Guía de despliegue de las directivas del acceso dinámico ASA 8.x (DAP)

Contenido

Introducción

Los gatewayes del Red privada virtual (VPN) actúan en los entornos dinámicos. Las variables múltiples pueden afectar a cada conexión VPN; por ejemplo, configuraciones del intranet que cambian con frecuencia, los diversos papeles que cada usuario puede habitar dentro de una organización, y logines de los sitios del Acceso Remoto con las diversos configuraciones y niveles de seguridad. La tarea de autorizar a los usuarios se complica mucho más en un entorno VPN dinámico que está en una red con una configuración estática.

Las directivas del acceso dinámico (DAP), una nueva función introducida en el código de la versión de software v8.0 del dispositivo de seguridad adaptante (ASA), le permiten para configurar la autorización que dirige la dinámica de los entornos VPN. Usted crea una directiva del acceso dinámico fijando una colección de atributos del control de acceso que usted asocie a un túnel o a una sesión específico del usuario. Estos atributos abordan las aplicaciones la calidad de miembro y la Seguridad de terminales de múltiples grupos.

Por ejemplo, el acceso de las concesiones del dispositivo de seguridad a un usuario determinado para una sesión específica basada en las directivas que usted define. Genera un DAP durante la autenticación de usuario seleccionando y/o agregando los atributos de uno o más expedientes DAP. Selecciona estos expedientes DAP basados en la información de Seguridad de terminales del dispositivo remoto y/o la información de la autorización AAA para el usuario autenticado. Entonces aplica el expediente DAP al túnel o a la sesión del usuario.

Nota: *El archivo dap.xml*, que contiene los atributos de la selección de las directivas DAP, se salva en el flash ASA. Aunque usted pueda exportar el apagado-cuadro del archivo dap.xml, editelo (si usted sabe sobre el sintaxis del xml), y reimpórtelo detrás, tenga muy cuidado, porque usted puede hacer el ASDM parar el procesar de los expedientes DAP si usted ha configurado mal algo. No hay CLI para manipular a esta parte de la configuración.

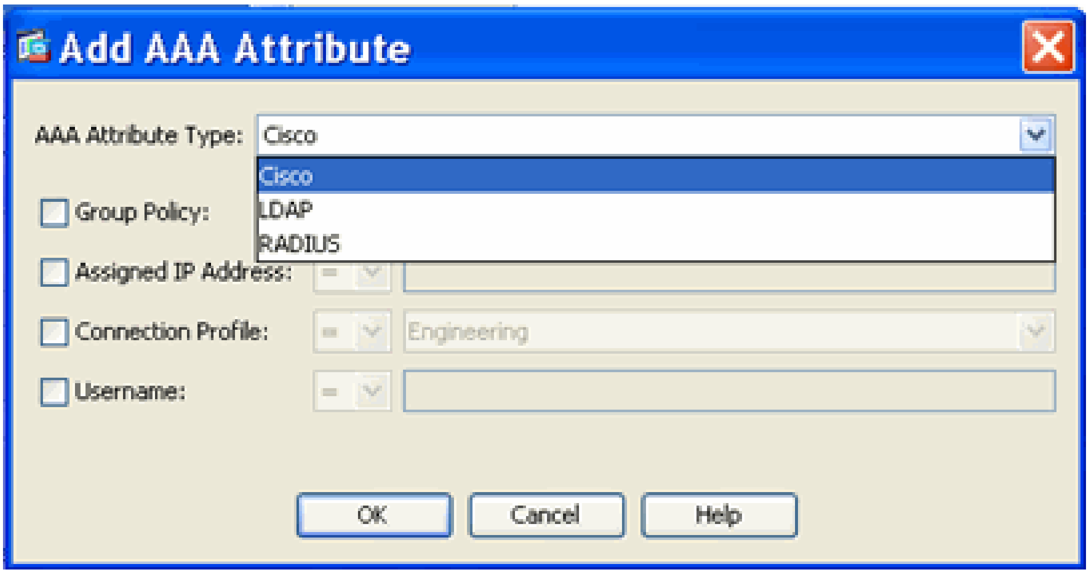
Nota: El intentar configurar los parámetros del *acceso del dinámico-acceso-directiva-expediente* vía el CLI puede hacer el DAP parar el trabajar aunque el ASDM manejara correctamente lo mismo. Evite el CLI, y utilice siempre el ASDM para manejar las directivas DAP.

Atributos DAP y AAA

El DAP complementa los servicios AAA y proporciona a un conjunto limitado de atributos de la autorización que puedan reemplazar los atributos que el AAA proporciona. El dispositivo de seguridad puede seleccionar los expedientes DAP basados en la información de la autorización AAA para el usuario. El dispositivo de seguridad puede seleccionar los expedientes múltiples DAP dependiendo de esta información, que entonces agrega para asignar a los atributos de la autorización DAP.

Usted puede especificar los atributos AAA de la jerarquía del atributo de Cisco AAA, o del Conjunto completo de atributos de la respuesta que el dispositivo de seguridad reciba de un RADIUS o de un servidor LDAP tal y como se muestra en del cuadro 1.

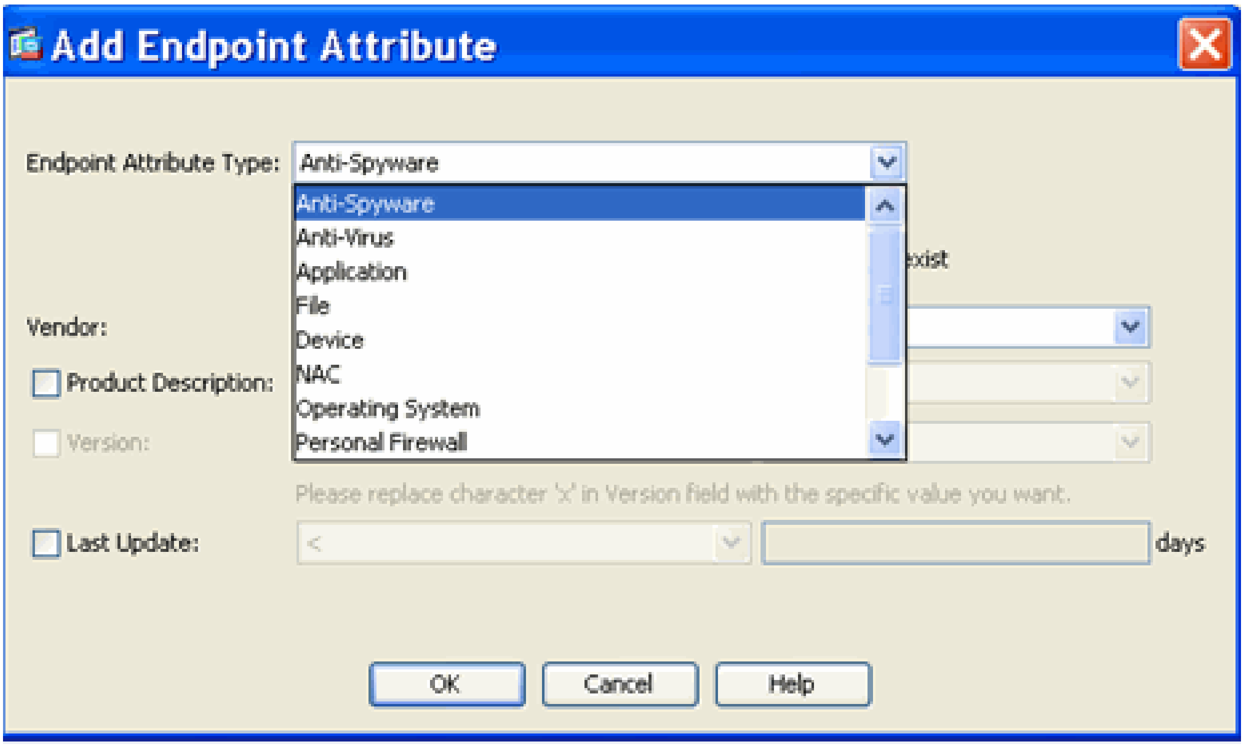
Cuadro 1. atributo GUI DAP AAA



DAP y atributos de Seguridad de terminales

Además de los atributos AAA, el dispositivo de seguridad puede también obtener los atributos de Seguridad de terminales usando los métodos de la evaluación de la postura que usted configura. Éstos incluyen la exploración básica del host, Secure Desktop, estándar/avanzó la evaluación del punto final y el NAC tal y como se muestra en del cuadro 2. atributos de la evaluación del punto final se obtiene y se envía al dispositivo de seguridad antes de la autenticación de usuario. Sin embargo, los atributos AAA, incluyendo el expediente total DAP, se validan durante la autenticación de usuario.

Cuadro 2. atributo GUI del punto final

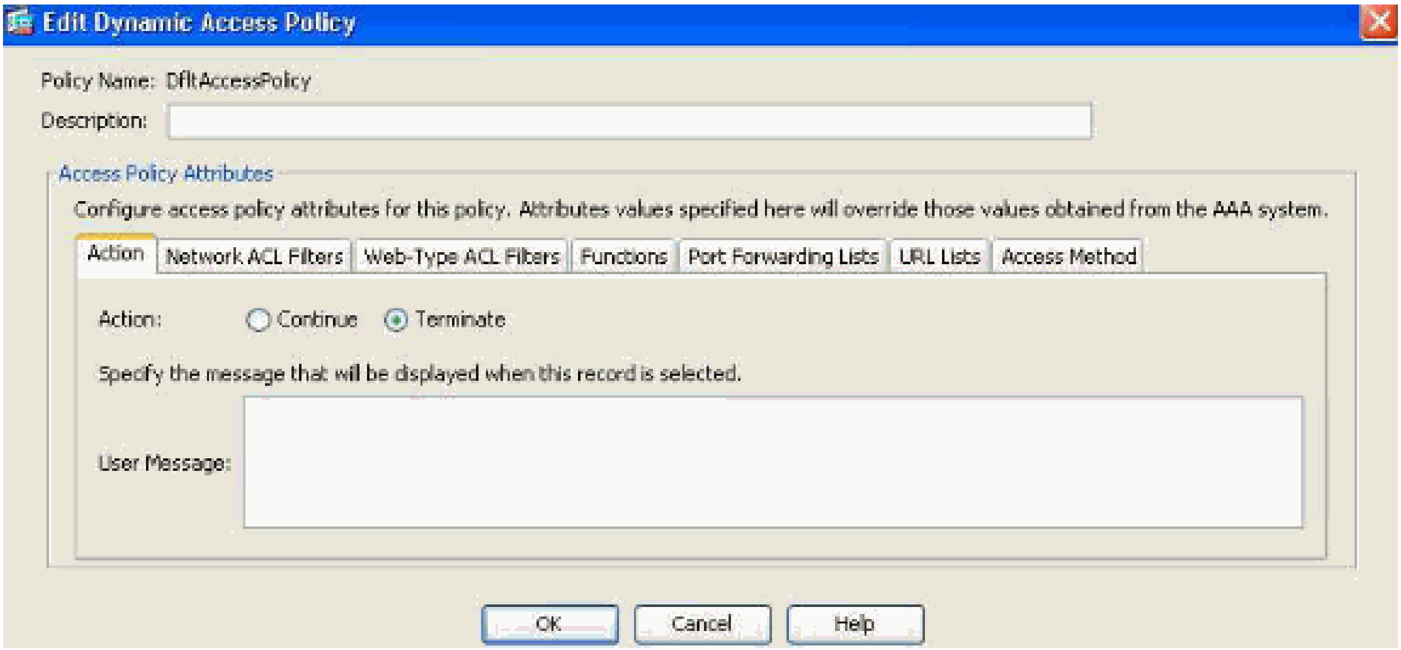


Directiva predeterminada del acceso dinámico

Antes de la introducción y de la implementación del DAP, el atributo de la política de acceso/los pares del valor que fueron asociados a un túnel o a una sesión específico del usuario fue definido localmente en el ASA, es decir, (los grupos de túnel y las directivas del grupo) o asociado vía los servidores de AAA externos. Sin embargo, en la versión v8.0, el DAP se puede configurar para complementar o para reemplazar el local y las directivas del acceso externo.

El DAP se aplica siempre por abandono. Sin embargo, para los administradores que prefiere el método de la aplicación de políticas de la herencia, por ejemplo, aplicando el control de acceso vía los grupos de túnel, las directivas del grupo y el AAA sin la aplicación explícita del DAP pueden todavía obtener este comportamiento. Para el comportamiento de la herencia, no se requiere ningunos cambios de configuración a la característica DAP, incluyendo el expediente del valor por defecto DAP, DfltAccessPolicy, tal y como se muestra en del cuadro 3.

Cuadro 3. directiva predeterminada del acceso dinámico



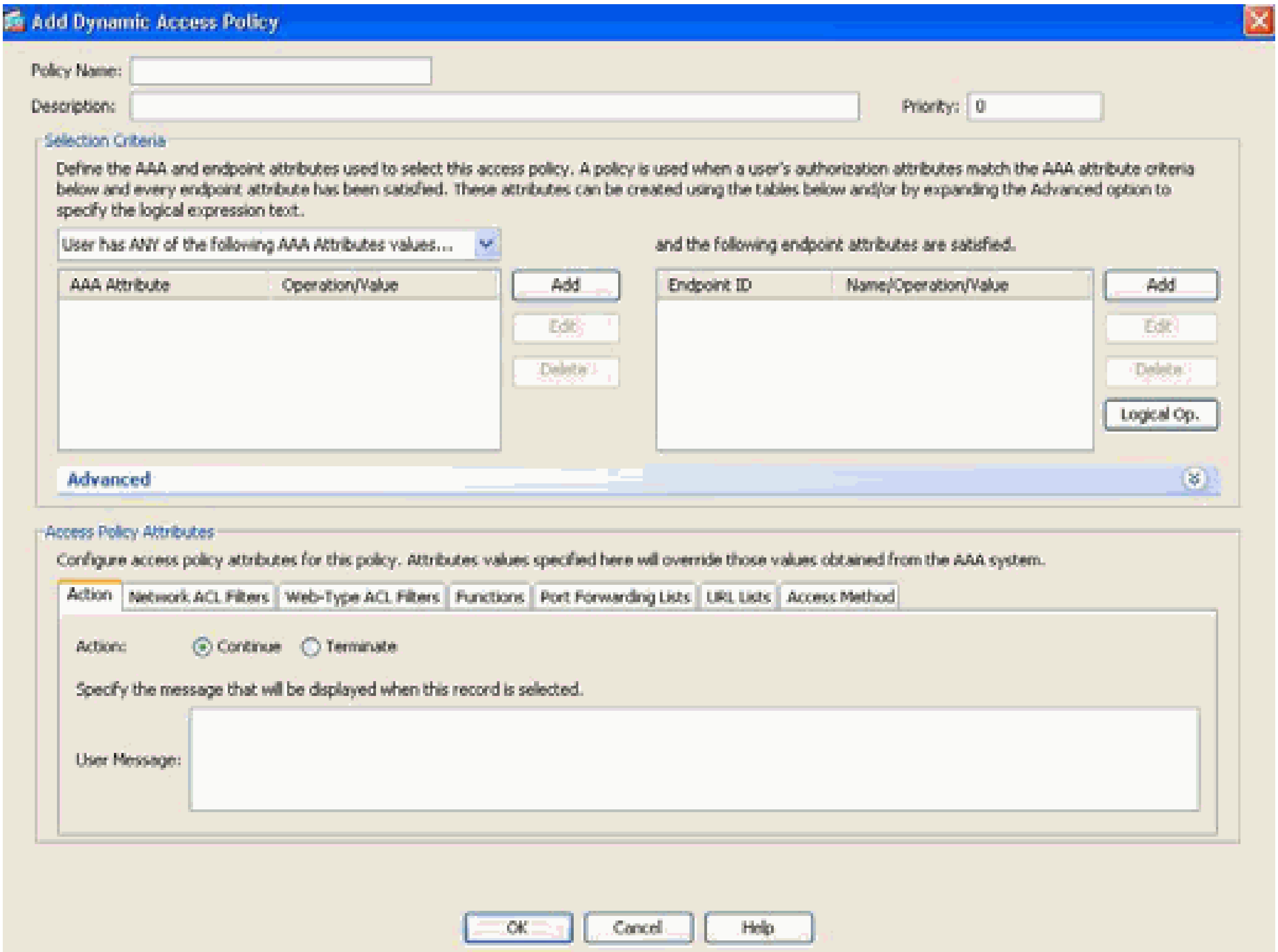
Sin embargo, si los valores predeterminados uces de los en un expediente DAP se cambian, por ejemplo, la acción: el parámetro en el DfltAccessPolicy se cambia de su valor predeterminado para terminar y los expedientes adicionales DAP no se configuran, los usuarios autenticados, por abandono, harán juego el expediente de DfltAccessPolicy DAP y serán negados el acceso VPN.

Por lo tanto, uno o más expedientes DAP necesitarán ser creados y ser configurados para autorizar la conectividad VPN y para definirla que autorizan los recursos de red un usuario autenticado a acceder. Así, el DAP, si está configurado, tomará la precedencia sobre la aplicación de políticas de la herencia.

Configurar las directivas del acceso dinámico

Al usar el DAP para definir al cual los recursos de red un usuario tienen acceso, hay muchos parámetros a considerar. Por ejemplo, entorno de identificación si el punto final de conexión está viniendo de un haber manejado, unmanaged o untrusted, determinando el Criterio de selección necesario identificar el punto final de conexión, y basado en la evaluación del punto final y/o las credenciales AAA, que autorizarán los recursos de red el usuario de conexión a acceder. Para lograr esto, usted primero necesitará hacer familiar con las características y las funciones DAP tal y como se muestra en del cuadro 4.

Cuadro 4. directiva del acceso dinámico



Al configurar un expediente DAP, hay dos componentes importantes a considerar:

- Criterio de selección incluyendo las opciones avanzadas
- Atributos de la política de acceso

El Criterio de selección de la sección es donde un administrador configuraría el AAA y los atributos del punto final usados para seleccionar un expediente específico DAP. Se utiliza un expediente DAP cuando los atributos de la autorización de un usuario hacen juego los criterios del atributo AAA y se ha satisfecho cada atributo del punto final.

Por ejemplo, si el tipo del atributo AAA: Se selecciona el LDAP (Active Directory), el name string del atributo es memberOf y la cadena del valor es contratistas, tal y como se muestra en de la figura 5a, el usuario de autenticidad debe ser un miembro de los contratistas del grupo del Active Directory para hacer juego los criterios del atributo AAA.

Además de satisfacer los criterios del atributo AAA, requerirán al usuario de autenticidad también satisfacer los criterios del atributo del punto final. Por ejemplo, si el administrador configuró el (CSD) del Cisco Secure Desktop para determinar la postura del punto final de conexión y basada en esa evaluación de la postura, el punto final fue puesto en la ubicación CSD Unmanaged, el administrador podría entonces utilizar esta información de la evaluación mientras que el Criterio de selección para el punto final atribuye mostrado en la figura 5b.

