejemplo, EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") y EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"), que representan operaciones lógicas de selección AAA o de terminales.

Las expresiones lógicas son útiles si necesita agregar criterios de selección distintos de los posibles en las áreas de atributos AAA y de punto final, como se ha mostrado anteriormente. Por ejemplo, aunque puede configurar los dispositivos de seguridad para que utilicen atributos AAA que satisfagan cualquiera, todos o ninguno de los criterios especificados, los atributos de terminal son acumulativos y deben cumplirse todos. Para permitir que el dispositivo de seguridad emplee un atributo de terminal u otro, debe crear las expresiones lógicas adecuadas en la sección Avanzadas del registro DAP.

Figura 7 GUI de expresión lógica para la creación de atributos avanzados

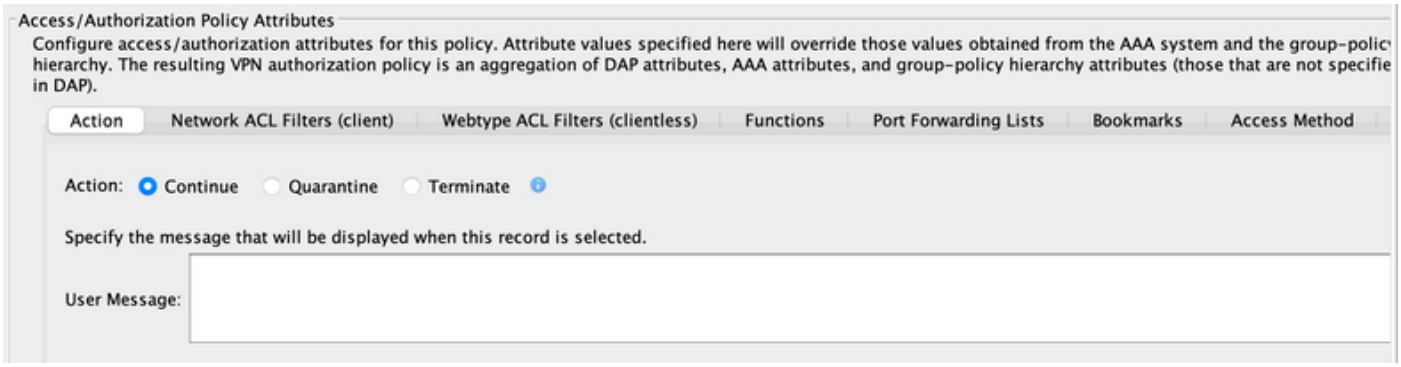


La sección Access Policy Attributes (Atributos de política de acceso), como se muestra en la figura 8, es donde un administrador configuraría los atributos de acceso VPN para un registro DAP específico. Cuando los atributos de autorización de usuario coinciden con los criterios de AAA, Extremo y/o Expresión Lógica, se pueden aplicar los valores de atributos de política de acceso configurados en esta sección. Los valores de atributo especificados aquí pueden reemplazar los valores obtenidos del sistema AAA, incluidos los de los registros de usuario, grupo, grupo de túnel y grupo predeterminado existentes.

Un registro DAP tiene un conjunto limitado de valores de atributo que se pueden configurar. Estos valores se incluyen en las fichas, como se muestra en las figuras 8 a 14:

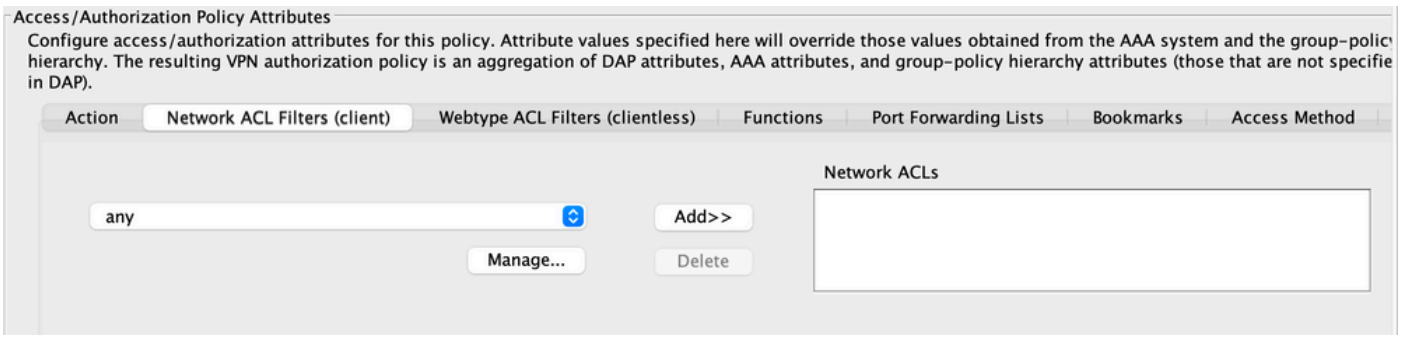
Figura 8 Acción: especifica el procesamiento especial que se aplicará a una conexión o sesión

específica.



- Continuar: (valor predeterminado) haga clic para aplicar atributos de política de acceso a la sesión.
- Terminar: haga clic para finalizar la sesión.
- Mensaje de usuario: introduzca un mensaje de texto para mostrar en la página del portal cuando se seleccione este registro DAP. Máximo 128 caracteres. Un mensaje de usuario se muestra como una esfera amarilla. Cuando un usuario inicia sesión, parpadea tres veces para llamar la atención y, a continuación, sigue parpadeando. Si se seleccionan varios registros DAP y cada uno de ellos tiene un mensaje de usuario, se mostrarán todos los mensajes de usuario. Además, puede incluir en dichos mensajes URL u otro texto incrustado, que requieren que utilice las etiquetas HTML correctas.

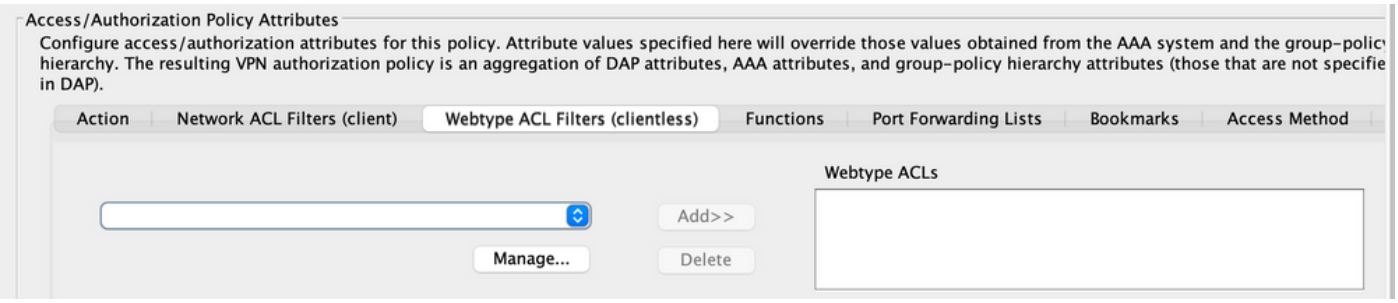
Figura 9. Ficha Filtros ACL de red: permite seleccionar y configurar las ACL de red para aplicarlas a este registro DAP. Una ACL para DAP puede contener reglas de permiso o denegación, pero no ambas. Si una ACL contiene reglas de permiso y de denegación, el dispositivo de seguridad rechaza la configuración de ACL.



- El cuadro desplegable Network ACL ya ha configurado las ACL de red para agregarlas a este registro DAP. Sólo se pueden seleccionar las ACL que tengan todas las reglas de permiso o denegación, y estas son las únicas ACL que se muestran aquí.
- Administrar: haga clic para agregar, editar y eliminar ACL de red.
- La ACL de red enumera las ACL de red para este registro DAP.
- Agregar: haga clic para agregar la ACL de red seleccionada del cuadro desplegable a la lista ACL de red de la derecha.

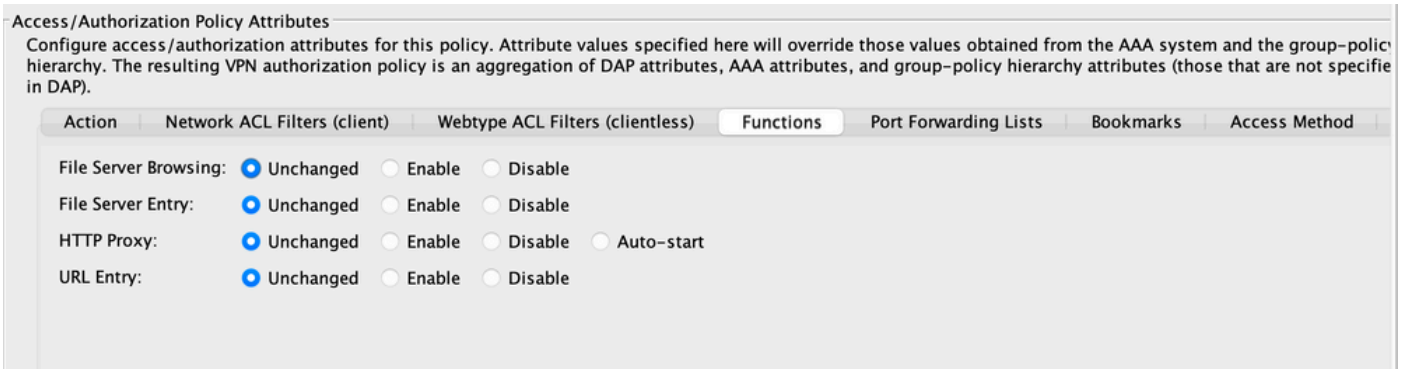
- Eliminar: haga clic para eliminar una ACL de red resaltada de la lista ACL de red. No puede eliminar una ACL si está asignada a un DAP u otro registro.

Figura 10. Ficha Filtros ACL de tipo Web: permite seleccionar y configurar ACL de tipo Web para aplicarlas a este registro DAP. Una ACL para DAP sólo puede contener reglas de permiso o denegación. Si una ACL contiene reglas de permiso y de denegación, el dispositivo de seguridad rechaza la configuración de ACL.



- Cuadro desplegable ACL de tipo web: seleccione las ACL de tipo web ya configuradas para agregarlas a este registro DAP. Sólo las ACL que tienen todas las reglas de permiso o de denegación son elegibles, y estas son las únicas ACL que se muestran aquí.
- Administrar...: haga clic para agregar, editar y eliminar ACL de tipo Web.
- Lista de ACL de tipo web: muestra las ACL de tipo web para este registro DAP.
- Agregar: haga clic para agregar la ACL de tipo web seleccionada del cuadro desplegable a la lista ACL de tipo web de la derecha.
- Eliminar: haga clic para eliminar una ACL de tipo Web de la lista ACL de tipo Web. No puede eliminar una ACL si está asignada a un DAP u otro registro.

Figura 11. Ficha Funciones: permite configurar la entrada y exploración del servidor de archivos, el proxy HTTP y la entrada de URL para el registro DAP.



- Exploración del servidor de archivos: habilita o deshabilita la exploración CIFS para servidores de archivos o funciones compartidas.
- Entrada de servidor de archivos: permite o deniega a un usuario la introducción de rutas y nombres de servidor de archivos en la página del portal. Cuando está habilitada, coloca la sección de entrada del servidor de archivos en la página del portal. Los usuarios pueden

escribir nombres de ruta de acceso a archivos de Windows directamente. Pueden descargar, editar, eliminar, cambiar el nombre y mover archivos. También pueden agregar archivos y carpetas. Los recursos compartidos también se deben configurar para el acceso de usuarios en los servidores de Microsoft Windows correspondientes. Se puede requerir a los usuarios que se autentiquen antes de acceder a los archivos, en función de los requisitos de red.