Figura 5a. Criterios del atributo AAA

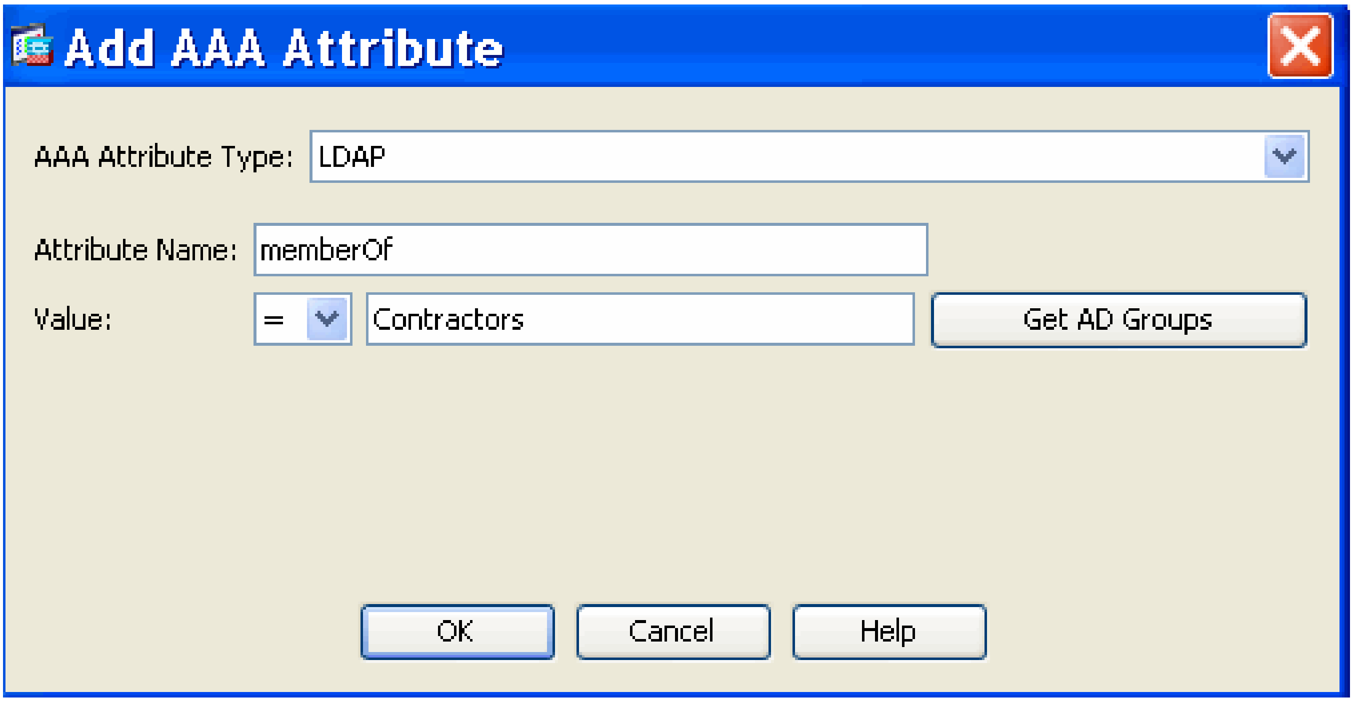
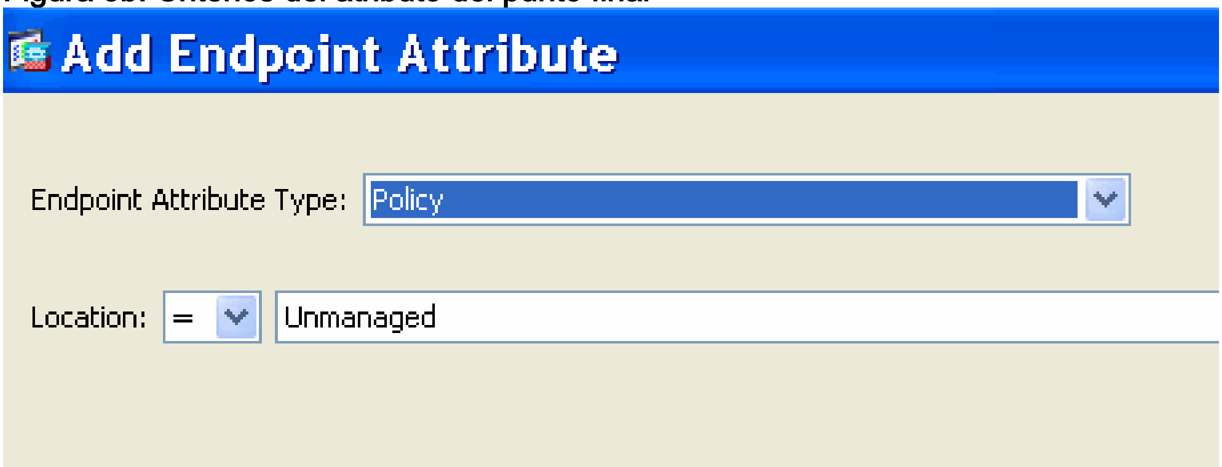
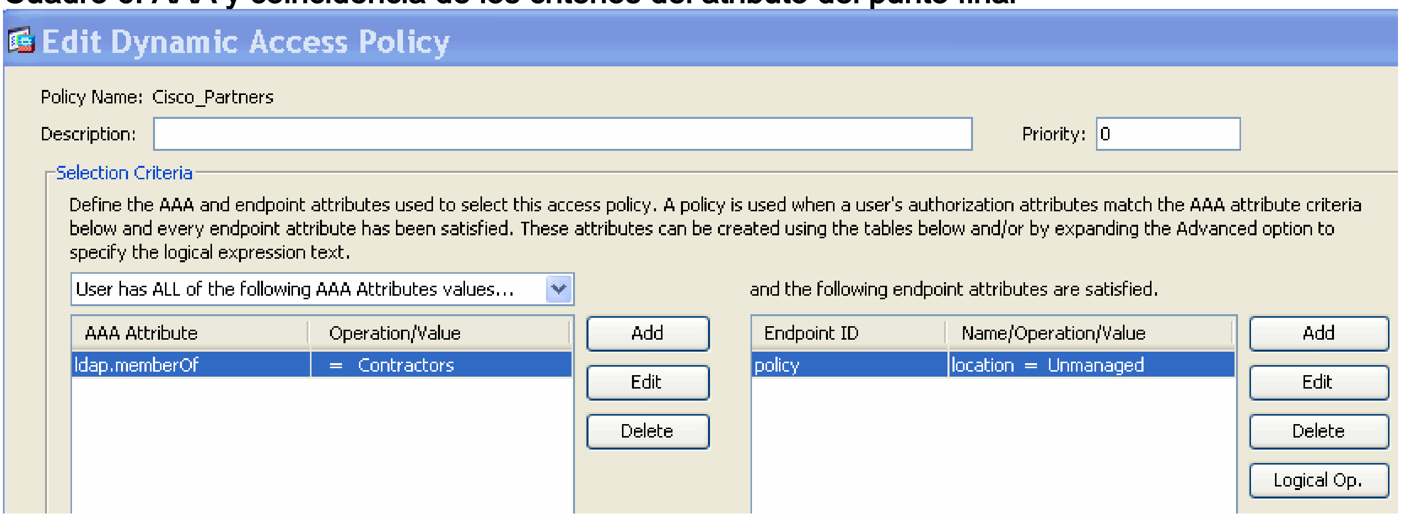


Figura 5b. Criterios del atributo del punto final



Así, hacer juego el expediente DAP mostrado en el cuadro 6, el usuario de autenticidad debe ser un miembro del grupo del Active Directory de los contratistas y su punto final de conexión debe satisfacer el valor de directiva CSD “sin cambiar,” para ser asignado el expediente DAP.

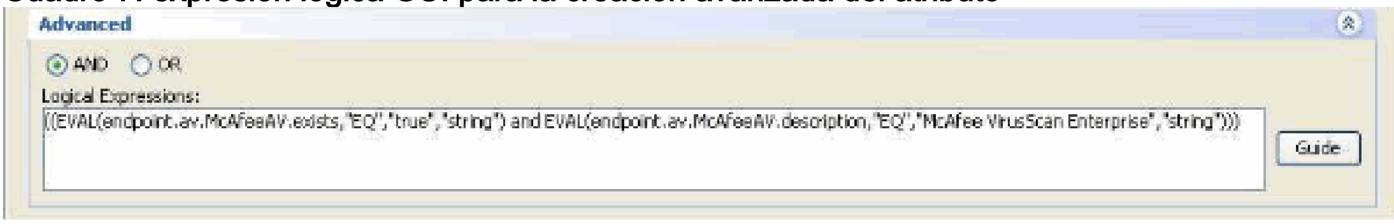
Cuadro 6. AAA y coincidencia de los criterios del atributo del punto final



El AAA y los atributos del punto final se pueden crear usando las tablas según lo descrito en el cuadro 6 y/o ampliando la opción avanzada para especificar una expresión lógica tal y como se muestra en del cuadro 7. Actualmente, la expresión lógica se construye con las funciones EVAL, por ejemplo, EVAL (endpoint.av.McAfeeAV.exists, “EQ”, “verdad”, “cadena”) y EVAL (endpoint.av.McAfeeAV.description, “EQ”, “empresa de VirusScan del McAfee”, “cadena”), que representan las operaciones lógicas de la selección AAA y/o del punto final.

Las expresiones lógicas son útiles para agregar el Criterio de selección con excepción de cuál es posible en las áreas del atributo AAA y del punto final arriba. Por ejemplo, mientras que usted puede configurar los dispositivos de seguridad para utilizar los atributos AAA que no satisfacen ningunos, todos los o ningunos criterios especificados, los atributos del punto final son acumulativos, y deben todos ser satisfechos. Para dejar el dispositivo de seguridad emplear un atributo u otro del punto final, usted necesita crear las expresiones lógicas apropiadas bajo sección avanzada del expediente DAP.

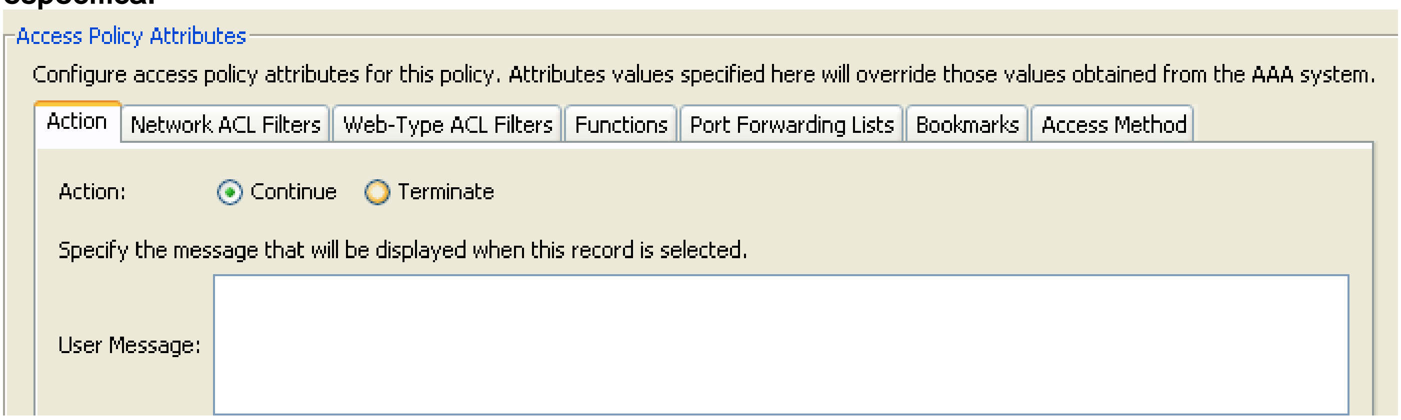
Cuadro 7. expresión lógica GUI para la creación avanzada del atributo



La sección de los atributos de la política de acceso tal y como se muestra en del cuadro 8 es donde un administrador configuraría los atributos del acceso VPN para un expediente específico DAP. Cuando los atributos de la autorización de un usuario hacen juego los criterios AAA, del punto final y/o de la expresión lógica; los valores de atributo de la política del acceso configurado en esta sección serán aplicados. Los valores de atributo especificados aquí reemplazarán esos valores obtenidos del sistema AAA, incluyendo ésos en el usuario, el grupo, el grupo de túnel, y los expedientes de grupo predeterminado existentes.

Un expediente DAP tiene un conjunto limitado de valores de atributo que puedan ser configurados. Estos valores bajan bajo lenguetas siguientes tal y como se muestra en de los cuadros 8 a 14:

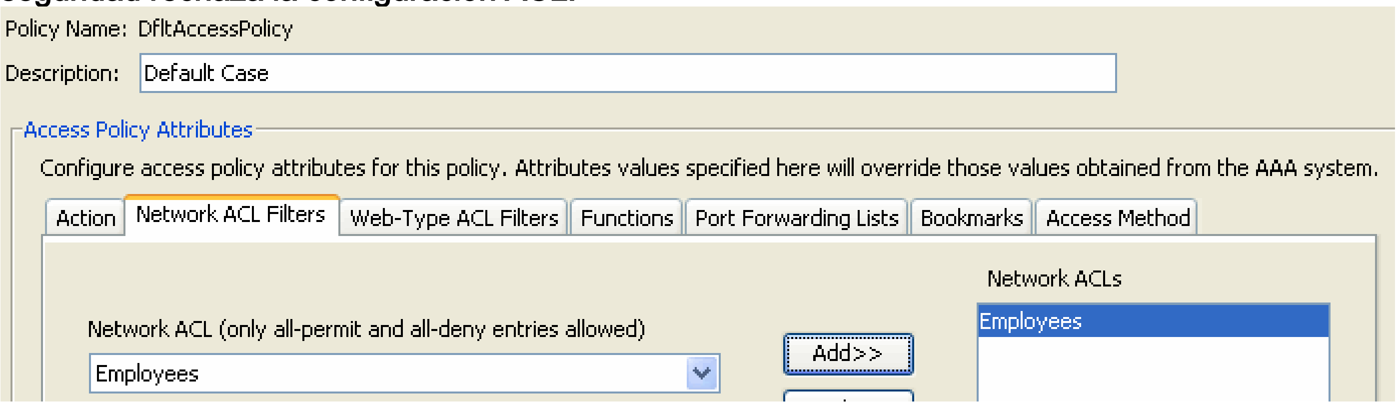
Cuadro 8. acción — Especifica el proceso especial a aplicarse a una conexión o a una sesión específica.



- Continúe — (predeterminado) haga clic para aplicar los atributos de la política de acceso a la sesión.
- Termine — Haga clic para terminar la sesión.
- Mensaje del usuario — Ingrese un mensaje de texto para visualizar en la página porta cuando se selecciona este expediente DAP. Caracteres máximos 128. Presentaciones del mensaje

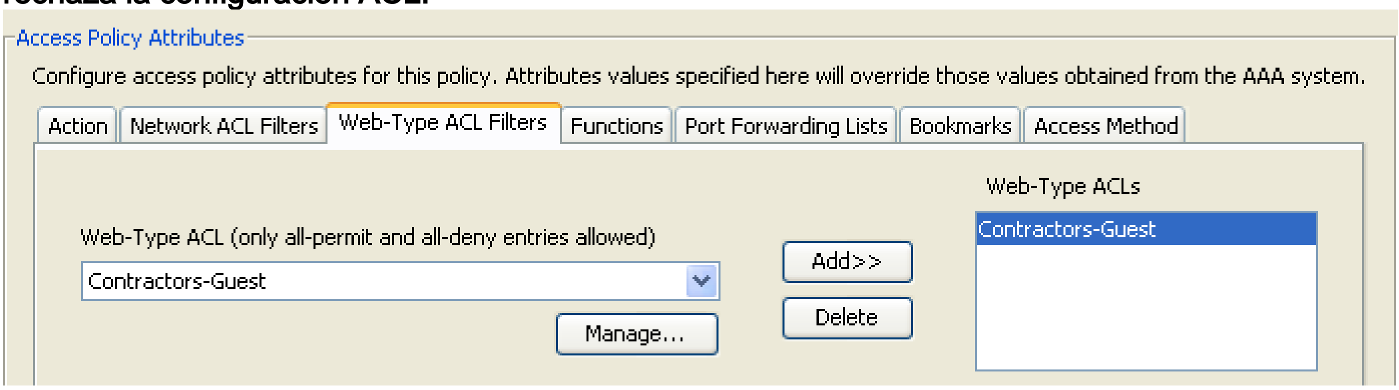
de un usuario como orbe amarillo. Cuando un usuario abre una sesión, centella tres veces de atraer la atención, y entonces todavía está. Si se seleccionan varios expedientes DAP, y cada uno de ellos tiene un mensaje del usuario, toda la visualización de mensajes del usuario. Además, usted puede incluir en los tales mensajes los URL o el otro texto integrado, que requieren que usted utilice las etiquetas HTML correctas.

Cuadro 9. lengueta de los filtros de la red ACL — Le deja seleccionar y configurar la red ACL para aplicarse a este expediente DAP. Un ACL para el DAP puede contener las reglas del permit or deny, pero no ambas. Si un ACL contiene el permiso y niega las reglas, el dispositivo de seguridad rechaza la configuración ACL.



- Casilla desplegable de la red ACL — Seleccione ya la red configurada ACL para agregar a este expediente DAP. Solamente los ACL que hacen que todos permitan o todos niegan las reglas son elegibles, y éstos son los únicos ACL que visualizan aquí.
- Maneje — Haga clic para agregar, para editar, y para borrar la red ACL.
- Lista de la red ACL — Visualiza la red ACL para este expediente DAP.
- Agregue — Haga clic para agregar la red seleccionada ACL de la casilla desplegable a la lista de la red ACL a la derecha.
- Cancelación — Haga clic para borrar una red resaltada ACL de la lista de la red ACL. Usted no puede borrar un ACL si se asigna a un DAP o a otro expediente.

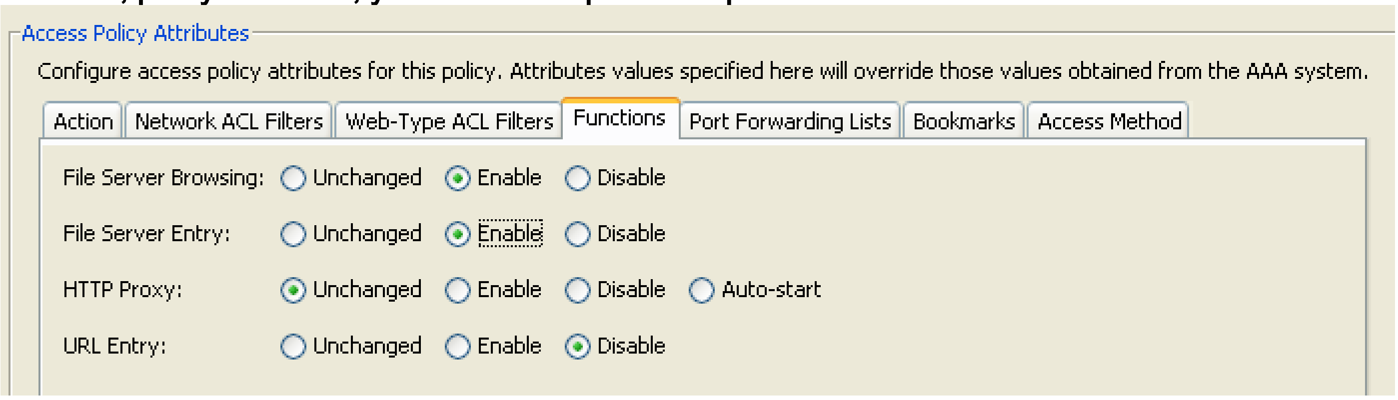
Cuadro 10. lengueta de los filtros del Red-tipo ACL — Le deja seleccionar y configurar el red-tipo ACL aplicarse a este expediente DAP. Un ACL para el DAP puede contener solamente las reglas del permit or deny. Si un ACL contiene el permiso y niega las reglas, el dispositivo de seguridad rechaza la configuración ACL.



- Casilla desplegable del Red-tipo ACL — Seleccione el red-tipo ya configurado ACL agregar a este expediente DAP. Solamente los ACL que hacen que todos permitan o todos niegan las reglas son elegibles, y éstos son los únicos ACL que visualizan aquí.
- Maneje… — Haga clic para agregar, para editar, y para borrar el red-tipo ACL.
- Lista del Red-tipo ACL — Visualiza el red-tipo ACL para este expediente DAP.

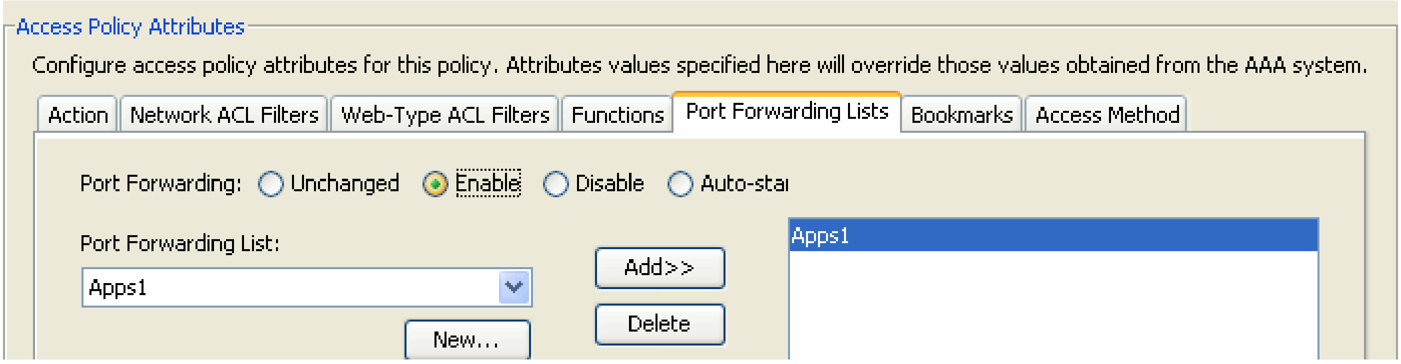
- Agregue — Haga clic para agregar el red-tipo seleccionado ACL de la casilla desplegable a la lista del Red-tipo ACL a la derecha.
- Cancelación — Haga clic para borrar un red-tipo ACL de la lista del Red-tipo ACL. Usted no puede borrar un ACL si se asigna a un DAP o a otro expediente.

Cuadro 11 lengueta de las funciones — Le deja configurar la entrada y ojeada del servidor de archivos, proxy de HTTP, y entrada URL para el expediente DAP.



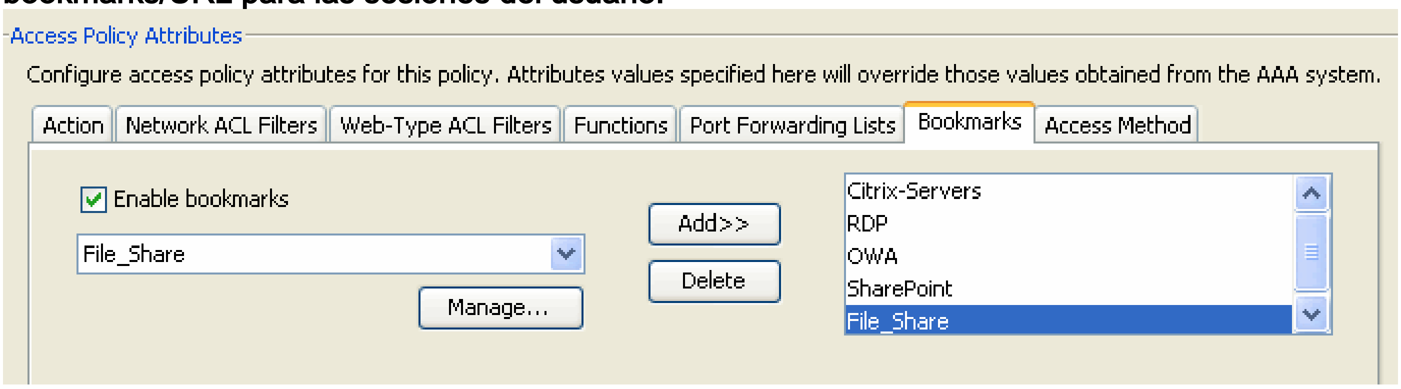
- Servidor de archivos que hojea — Permisos o neutralizaciones CIFS que hojean para los servidores de archivos o las características de la parte.
- Entrada del servidor de archivos — Permite o niega a un usuario de ingresar las trayectorias y los nombres del servidor de archivos en la página porta. Cuando está habilitado, coloca el cajón de la entrada del servidor de archivos en la página porta. Los usuarios pueden ingresar las cadenas de caracteres a los archivos de Windows directamente. Pueden descargar, editar, borrar, retitular, y mover los archivos. Pueden también agregar los archivos y las carpetas. Las partes se deben también configurar para el acceso del usuario en los servidores aplicables de Microsoft Windows. Los usuarios pudieron tener que ser autenticado antes de acceder los archivos, dependiendo de los requisitos de la red.
- Proxy de HTTP — Afecta a la expedición de un proxy del applet HTTP al cliente. El proxy es útil para las Tecnologías que interfieren con la transformación de contenido apropiada, tal como Javas, ActiveX, y Flash. Desvía la destrucción/el proceso de la reescritura mientras que asegura el uso continuo del dispositivo de seguridad. El proxy remitido modifica la vieja configuración de representación del navegador automáticamente y reorienta todas las peticiones HTTP y HTTPS a la nueva configuración de representación. Soporta virtualmente todas las Tecnologías del lado del cliente, incluyendo el HTML, el CSS, el Javascript, VBScript, ActiveX, y las Javas. El único navegador que soporta es Microsoft Internet Explorer.
- Entrada URL — Permite o evita que un usuario ingrese HTTP/HTTPS URL en la página porta. Si se habilita esta característica, los usuarios pueden ingresar a las direcciones Web en el rectángulo de la entrada URL, y utilizan el clientless SSL VPN para acceder esos Web site.
- Sin cambiar — (predeterminado) haga clic para utilizar los valores de la directiva del grupo que se aplica a esta sesión.
- Permiso/neutralización — Haga clic para habilitar o para inhabilitar la característica.
- Autoempezado — Tecleo para habilitar el proxy de HTTP y para hacer que el expediente DAP automáticamente comience los applet asociados a estas características.

Figura 12. Lengueta de las listas de la expedición del puerto — Le deja seleccionar y configurar la expedición del puerto enumera para las sesiones del usuario.



- Expedición del puerto — Seleccione una opción para las listas de la expedición del puerto que se aplican a este expediente DAP. Los otros atributos en este campo se habilitan solamente cuando usted set port que remite para habilitar o autoempezado.
- Sin cambiar — Haga clic para utilizar los valores de la directiva del grupo que se aplica a esta sesión.
- Permiso/neutralización — Tecleo para habilitar o para inhabilitar la expedición del puerto.
- Autoempezado — El tecleo para habilitar la expedición del puerto, y para hacer que el expediente DAP automáticamente comience los applet de la expedición del puerto asociados a su expedición del puerto enumera.
- Casilla desplegable de la lista de la expedición del puerto — Seleccione ya las listas de la expedición del puerto configurado para agregar al expediente DAP.
- Nuevo — Tecleo para configurar las nuevas listas de la expedición del puerto.
- Listas de la expedición del puerto — Visualiza la lista de la expedición del puerto para el expediente DAP.
- Agregue — Haga clic para agregar la lista de la expedición del puerto seleccionado de la casilla desplegable a la lista de la expedición del puerto a la derecha.
- Cancelación — Haga clic para borrar la lista de la expedición del puerto seleccionado de la lista de la expedición del puerto. Usted no puede borrar un ACL si se asigna a un DAP o a otro expediente.

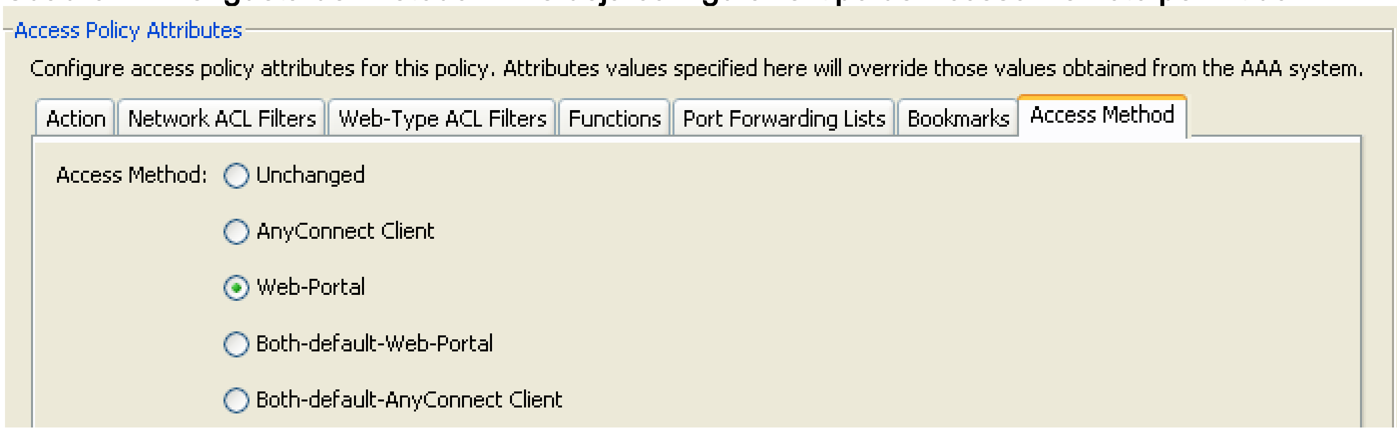
Cuadro 13. Lengueta de los marcadores — Le deja seleccionar y configurar las listas bookmarks/URL para las sesiones del usuario.



- Marcadores del permiso — Tecleo a habilitar. cuando este cuadro no se selecciona, ninguna visualización de las listas del marcador en la página porta para la conexión
- Maneje — Haga clic para agregar, para importar, para exportar, y las listas del marcador de la cancelación.
- Listas de los marcadores (descenso-abajo) — Visualiza las listas del marcador para el expediente DAP.
- Agregue — Haga clic para agregar la lista seleccionada del marcador de la casilla

desplegable al cuadro de lista del marcador a la derecha.
- Cancelación — Tecleo para borrar la lista seleccionada del marcador del cuadro de lista del marcador. Usted no puede borrar una lista del marcador del dispositivo de seguridad a menos que usted primero lo borre de los expedientes DAP.

Cuadro 14. Lengueta del método — Le deja configurar el tipo de Acceso Remoto permitido.



- Sin cambiar — Continúe con el método de Acceso Remoto actual fijado en la grupo-directiva para la sesión.
- Cliente de AnyConnect — Conecte usando el Cliente Cisco AnyConnect VPN.
- Portal web — Conecte con el clientless VPN.
- Ambo-valor por Defecto-Red-porta — Conecte vía el clientless o el cliente de AnyConnect, con un valor por defecto del clientless.
- cliente del Ambo-valor por defecto-AnyConnect — Conecte vía el clientless o el cliente de AnyConnect, con un valor por defecto de AnyConnect.

Según lo mencionado previamente, un expediente DAP tiene un conjunto limitado de valores de atributo predeterminados, sólo si se modifican tomarán la precedencia sobre el AAA existente, el usuario, el grupo, el grupo de túnel, y los expedientes de grupo predeterminado. Si los valores de atributo adicionales fuera del ámbito del DAP se requieren, por ejemplo, las listas del Túnel dividido, los banners, los túneles elegantes, los arreglos para requisitos particulares porta,… etc, entonces necesitarán ser aplicados vía el AAA, el usuario, el grupo, el grupo de túnel, y los expedientes de grupo predeterminado. En este caso, esos valores de atributo específicos complementarán el DAP y no lo reemplazarán. Así, el usuario conseguirá un conjunto acumulativo de los valores de atributo a través de todos los expedientes.

Agregación de las directivas múltiples del acceso dinámico

Un administrador puede configurar los expedientes múltiples DAP para dirigir muchas variables. Como consecuencia, es posible que un usuario de autenticidad satisfaga el AAA y los criterios del atributo del punto final de los expedientes múltiples DAP. En la consecuencia, los atributos de la política de acceso serán constantes o estarán en conflicto en estas directivas. En este caso, el usuario autorizado conseguirá el resultado acumulativo a través de todos los expedientes correspondidos con DAP.

Esto también incluye los valores de atributo único aplicados vía la autenticación, la autorización, el usuario, el grupo, el grupo de túnel, y los expedientes de grupo predeterminado. El resultado acumulativo de los atributos de la política de acceso crea la directiva del acceso dinámico. Los ejemplos de los atributos combinados de la política de acceso se enumeran en las tablas abajo. Estos ejemplos representan los resultados de 3 expedientes combinados DAP.

El atributo de la acción mostrado en el cuadro 1 tiene un valor que sea termine o continúe. El valor de atributo agregado será termina si el valor del terminal se configura en los expedientes seleccionados uces de los DAP y continuar si el valor de la continuación se configura en todos los expedientes seleccionados DAP.

Atributo de la acción del cuadro 1.

Nombre del atributo	DAP#1	DAP#2	DAP#3	DAP
Acción (ejemplo 1)	continúe	continúe	continúe	continúe
Acción (ejemplo 2)	Termine	continúe	continúe	termine

El atributo del usuario-mensaje mostrado en el cuadro 2 contiene un valor de la cadena. El valor de atributo agregado será una cadena separada del avance de línea (valor hex 0x0A) creada conectando juntos los valores de atributo de los expedientes seleccionados DAP. El ordenar de los valores de atributo en la cadena combinada es insignificante.

Atributo del Usuario-mensaje del cuadro 2.

Nombre del atributo	DAP#1	DAP#2	DAP#3	DAP
usuario-mensaje	el rápido	zorro marrón	Saltos encima	los fox<LF>jumps del quick<LF>brown encima

La característica del clientless que habilita los atributos (funciones) mostrados en el cuadro 3 contiene los valores que son autoempezado, habilita o inhabilita. El valor de atributo agregado será autoempezado si el valor del autoempezado se configura en los expedientes seleccionados uces de los DAP.

El valor de atributo agregado será permiso si no hay valor del autoempezado configurado en los expedientes seleccionados uces de los DAP, y el valor del permiso se configura en por lo menos uno de los expedientes seleccionados DAP.

El valor de atributo agregado será neutralización si no hay valor del autoempezado o del permiso configurado en los expedientes seleccionados uces de los DAP, y el valor de la “neutralización” se configura en por lo menos uno de los expedientes seleccionados DAP.

Característica del clientless del cuadro 3. habilitando los atributos (funciones)

Nombre del atributo	DAP#1	DAP#2	DAP#3	DAP
puerto-delantero	permiso	inhabilitar		permiso
ARCHIVO-ojeada	inhabilitar	permiso	inhabilitar	permiso

entrada de archivo			inhabilitar	inhabilitar
HTTP-proxy	inhabilitar	autoempezado	inhabilitar	autoempezado
URL-entrada	inhabilitar		permiso	permiso

La lista url y los atributos puerto-delanteros mostrados en el cuadro 4 contienen un valor que sea una cadena o una cadena separada coma. El valor de atributo agregado será una cadena separada coma creada conectando juntos los valores de atributo de los expedientes seleccionados DAP. Ningunos valor de atributo duplicado en la cadena combinada serán quitados. El ordenar de los valores de atributos en la cadena combinada es insignificante.

La lista url y el puerto del cuadro 4. remiten el List Attribute

Nombre del atributo	DAP#1	DAP#3	DAP#3	DAP
lista url	a	b, c	a	a, b, c
puerto-delantero		d, e	e, f	d, e, f

Los atributos del método de acceso especifican el método de acceso al cliente permitido para las conexiones VPN SSL. El método de acceso al cliente puede ser acceso al cliente de AnyConnect solamente, del portal web del acceso acceso solamente, del cliente de AnyConnect o del portal web con el acceso del portal web como el acceso del valor por defecto o del cliente o del portal web de AnyConnect con el acceso al cliente de AnyConnect como el valor por defecto. El valor de atributo agregado se resume en el cuadro 5.

Atributos del método de acceso del cuadro 5.

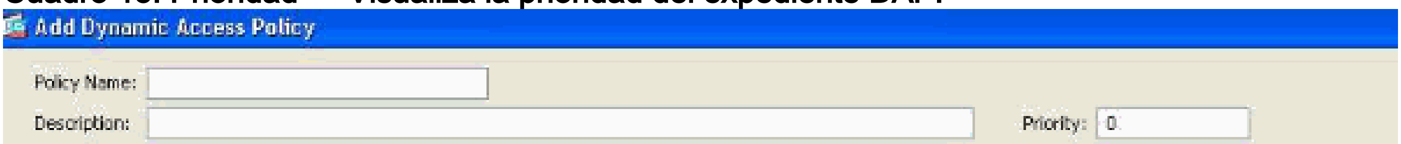
Valores de atributo seleccionados				Resultado de la agregación
Cliente de AnyConnect	**Portal web**	**Portal de la Ambo-valor por defecto-red**	**cliente del Ambo-valor por defecto-AnyConnect**	
			X	cliente del Ambo-valor por defecto-AnyConnect
		X		Ambo-valor por Defecto-Red-porta
		X	X	Ambo-valor por Defecto-Red-porta
	X			Portal web
	X		X	cliente del Ambo-valor por defecto-AnyConnect
	X	X		Ambo-valor por

				Defecto-Red-porta
	X	X	X	Ambo-valor por Defecto-Red-porta
X				Cliente de AnyConnect
X			X	cliente del Ambo-valor por defecto-AnyConnect
X		X		Ambo-valor por Defecto-Red-porta
X		X	X	Ambo-valor por Defecto-Red-porta
X	X			Ambo-valor por Defecto-Red-porta
X	X		X	cliente del Ambo-valor por defecto-AnyConnect
X	X	X		Ambo-valor por Defecto-Red-porta
X	X	X	X	Ambo-valor por Defecto-Red-porta

Al agregar los atributos del filtro de la red (Firewall) y del Red-tipo (clientless) ACL, la prioridad y DAP ACL DAP sea dos componentes importantes a considerar.