- Proxy HTTP: afecta al reenvío de un proxy de applet HTTP al cliente. El proxy es útil para tecnologías que interfieren con la transformación de contenido adecuada, como Java, ActiveX y Flash. Evita el proceso de manipular/reescribir al tiempo que garantiza el uso continuo del dispositivo de seguridad. El proxy reenviado modifica automáticamente la configuración de proxy anterior del navegador y redirige todas las solicitudes HTTP y HTTPS a la nueva configuración de proxy. Es compatible con prácticamente todas las tecnologías del cliente, incluidas HTML, CSS, JavaScript, VBScript, ActiveX y Java. El único explorador que admite es Microsoft Internet Explorer.

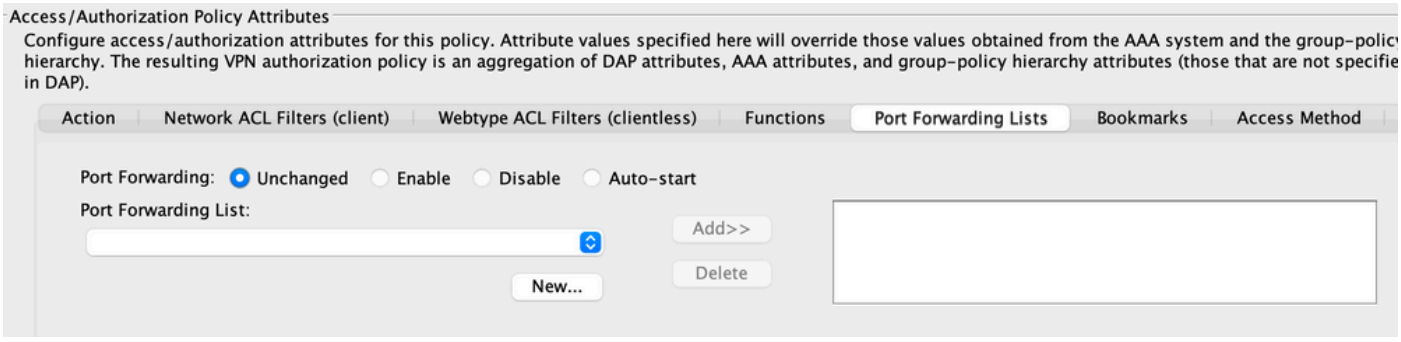
- Entrada de URL: permite o impide que un usuario introduzca URL HTTP/HTTPS en la página del portal. Si esta función está activada, los usuarios pueden introducir direcciones web en el cuadro de entrada de URL y utilizar VPN SSL sin cliente para acceder a esos sitios web.

- Sin cambiar (Unchanged): (valor predeterminado) haga clic para utilizar los valores de la directiva de grupo que se aplica a esta sesión.

- Activar/Desactivar: haga clic para activar o desactivar la función.

- Inicio automático: haga clic para activar el proxy HTTP y que el registro DAP inicie automáticamente los applets asociados con estas funciones.

Figura 12. Ficha Listas de reenvío de puertos: permite seleccionar y configurar listas de reenvío de puertos para las sesiones de usuario.

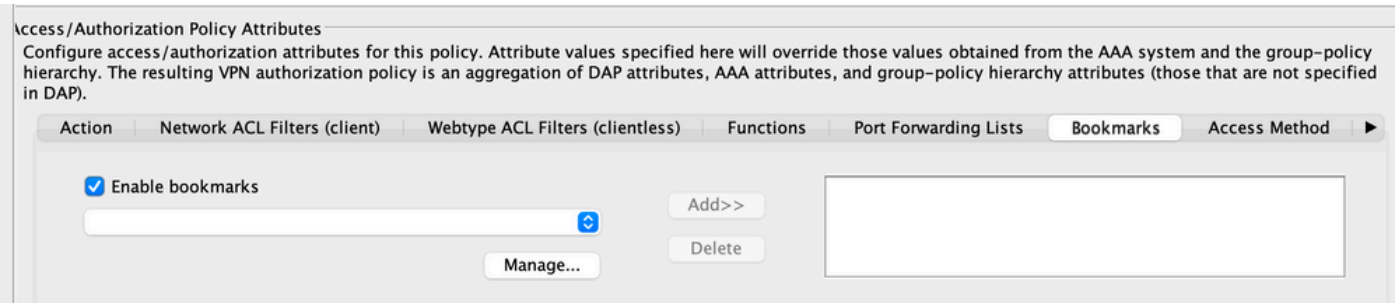


- Reenvío de puertos: seleccione una opción para las listas de reenvío de puertos que se aplican a este registro DAP. Los demás atributos de este campo se activan sólo cuando se establece Port Forwarding (Reenvío de puertos) en Enable (Activar) o Auto-start (Inicio automático).

- Sin cambiar: haga clic para utilizar los valores de la directiva de grupo que se aplica a esta sesión.

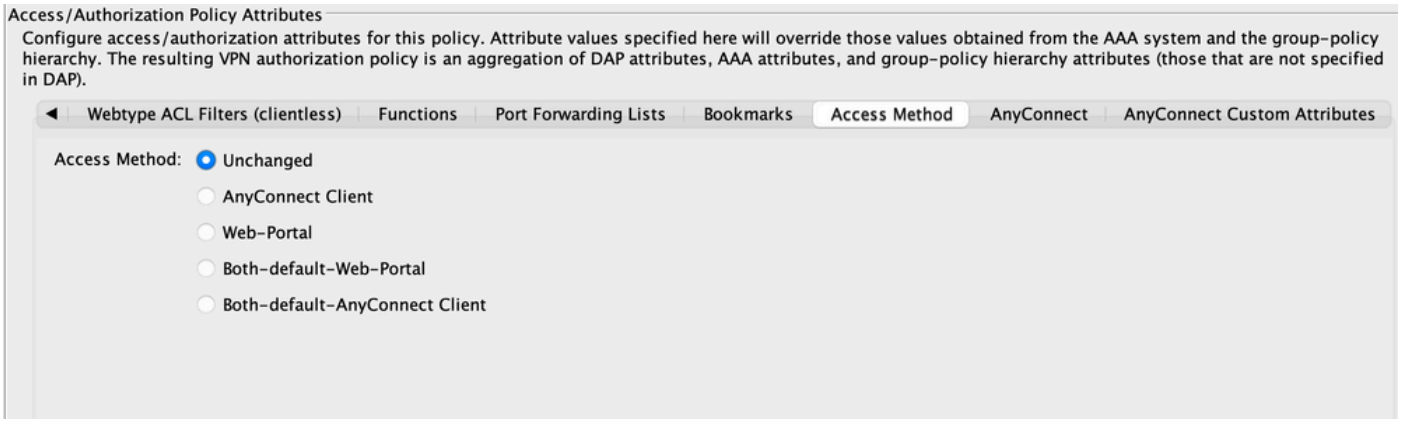
- Activar/Desactivar: haga clic para activar o desactivar el reenvío de puertos.
- Inicio automático: haga clic para activar el reenvío de puertos y para que el registro DAP inicie automáticamente los applets de reenvío de puertos asociados con sus listas de reenvío de puertos.
- Cuadro desplegable Lista de reenvío de puertos: seleccione las listas de reenvío de puertos ya configuradas para agregarlas al registro DAP.
- Nuevo: haga clic para configurar nuevas listas de reenvío de puertos.
- Listas de reenvío de puertos: muestra la lista de reenvío de puertos para el registro DAP.
- Agregar: haga clic para agregar la lista de reenvío de puertos seleccionada del cuadro desplegable a la lista de reenvío de puertos de la derecha.
- Eliminar: haga clic para eliminar la lista de reenvío de puertos seleccionada de la lista Reenvío de puertos. No puede eliminar una ACL si está asignada a un DAP u otro registro.

Figura 13. Ficha Marcadores: permite seleccionar y configurar marcadores o listas de direcciones URL para las sesiones de usuario.



- Habilitar marcadores: haga clic para habilitar. Cuando esta casilla no está activada, no se muestran listas de marcadores en la página del portal para la conexión
- Administrar: haga clic para agregar, importar, exportar y eliminar listas de marcadores.
- Listas de marcadores (desplegable): muestra las listas de marcadores del registro DAP.
- Agregar: haga clic para agregar la lista de marcadores seleccionada del cuadro desplegable al cuadro de lista de marcadores de la derecha.
- Eliminar: haga clic para eliminar la lista de marcadores seleccionada del cuadro de lista de marcadores. No puede eliminar una lista de marcadores del dispositivo de seguridad a menos que primero la elimine de los registros DAP.

Figura 14. Ficha Método: permite configurar el tipo de acceso remoto permitido.



- Sin cambios: continúe con el método de acceso remoto actual establecido en la directiva de grupo para la sesión.
- Cliente AnyConnect: conéctese mediante Cisco AnyConnect VPN Client.
- Portal web: conéctese a una VPN sin cliente.
- Both-default-Web-Portal: permite conectarse a través de sin cliente o del cliente AnyConnect, con un valor predeterminado de sin cliente.
- Both-default-AnyConnect Client: conéctese a través de sin cliente o del cliente AnyConnect, con el valor predeterminado de AnyConnect.

Como se ha mencionado anteriormente, un registro DAP tiene un conjunto limitado de valores de atributo predeterminados; sólo si se modifican, tienen prioridad sobre los registros AAA, de usuario, de grupo, de grupo de túnel y de grupo predeterminados actuales. Si se requieren valores de atributo adicionales fuera del ámbito de DAP, por ejemplo, listas de túnel divididas, banners, túneles inteligentes, personalizaciones de portal, etc., deben aplicarse a través de registros AAA, de usuario, de grupo, de grupo de túnel y de grupo predeterminado. En este caso, estos valores de atributo específicos pueden complementar a DAP y no se pueden invalidar. Por lo tanto, el usuario obtiene un conjunto acumulativo de valores de atributo en todos los registros.

Agregación de varias políticas de acceso dinámico

Un administrador puede configurar varios registros DAP para dirigir muchas variables. Como resultado, un usuario de autenticación puede satisfacer los criterios de atributos AAA y Endpoint de varios registros DAP. En consecuencia, los atributos de la política de acceso pueden ser coherentes o estar en conflicto en todas estas políticas. En este caso, el usuario autorizado puede obtener el resultado acumulado en todos los registros DAP coincidentes.

Esto también incluye valores de atributo únicos aplicados a través de los registros de autenticación, autorización, usuario, grupo, grupo de túnel y grupo predeterminado. El resultado acumulado de los atributos de la directiva de acceso crea la directiva de acceso dinámica. En las tablas siguientes se enumeran ejemplos de atributos de directiva de acceso combinados. Estos ejemplos representan los resultados de 3 registros DAP combinados.

El atributo action que se muestra en la tabla 1 tiene un valor que puede ser Terminate (Finalizar)

o Continue (Continuar). El valor del atributo agregado es Terminar si el valor Terminar está configurado en cualquiera de los registros DAP seleccionados y es Continuar si el valor Continuar está configurado en todos los registros DAP seleccionados.