El atributo de prioridad tal y como se muestra en del cuadro 15 no se agrega. El dispositivo de seguridad utiliza este valor para ordenar lógicamente las Listas de acceso al agregar la red y el Red-tipo ACL de los expedientes múltiples DAP. El dispositivo de seguridad pide los expedientes de lo más arriba posible al número de prioridad más bajo, con lo más bajo posible en la parte inferior de la tabla. Por ejemplo, un expediente DAP con un valor de 4 tiene una prioridad más alta que un expediente con un valor de 2. Usted no puede clasificarlos manualmente.

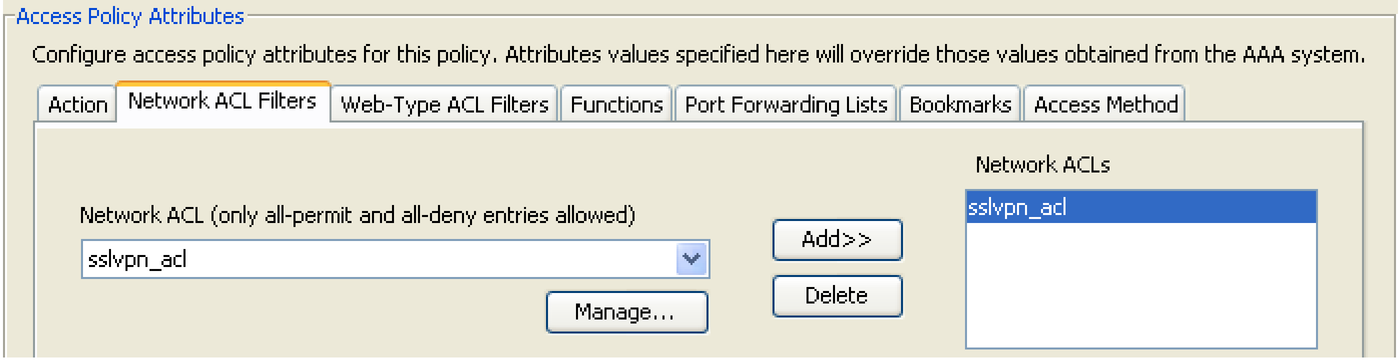
Cuadro 15. Prioridad — Visualiza la prioridad del expediente DAP.



- Nombre de la directiva — Visualiza el nombre del expediente DAP.
- Descripción — Describe el propósito del expediente DAP.

El atributo DAP ACL soporta solamente las listas de acceso que se ajustan a “Blanco-lista” o a un modelo estricto estricta ACL de la “lista negra”. En un modelo ACL de la “Blanco-lista”, las entradas de lista de acceso especifican las reglas que “permita” el acceso a las redes específicadas o a los host. En un modo ACL de la “lista negra”, las entradas de lista de acceso especifican las reglas que “niegue” a acceso a las redes específicadas o a los host. Una lista de acceso no conforme contiene las entradas de lista de acceso con una mezcla de “permiso” y “niegue” las reglas. Si una lista de acceso no conforme se configura para un expediente DAP, será rechazada como Error de configuración cuando el administrador intenta agregar el expediente. Si una lista de acceso de conformación se asigna a un expediente DAP, después cualquier modificación a la lista de acceso que cambia la característica de la conformidad será rechazada como Error de configuración.

Cuadro 16. DAP ACL — Le deja seleccionar y configurar la red ACL para aplicarse a este expediente DAP.



Cuando se seleccionan los expedientes múltiples DAP, los atributos de las listas de acceso especificados en la red (Firewall) ACL se agregan para crear una lista de acceso dinámica para el Firewall ACL DAP. De la misma manera, los atributos de las listas de acceso especificados en el Red-tipo (clientless) ACL se agregan para crear una lista de acceso dinámica para el clientless ACL DAP. El ejemplo abajo se centrará en cómo una lista de acceso dinámica del Firewall DAP se crea específicamente. Sin embargo, una lista de acceso dinámica del clientless DAP seguirá el mismo proceso.

Primero, el ASA creará dinámicamente un nombre único para el DAP RED-ACL tal y como se muestra en del cuadro 6.

Nombre dinámico del cuadro 6. DAP Red-ACL

Nombre DAP Red-ACL
DAP-Red-ACL-x (donde está un número entero X que incrementará para asegurar la unicidad)

En segundo lugar, el ASA extraerá el atributo Red-ACL de los expedientes seleccionados DAP tal y como se muestra en del cuadro 7.

Red ACL del cuadro 7.

Expedientes seleccionados DAP	Prioridad	Red-ACL	Entradas Red-ACL
DAP 1	1	101 y 102	El ACL 101 hace que 4 nieguen las reglas y el ACL 102 tiene 4 reglas del permiso
DAP 2	2	201 y 202	El ACL 201 tiene 3 reglas del permiso y el ACL 202

			hace que 3 nieguen las reglas
DAP 3	2	101 y 102	El ACL 101 hace que 4 nieguen las reglas y el ACL 102 tiene 4 reglas del permiso

Tercero, el ASA reordenará los Red-ACL primero por el número de prioridad del expediente DAP, y entonces por la lista negra primero si el valor de prioridad para expedientes 2 o seleccionada DAP son lo mismo. Después de esto, el ASA entonces extraerá las entradas Red-ACL de cada Red-ACL tal y como se muestra en del cuadro 8.

Prioridad del expediente del cuadro 8. DAP

Red-ACL	Prioridad	Modelo blanco/del negro de la lista de acceso	Entradas Red-ACL
101	2	Lista negra	4 niegue las reglas (DDDD)
202	2	Lista negra	3 niegue las reglas (el DDD)
102	2	Blanco-lista	4 reglas del permiso (PPPP)
202	2	Blanco-lista	3 reglas del permiso (PPP)
101	1	Lista negra	4 niegue las reglas (DDDD)
102	1	Blanco-lista	4 reglas del permiso (PPPP)

Pasado, el ASA combinará las entradas Red-ACL en el Red-ACL dinámicamente generado y después volverá el nombre del Red-ACL dinámico como el nuevo Red-ACL que se aplicará tal y como se muestra en del cuadro 9.

Cuadro 9. DAP dinámico Red-ACL

Nombre DAP Red-ACL	Entrada Red-ACL
DAP-Network-ACL-1	DDD PPPP PPP DDDD PPPP DDDD

Implementación DAP

Hay un host de las razones por las que un administrador debe considerar implementar el DAP. Algunas razones subyacentes son cuando la evaluación de la postura sobre un punto final debe ser aplicada, y/o cuando un AAA más granular o los atributos de la política debe ser considerado cuando autoriza el acceso del usuario a los recursos de red. En el ejemplo abajo, configuraremos el DAP y sus componentes para identificar un punto final de conexión y para autorizar el acceso del usuario a los diversos recursos de red.

Caso de prueba – Un cliente ha pedido un proof-of-concept con los requisitos siguientes del acceso VPN:

- La capacidad de detectar y de identificar un punto final de los empleados según lo manejado o Unmanaged. — Si el punto final se identifica como manejado (trabajo PC) pero falla los requisitos de la postura, ese punto final se debe entonces negar el acceso. Por otra parte, si el punto final del empleado se identifica como unmanaged (el PC casero), ese punto final se debe entonces conceder el acceso del clientless.
- La capacidad de invocar la limpieza de las sesiones Cookie y de ocultarla cuando una conexión del clientless termina.
- La capacidad de detectar y de aplicar las aplicaciones corrientes en los puntos finales de los empleados manejados, tales como antivirus del McAfee. Si no existe la aplicación, ese punto final se debe entonces negar el acceso.
- La capacidad de utilizar la autenticación AAA para determinar a lo que deben tener los usuarios autorizados de los recursos de red acceso. El dispositivo de seguridad debe soportar la autenticación Idap nativa MS y soportar los papeles múltiples de la membresía del grupo LDAP.
- La capacidad de permitir el acceso del LAN local a los recursos de red tales como faxes e impresoras de la red cuando estaba conectada vía un "cliente/una red" basó la conexión.
- La capacidad de proporcionar autorizó el acceso de invitado a los contratistas. Los contratistas y sus puntos finales deben conseguir el acceso del clientless, y su acceso porta a las aplicaciones debe limitado con respecto a un empleado.

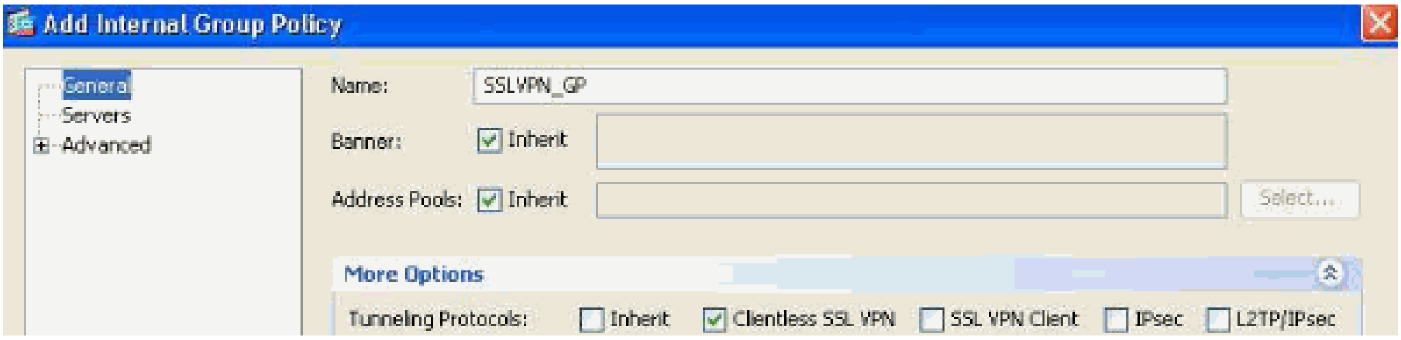
En este ejemplo, ejecutaremos una serie de pasos para la configuración en un esfuerzo para cumplir los requisitos del acceso VPN del cliente. Habrá los pasos para la configuración que son necesarios pero relacionados no no directamente con el DAP mientras que otras configuraciones serán relacionadas directamente con el DAP. El ASA es muy dinámico y puede adaptarse en muchos entornos de red. Como consecuencia, las soluciones de VPN pueden ser definidas en las distintas maneras y proporcionar en algunos casos la misma solución del extremo. El acercamiento tomado sin embargo es conducido por las necesidades y sus entornos de los clientes.

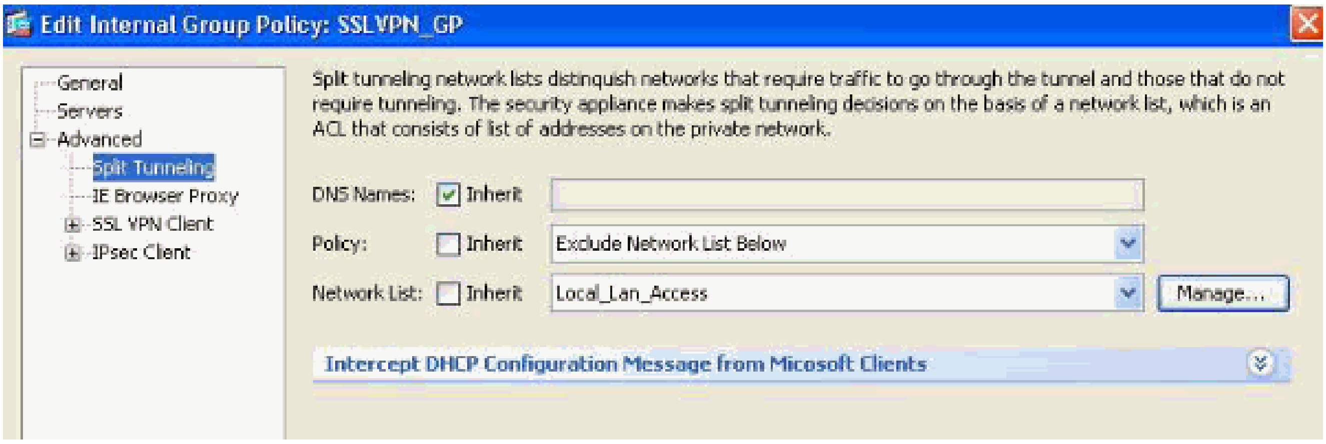
De acuerdo con la naturaleza de este papel y de los requisitos de cliente definidos, utilizaremos al Administrador de dispositivos de seguridad adaptante (ASDM) 6.0(x) y enfocaremos la mayor parte de nuestras configuraciones alrededor del DAP. Sin embargo, también configuraremos las directivas del grupo local para mostrar cómo el DAP puede complementar y/o reemplazar los atributos de la política local. Para la base de este caso de prueba, asumiremos a un grupo de servidor LDAP, lista de red con tunelización dividida y la conectividad de IP básica, incluyendo las agrupaciones IP y el grupo de servidores de DefaultDNS, se preconfigura.

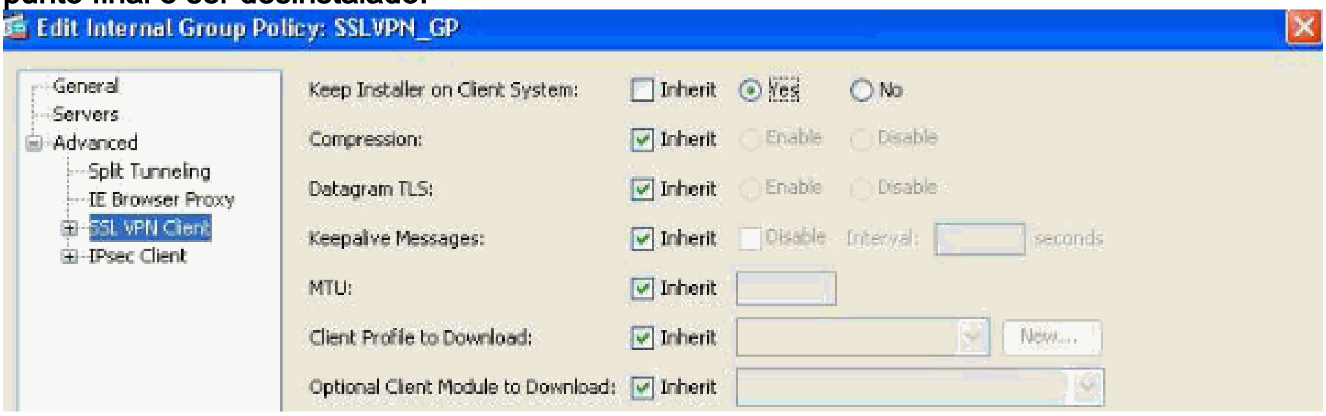
Definiendo una directiva del grupo — esta configuración es necesaria para definir los atributos de la política local. Algunos atributos definidos aquí no son configurables en el DAP para (ejemplo, acceso del LAN local). (Esta directiva también será utilizada para definir el clientless y los atributos basados cliente).

Navegue a la **configuración > al VPN de acceso remoto > las directivas al acceso > al grupo de la red (cliente)**, y agregue un Internal group policy (política grupal interna) haciendo el siguiente:

Cuadro 17. Directiva del grupo — Define los atributos específicos locales VPN.



1. Conforme al link general, configure el nombre **SSLVPN_GP** para la directiva del grupo.
2. También conforme al link general, haga clic **más opciones** y configure solamente el Tunneling Protocol: **Clientless SSLVPN**. (Configuraremos el DAP para reemplazar y para manejar el método de acceso.)
3. Bajo el avanzado > el link del Túnel dividido, configura el siguiente:**Cuadro 18. Túnel dividido — Permite que el tráfico especificado (red local) desvíe un túnel unencrypted durante una conexión cliente.**


Directiva: Desmarque **heredan** y selecto **excluya la lista de red abajo**.Lista de red: Desmarque **heredan** y seleccionan el nombre de la lista **Local_Lan_Access**. (Asumido preconfigurado.)
4. Bajo el avanzado > el link del cliente VPN SSL, configura el siguiente:**Cuadro 19. Instalador del cliente VPN SSL — Sobre la terminación VPN, el cliente SSL puede permanecer en el punto final o ser desinstalado.**


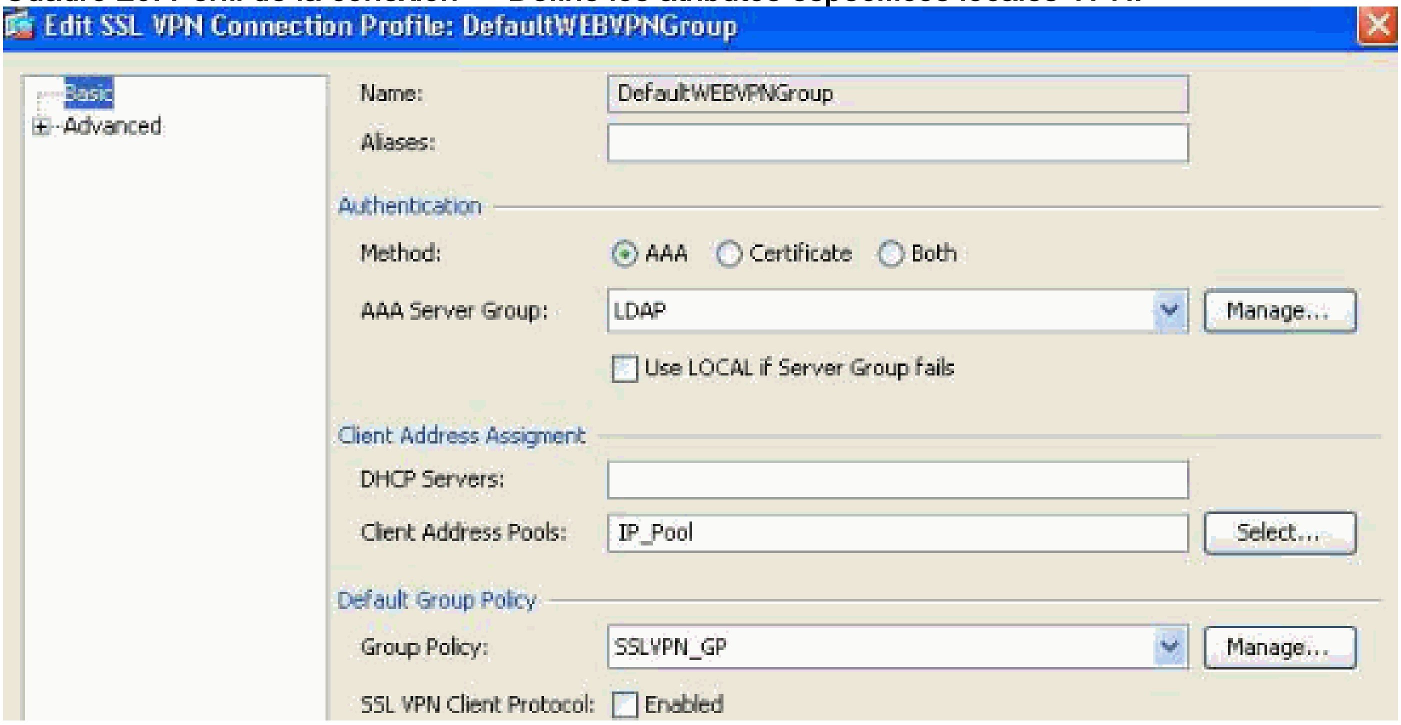
5. Guarde el instalador en el sistema del cliente: Desmarque **heredan** y después seleccionan **sí**.
6. El Haga Click en OK entonces **se aplica**.
7. Aplique sus cambios de configuración.

Definiendo un perfil de la conexión — esta configuración es necesaria para definir nuestro método de autenticación AAA, por ejemplo LDAP y aplicación de la directiva previamente configurada del

grupo (SSLVPN_GP) a este perfil de la conexión. Sujetarán a los usuarios que conectan vía este perfil de la conexión a los atributos definidos aquí así como a los atributos definidos en la directiva del grupo SSLVPN_GP. (Este perfil también será utilizado para definir el clientless y los atributos basados cliente).

Navegue a los **perfiles de la conexión VPN de la configuración > del acceso >SSL del VPN de acceso remoto > de la red (cliente)** y configure el siguiente:

Cuadro 20. Perfil de la conexión — Define los atributos específicos locales VPN.

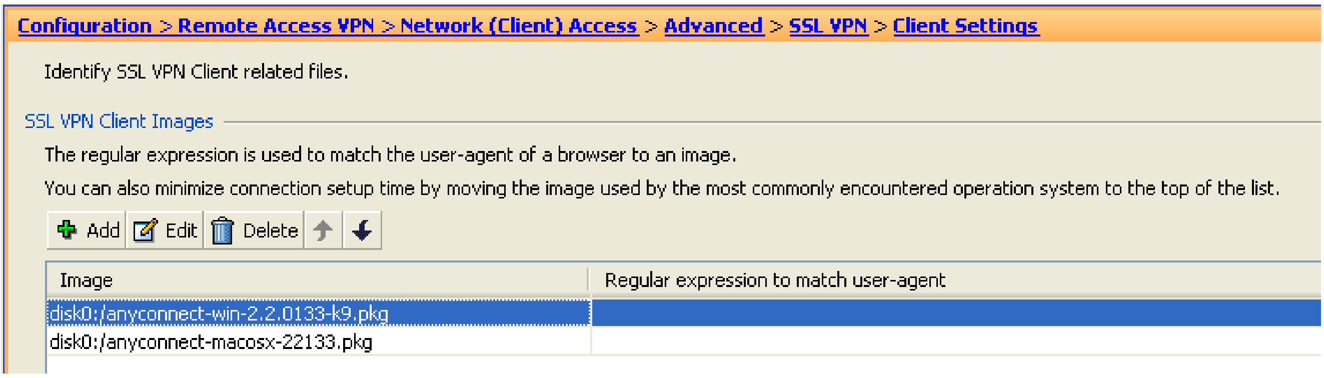


1. Bajo perfiles de la conexión seccione, edite el DefaultWEBVPNGroup y bajo configuración básica del link el siguiente:Método de autentificación: **AAA**Autenticación — Grupo de servidores AAA: **LDAP** (presunto preconfigurado)Asignación de dirección cliente — Pools de la dirección cliente: **IP_Pool** (presunto preconfigurado)Directiva del grupo de políticas del grupo predeterminado: Seleccione **SSLVPN_GP**
2. Aplique sus cambios de configuraciones.

Definiendo una interfaz IP para la conectividad VPN SSL — Esta configuración es necesaria para terminar las conexiones SSL del cliente y del clientless en una interfaz especificada.

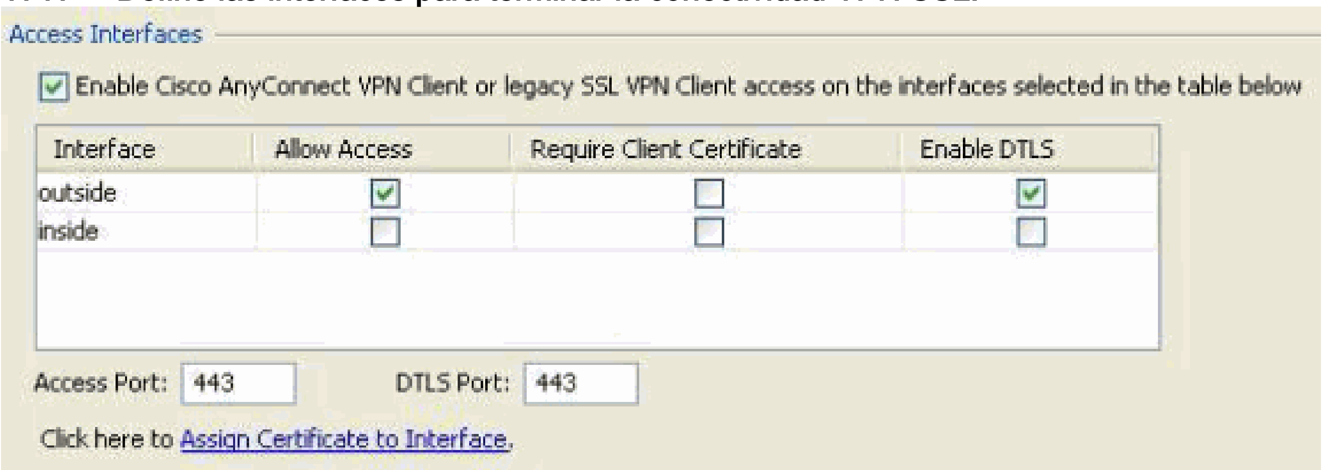
Antes de habilitar el acceso del /Network del cliente en una interfaz, usted debe primero definir una imagen del cliente VPN SSL.

1. Navegue a la **configuración > al acceso del VPN de acceso remoto > de la red (cliente) > avanzó > SSL VPN > las configuraciones del cliente**, y agregan la imagen siguiente del cliente VPN SSL del sistema de archivos Flash ASA: (Esta imagen se puede descargar del CCO, www.cisco.com)**Cuadro 21. La imagen del cliente VPN SSL instala — Define la imagen del cliente SSLVPN (AnyConnect) que se avanzará a los puntos finales de conexión.**



anyconnect-win-2.x.xxx-k9.pkg El Haga Click en OK, **AUTORIZACIÓN** otra vez, y entonces **se aplica**.

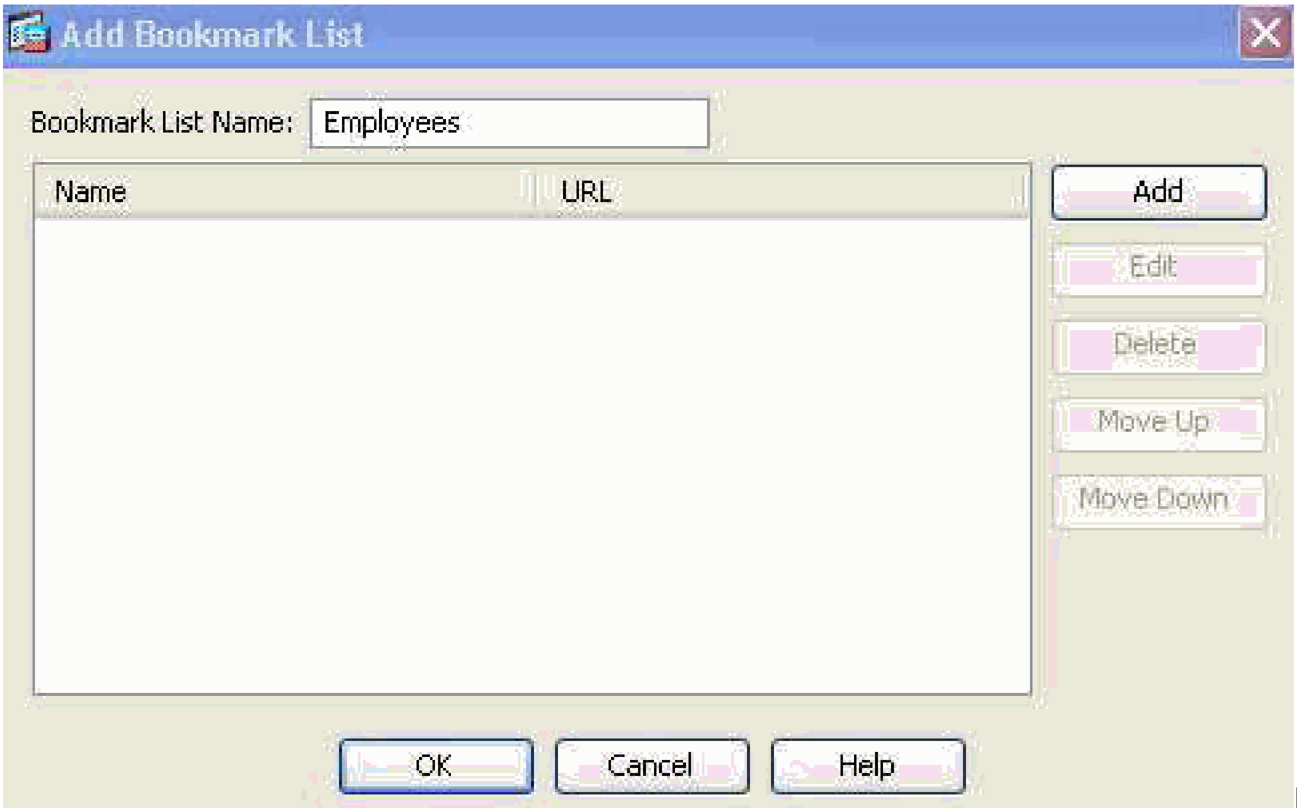
2. **Navegue a la configuración > al acceso del VPN de acceso remoto > de la red (cliente) > los perfiles a la conexión VPN SSL**, y habilite el siguiente:**Cuadro 22. Interfaz de acceso SSL VPN — Define las interfaces para terminar la conectividad VPN SSL.**



Bajo sección de la interfaz de acceso, permiso: **“Habilite el acceso del Cliente Cisco AnyConnect VPN o de cliente VPN de la herencia SSL en las interfaces seleccionadas en la tabla abajo.”**También bajo interfaces de acceso seccione, control **permiten el acceso** en la interfaz exterior. (Esta configuración también habilitará el acceso del clientless SSL VPN en la interfaz exterior.)Haga clic en Apply (Aplicar).

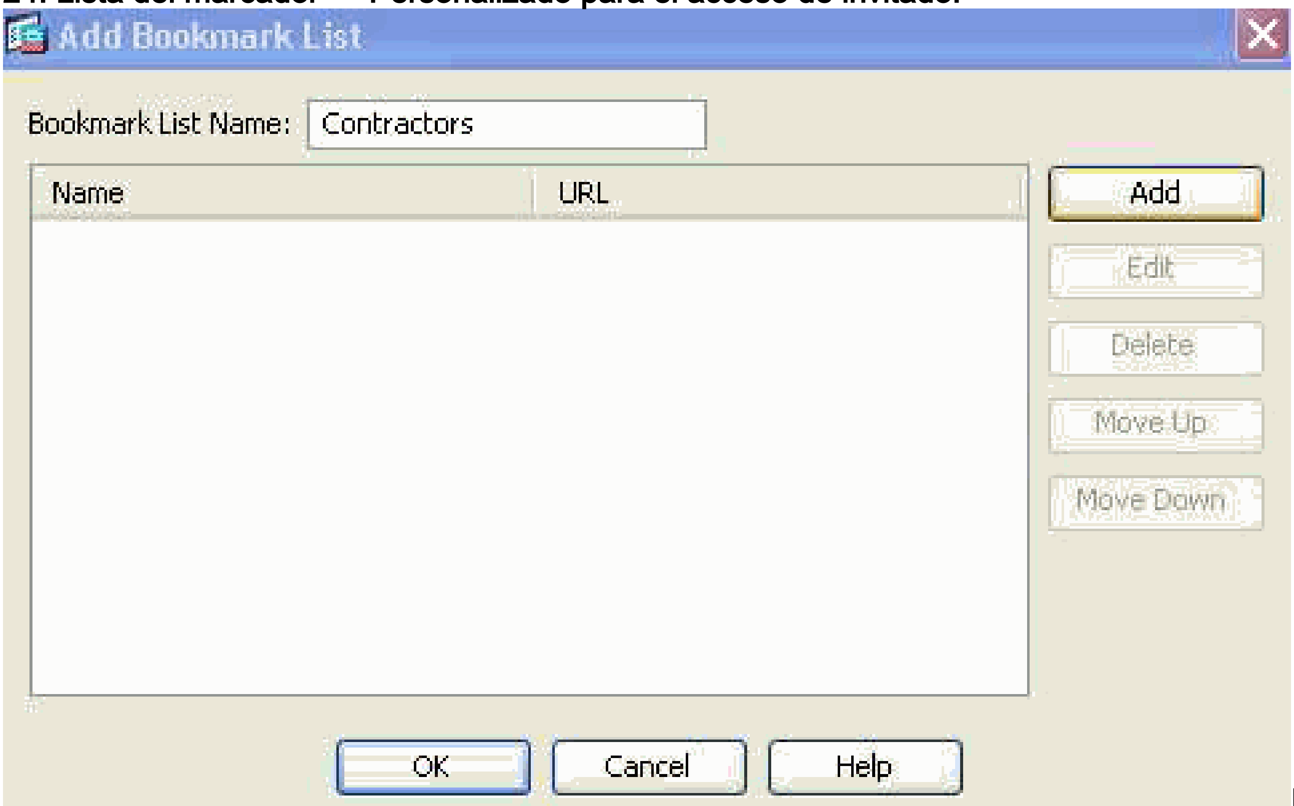
Definiendo las listas del marcador (listas url) para el acceso del clientless — esta configuración es necesaria para definir una aplicación en Internet que se publicará en el portal. Definiremos 2 listas url, una para los empleados y la otra para los contratistas.

1. Navegue a la **configuración > al VPN de acceso remoto > al acceso > al portal > a los marcadores del clientless SSL VPN**, el tecleo **+ agrega** y configura el siguiente:**Cuadro 23. Lista del marcador — Define los URL que se publicarán y accedidos del portal web. (Personalizado para el acceso del empleado).**



Nombre de la lista del marcador: **Empleados**, entonces haga click en AddTítulo del marcador: **Intranet de la compañía**Valor URL: **http://company.resource.com**El Haga Click en OK y entonces **APRUEBA** otra vez.

2. El tecleo **+ agrega** y configura una segunda lista del marcador (lista url) como sigue:**Cuadro 24. Lista del marcador — Personalizado para el acceso de invitado.**

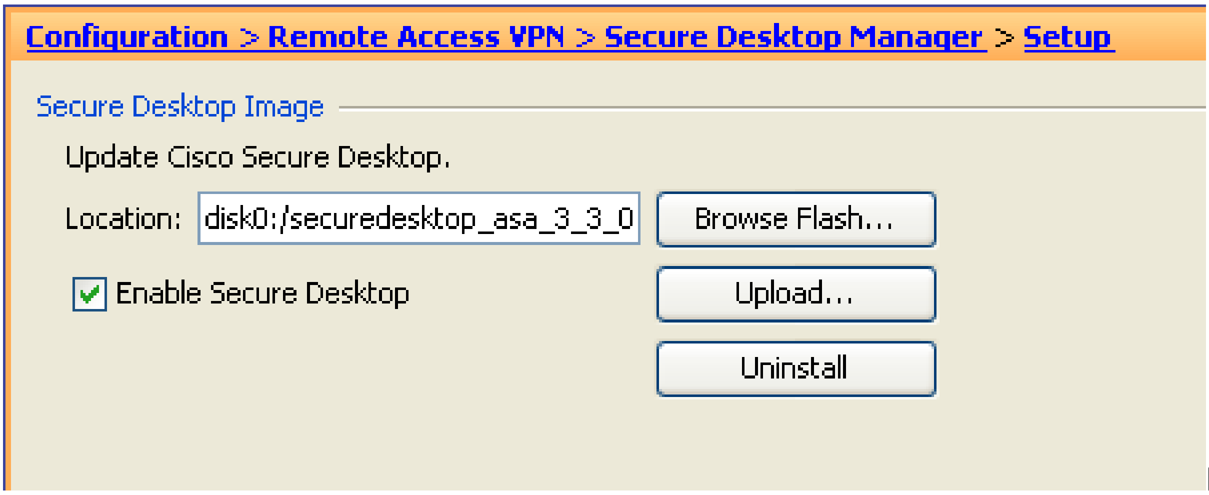


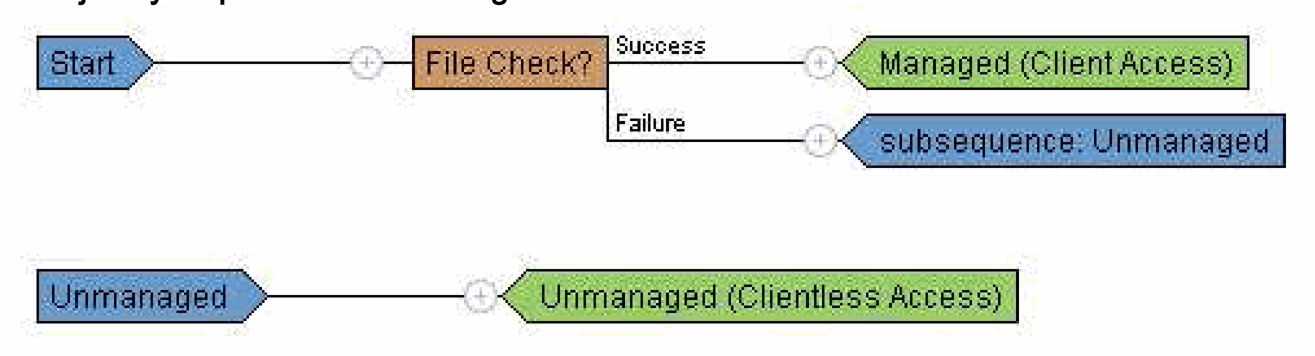
Nombre de la lista del marcador: **Contratistas**, entonces haga click en AddTítulo del marcador: **Acceso de invitado**Valor URL: **http://company.contractors.com**El Haga Click en OK y entonces **APRUEBA** otra vez.Haga clic en Apply (Aplicar).