Tabla 1. Atributo de acción

Nombre de atributo	DAP#1	DAP#2	DAP#3	DAP
Acción (ejemplo 1)	continúe	continúe	continúe	continúe
Acción (ejemplo 2)	Terminar	continúe	continúe	terminar

El atributo de mensaje de usuario que se muestra en la tabla 2 contiene un valor de cadena. El valor de atributo agregado puede ser una cadena separada por un salto de línea (valor hexadecimal 0x0A) creada mediante la vinculación de los valores de atributo de los registros DAP seleccionados. El orden de los valores de atributo en la cadena combinada es insignificante.

Tabla 2. Atributo de mensaje de usuario

Nombre de atributo	DAP#1	DAP#2	DAP#3	DAP
mensaje del usuario	la rápida	zorro marrón	Salta por encima	el rápido<LF>zorro marrón<LF>salta sobre

Los atributos de habilitación de la función Clientless (Funciones) que se muestran en la Tabla 3 contienen valores que son Auto-start, Enable o Disable. El valor del atributo agregado puede iniciarse automáticamente si el valor Inicio automático se configura en cualquiera de los registros DAP seleccionados.

El valor del atributo agregado puede ser Activado si no hay ningún valor de inicio automático configurado en ninguno de los registros DAP seleccionados, y el valor Activar se configura en al menos uno de los registros DAP seleccionados.

El valor de atributo agregado se puede inhabilitar si no hay ningún valor Auto-start o Enable configurado en cualquiera de los registros DAP seleccionados, y el valor "disable" se configura en al menos uno de los registros DAP seleccionados.

Tabla 3. Atributos de habilitación de funciones sin cliente (funciones)

Nombre de atributo	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable	inhabilitar		enable
exploración de archivos	inhabilitar	enable	inhabilitar	enable
entrada de archivo			inhabilitar	inhabilitar
HTTP-proxy	inhabilitar	inicio automático	inhabilitar	inicio automático
entrada de URL	inhabilitar		enable	enable

Los atributos URL list y port-forward que se muestran en la Tabla 4 contienen un valor que es una

cadena o una cadena separada por comas. El valor de atributo agregado puede ser una cadena separada por comas creada por cuando se vinculan los valores de atributo de los registros DAP seleccionados. Cualquier valor de atributo duplicado en la cadena combinada se puede eliminar. El orden de los valores de atributo en la cadena combinada es insignificante.

Tabla 4. Lista de URL y atributo de lista de mapeo de puertos

Nombre de atributo	DAP#1	DAP#3	DAP#3	DAP
url-list	a	b,c	a	a,b,c
port-forward		d,e	e,f	d,e,f

Los atributos Access Method especifican el método de acceso de cliente permitido para las conexiones VPN SSL. El método de acceso de cliente puede ser AnyConnect Client access only, Web-Portal access only, AnyConnect Client o Web-Portal access con Web-Portal access como valor predeterminado, o AnyConnect Client o Web-Portal access con AnyConnect Client access como valor predeterminado. El valor del atributo agregado se resume en la tabla 5.

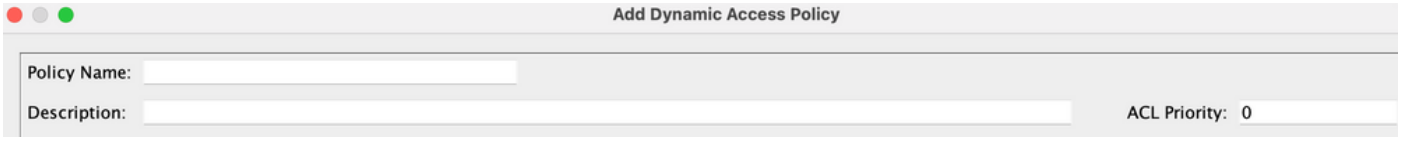
Tabla 5. Atributos de método de acceso

Valores de atributo seleccionados				Resultado de agregación
Cliente AnyConnect	Web-Portal	Both-default-Web-Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Portal web
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
X				Cliente AnyConnect
X			X	Both-default-AnyConnect Client
X		X		Both-default-Web-Portal
X		X	X	Both-default-Web-Portal
X	X			Both-default-Web-Portal
X	X		X	Both-default-AnyConnect Client
X	X	X		Both-default-Web-Portal
X	X	X	X	Both-default-Web-Portal

Al combinar los atributos Network (Firewall) y Web-Type (Clientless) ACL Filter, los componentes principales a tener en cuenta son DAP Priority y DAP ACL.

El tributo Priority que se muestra en la Figura 15 no se agrega. El dispositivo de seguridad utiliza este valor para secuenciar lógicamente las listas de acceso al agregar las ACL de red y tipo web desde varios registros DAP. El dispositivo de seguridad ordena los registros de mayor a menor número de prioridad, con el menor en la parte inferior de la tabla. Por ejemplo, un registro DAP con un valor de 4 tiene una prioridad más alta que un registro con un valor de 2. No se pueden ordenar manualmente.

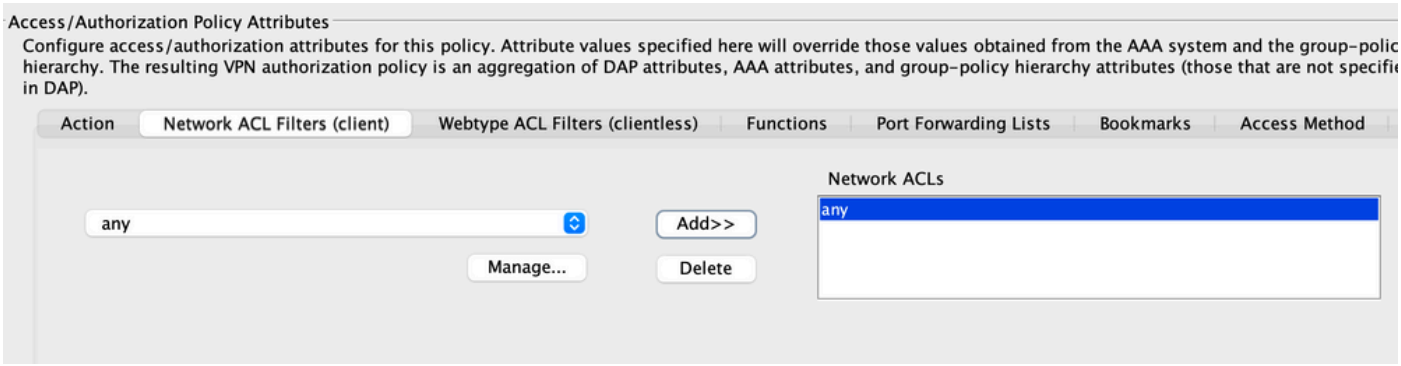
Figura 15 Prioridad: muestra la prioridad del registro DAP.



- Nombre de directiva: muestra el nombre del registro DAP.
- Descripción: describe la finalidad del registro DAP.

El atributo ACL de DAP sólo admite listas de acceso que se ajustan a un modelo de ACL Allow-List o Block-List estricto. En un modelo Allow-List ACL, las entradas de la lista de acceso especifican reglas que "permiten" el acceso a redes o hosts especificados. En el modo Block-List ACL, las entradas de la lista de acceso especifican reglas que deniegan el acceso a redes o hosts especificados. Una lista de acceso no conforme contiene entradas de la lista de acceso con una mezcla de reglas permit y deny. Si se configura una lista de acceso no conforme para un registro DAP, puede rechazarse como un error de configuración cuando el administrador intente agregar el registro. Si se asigna una lista de acceso que se ajusta a un registro DAP, cualquier modificación de la lista de acceso que cambie la característica de conformidad puede rechazarse como un error de configuración.

Figura 16 ACL DAP: permite seleccionar y configurar ACL de red para aplicarlas a este registro DAP.



Cuando se seleccionan varios registros DAP, los atributos de listas de acceso especificados en la ACL de red (firewall) se agregan para crear una lista de acceso dinámica para la ACL de firewall DAP. Del mismo modo, los atributos de listas de acceso especificados en la ACL de tipo web (sin cliente) se agregan para crear una lista de acceso dinámica para la ACL sin cliente DAP. El

siguiente ejemplo se centra en cómo se crea específicamente una lista de acceso dinámica de firewall DAP. Sin embargo, una lista de acceso sin cliente DAP dinámica también puede realizar el mismo proceso.

En primer lugar, ASA crea dinámicamente un nombre único para la ACL de red DAP como se muestra en la Tabla 6.

Tabla 6. Nombre de ACL de red DAP dinámica

Nombre de ACL de red DAP
DAP-Network-ACL-X (donde X es un entero que puede incrementarse para garantizar la unicidad)

En segundo lugar, ASA recupera el atributo Network-ACL de los registros DAP seleccionados, como se muestra en la Tabla 7.

Tabla 7. ACL de red

Registros DAP seleccionados	Prioridad	ACL de red	Entradas de ACL de red
DAP 1	1	101 y 102	ACL 101 tiene 4 reglas de denegación y ACL 102 tiene 4 reglas de permiso
DAP 2	2	201 y 202	ACL 201 tiene 3 reglas de permiso y ACL 202 tiene 3 reglas de denegación
DAP 3	2	101 y 102	ACL 101 tiene 4 reglas de denegación y ACL 102 tiene 4 reglas de permiso

En tercer lugar, ASA reordena la ACL de red primero por el número de prioridad del registro DAP, y luego por Block-List primero si el valor de prioridad para 2 o más registros DAP seleccionados es el mismo. Después de esto, el ASA puede recuperar las entradas de Network-ACL de cada Network-ACL como se muestra en la Tabla 8.

Tabla 8. Prioridad de registro DAP

ACL de red	Prioridad	Modelo de lista de acceso blanco/negro	Entradas de ACL de red
101	2	Lista negra	4 Reglas de denegación (DDDD)
202	2	Lista negra	3 Reglas de denegación (DDD)
102	2	Lista blanca	4 Reglas de permisos (PPP)
202	2	Lista blanca	3 Reglas de permisos (PPP)
101	1	Lista negra	4 Reglas de denegación (DDDD)
102	1	Lista blanca	4 Reglas de permisos (PPP)

Por último, ASA combina las entradas Network-ACL en la Network-ACL generada dinámicamente y luego devuelve el nombre de la Network-ACL dinámica como la nueva Network-ACL que se aplicará, como se muestra en la Tabla 9.

Tabla 9. ACL de red DAP dinámica

Nombre de ACL de red DAP	Entrada de ACL de red
DAP-Network-ACL-1	DDDD DDD PPP PPP DDDD PPP

Implementación de DAP

Hay una serie de razones por las que un administrador debe considerar implementar DAP. Algunas razones subyacentes son cuando se va a aplicar la evaluación de estado en un terminal o cuando se van a tener en cuenta atributos AAA o de política más granulares al autorizar el acceso de los usuarios a los recursos de red. En el siguiente ejemplo, puede configurar DAP y sus componentes para identificar un punto final de conexión y autorizar el acceso de los usuarios a varios recursos de red.