Cisco Secure Desktop — esta configuración es necesaria para definir los atributos de la evaluación del punto final. De acuerdo con los criterios que se satisfarán, los puntos finales de

conexión serán clasificados según lo manejado o Unmanaged. Las evaluaciones del Cisco Secure Desktop se ejecutan antes del proceso de autenticación.

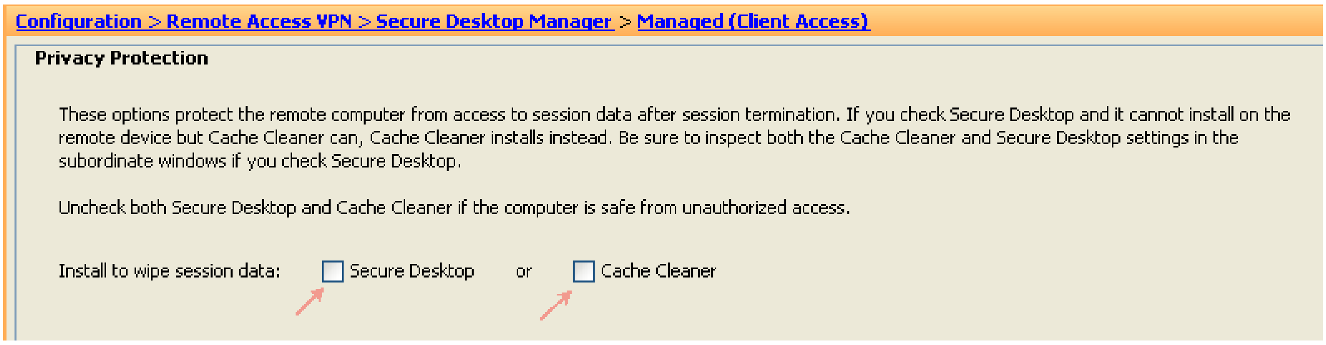
Configurar el Cisco Secure Desktop y pre un árbol de decisión del login para las ubicaciones de Windows:

1. Navegue al **administrador de la configuración > del VPN de acceso remoto > del Secure Desktop > puesto**, y configure el siguiente:**Cuadro 25. La imagen del Cisco Secure Desktop instala — Define la imagen del Cisco Secure Desktop que se avanzará a los puntos finales de conexión.**


Instale la imagen **disk0:/securedesktop-asa-3.3.-xxx-k9.pkg del** sistema de archivos Flash ASA.Marque el **Secure Desktop del permiso**.Haga clic en Apply (Aplicar).
2. Navegue a la **configuración > al administrador del VPN de acceso remoto > del Secure Desktop > a la directiva de Prelogin**, y configure el siguiente:**Cuadro 26. árbol de decisión del PRE-inicio — Personalizado vía el control del archivo para distinguir entre un punto final manejado y un punto final unmanaged.**


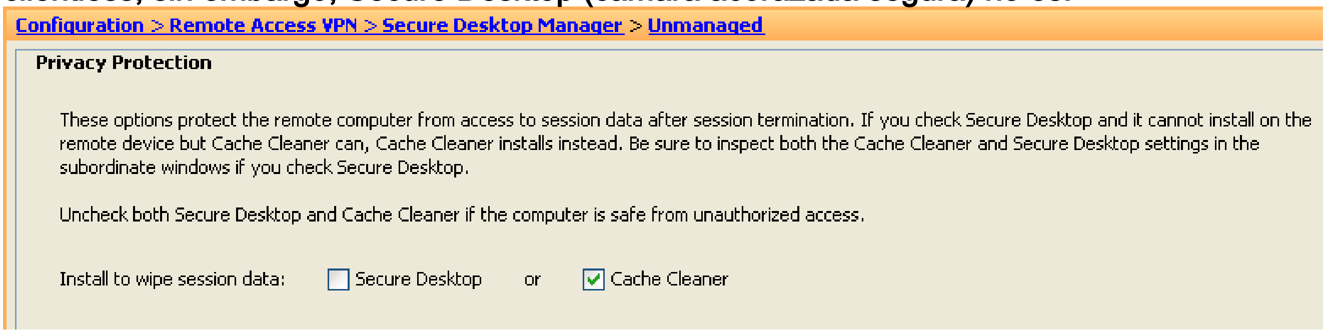
Haga clic el nodo **predeterminado** y retitule la escritura de la etiqueta **manejada (acceso al cliente)** y después haga clic la **actualización**.Haga clic "+" el símbolo al principio del nodo manejado.Para el control, seleccione y agregue el **control del archivo** que se insertará.Ingrese **C:\managed.txt** para el trayecto del archivo a "existe" y hace clic la **actualización**.Haga clic el **login negó el** nodo y después seleccionan **Subsequence**.Ingrese **Unmanaged** para la escritura de la etiqueta y después haga clic la **actualización**.Haga clic el **login negó el** nodo y después seleccionan la **ubicación**.Ingrese **Unmanaged (acceso del clientless)** para la escritura de la etiqueta y después haga clic la **actualización**.El tecleo **aplica todos**.
3. Navegue al **administrador de la configuración > del VPN de acceso remoto > del Secure Desktop >Managed (acceso al cliente)**, y configure el siguiente bajo sección de las configuraciones de ubicación:**Cuadro 27. Configuraciones de la protección de la**

ubicación/de la intimidad — El Secure Desktop (cámara acorazada segura) y el producto de limpieza de discos del caché (limpieza del navegador) no es un requisito para el acceso basado /Network del cliente.



Módulo de la ubicación: Desmarque el **Secure Desktop** y **oculte el producto de limpieza de discos** si está habilitado.El tecleo **aplica todos** si es necesario.

4. Navegue al **administrador de la configuración > del VPN de acceso remoto > del Secure Desktop > Unmanaged (acceso del clientless)**, y configure el siguiente bajo sección de las configuraciones de ubicación:**Cuadro 28. Configuraciones de ubicación — El producto de limpieza de discos del caché (limpieza del navegador) es un requisito para el acceso basado clientless, sin embargo, Secure Desktop (cámara acorazada segura) no es.**

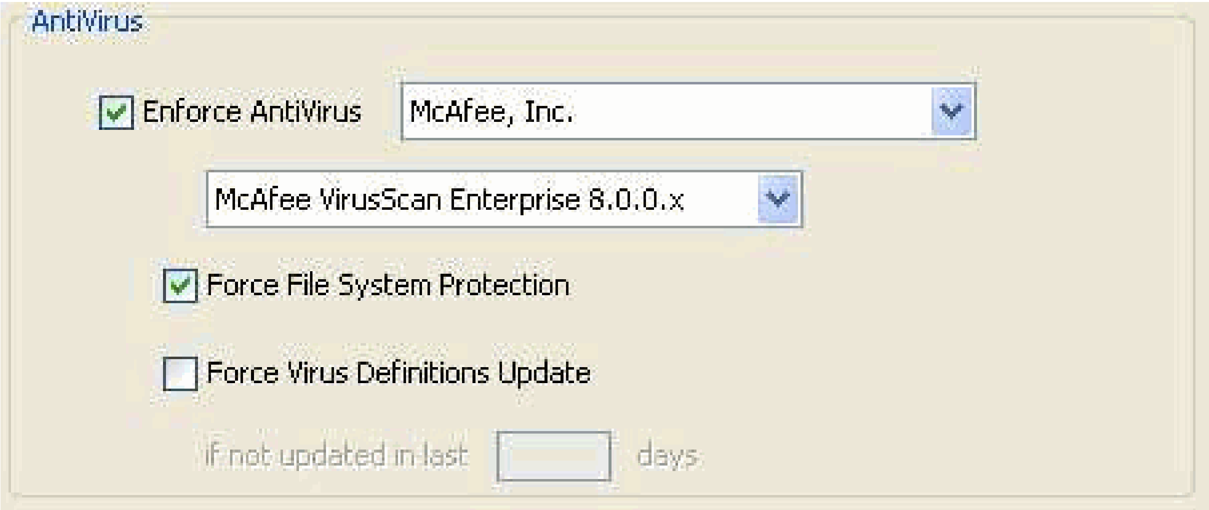


Módulo de la ubicación: Desmarque el **Secure Desktop** y marque el **producto de limpieza de discos del caché**.El tecleo **aplica todos**.

Evaluación avanzada del punto final — Esta configuración es necesaria para aplicar el antivirus, AntiSpyware y el escudo de protección personal en un punto final. Por ejemplo, esta evaluación verificará si el McAfee se está ejecutando en el punto final de conexión. (La evaluación avanzada del punto final es una función cubierta por la licencia y no es configurable si se inhabilita la característica del Cisco Secure Desktop).

Navegue a la **configuración > al VPN de acceso remoto > exploración al administrador > al host del Secure Desktop**, y configure el siguiente bajo sección de las Extensiones de la exploración del host:

Cuadro 29. Aplicación del antivirus — Personalizado para el acceso basado /Network del cliente.



Bajo sección de las Extensiones de la exploración del host, configure el siguiente:

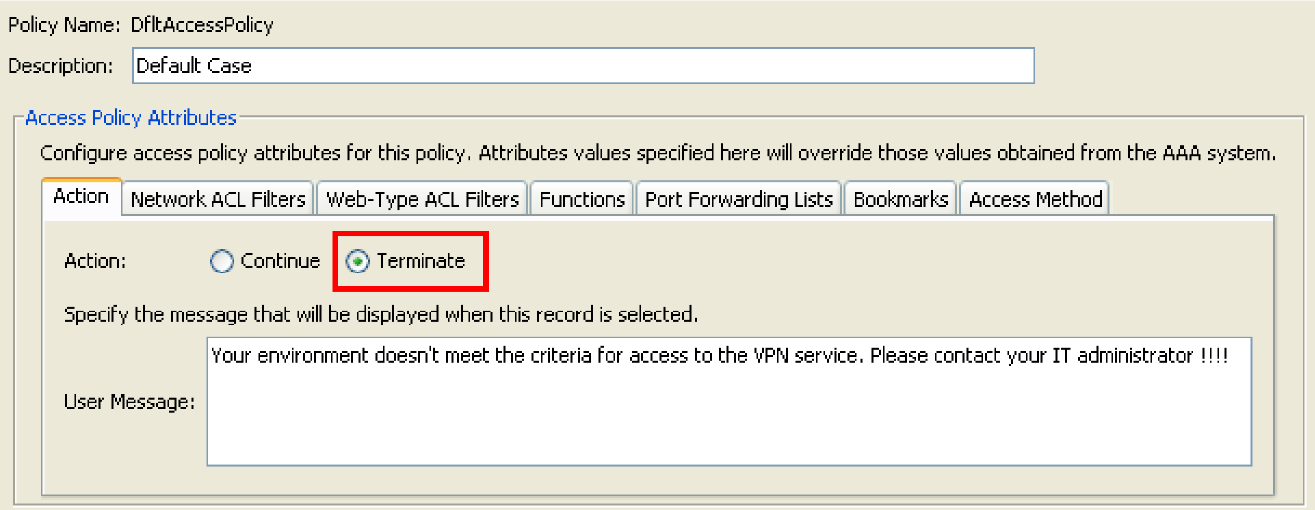
1. Seleccione el **ver avanzado 2.3.3.1 de la evaluación del punto final** y después **configurelo**.
2. Selecto **aplique el antivirus**.
3. Del menú desplegable del antivirus del aplicar, seleccione **McAfee, Inc.**
4. Del menú desplegable de la versión del antivirus seleccione la **empresa 8.0.0.x de VirusScan del McAfee**.
5. Seleccione la **protección de sistema de archivos de la fuerza** y después haga clic **aplican todos**.

Directivas del acceso dinámico — Esta configuración es necesaria para validar los usuarios de conexión y sus puntos finales contra los criterios de evaluación definidos AAA y/o del punto final. Si los criterios definidos de un expediente DAP se satisfacen, entonces concederán los usuarios de conexión el acceso a los recursos de red que se asocian a ese expediente o a los expedientes DAP. La autorización DAP se ejecuta durante el proceso de autenticación.

Para asegurarse de que una conexión VPN SSL termine en el caso predeterminado, e.g cuando el punto final no hace juego ninguna directivas configurada del acceso dinámico), configuraremos el siguiente:

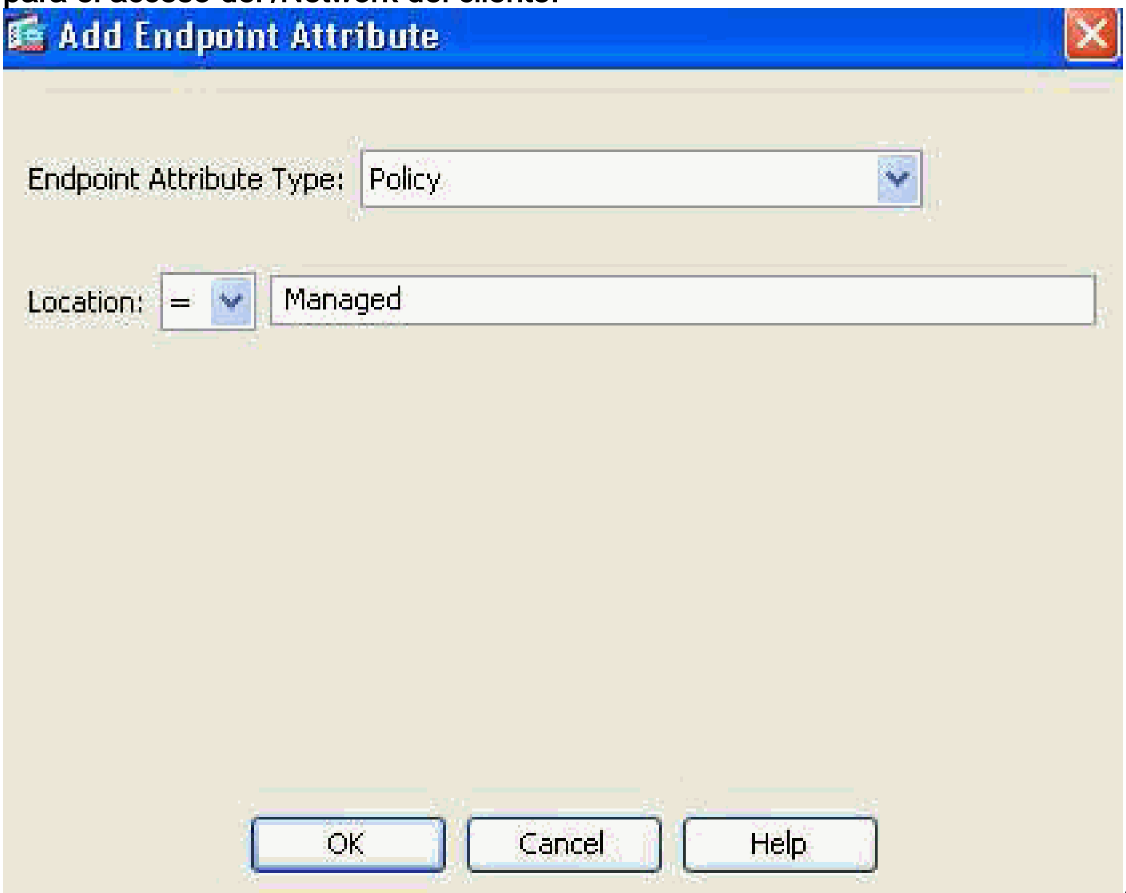
Nota: Al configurar las directivas del acceso dinámico por primera vez, un mensaje de error DAP.xml se visualiza que indica que no existe un archivo de configuración DAP (DAP.XML). Una vez que se modifica y después se guarda su configuración inicial DAP, este mensaje aparecerá no más.

1. Navegue a la **configuración > al VPN de acceso remoto > las directivas al acceso > al acceso dinámico del clientless SSL VPN**, y configure el siguiente:**Cuadro 30. Directiva predeterminada del acceso dinámico — si no se corresponde con ningunos expedientes predefinidos DAP, este expediente DAP será aplicado. Así, el acceso SSL VPN será negado.**

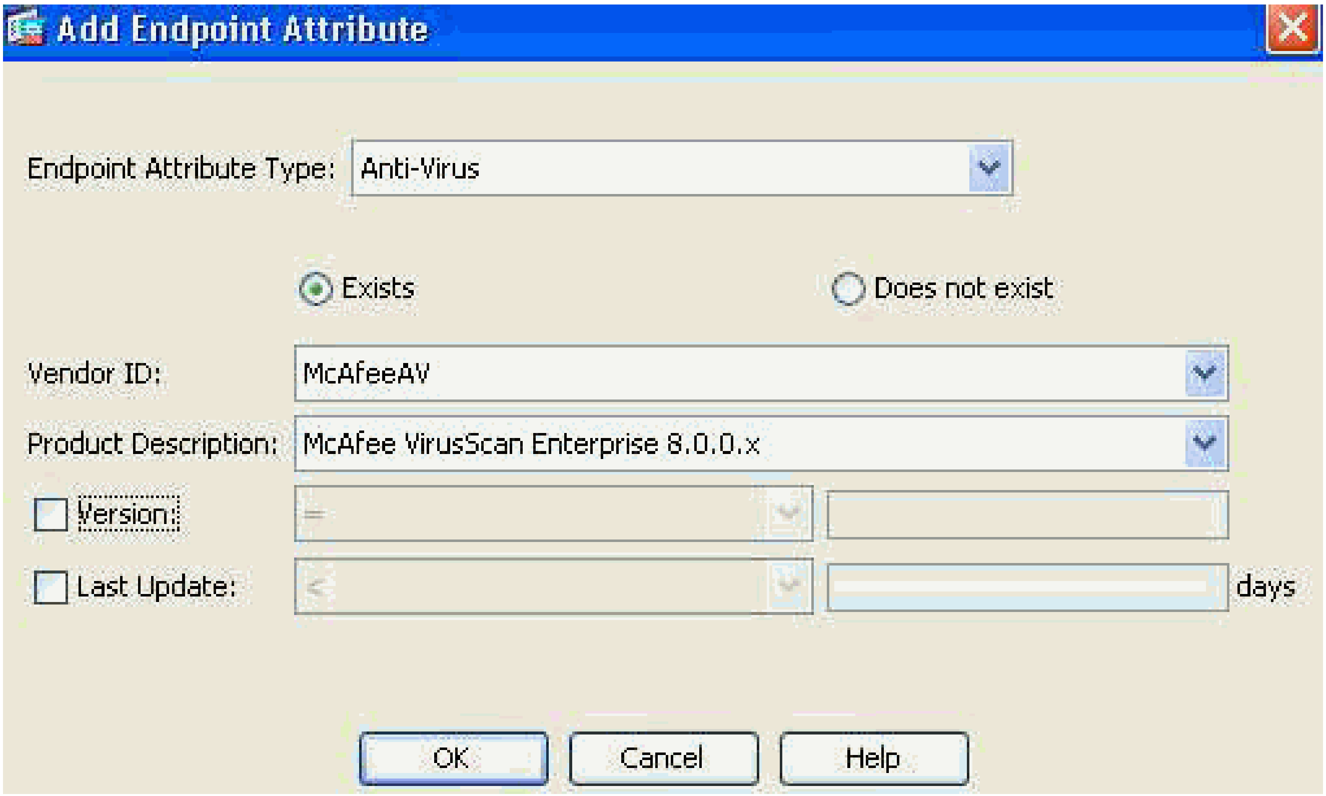


Edite el **DfltAccessPolicy** y fije la acción **para terminar**.Haga clic en OK.