Caso de prueba: un cliente ha solicitado una prueba de concepto con estos requisitos de acceso a VPN:

- Capacidad para detectar e identificar un terminal de empleado como administrado o no administrado. : si el terminal se identifica como gestionado (PC de trabajo) pero no cumple los requisitos de estado, se le debe denegar el acceso. Por otro lado, si el terminal del empleado se identifica como no gestionado (PC doméstico), se le debe conceder acceso sin cliente.
- Capacidad para invocar la limpieza de las cookies de sesión y la caché cuando finaliza una conexión sin cliente.
- La capacidad de detectar y aplicar aplicaciones en ejecución en terminales de empleados gestionados, como McAfee AntiVirus. Si la aplicación no existe, se debe denegar el acceso a ese extremo.
- La capacidad de utilizar la autenticación AAA para determinar a qué recursos de red deben tener acceso los usuarios autorizados. El dispositivo de seguridad debe admitir la autenticación LDAP de MS nativo y admitir varias funciones de pertenencia a grupos LDAP.
- Capacidad para permitir el acceso de LAN local a recursos de red, como faxes e impresoras, cuando se conecta mediante una conexión basada en cliente o red.
- La capacidad de proporcionar acceso de invitado autorizado a los contratistas. Los contratistas y sus terminales deben obtener acceso sin cliente, y el acceso del portal a las aplicaciones debe ser limitado en comparación con el acceso de los empleados.

En este ejemplo, puede ejecutar una serie de pasos de configuración para satisfacer los requisitos de acceso VPN del cliente. Puede haber pasos de configuración necesarios pero no relacionados directamente con DAP, mientras que otras configuraciones pueden estar relacionadas directamente con DAP. El ASA es muy dinámico y puede adaptarse a muchos entornos de red. Como resultado, las soluciones VPN se pueden definir de varias maneras y, en algunos casos, proporcionan la misma solución final. Sin embargo, el enfoque adoptado se basa

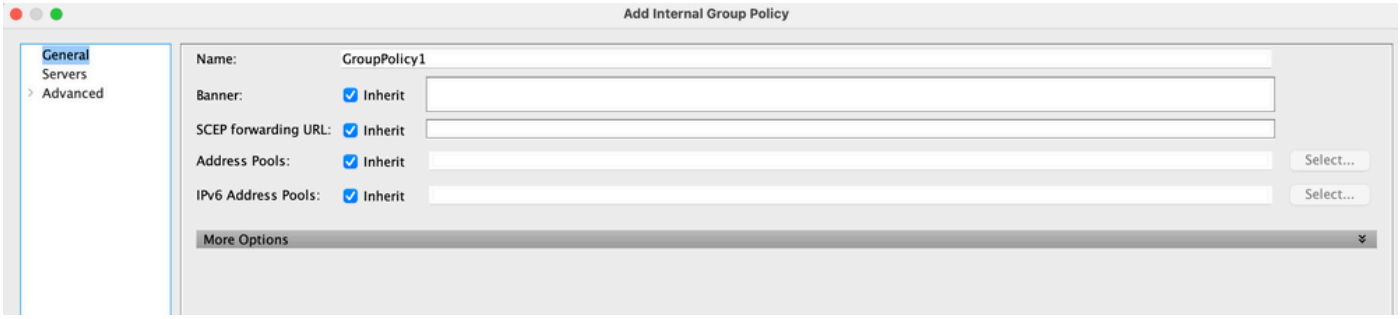
en las necesidades de los clientes y sus entornos.

Según la naturaleza de este documento y los requisitos del cliente definidos, puede utilizar Adaptive Security Device Manager (ASDM) y centrar la mayoría de nuestras configuraciones en DAP. Sin embargo, también puede configurar las políticas de grupo locales para mostrar cómo DAP puede complementar y/o invalidar los atributos de políticas locales. En función de este caso de prueba, puede suponer que hay un grupo de servidores LDAP, una lista de redes de tunelización dividida y conectividad IP básica, incluidos los grupos de IP y el grupo de servidores DNS predeterminado, preconfigurados.

Definición de una directiva de grupo: esta configuración es necesaria para definir atributos de directiva local. Algunos atributos definidos aquí no se pueden configurar en DAP para (por ejemplo, Acceso LAN local). (Esta política también se puede utilizar para definir los atributos basados en clientes y sin cliente).

Vaya a Configuration > Remote Access VPN > Network (Client) Access > Group Policies, y agregue una política de grupo interna como se muestra:

Figura 17 Directiva de grupo: define atributos específicos de VPN local.

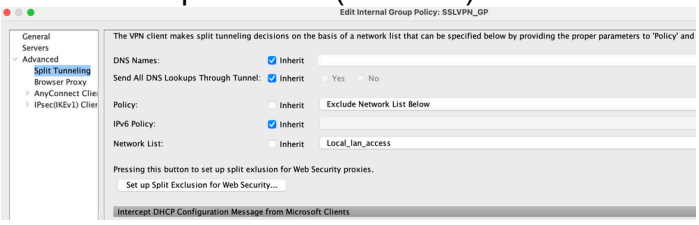


a. En el enlace General, configure el nombre SSLVPN_GP para la política de grupo.

b. También bajo el link General, haga clic en Más Opciones y configure solamente el Protocolo de Tunelización:SSLVPN sin Cliente. (Puede configurar DAP para invalidar y administrar el Método de Acceso.)

c. En el enlace Advanced > Split Tunneling, configure los siguientes pasos:

Figura 18 Tunelización dividida: permite que el tráfico especificado (red local) omita un túnel no cifrado durante una conexión de cliente.

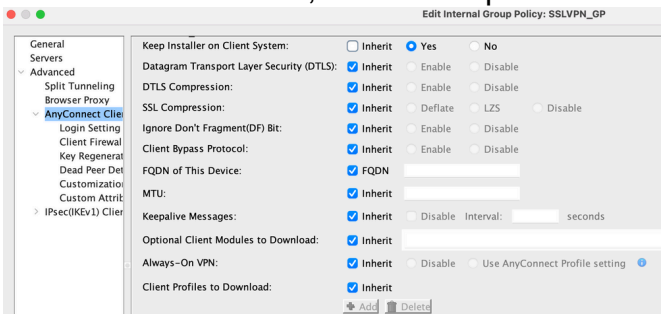


a. Política: Desmarque Hereday seleccione Excluir lista de redes.

b. Network List: UncheckInherit y seleccione el nombre de lista Local_Lan_Access. (Suponiendo que está preconfigurado.)

d. En el enlace Advanced > ANYCONNECT Client, configure los siguientes pasos:

Figura 19 Instalador de SSL VPN Client: tras la terminación de VPN, SSL Client puede permanecer en el terminal o ser desinstalado.



e. Mantener el instalador en el sistema cliente: DesactiveHereday, a continuación, seleccioneSí.

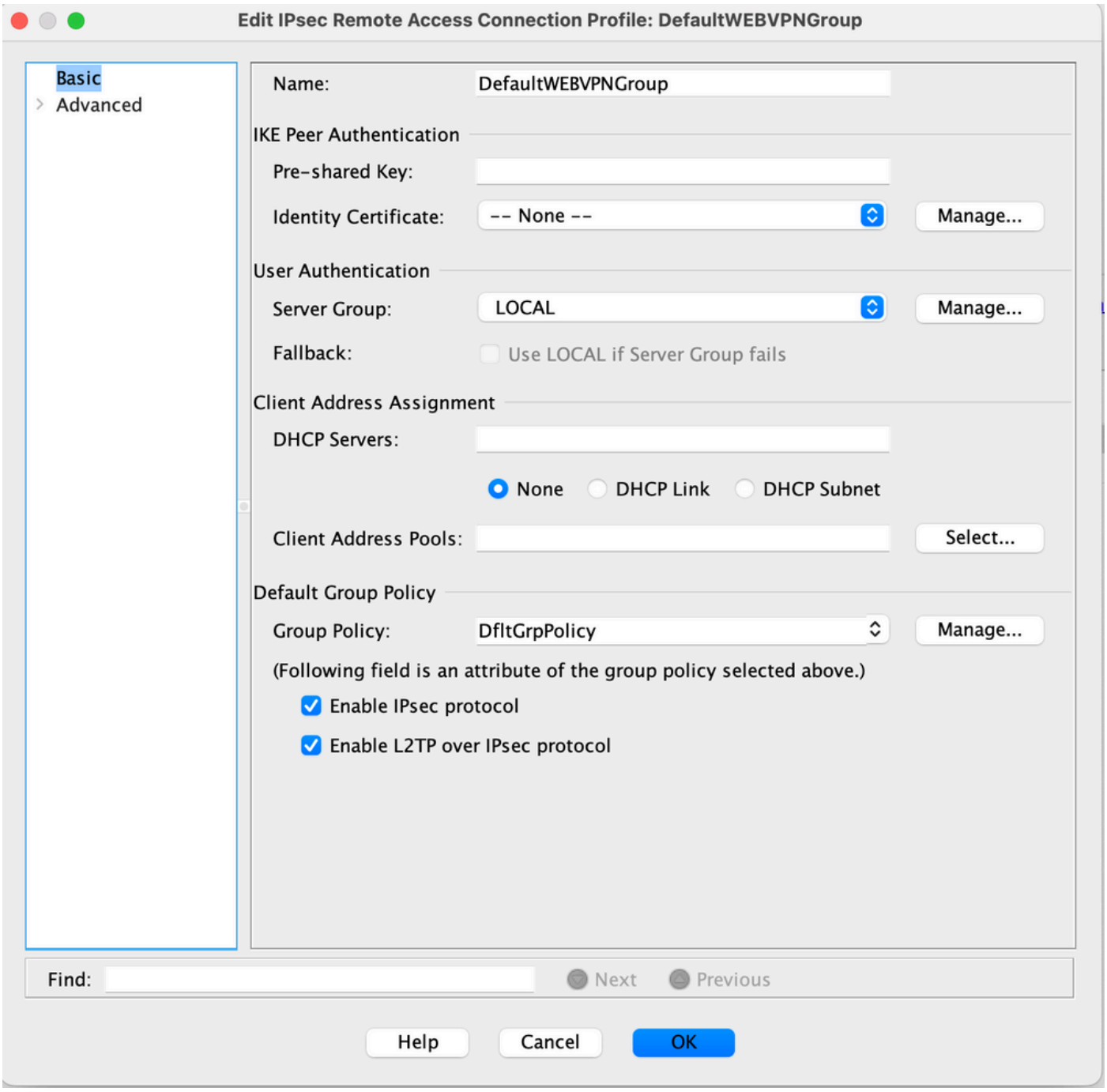
f. Haga clic en Aceptar y luego en Aplicar.

g. Aplique los cambios de configuración.

Definición de un perfil de conexión: esta configuración es necesaria para definir nuestro método de autenticación AAA, por ejemplo, LDAP, y aplicar la política de grupo previamente configurada (SSLVPN_GP) a este perfil de conexión. Los usuarios que se conectan a través de este perfil de conexión pueden estar sujetos a los atributos definidos aquí, así como a los atributos definidos en la política de grupo SSLVPN_GP. (Este perfil también se puede utilizar para definir tanto los atributos sin cliente como los basados en cliente).

Vaya a Configuration > Remote Access VPN > Network (Client) Access >IPsec Remote Access Connection Profile y configure:

Figura 20 Perfil de conexión: define atributos específicos de VPN local.



a. En la sección Perfiles de conexión, edite DefaultWEBVPNGroup y, en el vínculo Básico, configure los pasos siguientes:

   a. Autenticación: Método:AAA

   b. Autenticación: AAA Server Group:LDAP(se supone preconfigurado)

   c. Asignación de direcciones de cliente: Conjuntos de direcciones de cliente:IP_Pool(Se presupone preconfigurado)

   d. Directiva de grupo predeterminada: Directiva de grupo: SelectSSLVPN_GP

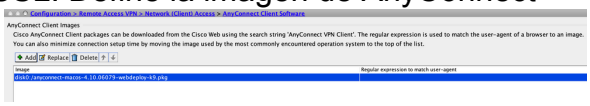
b. Aplique los cambios de configuración.

Definir una interfaz IP para la conectividad SSL VPN: esta configuración es necesaria para

terminar las conexiones SSL sin cliente y con cliente en una interfaz especificada.

Antes de habilitar el acceso de cliente/red en una interfaz, debe definir una imagen de SSL VPN Client.

1. Vaya a Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software, y Add the next image, the SSL VPN Client Image from the ASA Flash file system: (Esta imagen se puede descargar desde CCO, https://www.cisco.com)

   Figura 21 Instalación de la imagen de cliente VPN SSL: Define la imagen de AnyConnect Client que se enviará a los terminales de conexión. 

   a. anyconnect-mac-4.x.xxx-k9.pkg

   b. Haga clic en Aceptar,Aceptarde nuevo y, a continuaciónAplicar.

2. Vaya a Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles, y utilice los siguientes pasos para habilitar esto:

   Figura 22 Interfaz de acceso VPN SSL: Define las interfaces para terminar la conectividad VPN SSL. 

   a. En la sección Access Interface (Interfaz de acceso), habilite:Enable Cisco AnyConnect VPN Client o legacy SSL VPN Client access en las interfaces seleccionadas en la tabla siguiente.

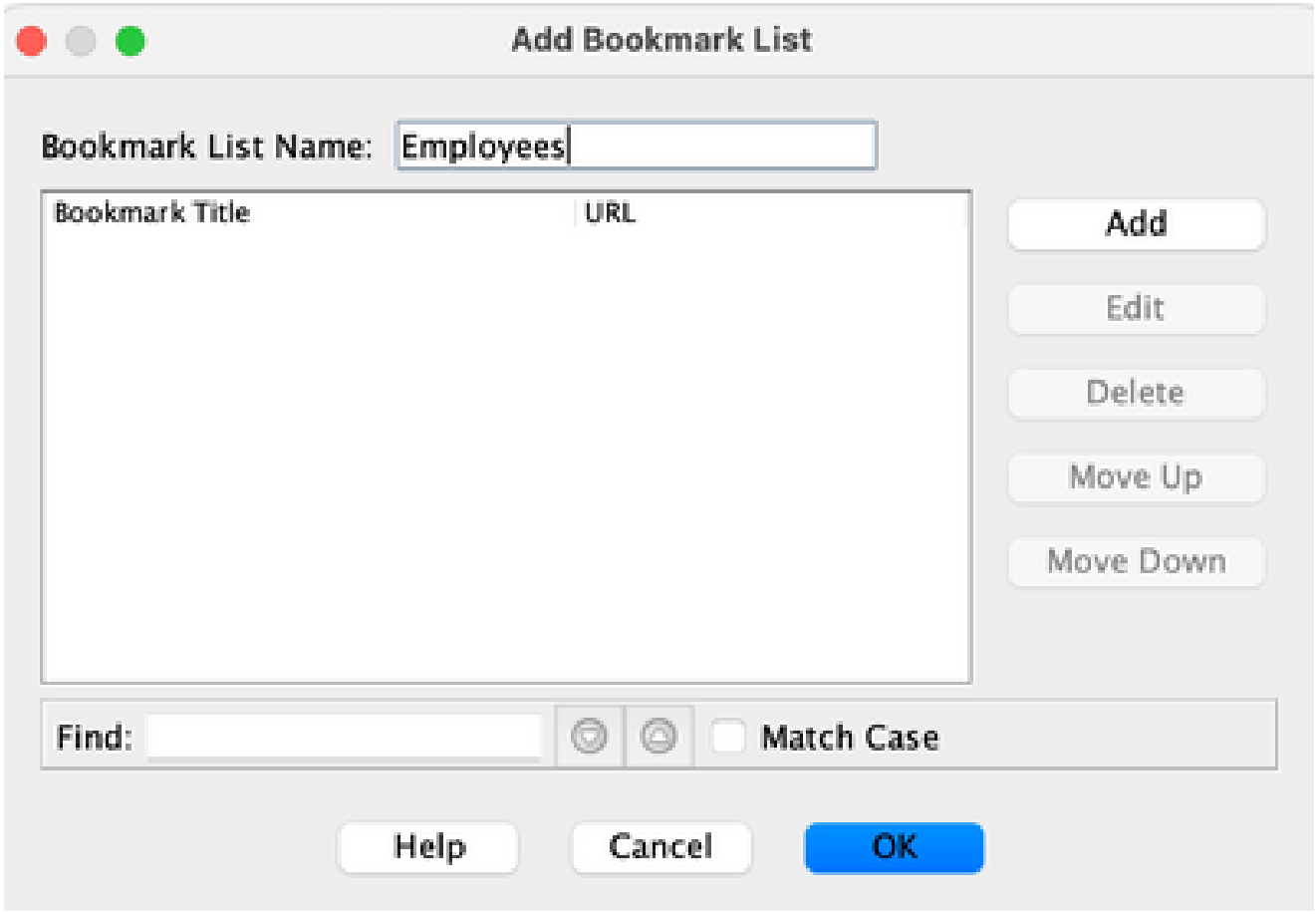
   b. También bajo la sección Interfaces de acceso, marque Permitir acceso a la interfaz exterior. (Esta configuración también puede habilitar el acceso sin cliente SSL VPN en la interfaz externa.)

   c. Haga clic en Aplicar.

Definición de Listas de Marcadores (Listas de URL) para el Acceso sin Cliente: Esta configuración es necesaria para definir una aplicación basada en Web que se publicará en el Portal. Puede definir 2 listas de URL, una para Empleados y otra para Contratistas.

1. Vaya a Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks, haga clic en + Add y configure los siguientes pasos:

   Figura 23 Lista de marcadores: define las URL que se publicarán y a las que se accederá desde el portal web. (Personalizado para acceso de empleado).



a. Nombre de la lista de marcadores:Empleados y, a continuación, haga clic en Agregar.

b. Título del marcador:Intranet de la empresa

c. Valor de URL: https://company.resource.com

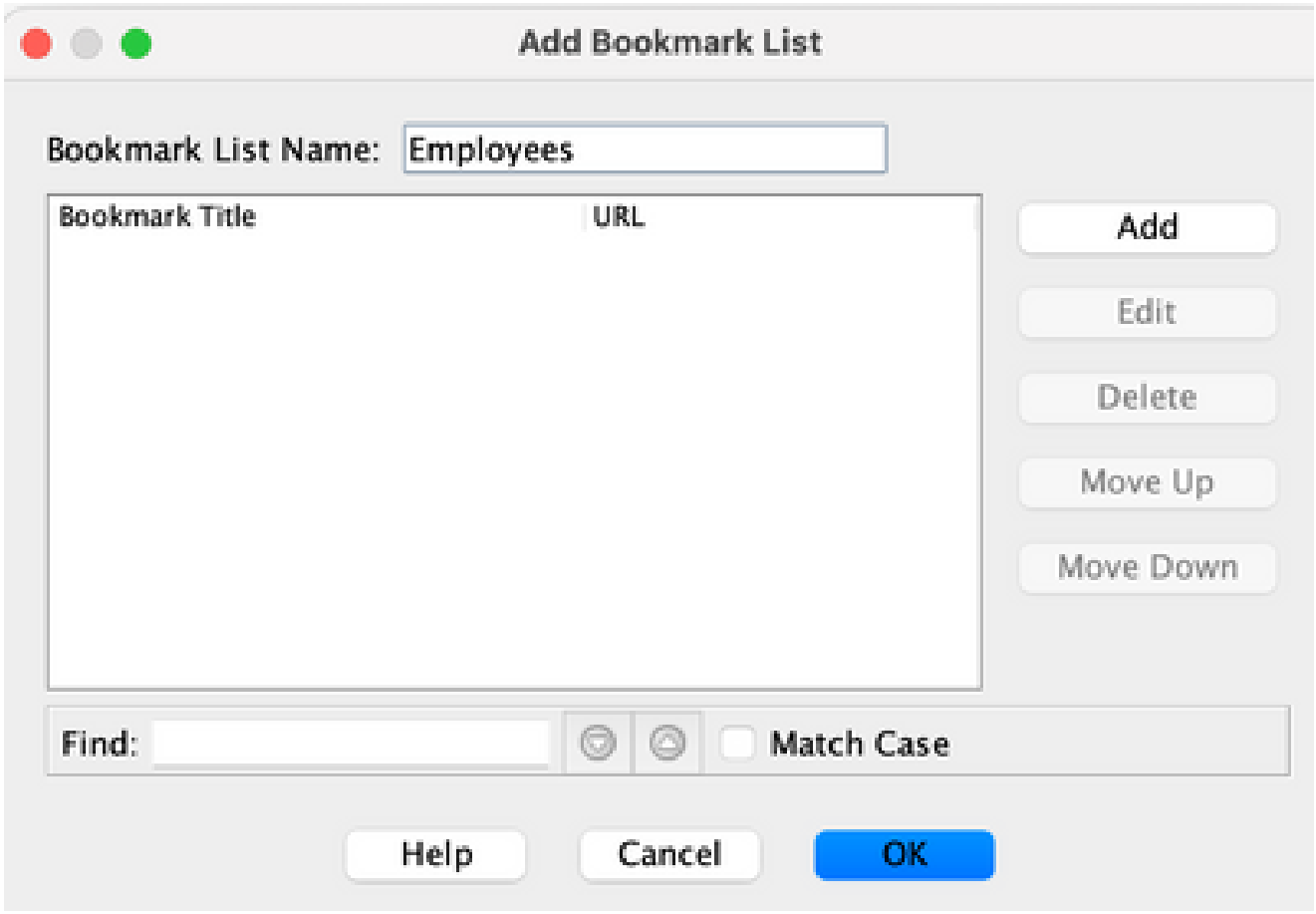
-

Haga clic enAceptar y vuelva a hacer clic enAceptar.

-

Haga clic en + Agregar y configure una segunda lista de marcadores (lista de URL) de la siguiente manera:

Figura 24 Lista de marcadores: personalizada para acceso de invitado.



a.

Nombre de la lista de marcadores:**Contratistas** y, a continuación, **haga clic en Agregar**.

b.

Título del marcador:**Acceso de invitado**

c.

Valor de URL: https://company.contractors.com

-

Haga clic enAceptar y vuelva a hacer clic enAceptar.

-

Haga clic en Aplicar.

Configurar HostScan:

- Vaya a **Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image**, y configure los siguientes pasos:

Figura 25 Instalación de HostScan Image: Define la imagen de HostScan que se va a enviar a los terminales de conexión. 

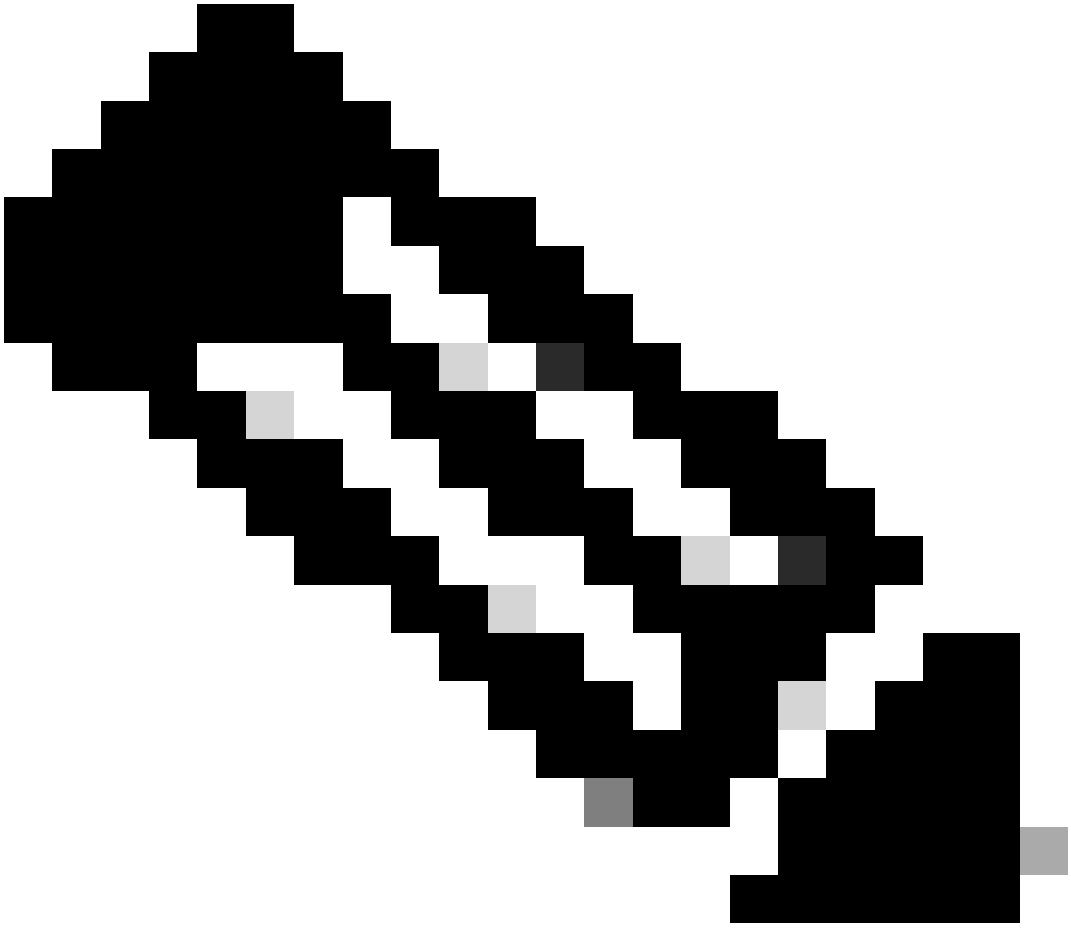
a. Instale **el disk0:/hostscan_4.xx.xxxxx-k9.**pkgimage desde el sistema de archivos Flash ASA.

b. **Active HostScan**.

c. **Haga clic en Aplicar**.

Políticas de acceso dinámicas: esta configuración es necesaria para validar los usuarios que se conectan y sus terminales con respecto a los criterios de evaluación de terminales o AAA definidos. Si se cumplen los criterios definidos de un registro DAP, se puede conceder acceso a los usuarios de conexión a los recursos de red asociados a dicho registro o registros DAP. La autorización DAP se ejecuta durante el proceso de autenticación.

Para asegurarse de que una conexión VPN SSL puede terminar en el caso predeterminado, por ejemplo, cuando el extremo no coincide con ninguna directiva de acceso dinámico configurada), puede configurarla con estos pasos:

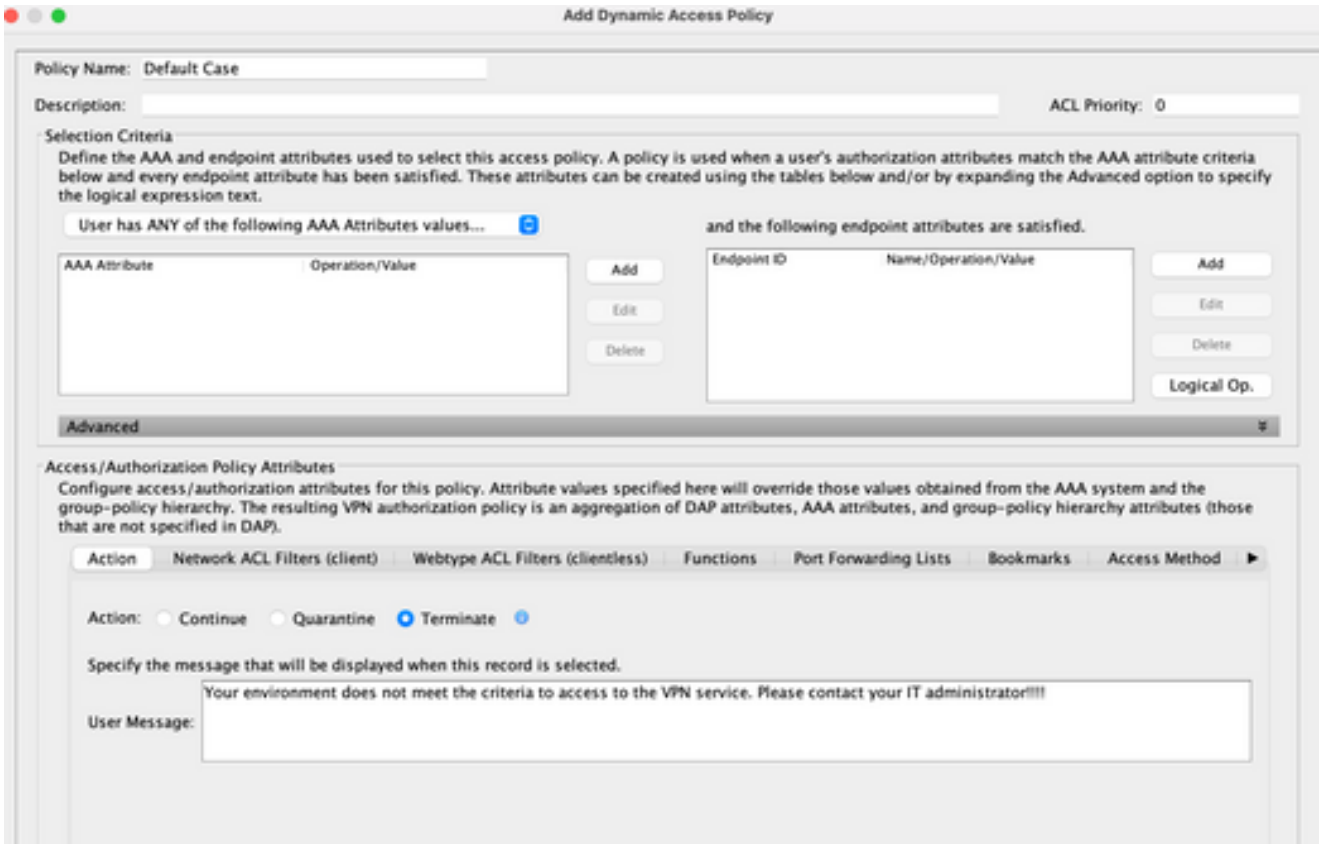


Nota: Al configurar las directivas de acceso dinámico por primera vez, se muestra un mensaje de error DAP.xml que indica que no existe un archivo de configuración DAP (DAP.XML). Una vez modificada y guardada la configuración inicial de DAP, este mensaje ya no puede aparecer.

-

Vaya a **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**, y configure los siguientes pasos:

Figura 30 Directiva de acceso dinámica predeterminada: si no se coincide con ningún registro DAP predefinido, se puede aplicar este registro DAP. Por lo tanto, se puede denegar el acceso VPN SSL.



a.

Edite laPolíticaDeAccesoDflt y establezca la Acción **en Terminar**.

b.

Haga clic en Aceptar.

•

Agregue una nueva directiva de acceso dinámica **denominada Managed_Endpoints**, como se indica a continuación:

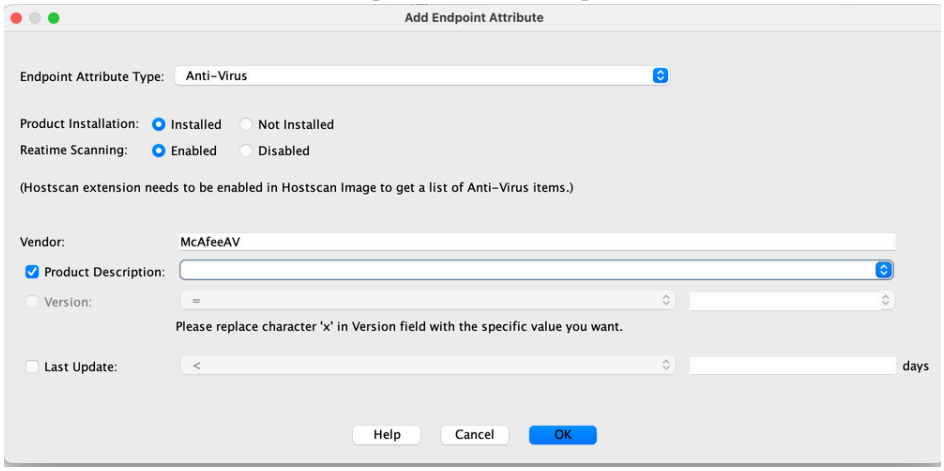
a.

Descripción:**Acceso de cliente de empleado**

b.

Agregue un tipo de atributo de terminal (antivirus) como se muestra en la figura 31. Haga clic en Aceptar cuando termine.

Figura 31 Atributo de terminal DAP: el antivirus Advanced Endpoint Assessment se puede utilizar como criterio DAP para el acceso de cliente/red.



c.

Como se muestra en la imagen anterior, en la lista desplegable de la sección Atributo AAA, seleccione User has ALL of the following AAA Attributes Values.

•

Agregue (situado a la derecha del cuadro Atributo AAA) un Tipo de atributo AAA (LDAP) como se muestra en las figuras 33 y 34. Haga clic en Aceptar cuando termine.

Figura 33 Atributo AAA de DAP: la pertenencia al grupo AAA se puede utilizar como criterio de DAP para identificar a un empleado.

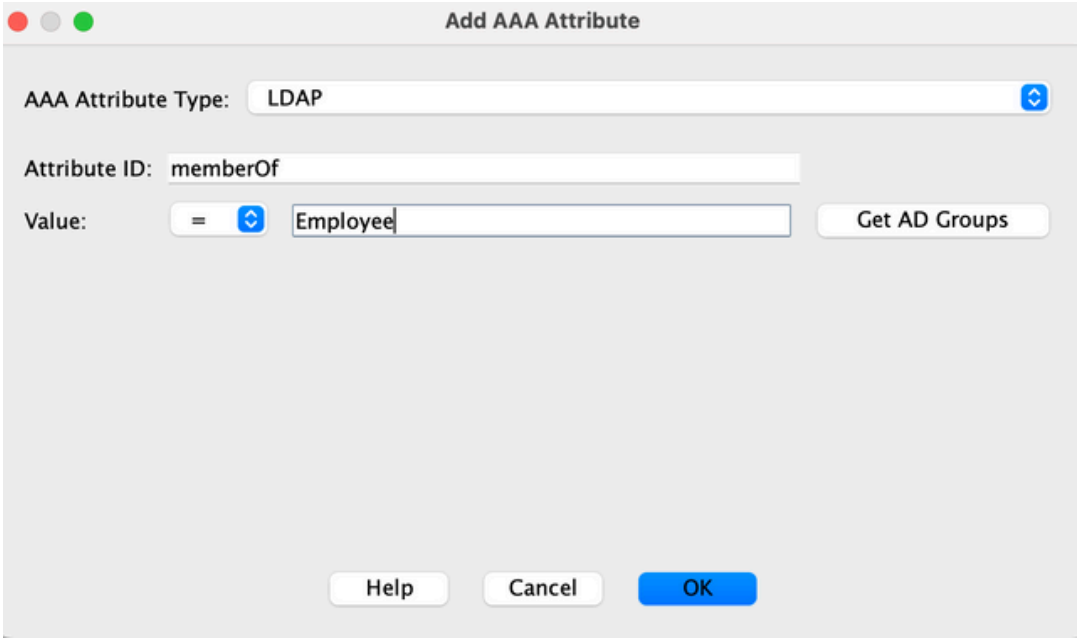
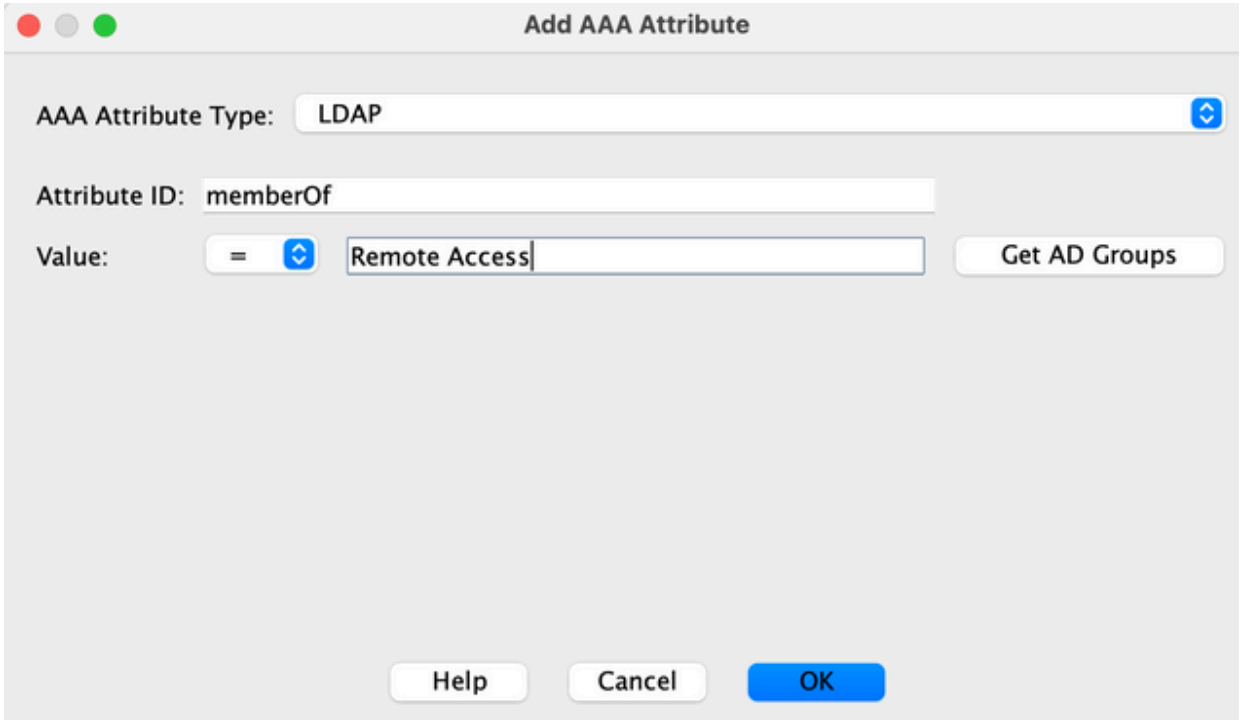


Figura 34 Atributo AAA de DAP: la pertenencia al grupo AAA se puede utilizar como criterio de DAP para permitir las funciones de acceso remoto.



-

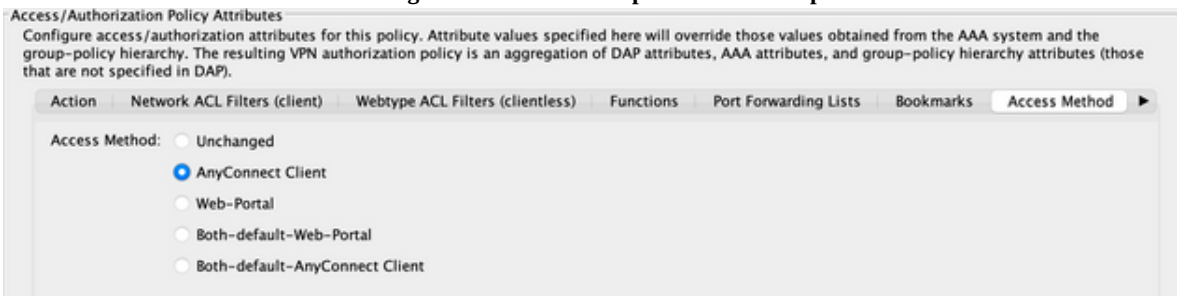
En la ficha Acción, verifique que la Acción esté establecida **en Continuar**, como se muestra en la Figura 35.

Figura 35 Ficha Acción: esta configuración es necesaria para definir un procesamiento especial para una conexión o sesión específica. Se puede denegar el acceso a VPN si un registro DAP coincide y la acción se establece en Finalizar.

-

En la pestaña Método de acceso, seleccione el **Método de accesoCliente AnyConnect**, como se muestra en la Figura 36.

Figura 36 Ficha Método de acceso: esta configuración es necesaria para definir los tipos de conexión del cliente SSL VPN.



-

Haga clic en Aceptar y, **a continuaciónAplicar**.

-

Agregue una segunda política de acceso dinámica **denominada Unmanaged_Endpoints**, como se describe a continuación:

a.

Descripción:**Employee Clientless Access**.

b.

En la lista desplegable de la imagen anterior de la sección de atributos AAA, seleccione User has ALL of the following AAA Attributes Values .

•

Agregue (ubicado a la derecha del tipo de atributo AAA) un tipo de atributo AAA (LDAP) como se muestra en las figuras 38 y 39. Haga clic en Aceptar cuando termine.

Figura 38 Atributo AAA de DAP: la pertenencia al grupo AAA se puede utilizar como criterio de DAP para identificar a un empleado.

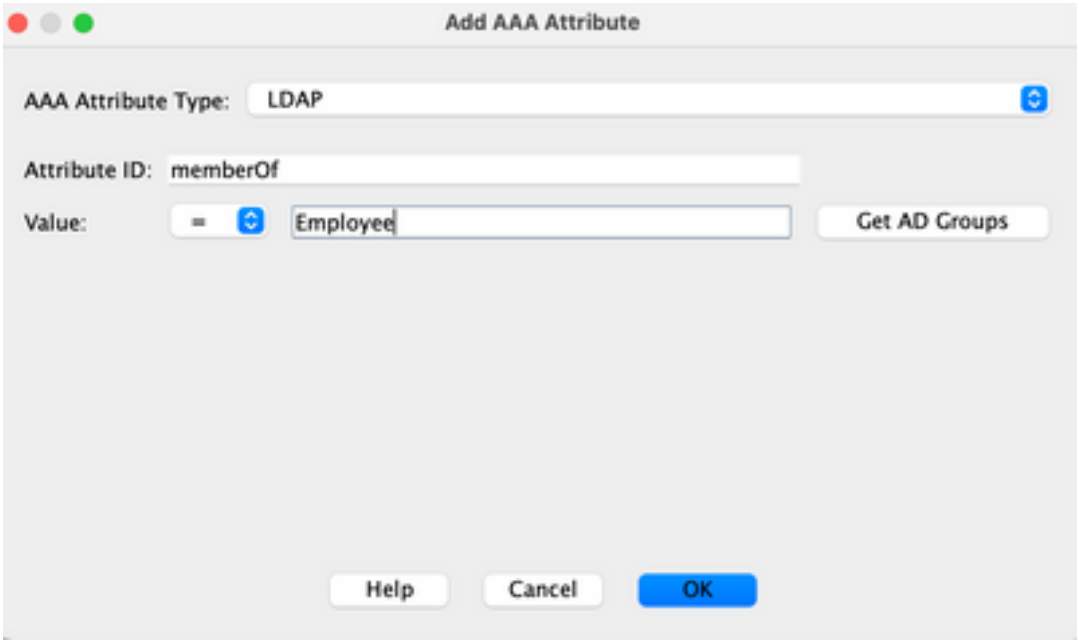
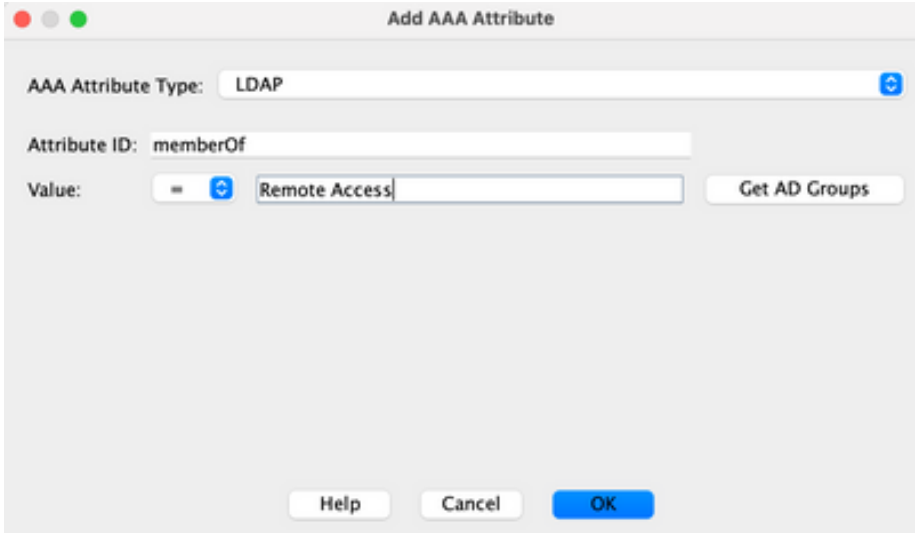


Figura 39 Atributo AAA de DAP: la pertenencia a un grupo AAA se puede utilizar como criterio de DAP para permitir las funciones de acceso remoto.

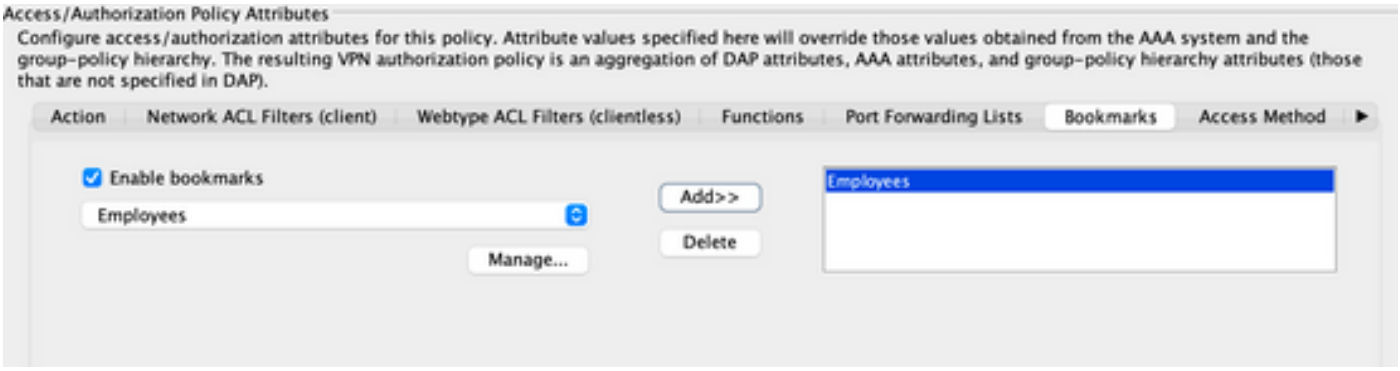


•

En la ficha Acción, compruebe que la acción está establecida **enContinuar**. (Figura 35)

- En la ficha Marcadores, seleccione la lista nombreEmpleados en la lista desplegable y, a continuación, **haga clic en Agregar**. Verifique también que los marcadores Enable (Activar) estén marcados como se muestra en la Figura 40.

Figura 40 Ficha Marcadores: permite seleccionar y configurar listas de direcciones URL para las sesiones de usuario.



- a. En la ficha Método de acceso, seleccione el **portal web** Método de acceso. (Figura 36)

- **Haga clic en Aceptar** y, **a continuaciónAplicar**.

1. Los contratistas solo se pueden identificar mediante atributos AAA de DAP. Como resultado, el tipo de atributos de terminal (política) no se puede configurar en el paso 4. Este enfoque solo pretende mostrar versatilidad dentro de DAP.

3. Agregue una tercera política de acceso dinámica **denominada Guest_Access** con lo siguiente:

- Descripción:**Guest Clientless Access**.

- Agregue (ubicado a la derecha del cuadro Endpoint Attribute) un Endpoint Attribute Type (Policy) como se muestra en la Figura 37. Haga clic en Aceptar cuando termine.

- En la Figura 40, en la lista desplegable de la Sección de Atributos AAA, seleccione User has ALL of the following AAA Attributes Values.

- Agregue (situado a la derecha del cuadro Atributo AAA) un Tipo de atributo AAA (LDAP) como se muestra en las figuras 41 y 42. Haga clic en Aceptar cuando termine.

Figura 41 Puede utilizar la pertenencia al grupo AAA del atributo AAA de DAP como criterio de DAP para identificar a un contratista

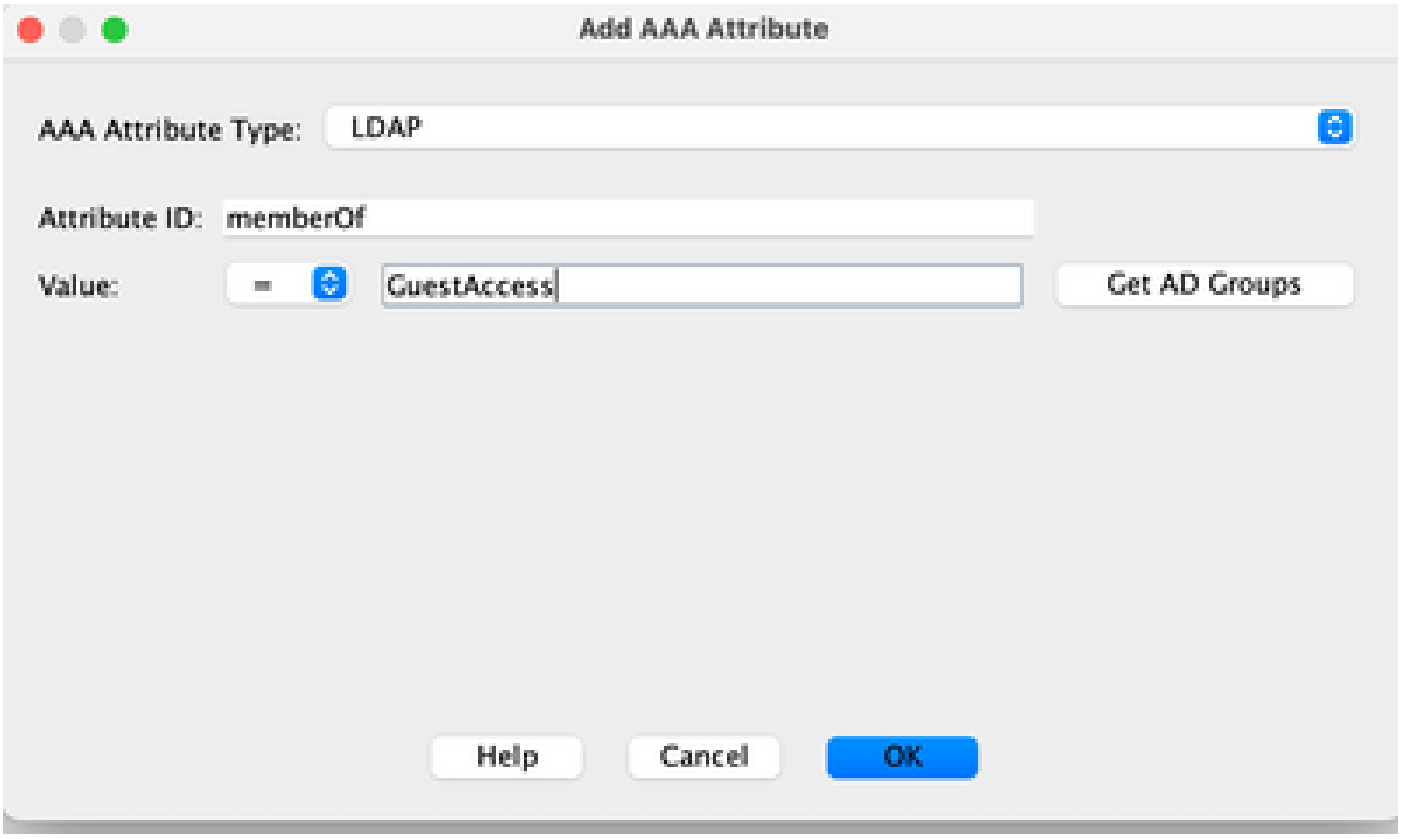
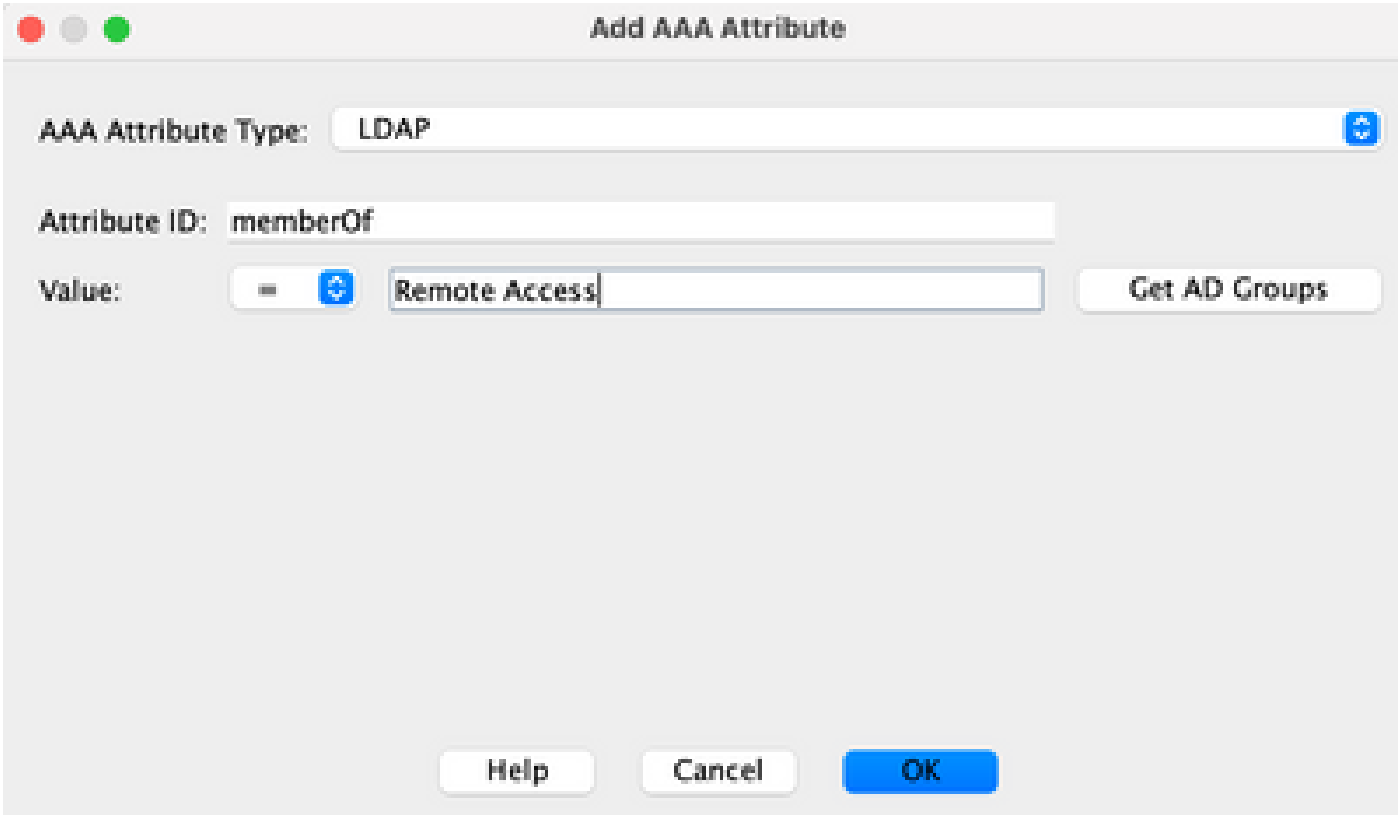


Figura 42 Atributo AAA de DAP: puede utilizar la pertenencia a un grupo AAA como criterio de DAP para permitir capacidades de acceso remoto



-

a.

En la ficha Acción, compruebe que la acción está establecida en **Continuar**. (Figura 35)

b.

En la ficha Marcadores, seleccione el nombre de la lista **Contratistas** en la lista desplegable y, a continuación, haga clic en Agregar. Además, verifique que los **marcadores Enable** estén marcados. (Figura de referencia 40.)

c.

En la ficha Método de acceso, seleccione el portal web Método de acceso. (Figura 36)

d.

Haga clic en **Aceptar** y, a continuación, en **Aplicar**.

Conclusión

Según los requisitos de VPN SSL de acceso remoto del cliente indicados en este ejemplo, esta solución satisface los requisitos de VPN de acceso remoto del cliente.

Con los entornos de VPN dinámicos y en evolución en la fusión, las políticas de acceso dinámico pueden adaptarse y ampliarse a los cambios frecuentes de configuración de Internet, a las diversas funciones que puede desempeñar cada usuario dentro de una organización y a los inicios de sesión de sitios de acceso remoto gestionados y no gestionados con diferentes configuraciones y niveles de seguridad.

Las políticas de acceso dinámicas se complementan con tecnologías nuevas y probadas como Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA y las políticas de acceso local. Como resultado, las organizaciones pueden ofrecer con confianza acceso VPN seguro a cualquier recurso de red desde cualquier ubicación.

Información Relacionada

- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).