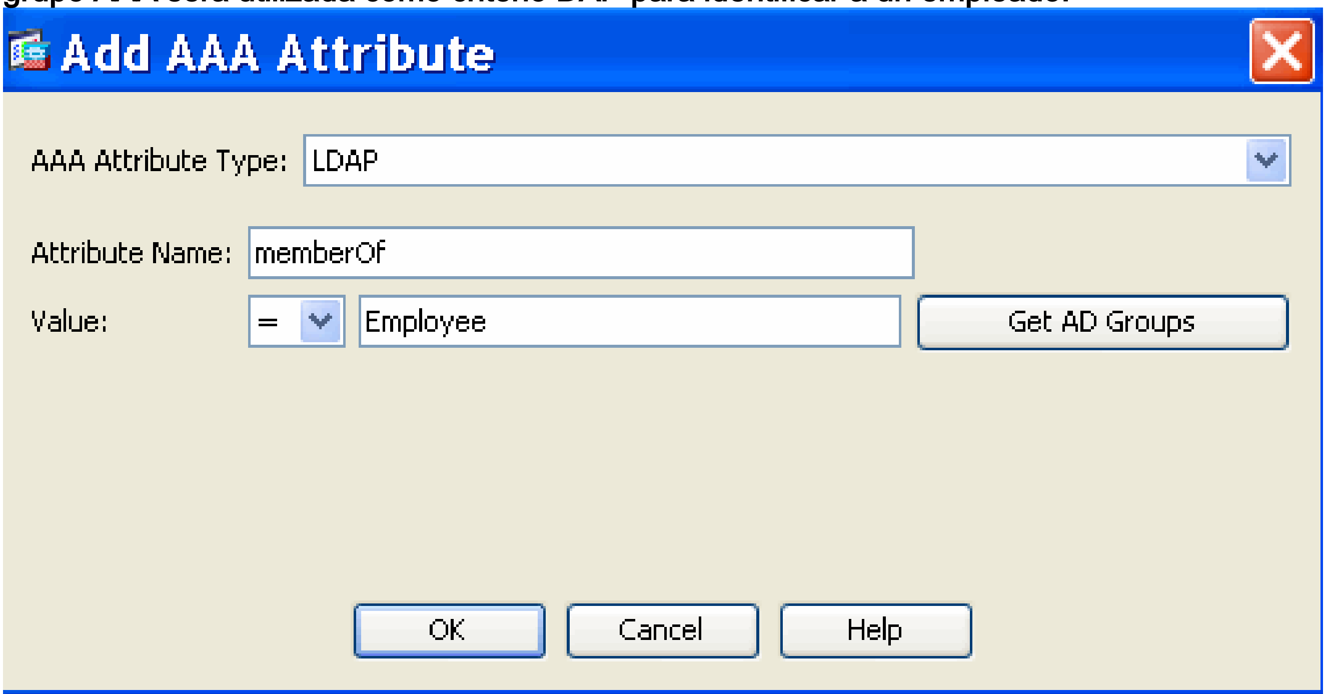
2. Agregue una nueva directiva del acceso dinámico nombrada **Managed_Endpoints**, como sigue:Descripción: **Acceso al cliente del empleado**Agregue (localizado a la derecha del tipo del atributo del punto final) un tipo del atributo del punto final (directiva) tal y como se muestra en del cuadro 31. Haga Click en OK cuando es completo.**Cuadro 31. Atributo del punto final DAP — La ubicación del Cisco Secure Desktop será utilizada como criterio DAP para el acceso del /Network del cliente.**



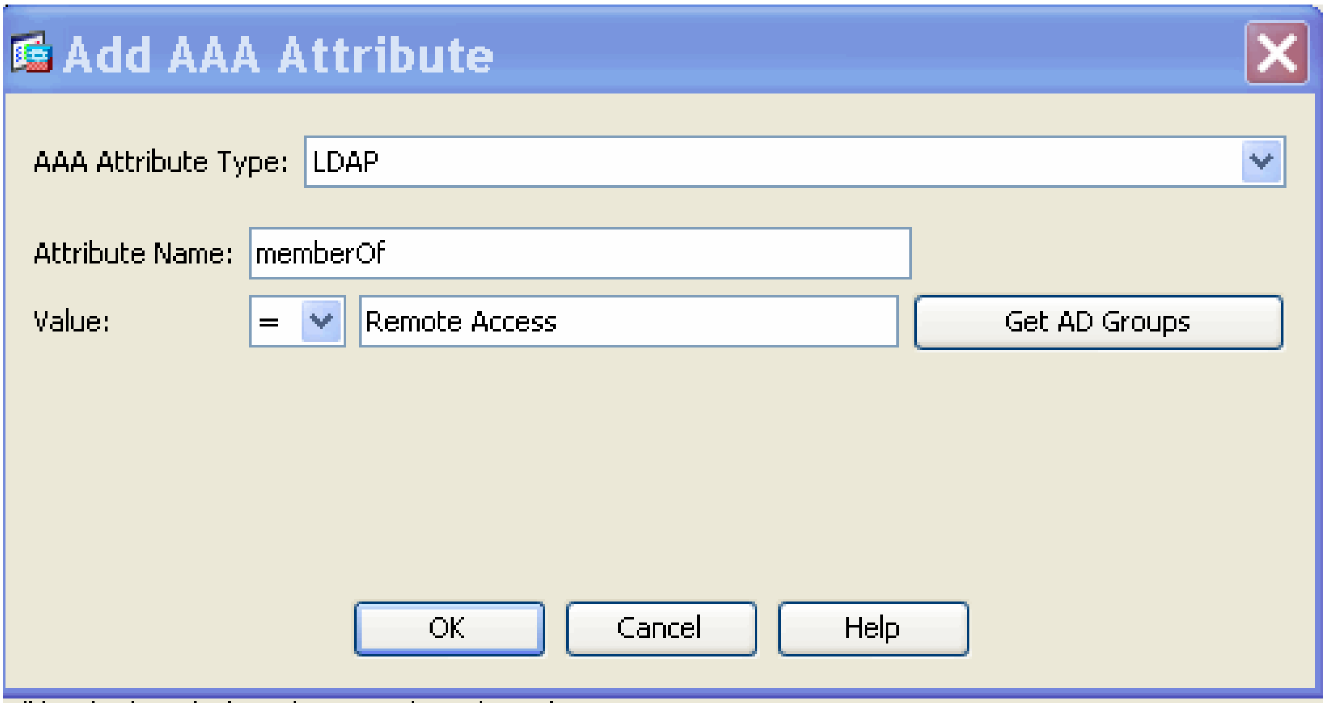
Agregue un segundo tipo del atributo del punto final (contra virus) tal y como se muestra en del cuadro 32. Haga Click en OK cuando es completo.**Cuadro 32. Atributo del punto final DAP — El antivirus avanzado de la evaluación del punto final será utilizado como criterio DAP para el acceso del /Network del cliente.**



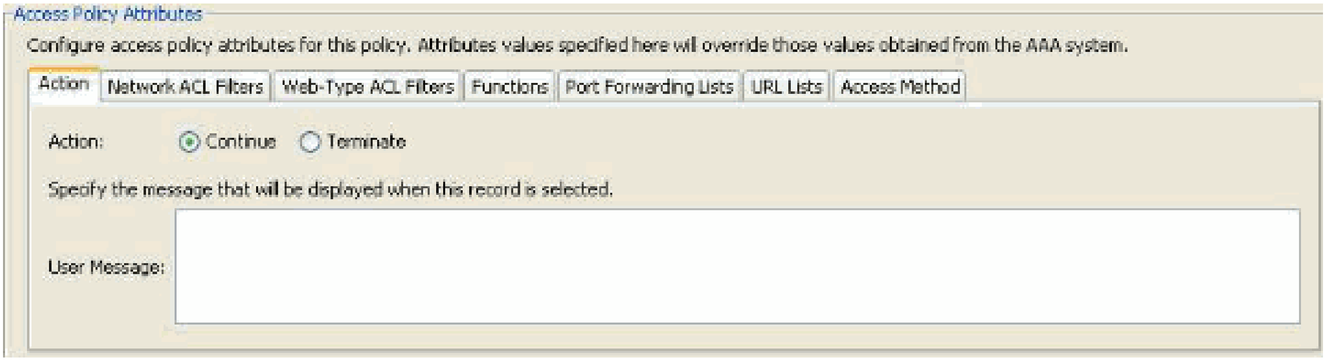
Del menú desplegable sobre la sección del atributo AAA, el **usuario** selecto **tiene todos los valores de atributos de siguiente AAA…**Agregue (localizado a la derecha del cuadro del atributo AAA) un tipo del atributo AAA (LDAP) tal y como se muestra en del cuadro 33 y 34. Haga Click en OK cuando es completo.**Cuadro 33. Atributo DAP AAA — La membresía del grupo AAA será utilizada como criterio DAP para identificar a un empleado.**



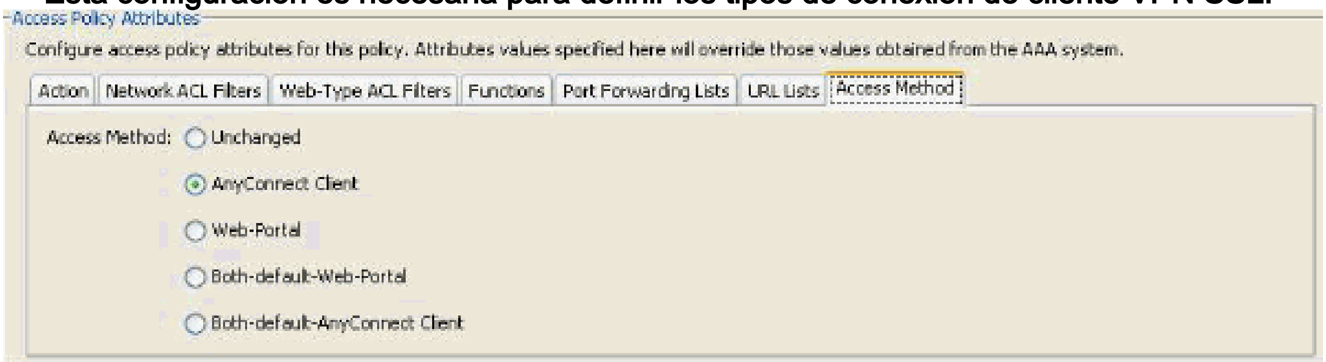
Cuadro 34. Atributo DAP AAA — La membresía del grupo AAA será utilizada como criterio DAP para permitir las capacidades de Acceso Remoto.



Bajo lengueta de la acción, verifique que la acción esté fijada **para continuar**, tal y como se muestra en del cuadro 35.**Cuadro 35. Lengueta de la acción — Esta configuración es necesaria para definir el proceso especial para una conexión o una sesión específica. El acceso VPN será negado si un expediente DAP es coincidencia y la acción se fija para terminar.**



Bajo lengueta del método de acceso, seleccione al **cliente de AnyConnect del** método de acceso, tal y como se muestra en del cuadro 36.**Cuadro 36. Lengueta del método de acceso — Esta configuración es necesaria para definir los tipos de conexión de cliente VPN SSL.**

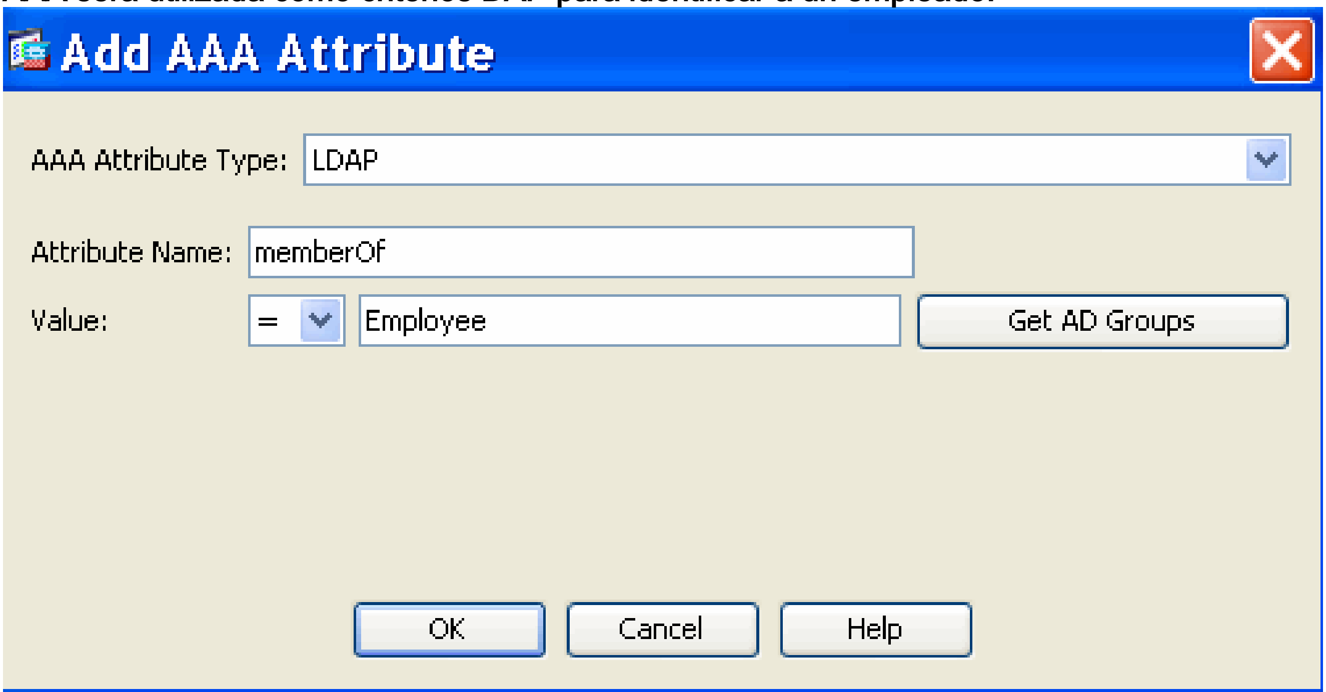


El Haga Click en OK, y entonces **se aplica**.

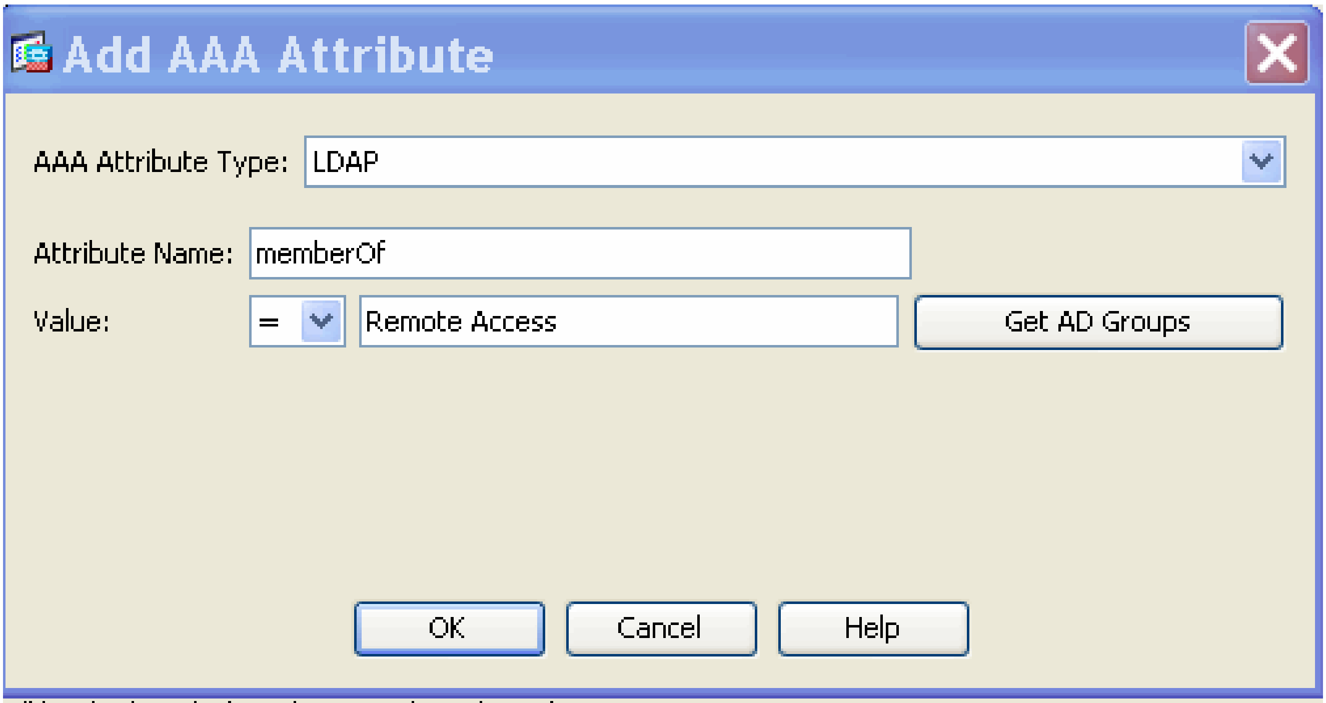
3. Agregue un segundo acceso dinámico **Unmanaged_Endpoints** nombrado directiva, como sigue:Descripción: **Acceso del clientless del empleado**.Agregue (localizado a la derecha del cuadro del atributo del punto final) un tipo del atributo del punto final (directiva) tal y como se muestra en del cuadro 37. Haga Click en OK cuando es completo.**Cuadro 37. Atributo del punto final DAP — La ubicación del Cisco Secure Desktop será utilizada como criterios DAP**

para el acceso del clientless.

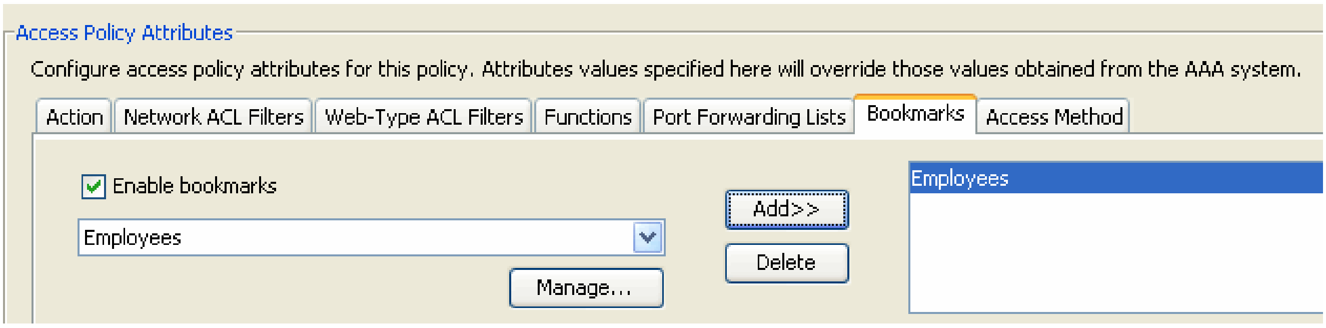
Del menú desplegable sobre la sección del atributo AAA, el **usuario** selecto **tiene todos los valores de atributos de siguiente AAA…**Agregue (localizado a la derecha del tipo del atributo AAA) un tipo del atributo AAA (LDAP) tal y como se muestra en del cuadro 38 y 39. Haga Click en OK cuando es completo.**Cuadro 38. Atributo DAP AAA — La membresía del grupo AAA será utilizada como criterios DAP para identificar a un empleado.**



Cuadro 39. Atributo DAP AAA — La membresía del grupo AAA será utilizada como criterio DAP para permitir las capacidades de Acceso Remoto.

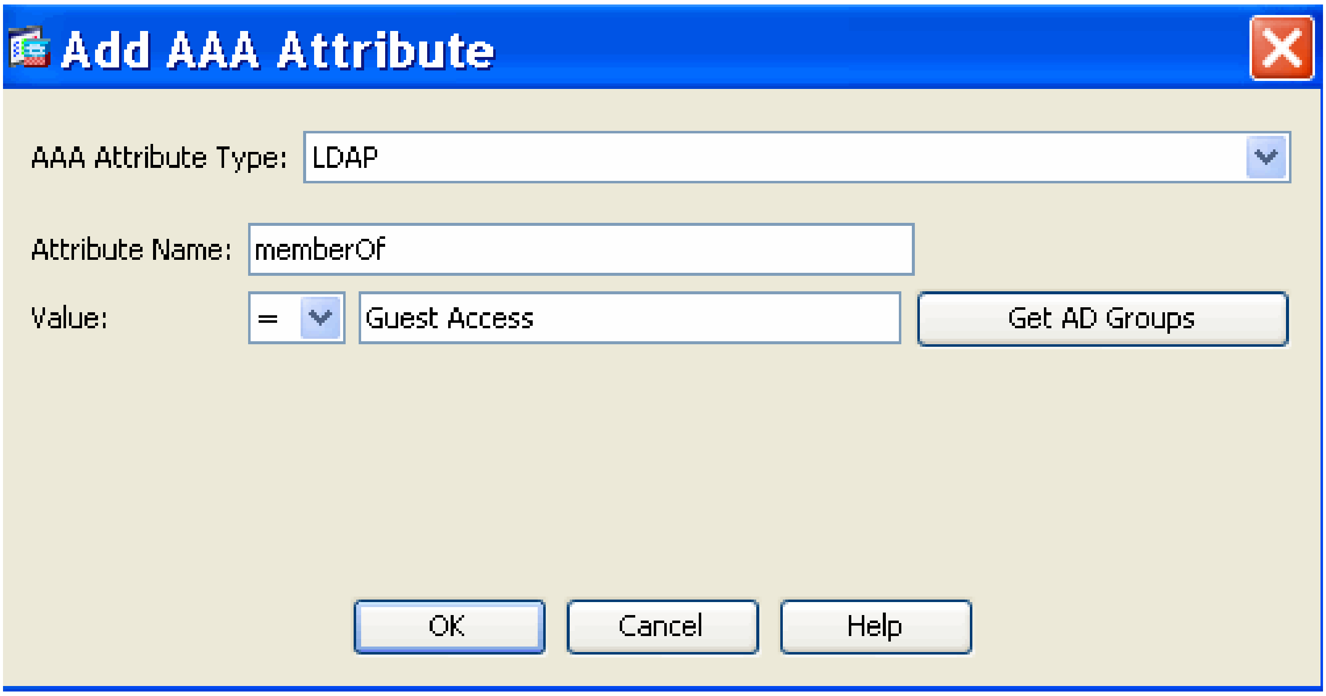


Bajo lengueta de la acción, verifique que la acción esté fijada **para continuar**. (Cuadro 35 de la referencia.)Bajo los marcadores tabule, seleccione a los **empleados del** nombre de la lista del descenso-abajo y entonces del haga click en Add También, verifique que los marcadores del permiso estén marcados tal y como se muestra en del cuadro 40.**Cuadro 40. Lengueta de los marcadores — Le deja seleccionar y configurar las listas url para las sesiones del usuario.**

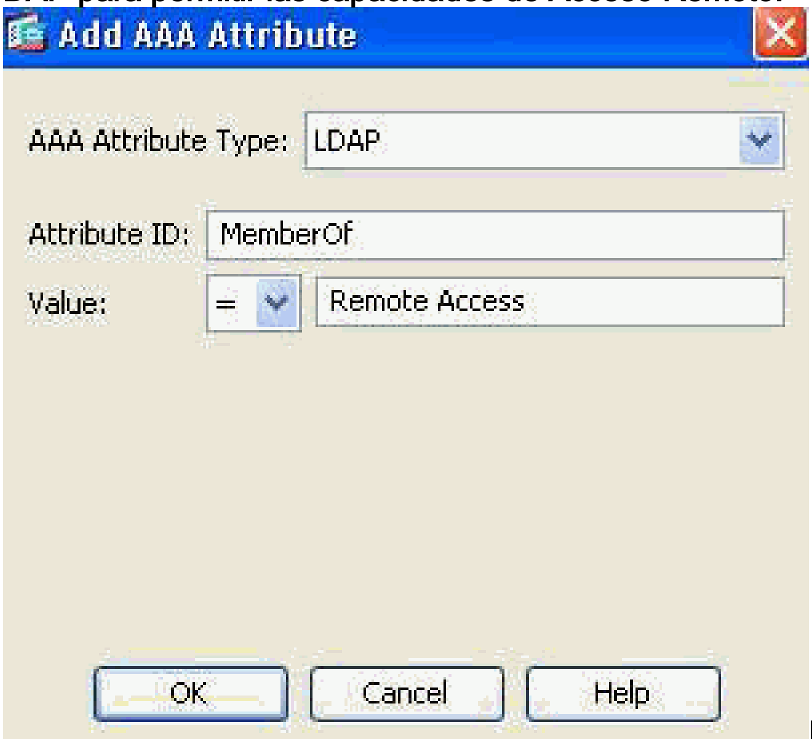


Bajo lengueta del método de acceso, seleccione el **portal web del** método de acceso. (Cuadro 36 de la referencia.)El Haga Click en OK, y entonces **se aplica**.Los contratistas serán identificados por los atributos DAP AAA solamente. Como consecuencia, tipo de los atributos del punto final: (Directiva) no será configurado en el paso 4. Este acercamiento se significa solamente para mostrar la flexibilidad dentro del DAP.

4. Agregue un tercer acceso dinámico **Guest_Access** nombrado directiva y con el siguiente:Descripción: **Acceso del clientless del invitado**.Agregue (localizado a la derecha del cuadro del atributo del punto final) un tipo del atributo del punto final (directiva) tal y como se muestra en del cuadro 37 antedicho. Haga Click en OK cuando es completo.Del menú desplegable sobre la sección del atributo AAA, el **usuario** selecto **tiene todos los valores de atributos de siguiente AAA…**Agregue (localizado a la derecha del cuadro del atributo AAA) un tipo del atributo AAA (LDAP) tal y como se muestra en del cuadro 41 y 42. Haga Click en OK cuando es completo.**Cuadro 41. Atributo DAP AAA — La membresía del grupo AAA será utilizada como criterio DAP para identificar un contratista.**



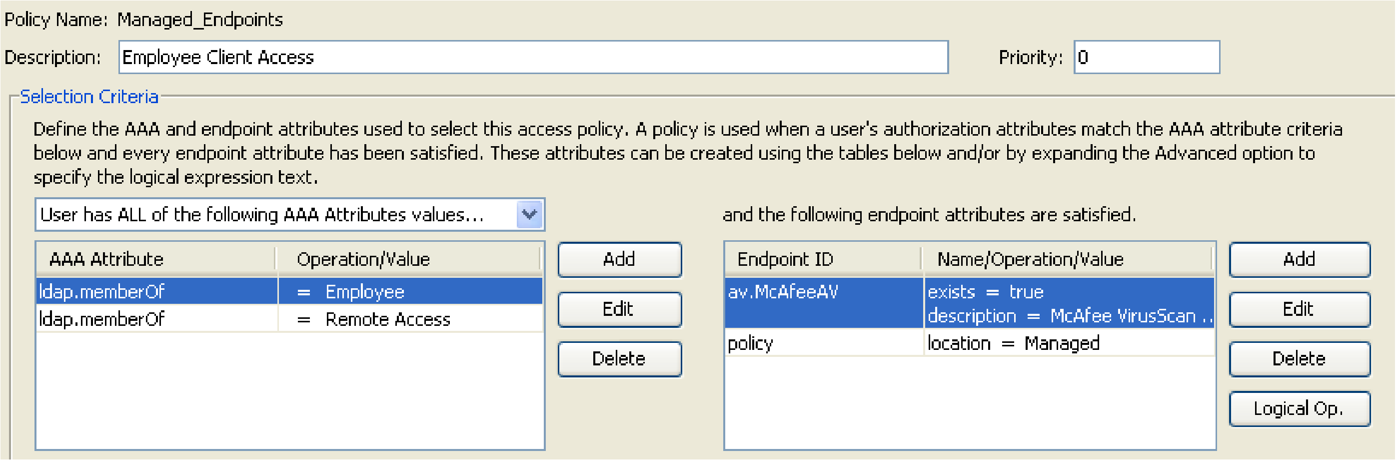
Cuadro 42. Atributo DAP AAA — La membresía del grupo AAA será utilizada como criterio DAP para permitir las capacidades de Acceso Remoto.



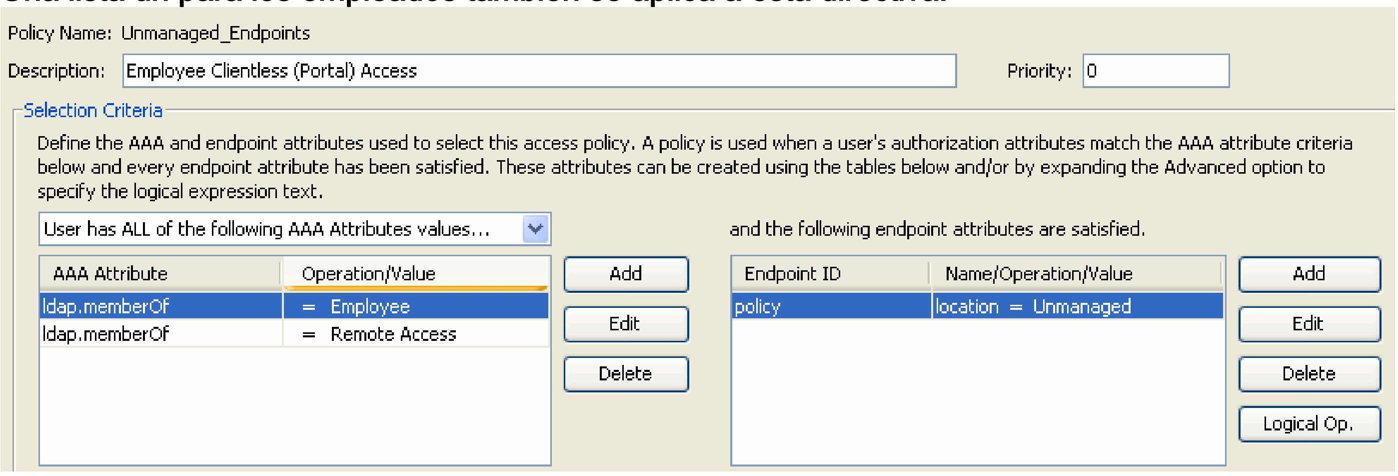
Bajo lengueta de la acción, verifique que la acción esté fijada **para continuar**. (Cuadro 35 de la referencia.)Bajo los marcadores tabule, seleccione los **contratistas del** nombre de la lista del descenso-abajo y entonces del haga click en Add También, verifique que los **marcadores del permiso** estén marcados. (Cuadro 40 de la referencia.)Bajo lengueta del método de acceso, seleccione el **portal web del** método de acceso. (Cuadro 36 de la referencia.)El Haga Click en OK, y entonces **se aplica**.

Criterio de selección DAP — De acuerdo con los Procedimientos de configuración ese DAP arriba, su Criterio de selección para las 4 directivas DAP definidas, debe ser constante con los cuadros 43, 44, 45 y 46.

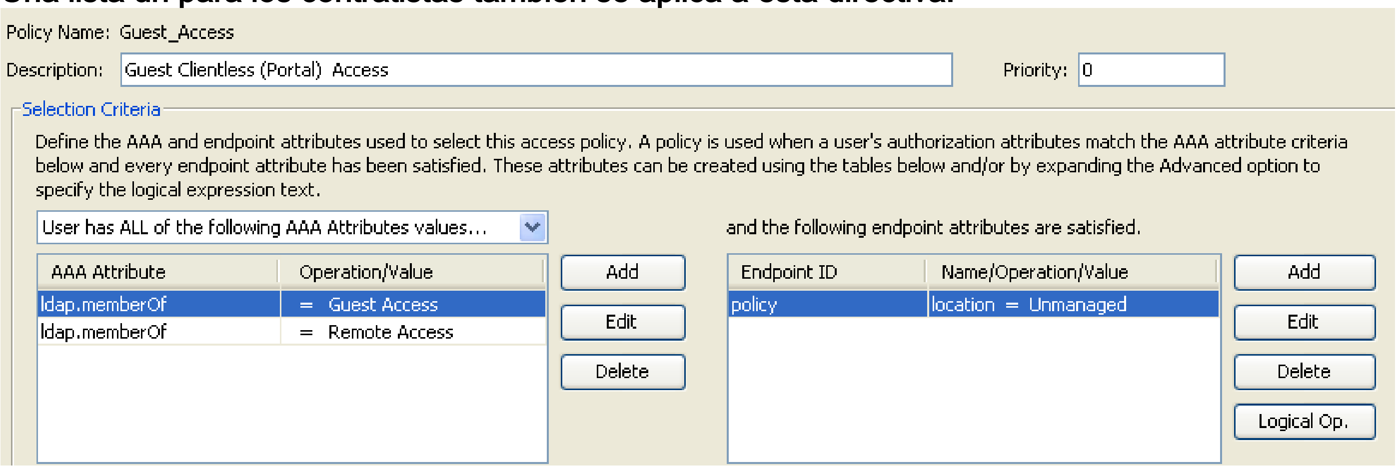
Cuadro 43. Puntos finales manejados — Si los criterios de este expediente DAP se satisfacen, los empleados tendrán acceso a los recursos corporativos vía una conexión del cliente/de la red (cliente de AnyConnect).



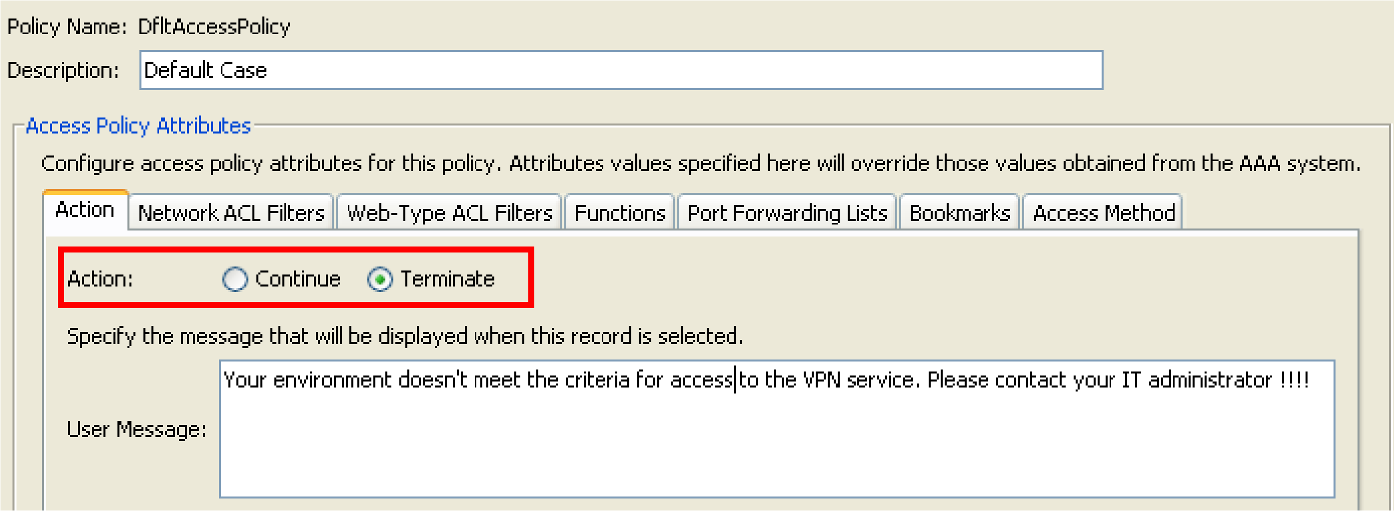
Cuadro 44. Puntos finales Unmanaged — Si los criterios de este expediente DAP se satisfacen, los empleados tendrán acceso a los recursos corporativos vía una conexión (porta) del clientless. Una lista url para los empleados también se aplica a esta directiva.



Cuadro 45. Acceso de invitado — Si los criterios de este expediente DAP se satisfacen, los contratistas tendrán acceso a los recursos corporativos vía una conexión (porta) del clientless. Una lista url para los contratistas también se aplica a esta directiva.



Cuadro 46. Directiva predeterminada DAP — Si los criterios para todos los expedientes DAP arriba no se satisfacen, negarán los empleados y los contratistas, por abandono, el acceso.



Conclusión

De acuerdo con los requisitos del Acceso Remoto SSL VPN del cliente conocidos en este ejemplo, esta solución satisfará sus requisitos del VPN de acceso remoto.

Con los entornos VPN de desarrollo y dinámicos en la fusión, las directivas del acceso dinámico pueden adaptarse y escalar para frecuentar los cambios de configuración de Internet, los diversos papeles que cada usuario puede habitar dentro de una organización, y los logines de los sitios manejados y unmanaged del Acceso Remoto con las diversos configuraciones y niveles de seguridad.

Las directivas del acceso dinámico son complementadas por las nuevas y probadas Tecnologías de la herencia incluyendo, la evaluación del punto final, la exploración del host, el Secure Desktop, el AAA y las directivas avanzados del Acceso local. Como consecuencia, las organizaciones pueden entregar con confianza el acceso del VPN seguro a cualquier recurso de red de cualquier ubicación.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems