# Guia de distribuição das políticas do acesso dinâmico ASA 8.x (DAP)

## Índice



## Introdução

Os gateways do Virtual Private Network (VPN) operam-se nos ambientes dinâmicos. Os variáveis múltipla podem afetar cada conexão de VPN; por exemplo, configurações do intranet que mudam frequentemente, os vários papéis que cada usuário pode habitar dentro de uma organização, e inícios de uma sessão dos locais do Acesso remoto com configurações e níveis de segurança diferentes. A tarefa de autorizar usuários é complicada muito mais em um ambiente VPN dinâmico do que está em uma rede com uma configuração estática.

As políticas do acesso dinâmico (DAP), uns novos recursos introduzidos no código do software release v8.0 da ferramenta de segurança adaptável (ASA), permitem-no de configurar a autorização que endereça a dinâmica dos ambientes VPN. Você cria uma política do acesso dinâmico ajustando uma coleção dos atributos do controle de acesso que você associa com um túnel ou uma sessão específica do usuário. Estes atributos endereçam introduções da sociedade e da Segurança de terminal de grupo múltiplo.

Por exemplo, a ferramenta de segurança concede o acesso a um usuário particular para uma sessão particular baseada nas políticas que você define. Gerencie um DAP durante a autenticação de usuário selecionando e/ou agregando atributos de uns ou vários registros DAP. Seleciona estes registros DAP baseados na informação de Segurança de terminal do dispositivo remoto e/ou na informação da autorização de AAA para o usuário autenticado. Aplica então o registro DAP ao túnel ou à sessão do usuário.

**Nota:** *O arquivo dap.xml*, que contém os atributos da seleção das políticas DAP, é armazenado no flash do ASA. Embora você possa exportar a fora-caixa do arquivo dap.xml, edite a (se você sabe sobre a sintaxe do xml), e a re-importação ele para trás, seja muito cuidadoso, porque você pode fazer com que o ASDM pare de processar registros DAP se você desconfigurou algo. Não há nenhum CLI para manipular parte de isto a configuração.

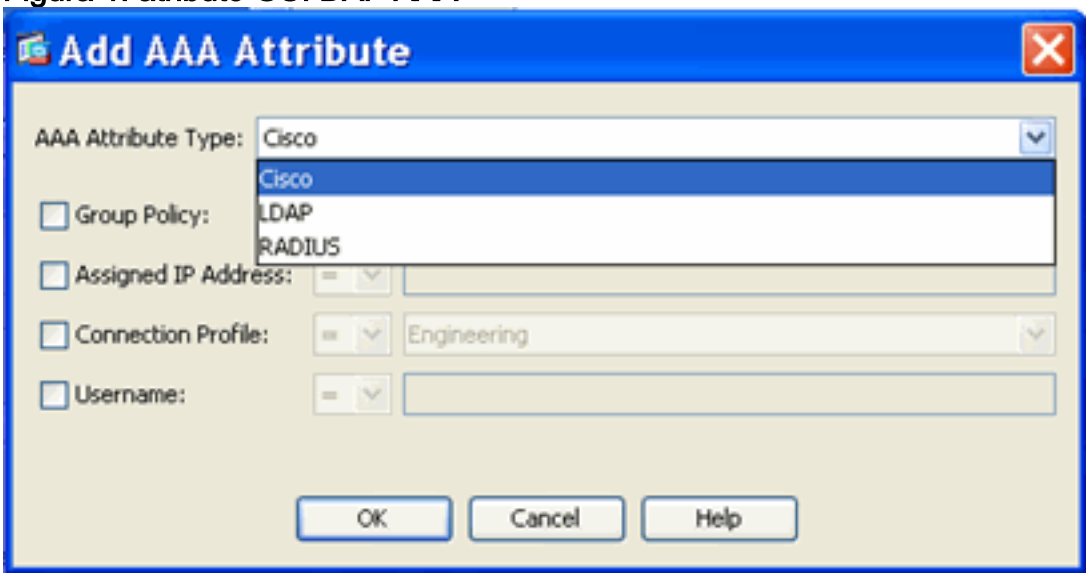
**Nota:** Tentar configurar os parâmetros do *acesso do dinâmico-acesso-política-registro* através do CLI pode fazer com que o DAP pare de trabalhar embora o ASDM controle corretamente o mesmos. Evite o CLI, e use sempre o ASDM para controlar políticas DAP.

## Atributos DAP e AAA

O DAP complementa serviços AAA e fornece um conjunto limitado de atributos da autorização que podem cancelar os atributos que o AAA fornece. A ferramenta de segurança pode selecionar os registros DAP baseados na informação da autorização de AAA para o usuário. A ferramenta de segurança pode selecionar registros múltiplos DAP segundo esta informação, que agrega então para atribuir a atributos da autorização DAP.

Você pode especificar atributos AAA da hierarquia do atributo de Cisco AAA, ou da definição completa dos atributos da resposta que a ferramenta de segurança recebe de um RAIO ou de um servidor ldap segundo as indicações de figura 1.

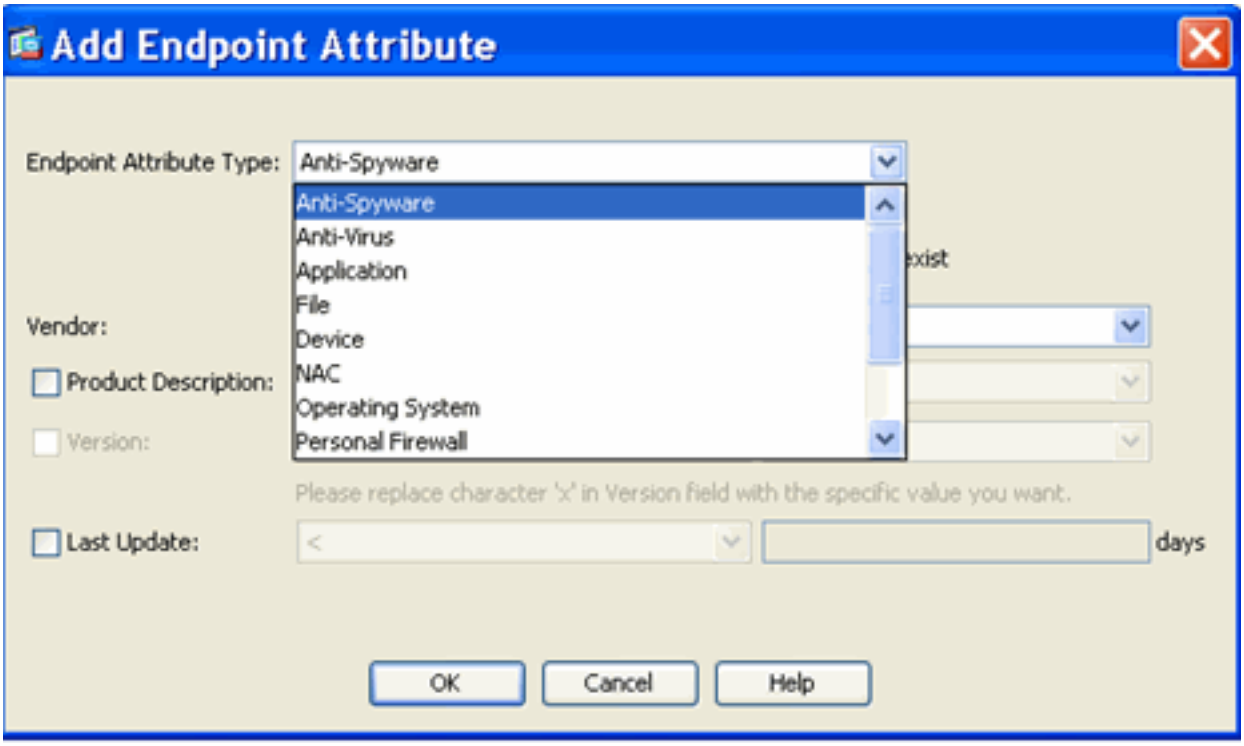
**Figura 1. atributo GUI DAP AAA**




## DAP e atributos de Segurança de terminal

Além do que atributos AAA, a ferramenta de segurança pode igualmente obter atributos de Segurança de terminal usando os métodos da avaliação da postura que você configura. Estes incluem a varredura básica do host, Secure Desktop, o padrão/avançou a avaliação do valor-limite e o NAC segundo as indicações da figura 2. atributos da avaliação do valor-limite é obtido e enviado à ferramenta de segurança antes da autenticação de usuário. Contudo, os atributos AAA, incluindo o registro total DAP, são validados durante a autenticação de usuário.

**Figura 2. atributo GUI do valor-limite**

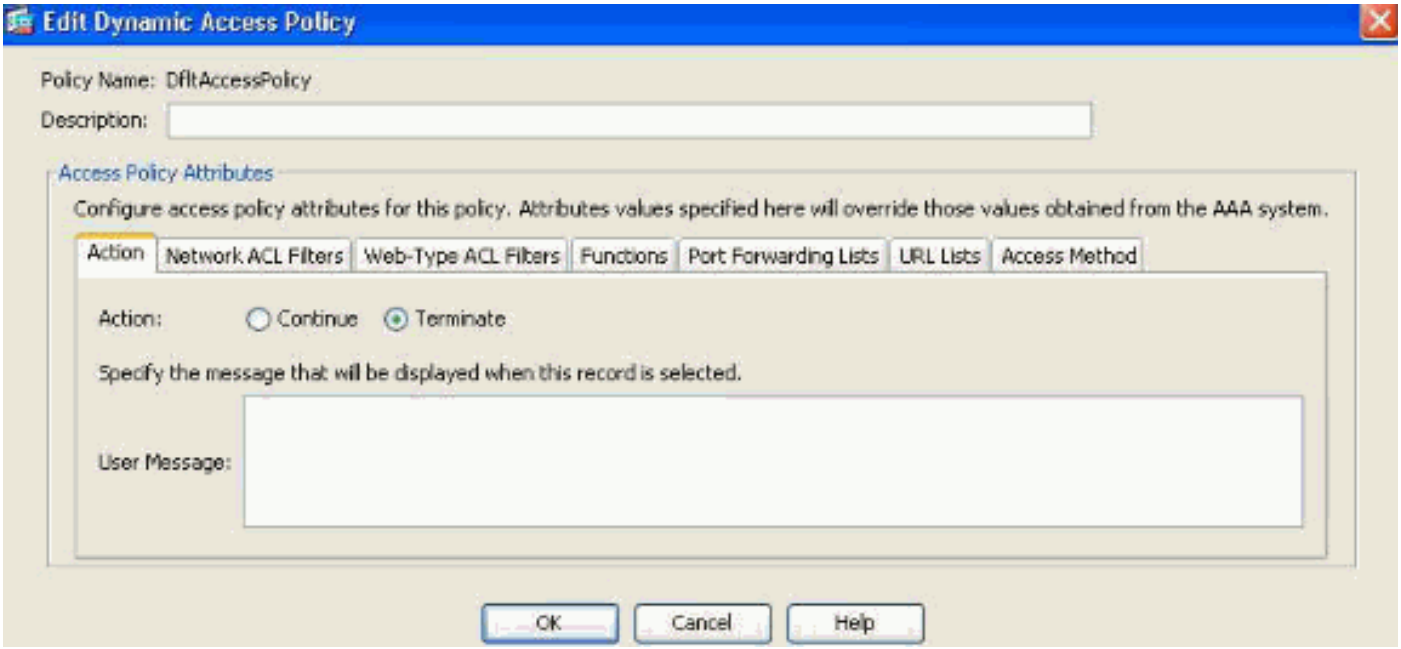



## Política do acesso dinâmico do padrão

Antes da introdução e da aplicação do DAP, o atributo da política de acesso/pares do valor que foram associados com um túnel ou uma sessão específica do usuário foi definido localmente no ASA, isto é, (grupos de túneis e políticas do grupo) ou traçado através dos servidores AAA externos. Contudo, na liberação v8.0, o DAP pode ser configurado para complementar ou cancelar o local e as políticas do acesso externo.

O DAP é reforçado sempre à revelia. Contudo, para administradores que prefere o método do reforço de política do legado, por exemplo, reforçando o controle de acesso através dos grupos de túneis, as políticas do grupo e o AAA sem a aplicação explícita do DAP podem ainda obter este comportamento. Para o comportamento do legado, nenhuma alteração de configuração à característica DAP, incluindo o registro do padrão DAP, DfltAccessPolicy, é exigida segundo as indicações de figura 3.

**Figura 3. política do acesso dinâmico do padrão**



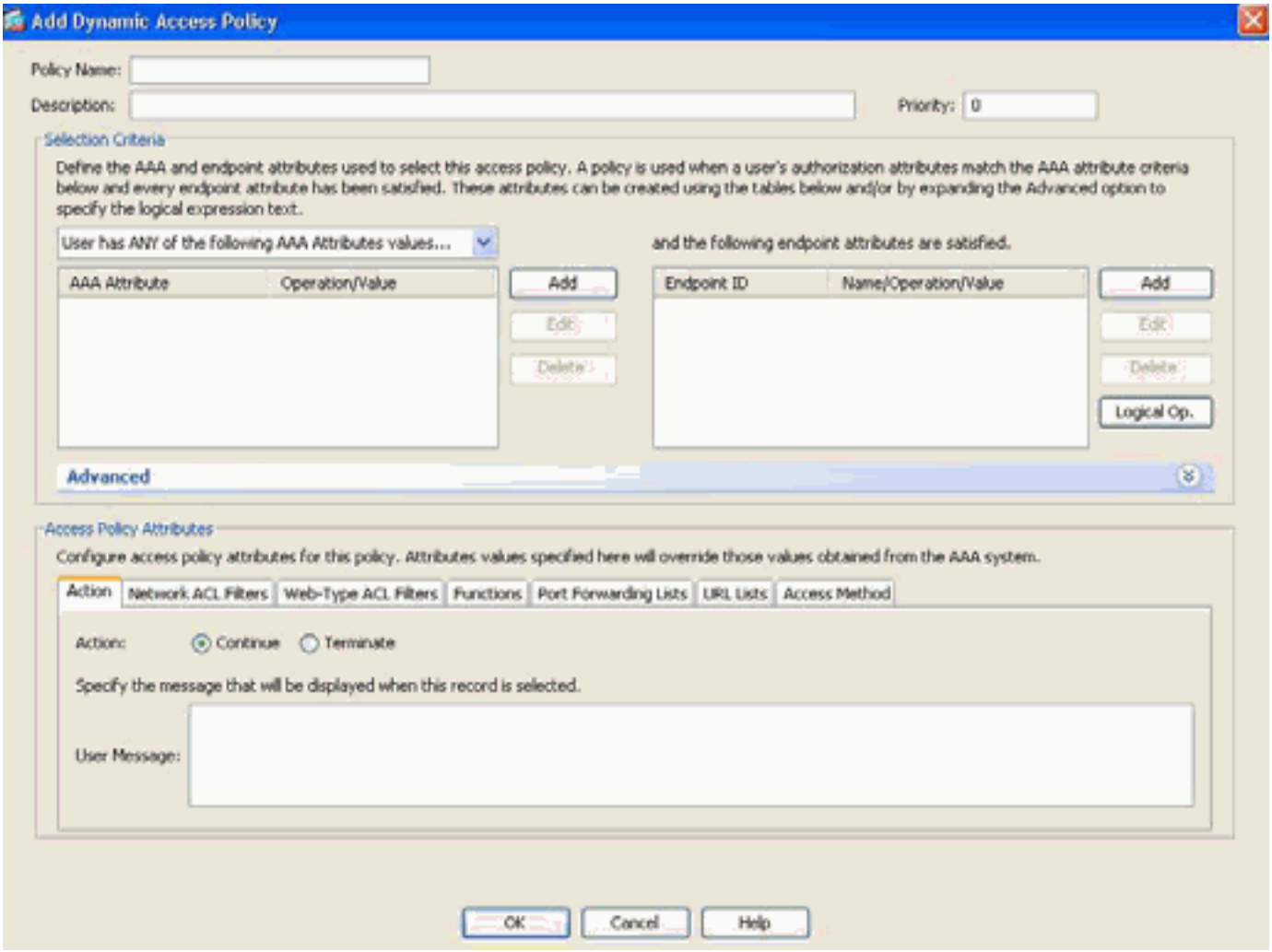

Não obstante, se alguns dos valores padrão em um registro DAP são mudados, por exemplo, a ação: o parâmetro no DfltAccessPolicy é mudado de seu valor padrão para terminar e os registros adicionais DAP não são configurados, usuários autenticados, combinarão o registro de DfltAccessPolicy DAP e serão negados à revelia o acesso VPN.

Consequentemente, uns ou vários registros DAP deverão ser criados e configurado para autorizar a conectividade de VPN e defini-la que os recursos de rede um usuário autenticado são autorizados alcançar. Assim, o DAP, se configurado, tomará a precedência sobre o reforço de política do legado.

## Configurando políticas do acesso dinâmico

Ao usar o DAP para definir a que os recursos de rede um usuário têm o acesso, há muitos parâmetros a considerar. Por exemplo, ambiente identificando se o valor-limite de conexão está vindo de um controlado, unmanaged ou não confiável, determinando os critérios de seleção necessários identificar o valor-limite de conexão, e baseado na avaliação do valor-limite e/ou nas credenciais AAA, que os recursos de rede o usuário de conexão serão autorizados alcançar. Para realizar isto, você precisará primeiramente de tornar-se familiar com as características e as funções DAP segundo as indicações de figura 4.

**Figura 4. política do acesso dinâmico**




Ao configurar um registro DAP, há dois componentes principais a considerar:

- Critérios de seleção que incluem opções avançadas
- Atributos da política de acesso

Os critérios de seleção da seção são onde um administrador configuraria o AAA e os atributos do valor-limite usados para selecionar um registro específico DAP. Um registro DAP está usado quando a autorização de um usuário atribui o fósforo os critérios do atributo AAA e cada atributo do valor-limite esteve satisfeito.

Por exemplo, se o tipo do atributo AAA: O LDAP (diretório ativo) é selecionado, a série de nome do atributo é memberOf e a corda do valor é contratantes, segundo as indicações da figura 5a, o usuário de autenticação deve ser um membro dos contratantes do grupo do diretório ativo para combinar os critérios do atributo AAA.

Além do que a satisfação dos critérios do atributo AAA, o usuário de autenticação será exigido igualmente satisfazer os critérios do atributo do valor-limite. Por exemplo, se o administrador configurou o Cisco Secure Desktop (CSD) para determinar a postura do valor-limite de conexão e baseada nessa avaliação da postura, o valor-limite esteve colocado no lugar CSD Unmanaged, o administrador poderia então usar esta informação da avaliação enquanto os critérios de seleção para o valor-limite atribuem mostrado na figura 5b.

**Figura 5a. Critérios do atributo AAA**

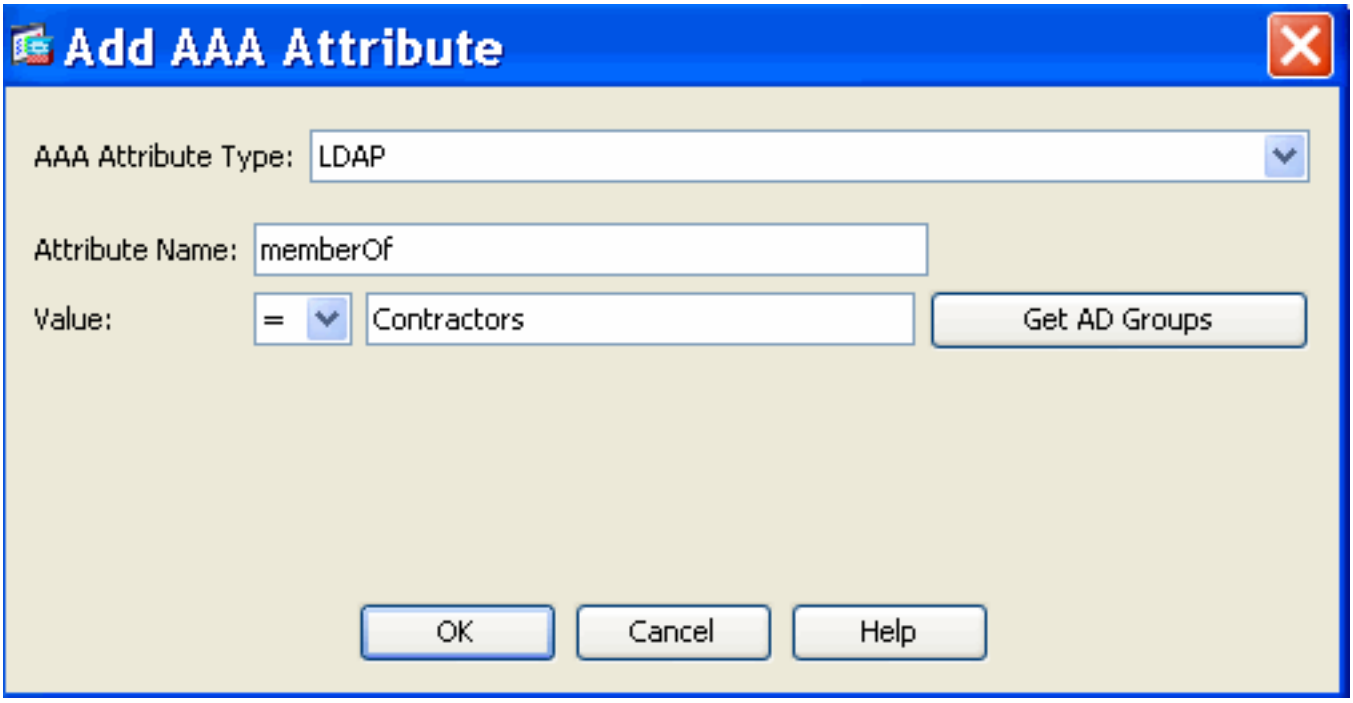
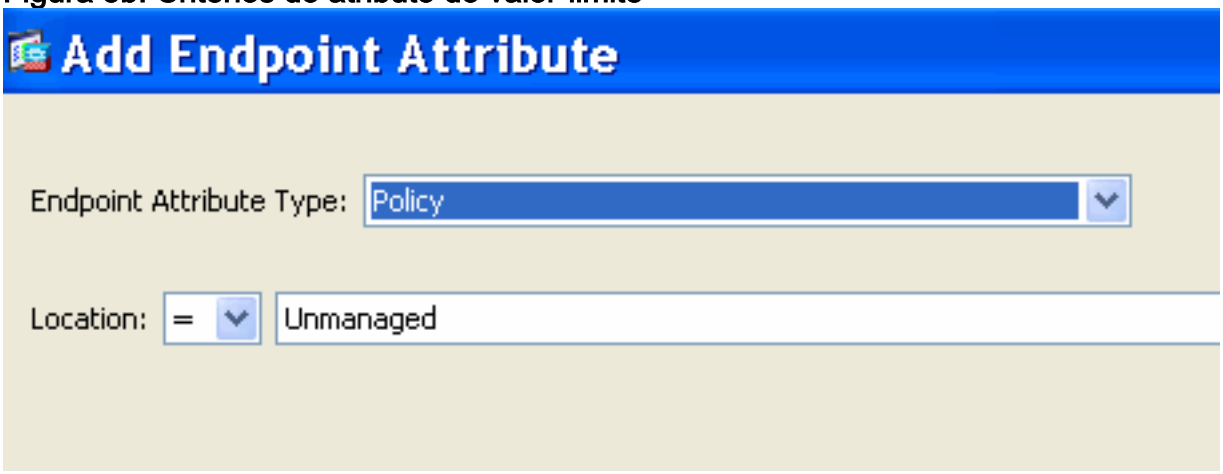
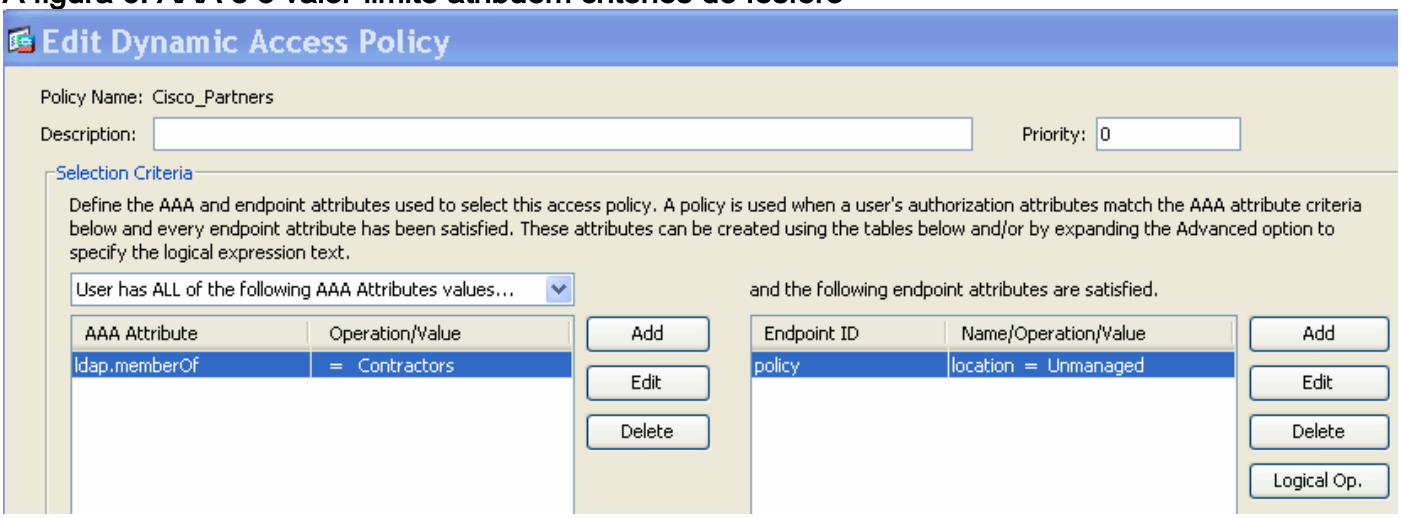



Figura 5b. Critérios do atributo do valor-limite




Assim, para combinar o registro DAP mostrado na figura 6, o usuário de autenticação deve ser um membro do grupo do diretório ativo dos contratantes e seu valor-limite de conexão deve satisfazer o valor de política CSD “inalterado,” para ser atribuído o registro DAP.

A figura 6. AAA e o valor-limite atribuem critérios do fósforo

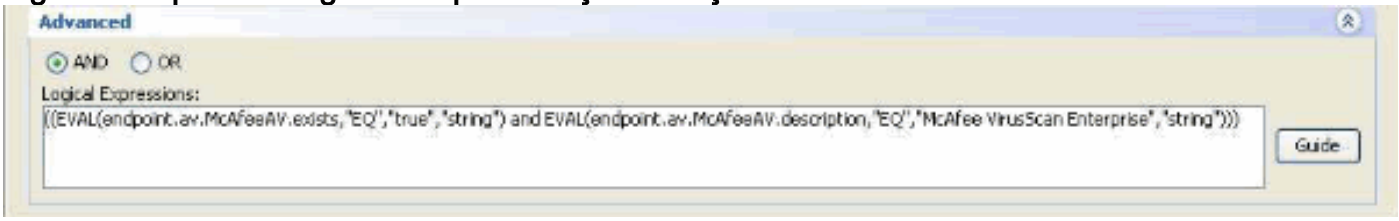



O AAA e os atributos do valor-limite podem ser criados usando as tabelas como descrito na figura

6 e/ou expandindo a opção avançada para especificar uma expressão lógica segundo as indicações da figura 7. Atualmente, a expressão lógica é construída com funções EVAL, por exemplo, EVAL (endpoint.av.McAfeeAV.exists, “EQ”, “verdadeiro”, “corda”) e EVAL (endpoint.av.McAfeeAV.description, “EQ”, da “empresa de VirusScan McAfee”, “corda”), que representam operações lógica da seleção AAA e/ou de valor-limite.

As expressões lógicas são úteis para adicionar critérios de seleção diferentes do que é possível nas áreas do atributo AAA e de valor-limite acima. Por exemplo, quando você puder configurar as ferramentas de segurança para usar os atributos AAA que não satisfazem alguns, todos os ou nenhuns critérios especificados, os atributos do valor-limite são cumulativos, e devem tudo ser satisfeitos. Para deixar a ferramenta de segurança empregar um atributo ou outro do valor-limite, você precisa de criar expressões lógicas apropriadas sob a seção avançada do registro DAP.

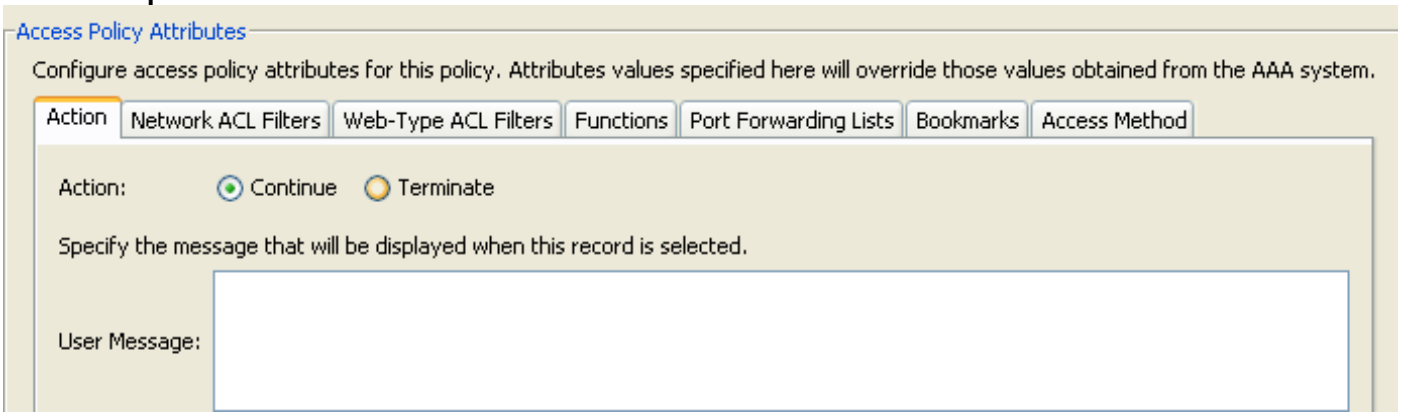
**Figura 7. expressão lógica GUI para criação avançada do atributo**




A seção dos atributos da política de acesso segundo as indicações de figura 8 é onde um administrador configuraria atributos do acesso VPN para um registro específico DAP. Quando a autorização de um usuário atribuir o fósforo os critérios AAA, de valor-limite e/ou da expressão lógica; os valores de atributo de política do acesso configurado nesta seção serão reforçados. Os valores de atributo especificados aqui cancelarão aqueles valores obtidos do sistema AAA, incluindo aqueles em usuário existente, o grupo, o grupo de túneis, e os registros de grupo padrão.

Um registro DAP tem um conjunto limitado de valores de atributo que podem ser configurados. Estes valores caem sob as seguintes abas segundo as indicações de figuras 8 a 14:

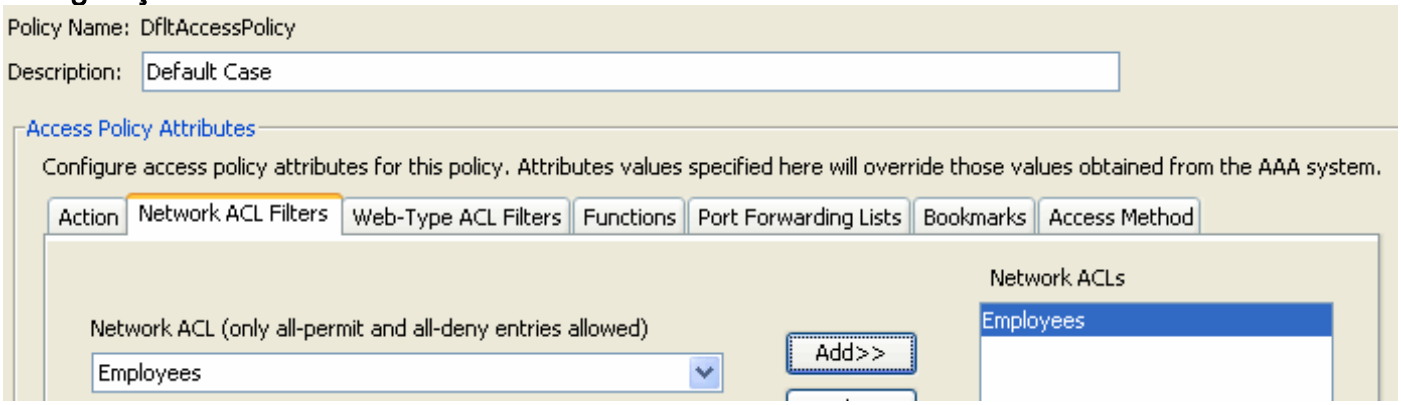
**Figura 8. ação — Especifica o processamento especial a aplicar-se a uma conexão ou a uma sessão específica.**




- Continue — (padrão) clique para aplicar atributos da política de acesso à sessão.
- Termine — Clique para terminar a sessão.
- Mensagem do usuário — Incorpore um mensagem de texto para indicar na página portal quando este registro DAP é selecionado. Caráteres 128 máximos. Exibições de mensagem de um usuário como uma esfera amarela. Quando um usuário entra, pisca três vezes atrair a atenção, e então é ainda. Se diversos registros DAP estão selecionados, e cada um deles tem uma mensagem do usuário, todo o indicador de mensagens do usuário. Adicionalmente,

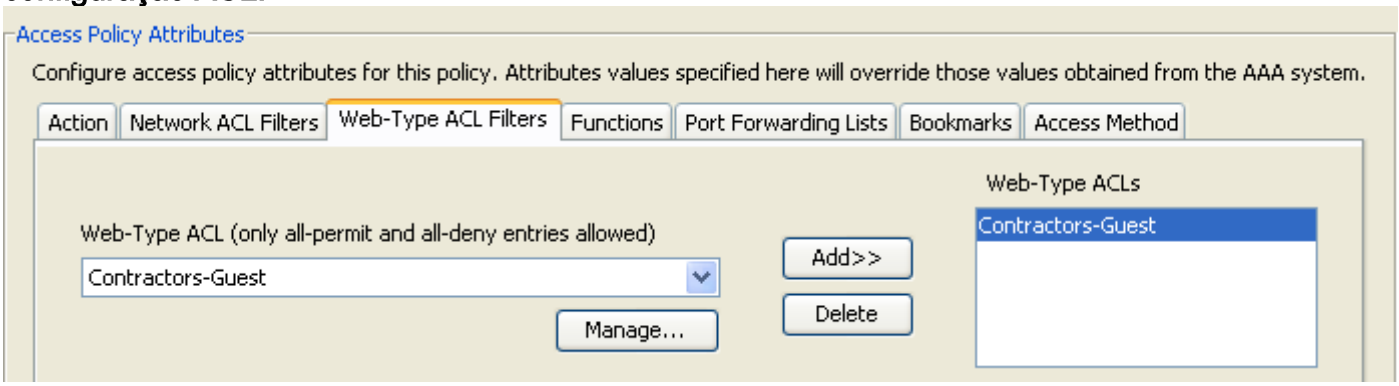
você pode incluir em tais mensagens as URL ou no outro texto encaixado, que exigem que você usa as etiquetas corretas HTML.

**Figura 9. aba dos filtros da rede ACL — Deixa-o selecionar e configurar a rede ACL para aplicar-se a este registro DAP. Um ACL para o DAP pode conter regras do permit or deny, mas não ambas. Se um ACL contém a licença e nega regras, a ferramenta de segurança rejeita a configuração ACL.**




- Caixa suspensa da rede ACL — Selecione já a rede configurada ACL para adicionar a este registro DAP. Somente os ACL que mandam tudo permitir ou todos negam regras são elegíveis, e estes são os únicos ACL que indicam aqui.
- Controle — Clique para adicionar, editar, e suprimir da rede ACL.
- Lista da rede ACL — Indica a rede ACL para este registro DAP.
- Adicionar — Clique para adicionar a rede selecionada ACL da caixa suspensa à lista da rede ACL à direita.
- Supressão — Clique para suprimir de uma rede destacada ACL da lista da rede ACL. Você não pode suprimir de um ACL se é atribuído a um DAP ou a outro registro.

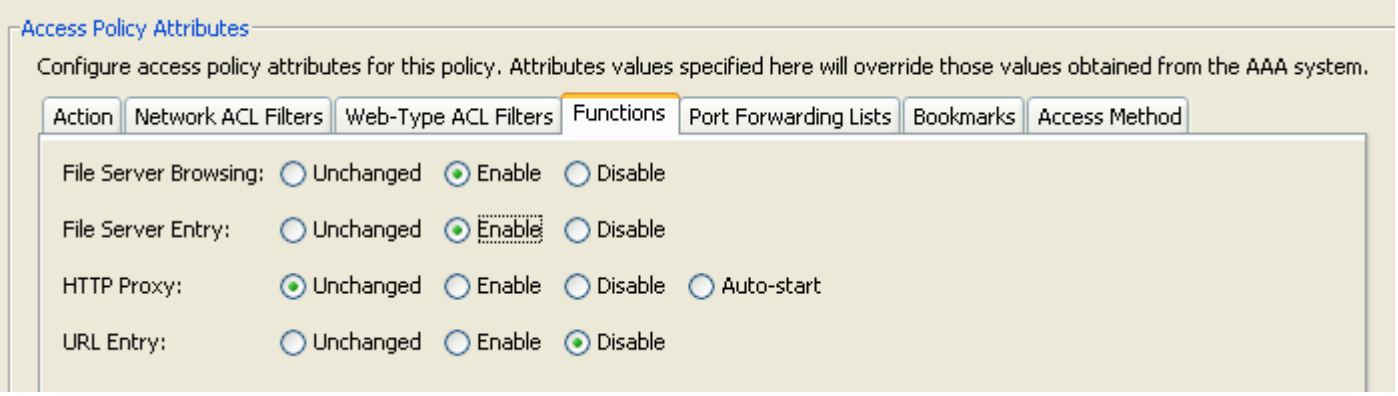
**Figura 10. Web-tipo aba dos filtros ACL — Deixa-o selecionar e configurar o Web-tipo ACL para aplicar-se a este registro DAP. Um ACL para o DAP pode conter somente regras do permit or deny. Se um ACL contém a licença e nega regras, a ferramenta de segurança rejeita a configuração ACL.**




- Web-tipo caixa suspensa ACL — Selecione o Web-tipo já configurado ACL para adicionar a este registro DAP. Somente os ACL que mandam tudo permitir ou todos negam regras são elegíveis, e estes são os únicos ACL que indicam aqui.
- Controle… — Clique para adicionar, editar, e suprimir do Web-tipo ACL.
- Web-tipo lista ACL — Indica o Web-tipo ACL para este registro DAP.
- Adicionar — Clique para adicionar o Web-tipo selecionado ACL da caixa suspensa ao Web-tipo lista ACL à direita.
- Supressão — Clique para suprimir de um Web-tipo ACL do Web-tipo lista ACL. Você não

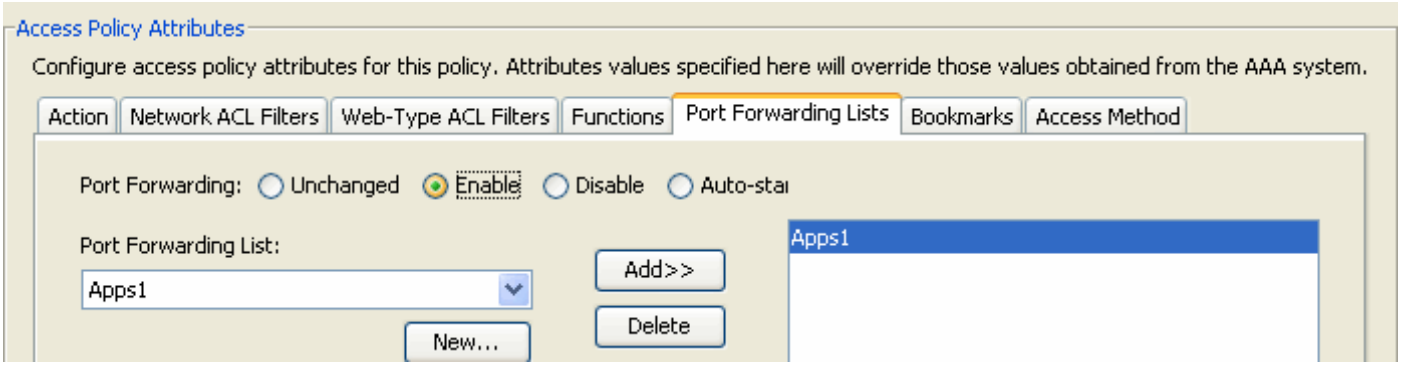
pode suprimir de um ACL se é atribuído a um DAP ou a outro registro.

**Figura 11. aba das funções — Deixa-o configurar a entrada e a consultação do servidor de arquivo, o proxy HTTP, e a entrada URL para o registro DAP.**



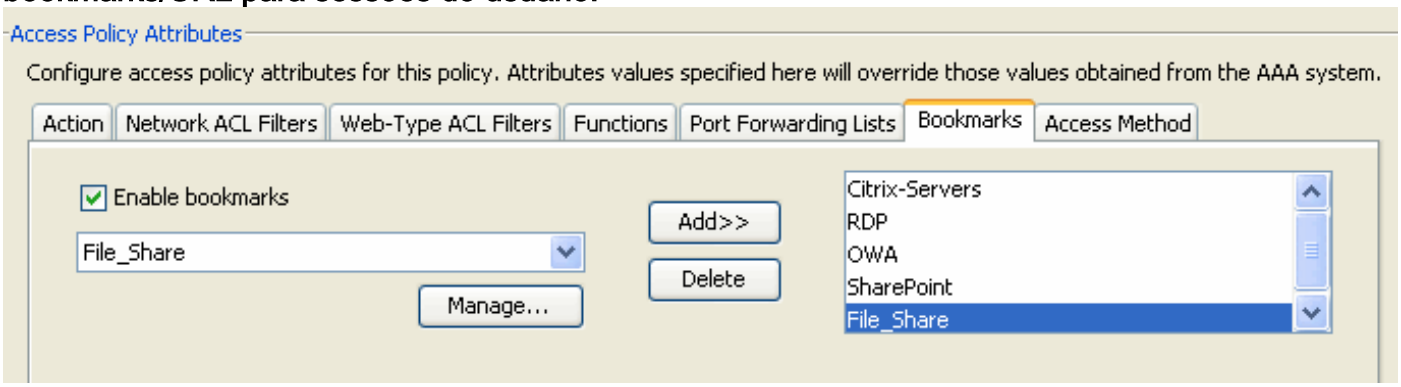

- Servidor de arquivo que consulta — Permite ou desabilita CIFS que consulta para servidores de arquivo ou características da parte.
- Entrada do servidor de arquivo — Permite ou nega um usuário dos trajetos entrando do servidor de arquivo e nomes na página portal. Quando permitido, coloca a gaveta da entrada do servidor de arquivo na página portal. Os usuários podem incorporar pathnames aos arquivos de Windows diretamente. Podem transferir, editar, suprimir, rebatizar, e mover de arquivos. Podem igualmente adicionar arquivos e dobradores. As partes devem igualmente ser configuradas para o acesso de usuário nos server aplicáveis de Microsoft Windows. Os usuários puderam ter que ser autenticado antes de alcançar arquivos, segundo requisitos de rede.
- Proxy HTTP — Afeta a transmissão de um proxy do applet HTTP ao cliente. O proxy é útil para as Tecnologias que interferem com a transformação de conteúdo apropriada, tal como Javas, ActiveX, e flash. Contorneia o massacre/processo da reescrita ao assegurar o uso continuado da ferramenta de segurança. O proxy enviado altera a configuração de proxy velha do navegador automaticamente e reorienta todos os pedidos HTTP e HTTPS à configuração de proxy nova. Apoia virtualmente todas as Tecnologias do lado do cliente, incluindo o HTML, o CSS, o Javascript, o VBScript, o ActiveX, e as Javas. O único navegador que apoia é Microsoft Internet explorer.
- Entrada URL — Permite ou impede que um usuário incorpore HTTP/HTTPS URL na página portal. Se esta característica é permitida, os usuários podem incorporar endereços de web à caixa da entrada URL, e usam os sem clientes SSL VPN para alcançar aqueles Web site.
- Inalterado — (padrão) clique para usar valores da política do grupo que se aplica a esta sessão.
- Permita/desabilitação — Clique para permitir ou desabilitar a característica.
- Arranque automático — Clique para permitir automaticamente o proxy HTTP e para mandar o registro DAP começar os applet associados com estas características.

**Figura 12. A transmissão da porta alista a aba — Deixa-o selecionar e configurar a transmissão da porta alista para sessões do usuário.**




- Transmissão da porta — Selecione uma opção para as lista da transmissão da porta que se aplicam a este registro DAP. Os outros atributos neste campo forem permitidos somente quando você set port que enviam para permitir ou arranque automático.
- Inalterado — Clique para usar valores da política do grupo que se aplica a esta sessão.
- Permita/desabilitação — Clique para permitir ou desabilitar a transmissão da porta.
- Arranque automático — Clique para permitir automaticamente a transmissão da porta, e para mandar o registro DAP começar os applet da transmissão da porta associados com suas lista da transmissão da porta.
- Mova a caixa suspensa da lista da transmissão — Selecione já lista da transmissão da porta configurada para adicionar ao registro DAP.
- Novo — Clique para configurar lista novas da transmissão da porta.
- Mova lista da transmissão — Indica a lista da transmissão da porta para o registro DAP.
- Adicionar — Clique para adicionar a lista da transmissão da porta selecionada da caixa suspensa à lista da transmissão da porta à direita.
- Supressão — Clique para suprimir da lista da transmissão da porta selecionada da lista da transmissão da porta. Você não pode suprimir de um ACL se é atribuído a um DAP ou a outro registro.

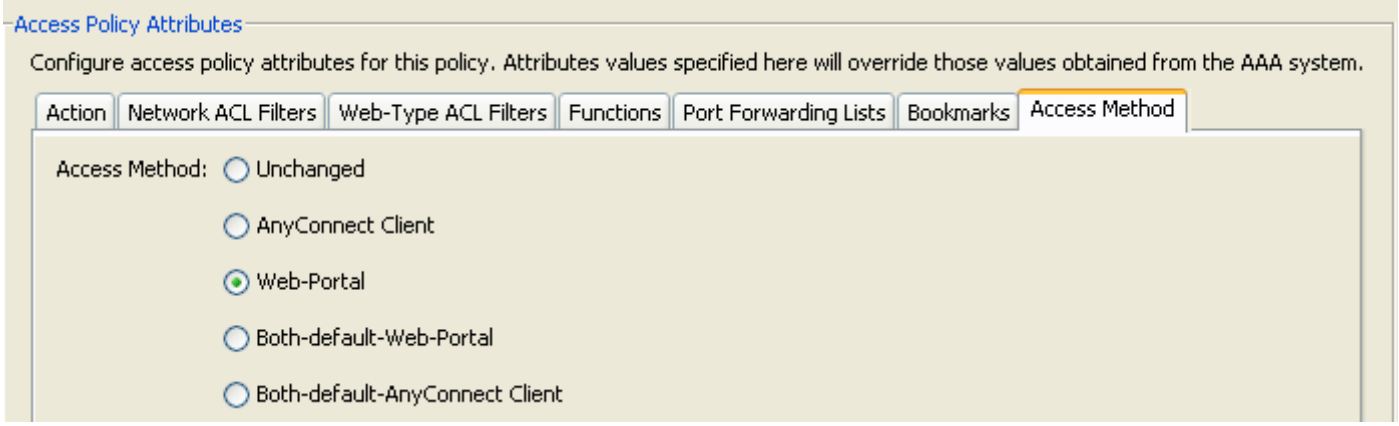
**Figura 13. Marca um endereço da Internet a aba — Deixa-o selecionar e configurar lista bookmarks/URL para sessões do usuário.**




- Permita endereços da Internet — Clique para permitir. quando esta caixa não for selecionada, nenhum indicador das lista do endereço da Internet na página portal para a conexão
- Controle — Clique para adicionar, importar, exportar, e suprimir de lista do endereço da Internet.
- Lista dos endereços da Internet (gota-para baixo) — Indica as lista do endereço da Internet para o registro DAP.
- Adicionar — Clique para adicionar a lista selecionada do endereço da Internet da caixa suspensa à caixa de lista do endereço da Internet à direita.
- Supressão — Clique para suprimir da lista selecionada do endereço da Internet da caixa de

lista do endereço da Internet. Você não pode suprimir de uma lista do endereço da Internet da ferramenta de segurança a menos que você suprimir primeiramente d dos registros DAP.

**Figura 14. Aba do método — Deixa-o configurar o tipo de Acesso remoto permitido.**




- Inalterado — Continue com o método atual do Acesso remoto ajustado na grupo-política para a sessão.
- Cliente de AnyConnect — Conecte usando o Cisco AnyConnect VPN Client.
- Portal da web — Conecte com os sem clientes VPN.
- Ambo-padrão-Web-portal — Conecte através dos sem clientes ou do cliente de AnyConnect, com um padrão dos sem clientes.
- cliente do Ambo-padrão-AnyConnect — Conecte através dos sem clientes ou do cliente de AnyConnect, com um padrão de AnyConnect.

Como mencionado previamente, um registro DAP tem um conjunto limitado de valores de atributo do padrão, simplesmente se são alterados tomarão a precedência sobre o AAA existente, o usuário, o grupo, o grupo de túneis, e os registros de grupo padrão. Se os valores de atributo adicionais fora do âmbito do DAP são exigidos, por exemplo, lista do Split Tunneling, bandeiras, túneis espertos, as personalizações portais,… etc., deverão então ser reforçadas através do AAA, do usuário, do grupo, do grupo de túneis, e dos registros de grupo padrão. Neste caso, aqueles valores de atributo específicos complementarão o DAP e não o estarão cancelando. Assim, o usuário obterá um grupo cumulativo de valores de atributo através de todos os registros.

## Agregando políticas múltiplas do acesso dinâmico

Um administrador pode configurar registros múltiplos DAP para endereçar muitas variáveis. Em consequência, é possível para um usuário de autenticação satisfazer o AAA e os critérios do atributo do valor-limite de registros múltiplos DAP. Na consequência, os atributos da política de acesso serão consistentes ou oporão durante todo estas políticas. Neste caso, o usuário autorizado obterá o resultado cumulativo através de todos os registros combinados DAP.

Isto igualmente inclui os valores de atributo exclusivo reforçados através da autenticação, da autorização, do usuário, do grupo, do grupo de túneis, e dos registros de grupo padrão. O resultado cumulativo de atributos da política de acesso cria a política do acesso dinâmico. Os exemplos de atributos combinados da política de acesso são alistados nas tabelas abaixo. Estes exemplos descrevem os resultados de 3 registros combinados DAP.

O atributo da ação mostrado na tabela 1 tem um valor que seja termine ou continue. O valor de atributo agregado será termina se o valor da terminação está configurado em alguns dos registros selecionados DAP e para continuar se o valor da continuação está configurado em todos os registros selecionados DAP.

Atributo da ação da tabela 1.

| Nome do atributo | DAP#1 | DAP#2 | DAP#3 | DAP |
|---|---|---|---|---|
| Ação (exemplo 1) | continuar | continuar | continuar | continuar |
| Ação (exemplo 2) | Termine | continuar | continuar | termine |

O atributo da USER-mensagem mostrado na tabela 2 contém um valor de série. O valor de atributo agregado será uma corda separada da LINE FEED (valor de HEX 0x0A) criada ligando junto os valores de atributo dos registros selecionados DAP. Pedir dos valores de atributo na corda combinada é insignificante.

Atributo da USER-mensagem da tabela 2.

| Nome do atributo | DAP#1 | DAP#2 | DAP#3 | DAP |
|---|---|---|---|---|
| USER-mensagem | o rápido | raposa marrom | Saltos sobre | os fox<LF>jumps do quick<LF>brown sobre |

A característica dos sem clientes que permite os atributos (funções) mostrados na tabela 3 contém os valores que são arranque automático, permite ou desabilita. O valor de atributo agregado será arranque automático se o valor do arranque automático é configurado em alguns dos registros selecionados DAP.

O valor de atributo agregado será permite se não há nenhum valor do arranque automático configurado em alguns dos registros selecionados DAP, e o valor da possibilidade está configurado pelo menos em um dos registros selecionados DAP.

O valor de atributo agregado será desabilitação se não há nenhum arranque automático ou para permitir o valor configurado em alguns dos registros selecionados DAP, e o valor do “desabilitação” está configurado pelo menos em um dos registros selecionados DAP.

Característica dos sem clientes da tabela 3. permitindo atributos (funções)

| Nome do atributo | DAP#1 | DAP#2 | DAP#3 | DAP |
|---|---|---|---|---|
| porta-dianteiro | enable | disable | | enable |
| arquivo-consultação | disable | enable | disable | enable |
| entrada de arquivo | | | disable | disable |
| proxy HTTP | disable | arranque automático | disable | arranque automático |
| URL-entrada | disabl | | enabl | enable |

| | | | | |
|---|---|---|---|---|
| | e | | e | |

A lista URL e os atributos porta-dianteiros mostrados na tabela 4 contêm um valor que seja uma corda ou uma corda separada vírgula. O valor de atributo agregado será uma corda separada vírgula criada ligando junto os valores de atributo dos registros selecionados DAP. Alguns valor de atributo duplicado na corda combinada serão removidos. Pedir dos valores de atributos na corda combinada é insignificante.

A lista URL e a porta da tabela 4. enviam o atributo de lista

| Nome do atributo | DAP#1 | DAP#3 | DAP#3 | DAP |
|---|---|---|---|---|
| lista URL | a | b, c | a | a, b, c |
| porta-dianteiro | | d, e | e, f | d, e, f |

Os atributos do método de acesso especificam o método do acesso do cliente permitido para conexões de VPN SSL. O método do acesso do cliente pode ser acesso do cliente de AnyConnect somente, do acesso do portal da web acesso somente, do cliente de AnyConnect ou do portal da web com acesso do portal da web como o acesso do padrão ou do cliente ou do portal da web de AnyConnect com acesso do cliente de AnyConnect como o padrão. O valor de atributo agregado é resumido na tabela 5.

Atributos do método de acesso da tabela 5.

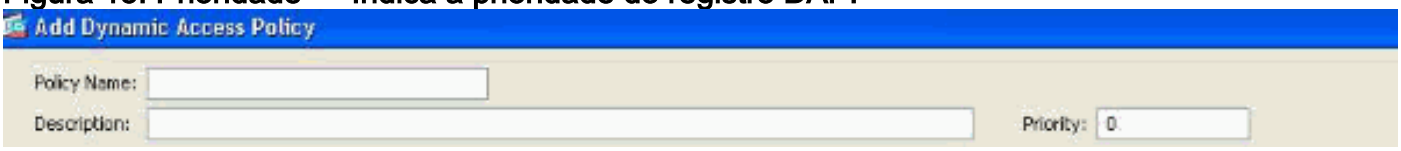
| Valores de atributo selecionados | | | | Resultado da agregação |
|---|---|---|---|---|
| Cliente de AnyConnect | Portal da web | Portal de Ambo-padrão-Web | cliente do Ambo-padrão-AnyConnect | |
| | | | X | cliente do Ambo-padrão-AnyConnect |
| | | X | | Ambo-padrão-Web-portal |
| | | X | X | Ambo-padrão-Web-portal |
| | X | | | Portal da web |
| | X | | X | cliente do Ambo-padrão-AnyConnect |
| | X | X | | Ambo-padrão-Web-portal |
| | X | X | X | Ambo-padrão-Web-portal |
| X | | | | Cliente de AnyConnect |
| X | | | X | cliente do Ambo-padrão-AnyConnect |
| X | | X | | Ambo-padrão- |

| | | | | |
|---|---|---|---|---|
| | | | | Web-portal |
| X | | X | X | Ambo-padrão-Web-portal |
| X | X | | | Ambo-padrão-Web-portal |
| X | X | | X | cliente do Ambo-padrão-AnyConnect |
| X | X | X | | Ambo-padrão-Web-portal |
| X | X | X | X | Ambo-padrão-Web-portal |

Quando agregar a rede (Firewall) e o Web-tipo (sem clientes) atributos do filtro ACL, a prioridade DAP e DAP ACL é dois componentes principais a considerar.

O atributo de prioridade segundo as indicações de figura 15 não é agregado. A ferramenta de segurança usa este valor para arranjar em sequência logicamente as Listas de acesso ao agregar a rede e o Web-tipo ACL dos registros múltiplos DAP. A ferramenta de segurança pede os registros do mais altamente ao mais baixo número de prioridade, com o mais baixo na parte inferior da tabela. Por exemplo, um registro DAP com um valor de 4 tem uma prioridade mais alta do que um registro com um valor de 2. Você não pode manualmente classificá-los.

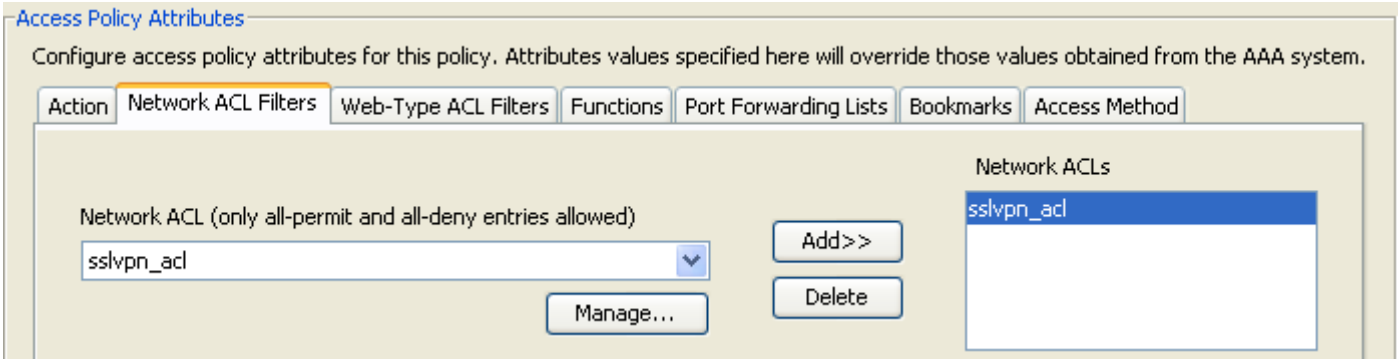
**Figura 15. Prioridade — Indica a prioridade do registro DAP.**




- Nome da política — Indica o nome do registro DAP.
- Descrição — Descreve a finalidade do registro DAP.

O atributo DAP ACL apoia somente as listas de acesso que se conformam a “Branco-lista” ou a um modelo restrito restrito ACL da “lista negra”. Em um modelo ACL da “Branco-lista”, as entradas de lista de acesso especificam as regras que “permita” o acesso às redes especificadas ou aos anfitriões. Em um modo ACL da “lista negra”, as entradas de lista de acesso especificam as regras que “negue” a acesso às redes especificadas ou aos anfitriões. Uma lista de acesso deconformação contém entradas de lista de acesso com uma mistura da “licença” e “negue” regras. Se uma lista de acesso nonconforming é configurada para um registro DAP, estará rejeitada como um erro de configuração quando o administrador tenta adicionar o registro. Se uma lista de acesso de conformação é atribuída a um registro DAP, a seguir toda a alteração à lista de acesso que muda a característica da conformidade estará rejeitada como um erro de configuração.

**Figura 16. DAP ACL — Deixa-o selecionar e configurar a rede ACL para aplicar-se a este registro DAP.**




Quando os registros múltiplos DAP são selecionados, os atributos das listas de acesso especificados na rede (Firewall) ACL estão agregados para criar uma lista de acesso dinâmica para o Firewall ACL DAP. Da mesma forma, os atributos das listas de acesso especificados no Web-tipo (sem clientes) ACL são agregados para criar uma lista de acesso dinâmica para os sem clientes ACL DAP. O exemplo abaixo focalizará em como uma lista de acesso dinâmica do Firewall DAP é criada especificamente. Contudo, uma lista de acesso dinâmica dos sem clientes DAP seguirá o mesmo processo.

Primeiramente, o ASA criará dinamicamente um nome exclusivo para o DAP REDE-ACL segundo as indicações da tabela 6.

**Nome dinâmico da tabela 6. DAP Rede-ACL**

| Nome DAP Rede-ACL |
|---|
| DAP-Rede-ACL-x (onde X é um inteiro que incremente para assegurar a unicidade) |

Em segundo, o ASA recuperará o atributo Rede-ACL dos registros selecionados DAP segundo as indicações da tabela 7.

**Rede ACL da tabela 7.**

| Registros selecionados DAP | Prioridade | Rede-ACL | Entradas Rede-ACL |
|---|---|---|---|
| DAP 1 | 1 | 101 e 102 | O ACL 101 manda 4 negar regras e o ACL 102 tem 4 regras da licença |
| DAP 2 | 2 | 201 e 202 | O ACL 201 tem 3 regras da licença e o ACL 202 manda 3 negar regras |
| DAP 3 | 2 | 101 e 102 | O ACL 101 manda 4 negar regras e o ACL 102 tem 4 regras da licença |

Em terceiro lugar, o ASA requisitará novamente os Rede-ACL primeiramente pelo número de prioridade do registro DAP, e então pela lista negra primeiramente se o valor de prioridade para os registros 2 ou mais selecionados DAP são os mesmos. Depois disto, o ASA recuperará então as entradas Rede-ACL de cada Rede-ACL segundo as indicações da tabela 8.

**Prioridade do registro da tabela 8. DAP**

| Rede-ACL | Prioridade | Modelo branco/do preto lista de acesso | Entradas Rede-ACL |
|---|---|---|---|
| 101 | 2 | Lista negra | 4 negue as regras (DDDD) |
| 202 | 2 | Lista negra | 3 negue regras (o DDD) |
| 102 | 2 | Branco-lista | 4 regras da licença (PPPP) |
| 202 | 2 | Branco-lista | 3 regras da licença (PPP) |
| 101 | 1 | Lista negra | 4 negue as regras (DDDD) |
| 102 | 1 | Branco-lista | 4 regras da licença (PPPP) |

Ultimamente, o ASA fundirá as entradas Rede-ACL no Rede-ACL dinamicamente gerado e retornará então o nome do Rede-ACL dinâmico como o Rede-ACL novo a ser reforçado segundo as indicações da tabela 9.

**Tabela 9. DAP dinâmico Rede-ACL**

| Nome DAP Rede-ACL | Entrada Rede-ACL |
|---|---|
| DAP-Network-ACL-1 | DDD PPPP PPP<br>DDDD PPPP DDDD |

## Aplicação DAP

Há um host das razões pelas quais um administrador deve considerar executar o DAP. Algumas razões subjacentes são quando a avaliação da postura em um valor-limite deve ser reforçado, e/ou quando um AAA mais granulado ou os atributos de política devem ser considerada quando autorizando o acesso de usuário aos recursos de rede. No exemplo abaixo, nós configuraremos o DAP e os seus componentes para identificar um valor-limite de conexão e para autorizar o acesso de usuário aos vários recursos de rede.

Caso de teste – Um cliente pediu um proof-of-concept com as seguintes exigências do acesso VPN:

- A capacidade para detectar e identificar um valor-limite dos empregados como controlado ou Unmanaged. — Se o valor-limite está identificado como controlado (trabalho PC) mas falha as exigências da postura, esse valor-limite deve então ser negado o acesso. Por outro lado, se o valor-limite do empregado está identificado como unmanaged (o PC home), esse valor-limite deve então ser concedido o acesso dos sem clientes.
- A capacidade para invocar a limpeza de Cookie da sessão e para pô-la em esconderijo quando uma conexão dos sem clientes terminar.
- A capacidade para detectar e reforçar aplicativos running nos valores-limite dos empregados controlados, tais como o AntiVirus da McAfee. Se o aplicativo não existe, esse valor-limite deve então ser negado o acesso.

- A capacidade para usar a autenticação de AAA para determinar que usuários autorizados dos recursos de rede deve ter o acesso. A ferramenta de segurança deve apoiar a autenticação LDAP nativa MS e apoiar papéis múltiplos da membrasia do clube LDAP.
- A capacidade para permitir o acesso do LAN local aos recursos de rede tais como fax e impressoras da rede quando conectada através de um “cliente/rede” baseou a conexão.
- A capacidade para fornecer autorizou o acesso do convidado aos contratantes. Os contratantes e seus valores-limite devem obter o acesso dos sem clientes, e seu acesso portal aos aplicativos deve limitado em comparação com um empregado.

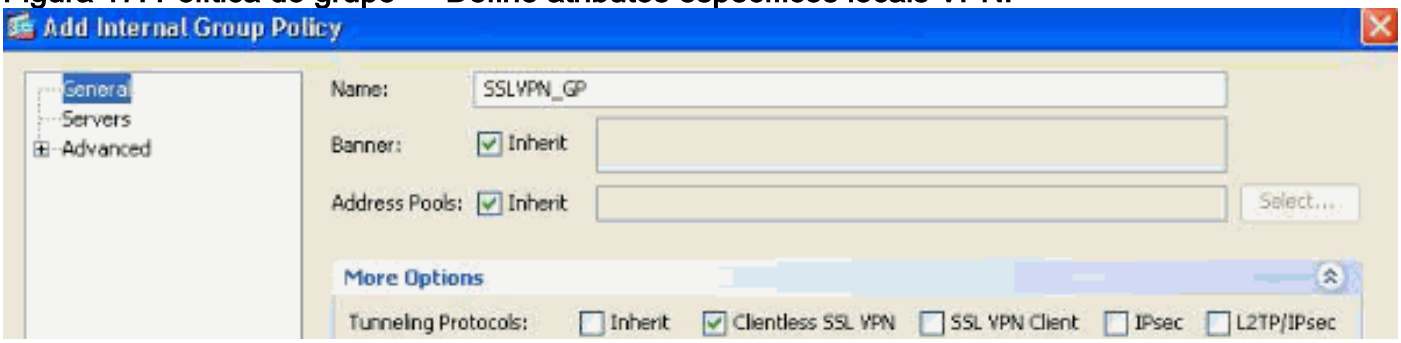
Neste exemplo, nós executaremos uma série de etapas de configuração em um esforço para cumprir as exigências do acesso VPN do cliente. Haverá as etapas de configuração que são necessárias mas relativas não diretamente ao DAP quando outras configurações serão relacionadas diretamente ao DAP. O ASA é muito dinâmico e pode adaptar-se em muitos ambientes de rede. Em consequência, as soluções de VPN podem ser definidas em várias maneiras e para fornecer em alguns casos as mesmas terminam a solução. A aproximação tomada contudo é conduzida pelos seus ambientes dos clientes pelas necessidades e.

Baseado na natureza deste papel e das exigências de cliente definidas, nós usaremos o Security Device Manager adaptável (ASDM) 6.0(x) e focalizaremos a maioria de nossas configurações em torno do DAP. Contudo, nós igualmente configuraremos políticas do grupo local para mostrar como o DAP pode complementar e/ou cancelar atributos da política local. Para a base deste caso de teste, nós suporemos um grupo de servidor ldap, lista de redes de split tunneling e a conectividade básica IP, incluindo associações IP e o grupo de servidor de DefaultDNS, preconfigured.

**Definindo uma política do grupo — esta configuração é necessária para definir atributos da política local. Alguns atributos definidos aqui não são configuráveis no DAP para (exemplo, acesso do LAN local). (Esta política será usada igualmente para definir sem clientes e atributos baseados cliente).**

Navegue à **configuração > ao acesso remoto VPN > ao acesso > ao grupo da rede (cliente) políticas**, e adicionar uma Política interna de grupo fazendo o seguinte:

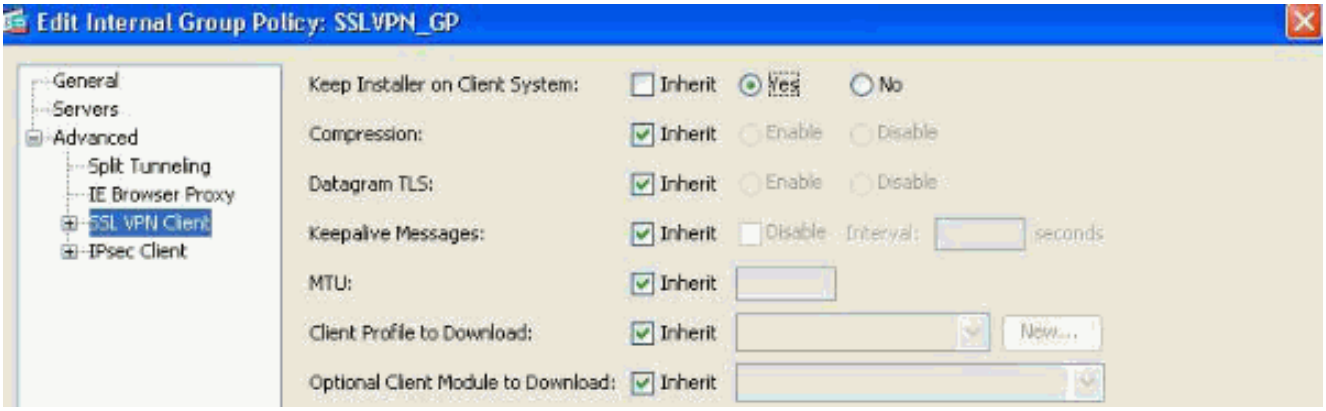
**Figura 17. Política do grupo — Define atributos específicos locais VPN.**




1. Sob o link geral, configurar o nome **SSLVPN_GP** para a política do grupo.
2. Igualmente sob o link geral, clique **mais opções** e configurar somente o protocolo de tunelamento: **Sem clientes SSLVPN**. (Nós configuraremos o DAP para cancelar e controlar o método de acesso.)
3. Sob o avançado > o link do Split Tunneling, configura o seguinte:**Figura 18. Split Tunneling — Permite que o tráfego especificado (rede local) contorneie um túnel unencrypted durante uma conexão de cliente.**


Política: Desmarcar **herdam** e seleto **exclua o liste de redes abaixo**.Liste de redes: Desmarcar **herdam** e selecionam o nome de lista **Local_Lan_Access**. (Suposto preconfigured.)

4. Sob o avançado > o link do cliente VPN SSL, configura o seguinte:**Figura 19. Instalador do cliente VPN SSL — Em cima da terminação VPN, o cliente SSL pode permanecer no valor-limite ou ser desinstalado.**

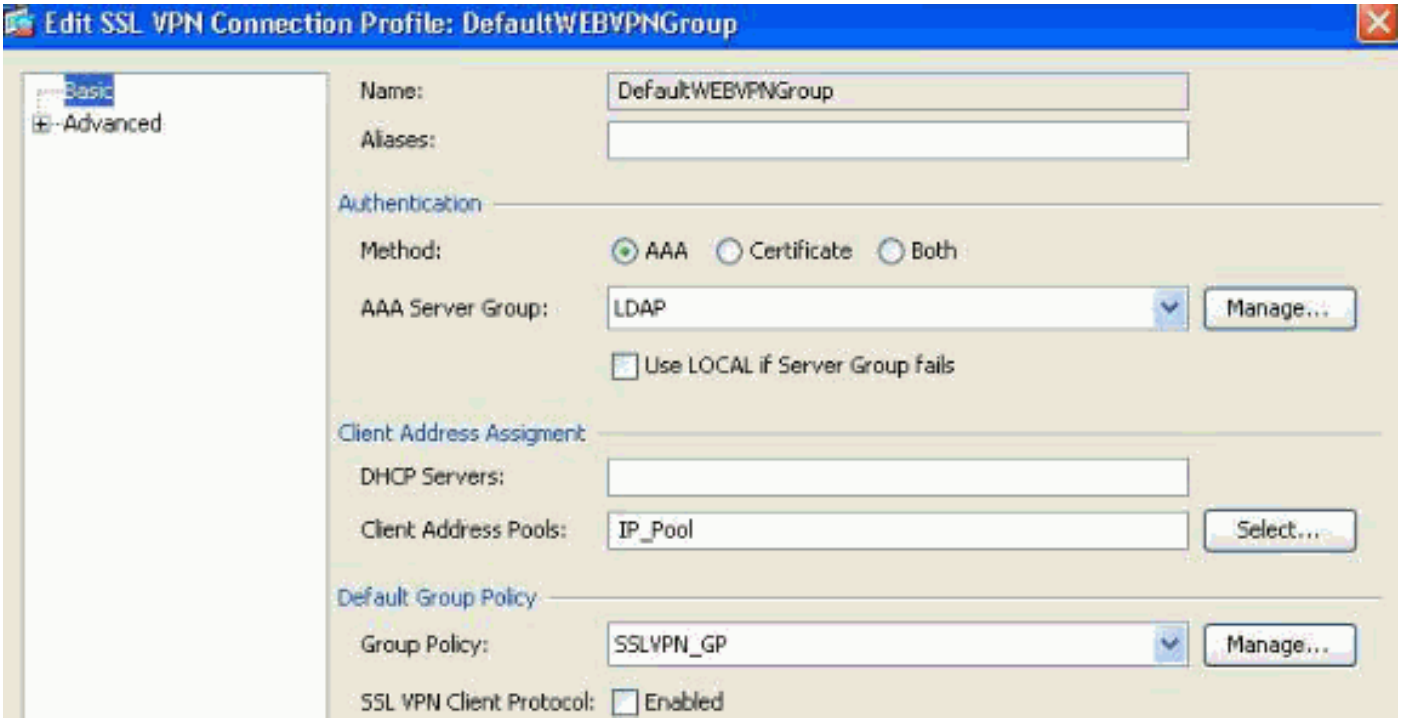



5. Mantenha o instalador no sistema de cliente: Desmarcar **herdam** e selecionam então **sim**.
6. **A APROVAÇÃO do** clique **aplica-se** então.
7. Aplique suas alterações de configuração.

**Definindo um perfil de conexão — esta configuração é necessária para definir nosso método de autenticação de AAA, por exemplo LDAP e aplicação da política previamente configurada do grupo (SSLVPN_GP) a este perfil de conexão. Os usuários que conectam através deste perfil de conexão serão sujeitados aos atributos definidos aqui assim como aos atributos definidos na política do grupo SSLVPN_GP. (Este perfil será usado igualmente para definir sem clientes e atributos baseados cliente).**

Navegue aos **perfis da conexão de VPN da configuração > do acesso >SSL do acesso remoto VPN > da rede (cliente)** e configurar o seguinte:

**Figura 20. Perfil de conexão — Define atributos específicos locais VPN.**

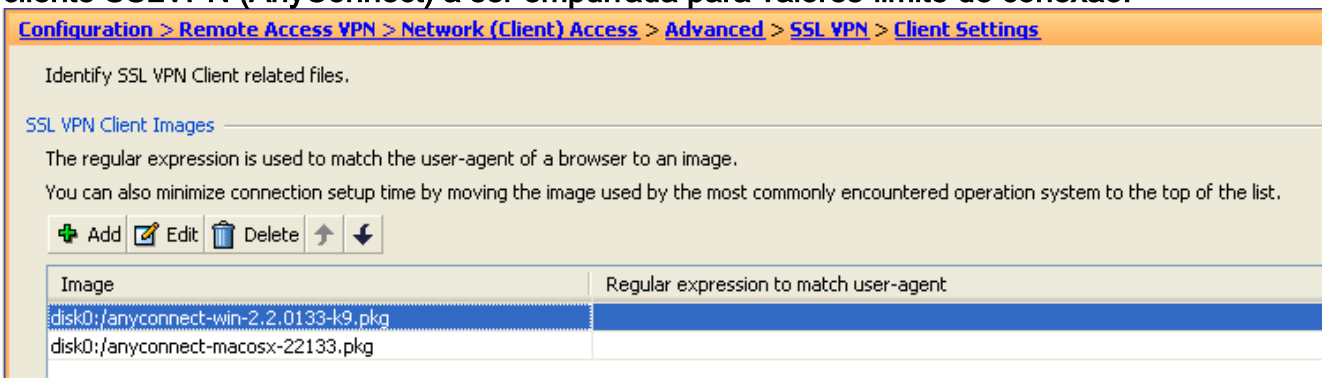



1. Sob os perfis de conexão secione, edite o DefaultWEBVPNGroup e sob o link básico configurar o seguinte:Método de autenticação: **AAA**Autenticação — Grupo de servidores AAA: **LDAP** (suposto preconfigured)Atribuição de endereço de cliente — Associações do endereço de cliente: **IP_Pool** (suposto preconfigured)Política do grupo de política do grupo padrão: Selecione **SSLVPN_GP**
2. Aplique suas mudanças de configurações.

**Definindo uma interface IP para a conectividade de VPN SSL — Esta configuração é necessária para terminar conexões SSL do cliente e dos sem clientes em uma interface especificada.**

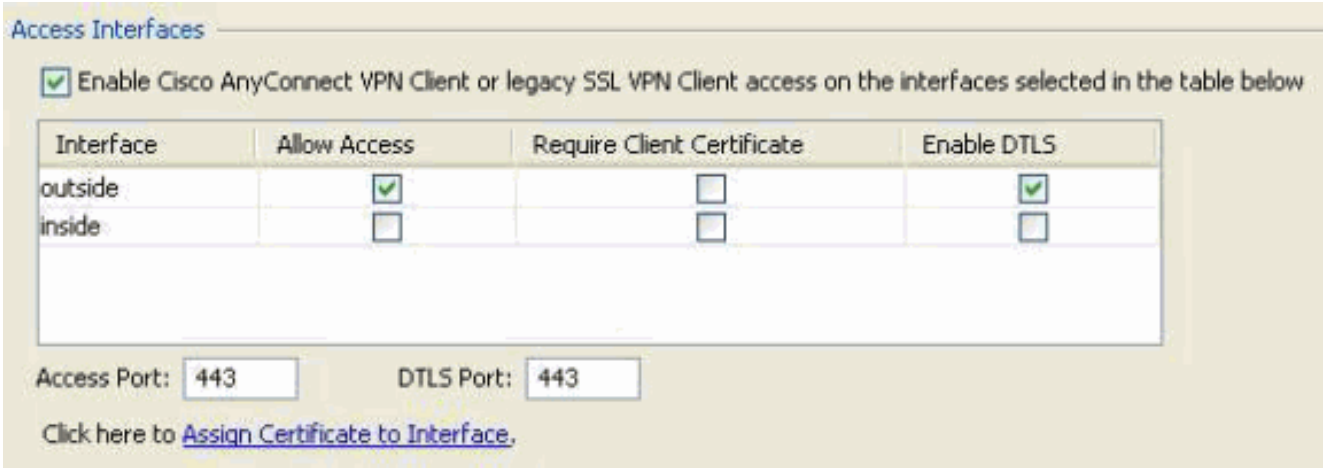
Antes de permitir o acesso do /Network do cliente em uma relação, você deve primeiramente definir uma imagem do cliente VPN SSL.

1. Navegue à **configuração > ao acesso do acesso remoto VPN > da rede (cliente) > avançou > SSL VPN > ajustes do cliente**, e adicionam a seguinte imagem do cliente VPN SSL do sistema de arquivo flash ASA: (Esta imagem pode ser transferida do CCO, www.cisco.com)**Figura 21. A imagem do cliente VPN SSL instala — Define a imagem do cliente SSLVPN (AnyConnect) a ser empurrada para valores-limite de conexão.**




**anyconnect-win-2.x.xxx-k9.pkg**Clique a **APROVAÇÃO**, **APROVAÇÃO** outra vez, e **aplique-a** então.

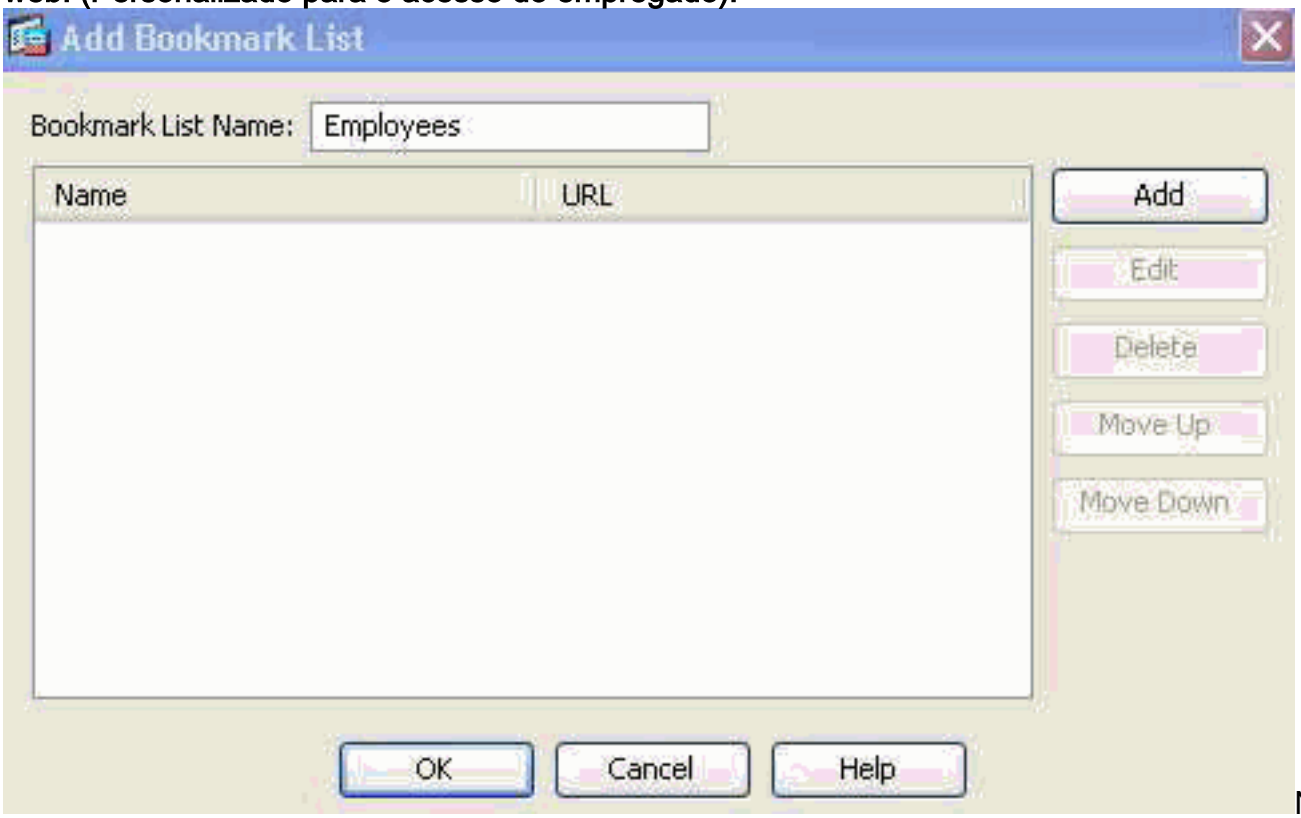
2. **Navegue à configuração > ao acesso do acesso remoto VPN > da rede (cliente) > à conexão de VPN SSL perfis**, e permita o seguinte:**Figura 22. Interface de acesso SSL VPN — Define as relações para terminar a conectividade de VPN SSL.**




Sob a seção da interface de acesso, permita: **"Permita o acesso do Cisco AnyConnect VPN Client ou de cliente VPN do legado SSL nas relações selecionadas na tabela abaixo."**Igualmente sob as interfaces de acesso secione, verificação **permitem o acesso na** interface externa. (Esta configuração igualmente permitirá o acesso dos sem clientes SSL VPN na interface externa.)Clique em Apply.

**Definir o endereço da Internet alista (listas URL) para o acesso dos sem clientes — esta configuração é necessária para definir um aplicativo baseado Web ser publicado no portal. Nós definiremos 2 listas URL, uma para empregados e a outro para contratantes.**

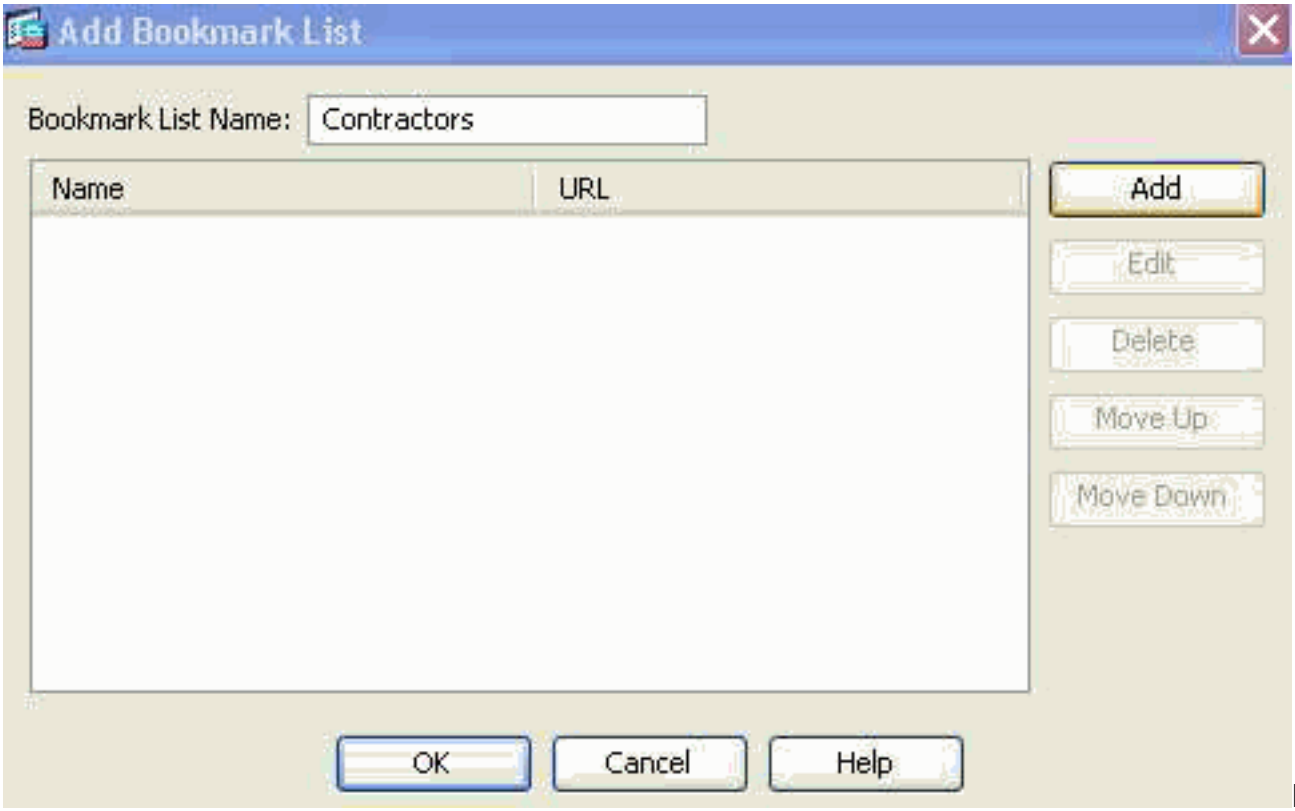
1. Navegue à **configuração > ao acesso remoto VPN > ao acesso > ao portal > aos endereços da Internet dos sem clientes SSL VPN**, o clique **+ adiciona** e configura o seguinte:**Figura 23. Lista do endereço da Internet — Define as URL a ser publicadas e alcançado do portal da web. (Personalizado para o acesso do empregado).**




N ome de lista do endereço da Internet: **Os empregados**, clicam então **adicionam**.Título do endereço da Internet: **Intranet da empresa**Valor URL: **http://company.resource.comA APROVAÇÃO do** clique e **APROVA** então outra vez.

2. O clique **+ adiciona** e configura uma segunda lista do endereço da Internet (lista URL) como segue:**Figura 24. Lista do endereço da Internet — Personalizado para o acesso do**

convidado.

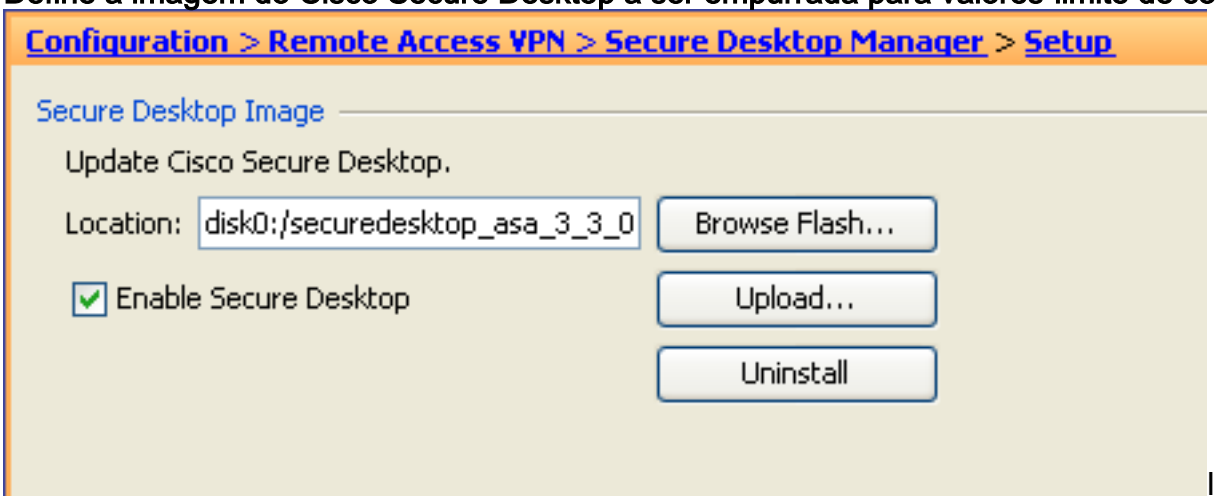



N
ome de lista do endereço da Internet: **Os contratantes**, clicam então **adicionam**.Título do endereço da Internet: **Acesso do convidado**Valor URL: **http://company.contractors.comA APROVAÇÃO do** clique e **APROVA** então outra vez.Clique em Apply.

**Cisco Secure Desktop — esta configuração é necessária para definir atributos da avaliação do valor-limite. Baseado nos critérios a ser satisfeitos, os valores-limite de conexão serão classificados como controlados ou Unmanaged. As avaliações do Cisco Secure Desktop são executadas antes do processo de autenticação.**

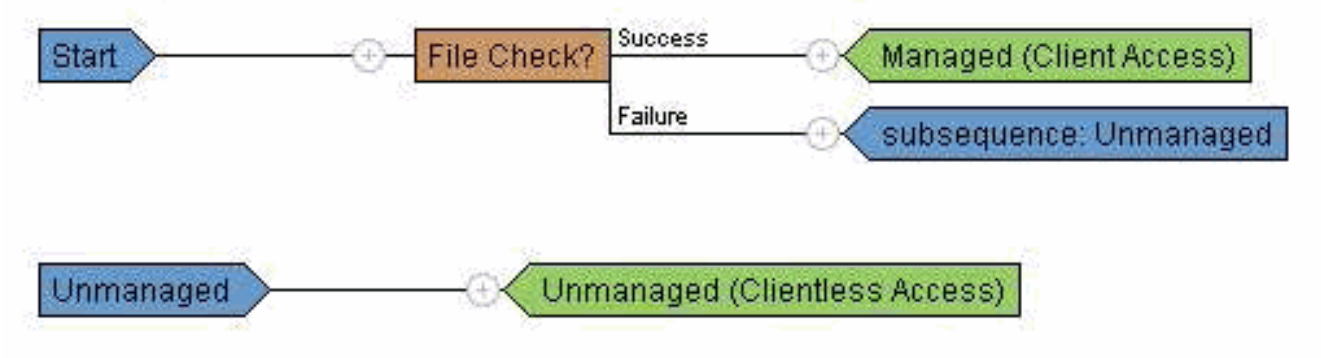
Configurando o Cisco Secure Desktop e pre uma árvore de decisão do início de uma sessão para lugar de Windows:

1. Navegue ao **gerente da configuração > do acesso remoto VPN > do Secure Desktop > Setup**, e configurar o seguinte:**Figura 25. A imagem do Cisco Secure Desktop instala — Define a imagem do Cisco Secure Desktop a ser empurrada para valores-limite de conexão.**



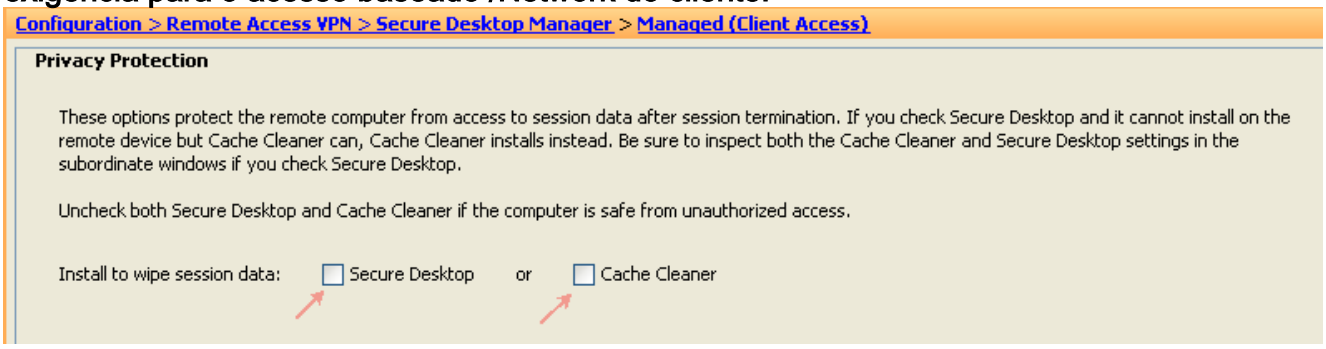

Instale a imagem **disk0:/securedesktop-asa-3.3.-xxx-k9.pkg do** sistema de arquivo flash ASA.A verificação **permite o Secure Desktop**.Clique em Apply.
2. Navegue à **configuração > ao gerente do acesso remoto VPN > do Secure Desktop > à**

**política de Prelogin**, e configurar o seguinte:**Figura 26. árvore de decisão do PRE-fazer logon — Personalizado através da verificação do arquivo para distinguir entre um valor-limite controlado e um valor-limite unmanaged.**



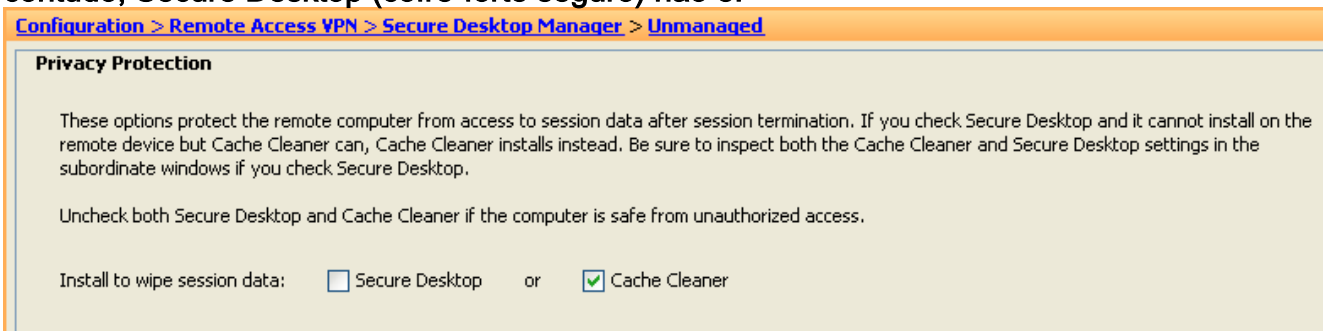

Clique o nó do **padrão** e rebatize a etiqueta **controlada (acesso do cliente)** e clique então a **atualização**.Clique " + " o símbolo no início do nó controlado.Para a verificação, selecione e adicionar a **verificação do arquivo** a ser introduzida.Entre em **C:\managed.txt** para o caminho de arquivo a "existe" e clicam a **atualização**.Clique o **início de uma sessão negou o** nó e selecionam então **Subsequence**.Entre em **Unmanaged** para a etiqueta e clique então a **atualização**.Clique o **início de uma sessão negou o** nó e selecionam então o **lugar**.Entre em **Unmanaged (acesso dos sem clientes)** para a etiqueta e clique então a **atualização**.O clique **aplica tudo**.

3. Navegue ao **gerente da configuração > do acesso remoto VPN > do Secure Desktop >Managed (acesso do cliente)**, e configurar o seguinte sob a seção das configurações de local:**Figura 27. Ajustes do lugar/proteção de privacidade — O Secure Desktop (cofre-forte seguro) e o líquido de limpeza do esconderijo (limpeza do navegador) não são uma exigência para o acesso baseado /Network do cliente.**




Módulo do lugar: Desmarcar o **Secure Desktop** e o **líquido de limpeza do esconderijo** se permitido.O clique **aplica tudo** se necessário.

4. Navegue ao **gerente da configuração > do acesso remoto VPN > do Secure Desktop > Unmanaged (acesso dos sem clientes)**, e configurar o seguinte sob a seção das configurações de local:**Figura 28. Configurações de local — O líquido de limpeza do esconderijo (limpeza do navegador) é uma exigência para o acesso baseado sem clientes, contudo, Secure Desktop (cofre-forte seguro) não é.**

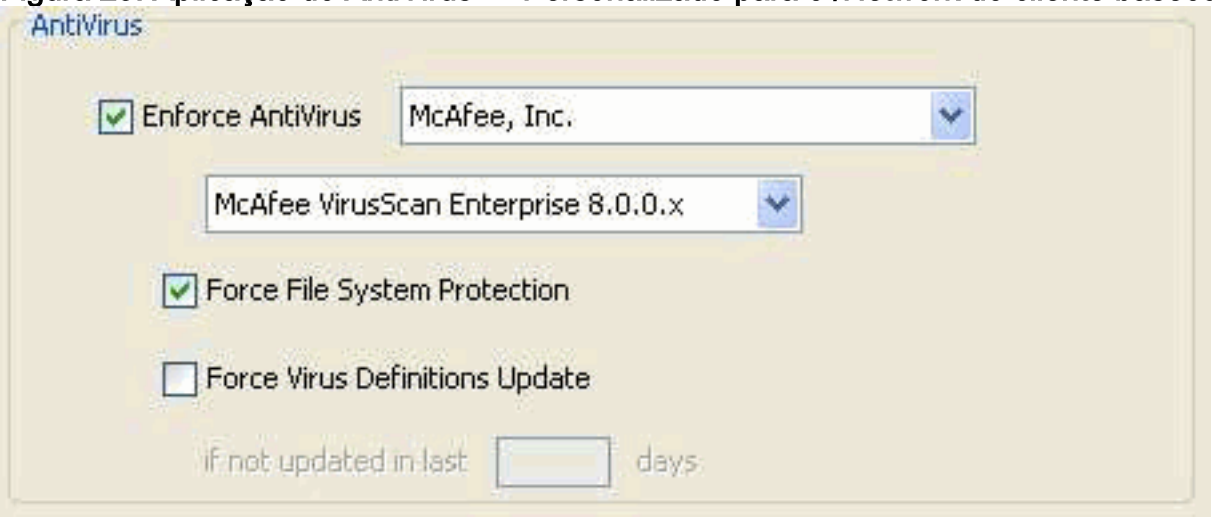


Módulo do lugar: Desmarcar o **Secure Desktop** e verifique o **líquido de limpeza do esconderijo**.O clique **aplica tudo**.

**Avaliação avançada do valor-limite — Esta configuração é necessária para reforçar o AntiVirus, o AntiSpyware e o firewall pessoal em um valor-limite. Por exemplo, esta avaliação verificará se a McAfee está sendo executado no valor-limite de conexão. (A avaliação avançada do valor-limite é uns recursos licenciado e não é configurável se a característica do Cisco Secure Desktop é desabilitada).**

Navegue à **configuração > ao acesso remoto VPN > ao gerente > ao host do Secure Desktop varredura**, e configurar o seguinte sob a seção dos Ramais da varredura do host:

**Figura 29. Aplicação do AntiVirus — Personalizado para o /Network do cliente baseou o acesso.**




Sob o host os Ramais da varredura que secionam, configuram o seguinte:

1. Selecione **ver avançado 2.3.3.1 da avaliação do valor-limite** e **configurar-lo** então.
2. Seleto **reforce o AntiVirus**.
3. Do AntiVirus do reforço deixe cair para baixo a lista, selecionam **McAfee, Inc.**
4. Da versão do AntiVirus deixe cair para baixo a lista selecionam a **empresa 8.0.0.x de VirusScan da McAfee**.
5. Selecione a **proteção de sistema de arquivos da força** e clique-a então **aplicam tudo**.

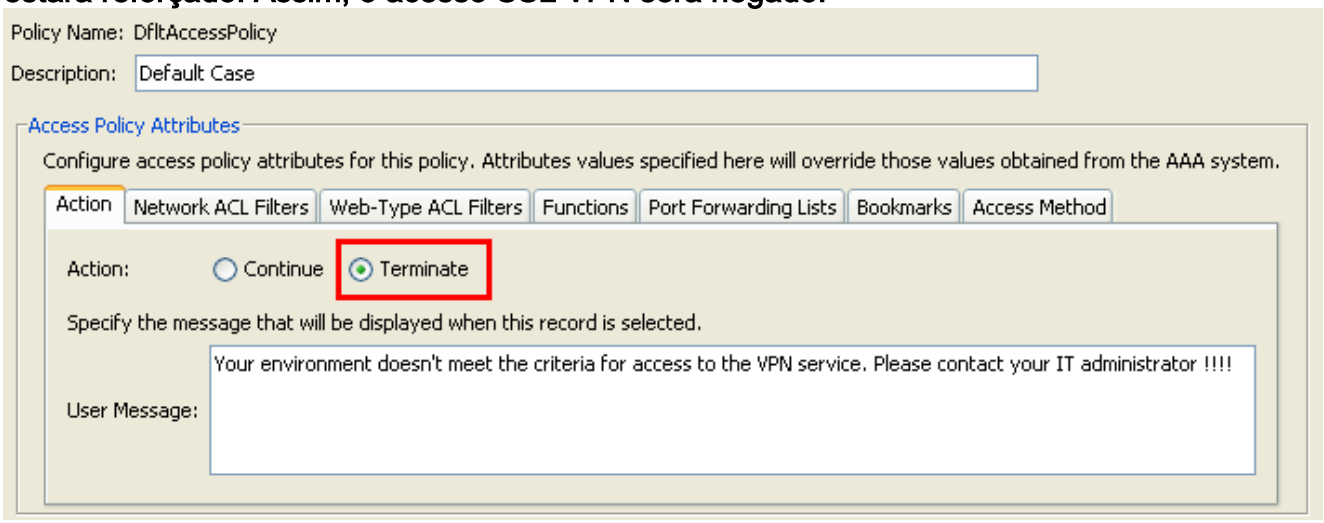
**Políticas do acesso dinâmico — Esta configuração é necessária para validar usuários de conexão e seus valores-limite contra critérios de avaliação definidos AAA e/ou de valor-limite. Se os critérios definidos de um registro DAP são satisfeitos, os usuários de conexão estarão concedidos então o acesso aos recursos de rede que são associados com esse registro ou registros DAP. A autorização DAP é executada durante o processo de autenticação.**

Para assegurar-se de que uma conexão de VPN SSL termine no exemplo do padrão, por exemplo quando o valor-limite não combina nenhuma políticas configurada do acesso dinâmico), nós configuraremos o seguinte:

**Nota:** Ao configurar políticas do acesso dinâmico pela primeira vez, um Mensagem de Erro DAP.xml é indicado que indica que um arquivo de configuração DAP (DAP.XML) não existe. Uma vez que sua configuração inicial DAP é alterada e salvar então, esta mensagem já não aparecerá.

1. Navegue à **configuração > ao acesso remoto VPN > ao acesso > ao acesso dinâmico dos sem clientes SSL VPN políticas**, e configurar o seguinte:**Figura 30. Política do acesso dinâmico do padrão — se nenhum registro predefinido DAP é combinado, este registro DAP**

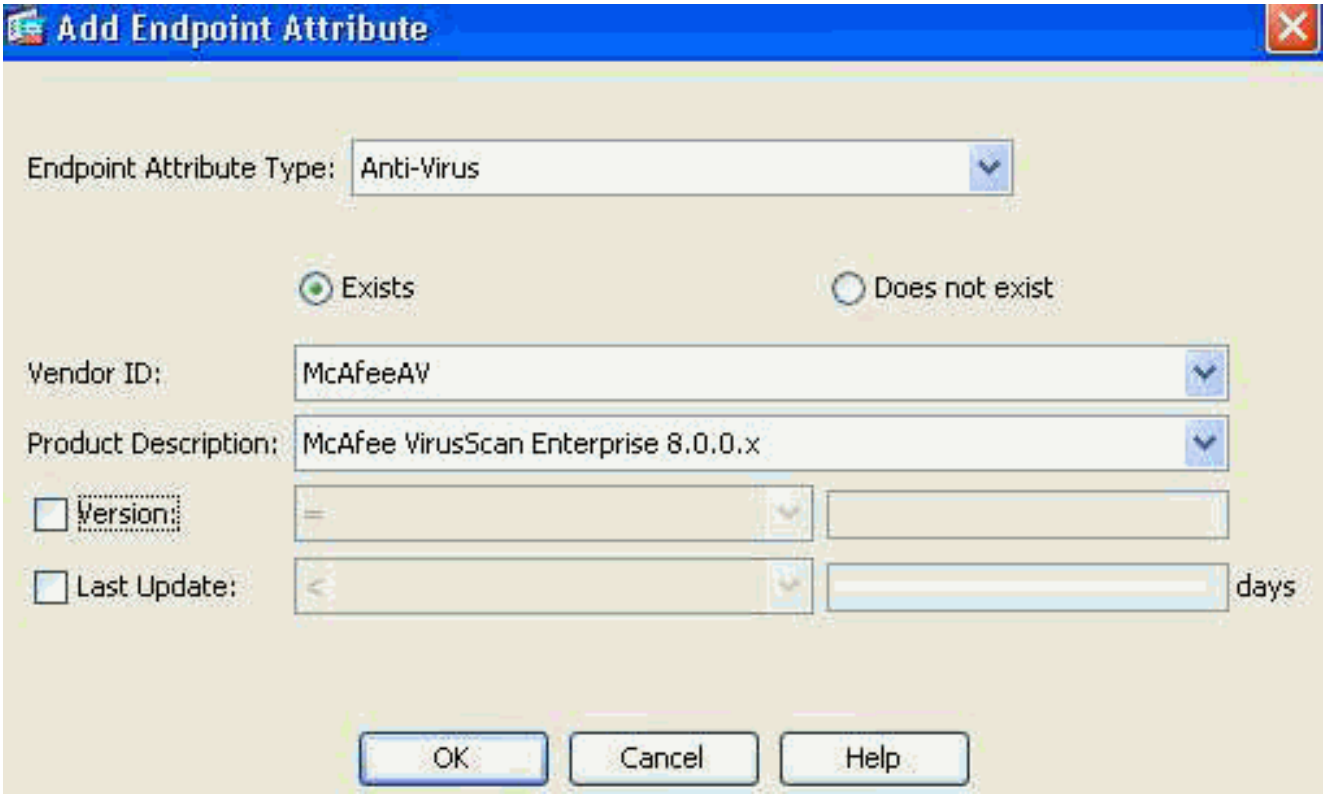
**estará reforçado. Assim, o acesso SSL VPN será negado.**




Edite o **DfltAccessPolicy** e ajuste a ação **para terminar**.Clique em **OK**.

2. Adicionar uma política nova do acesso dinâmico nomeada **Managed_Endpoints**, como segue:Descrição: **Acesso do cliente do empregado**Adicionar (localizado à direita do tipo do atributo do valor-limite) um tipo do atributo do valor-limite (política) segundo as indicações de figura 31. Clique a **APROVAÇÃO** quando completo.**Figura 31. Atributo do valor-limite DAP — O lugar do Cisco Secure Desktop será usado como um critério DAP para o acesso do /Network do cliente.**


Adicionar um segundo tipo do atributo do valor-limite (anti-vírus) segundo as indicações de figura 32. Clique a **APROVAÇÃO** quando completo.**Figura 32. Atributo do valor-limite DAP — O AntiVirus avançado da avaliação do valor-limite será usado como um critério DAP para o acesso do /Network do cliente.**




De gota da lista para baixo acima da seção do atributo AAA, o **usuário** seleto **tem todos os valores de atributos de seguimento AAA...**Adicionar (localizado à direita da caixa do atributo AAA) um tipo do atributo AAA (LDAP) segundo as indicações de figura 33 e 34. Clique a **APROVAÇÃO** quando completo.**Figura 33. Atributo DAP AAA — A membrasia do clube AAA será usada como um critério DAP para identificar um empregado.**

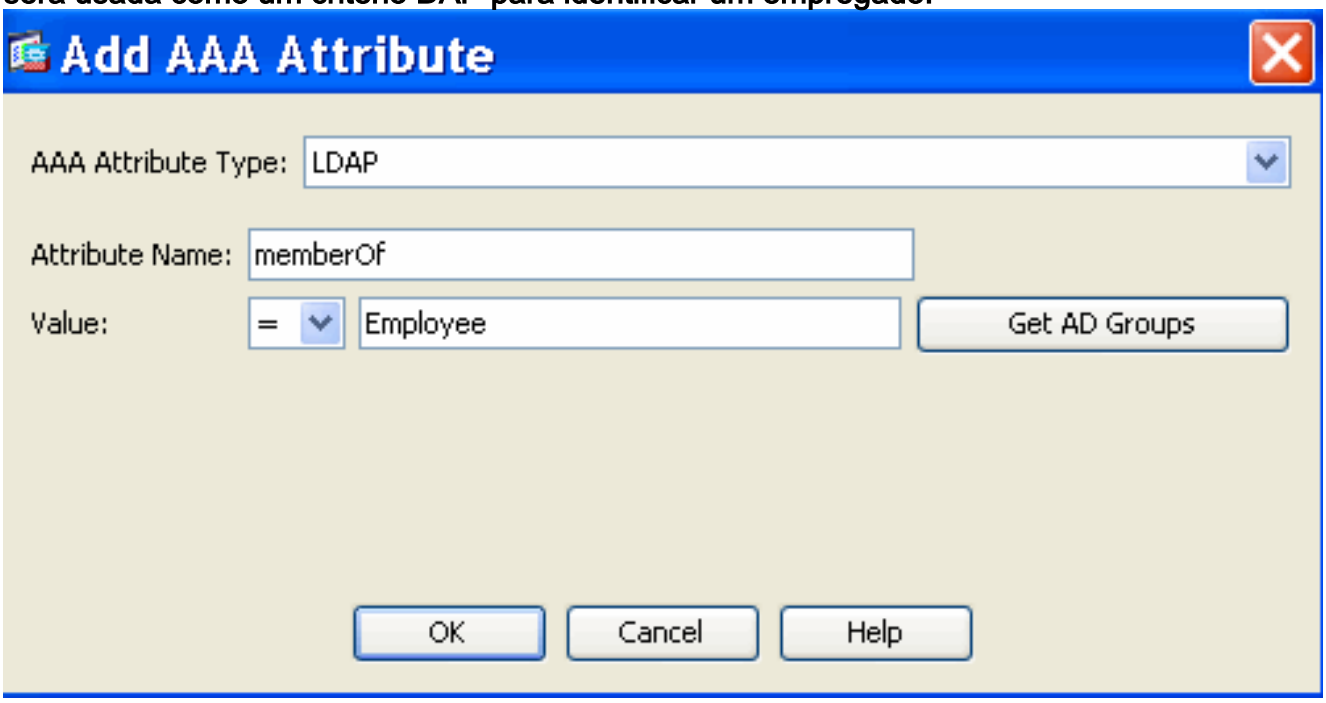
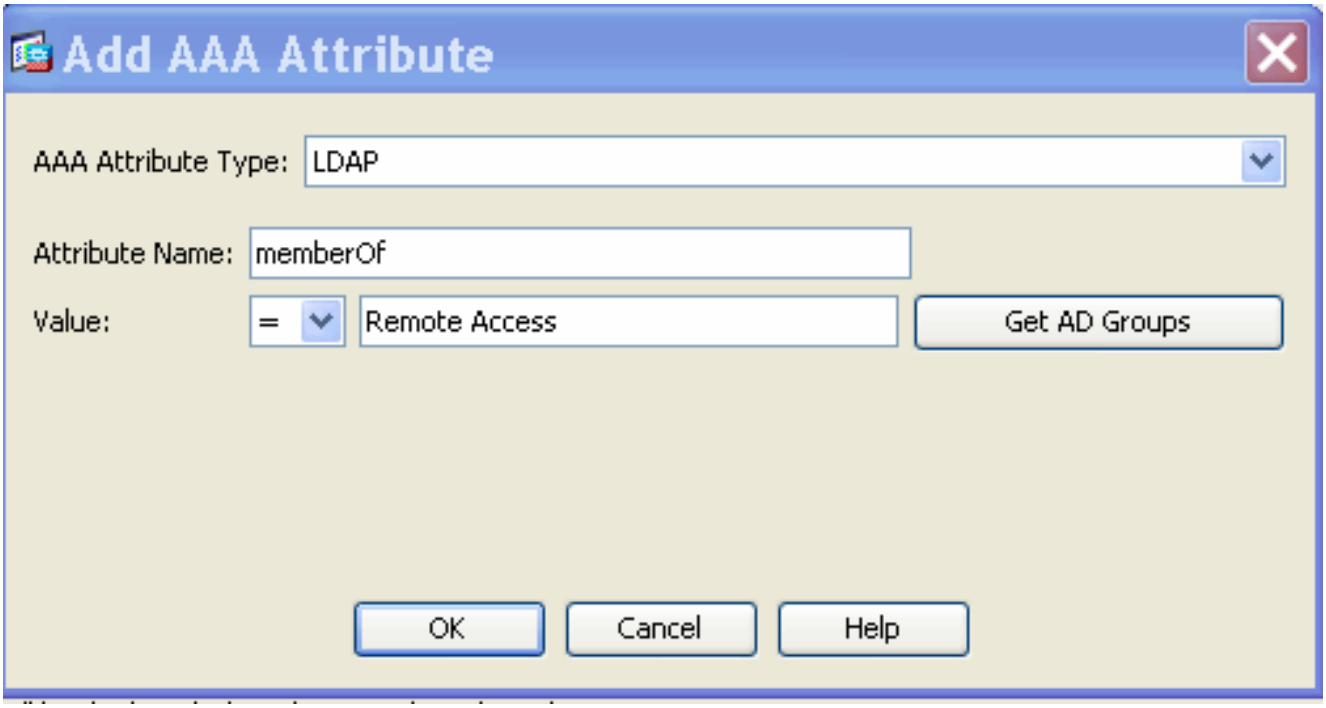
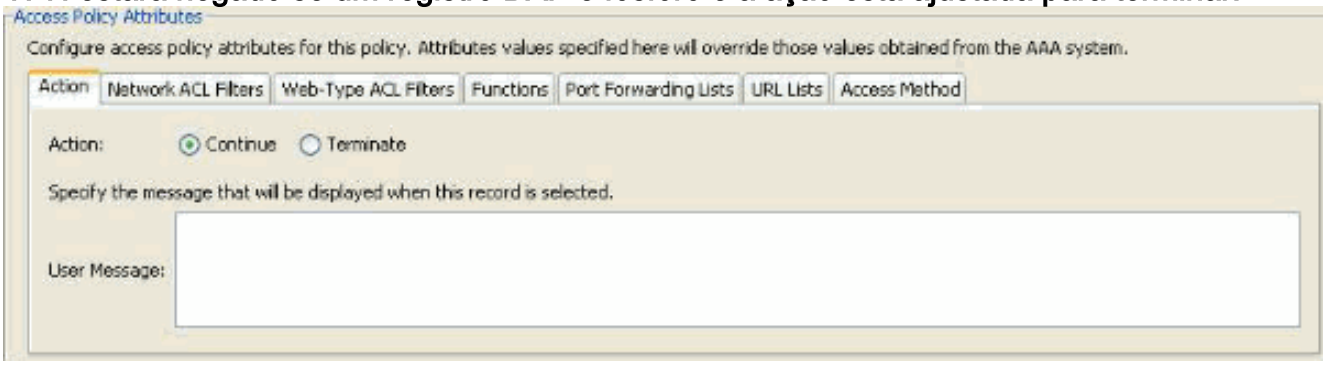


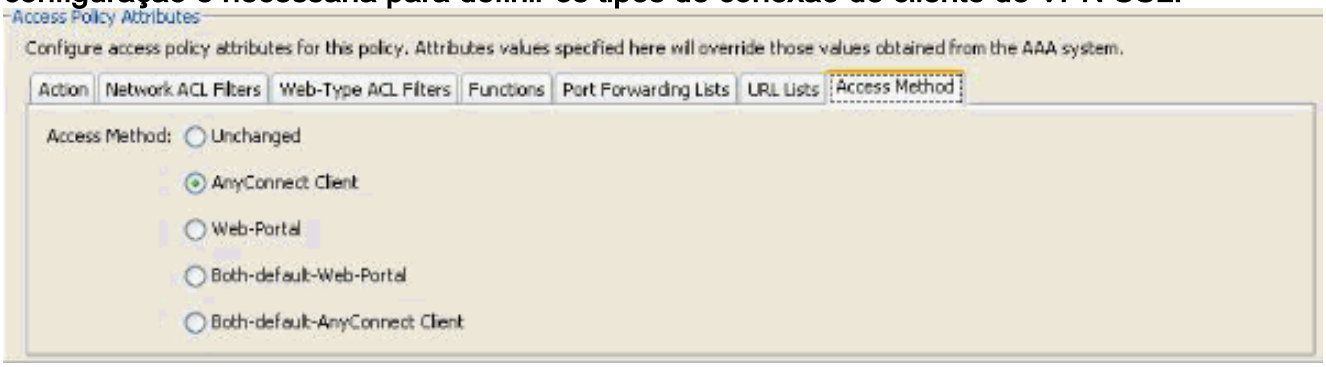

**Figura 34. Atributo DAP AAA — A membrasia do clube AAA será usada como um critério DAP para permitir capacidades de Acesso remoto.**




Sob a aba da ação, verifique que a ação está ajustada **para continuar**, segundo as indicações de figura 35.**Figura 35. Aba da ação — Esta configuração é necessária para definir o processamento especial para uma conexão ou uma sessão específica. O acesso VPN estará negado se um registro DAP é fósforo e a ação está ajustada para terminar.**




Sob a aba do método de acesso, selecione o **cliente de AnyConnect do** método de acesso, segundo as indicações de figura 36.**Figura 36. Aba do método de acesso — Esta configuração é necessária para definir os tipos de conexão de cliente de VPN SSL.**




Clique a **APROVAÇÃO**, e **aplique-a** então.

3. Adicionar um segundo acesso dinâmico **Unmanaged_Endpoints** nomeado política, como segue:Descrição: **Acesso dos sem clientes do empregado**.Adicionar (localizado à direita da caixa do atributo do valor-limite) um tipo do atributo do valor-limite (política) segundo as indicações de figura 37. Clique a **APROVAÇÃO** quando completo.**Figura 37. Atributo do valor-limite DAP — O lugar do Cisco Secure Desktop será usado como critérios DAP para o acesso dos sem clientes.**


De gota da lista para baixo acima da seção do atributo AAA, o **usuário** seleto **tem todos os valores de atributos de seguimento AAA**...Adicionar (localizado à direita do tipo do atributo AAA) um tipo do atributo AAA (LDAP) segundo as indicações de figura 38 e 39. Clique a **APROVAÇÃO** quando completo.**Figura 38. Atributo DAP AAA — A membrasia do clube AAA será usada como critérios DAP para identificar um empregado.**

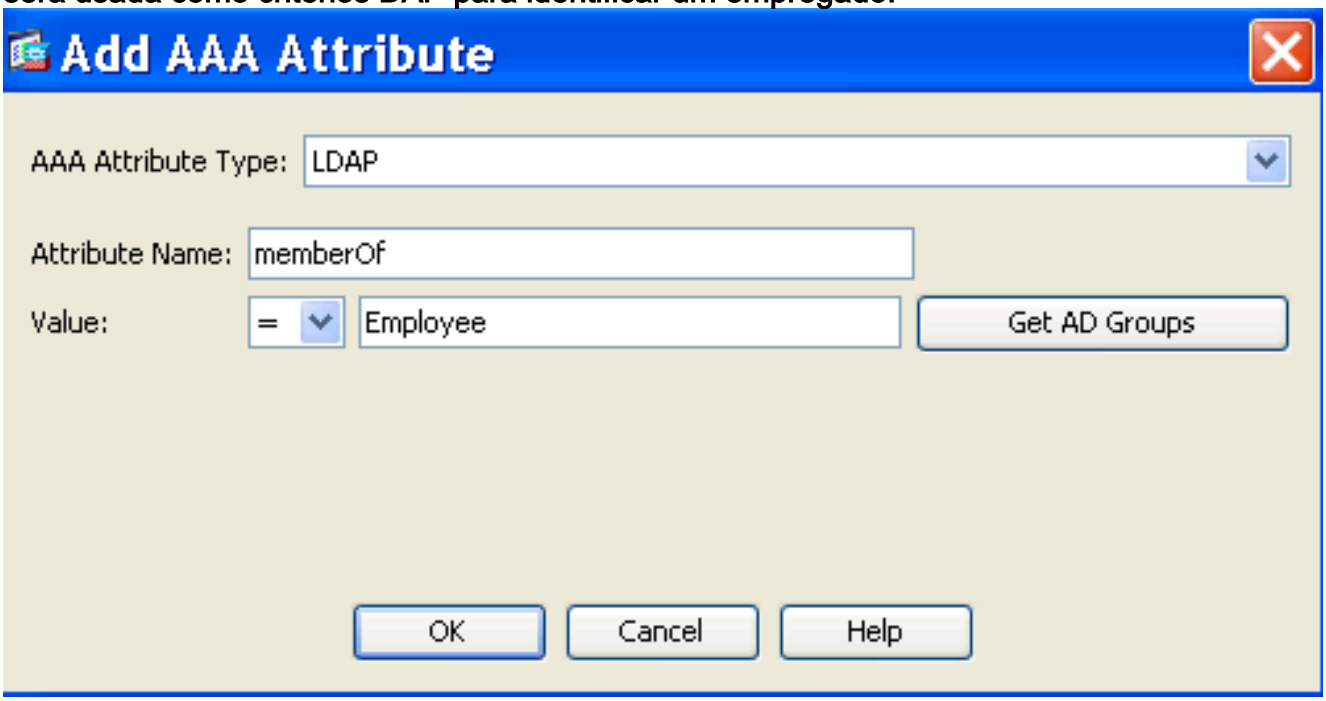
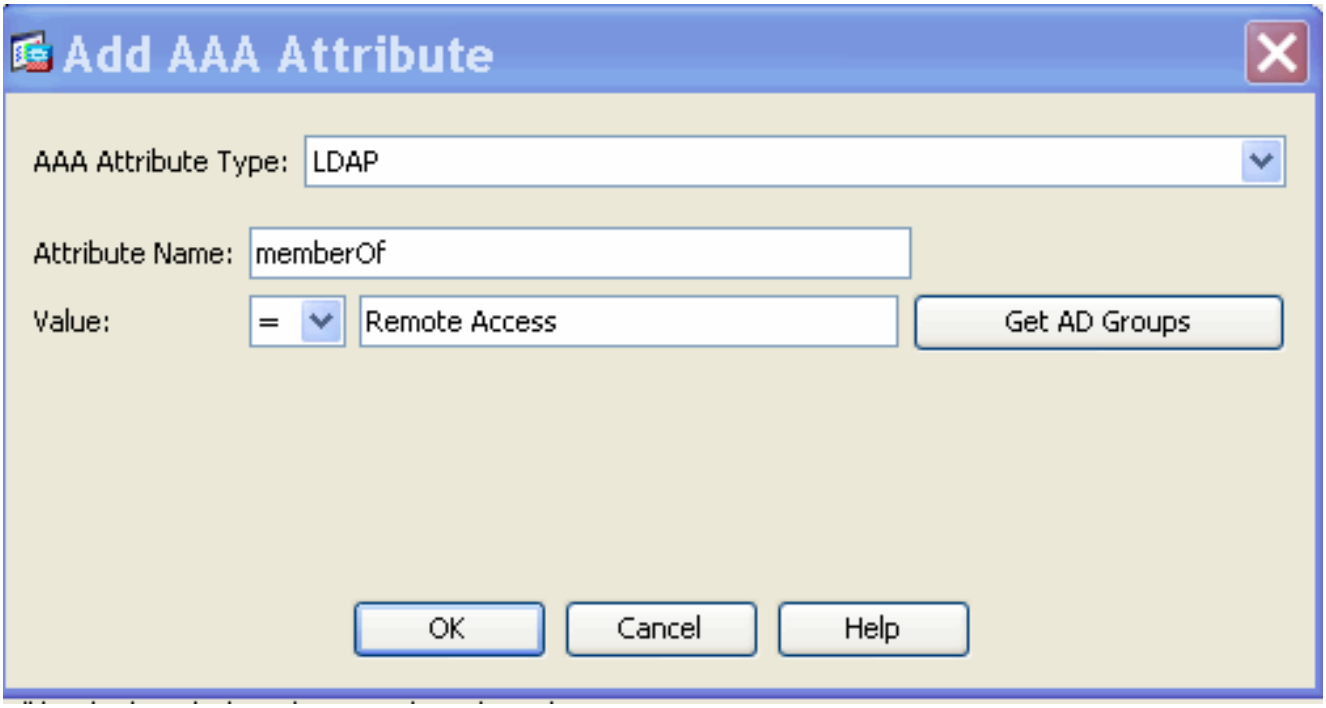
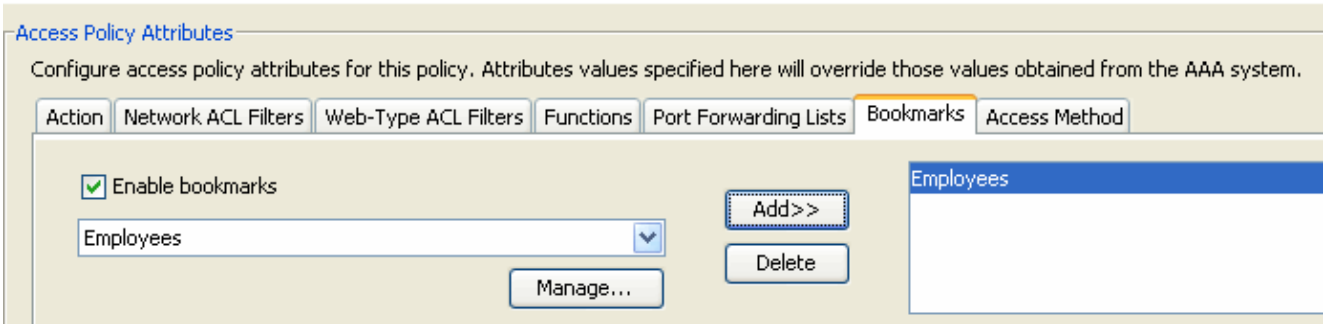



**Figura 39. Atributo DAP AAA — A membrasia do clube AAA será usada como um critério DAP para permitir capacidades de Acesso remoto.**




Sob a aba da ação, verifique que a ação está ajustada **para continuar**. (Figura 35 da referência.)Sob os endereços da Internet catalogue, selecione os **empregados do** nome de lista da gota-para baixo e clique-os então **adicionam**. Também, verifique que os endereços da Internet da possibilidade estão verificados segundo as indicações de figura 40.**Figura 40. Aba dos endereços da Internet — Deixa-o selecionar e configurar listas URL para sessões do usuário.**




Sob a aba do método de acesso, selecione o **portal da web do** método de acesso. (Figura 36 da referência.)Clique a **APROVAÇÃO**, e **aplique-a** então.Os contratantes serão identificados por atributos DAP AAA somente. Em consequência, o valor-limite atribui o tipo: (Política) não será configurado em etapa 4. Esta aproximação é significada somente mostrar a versatilidade dentro do DAP.

4. Adicionar um terceiro acesso dinâmico **Guest_Access** nomeado política e com o seguinte:Descrição: **Acesso dos sem clientes do convidado**.Adicionar (localizado à direita da caixa do atributo do valor-limite) um tipo do atributo do valor-limite (política) segundo as indicações de figura 37 acima. Clique a **APROVAÇÃO** quando completo.De gota da lista para baixo acima da seção do atributo AAA, o **usuário** seleto **tem todos os valores de atributos de seguimento AAA…**Adicionar (localizado à direita da caixa do atributo AAA) um tipo do atributo AAA (LDAP) segundo as indicações de figura 41 e 42. Clique a **APROVAÇÃO** quando completo.**Figura 41. Atributo DAP AAA — A membrasia do clube AAA será usada como um critério DAP para identificar um contratante.**

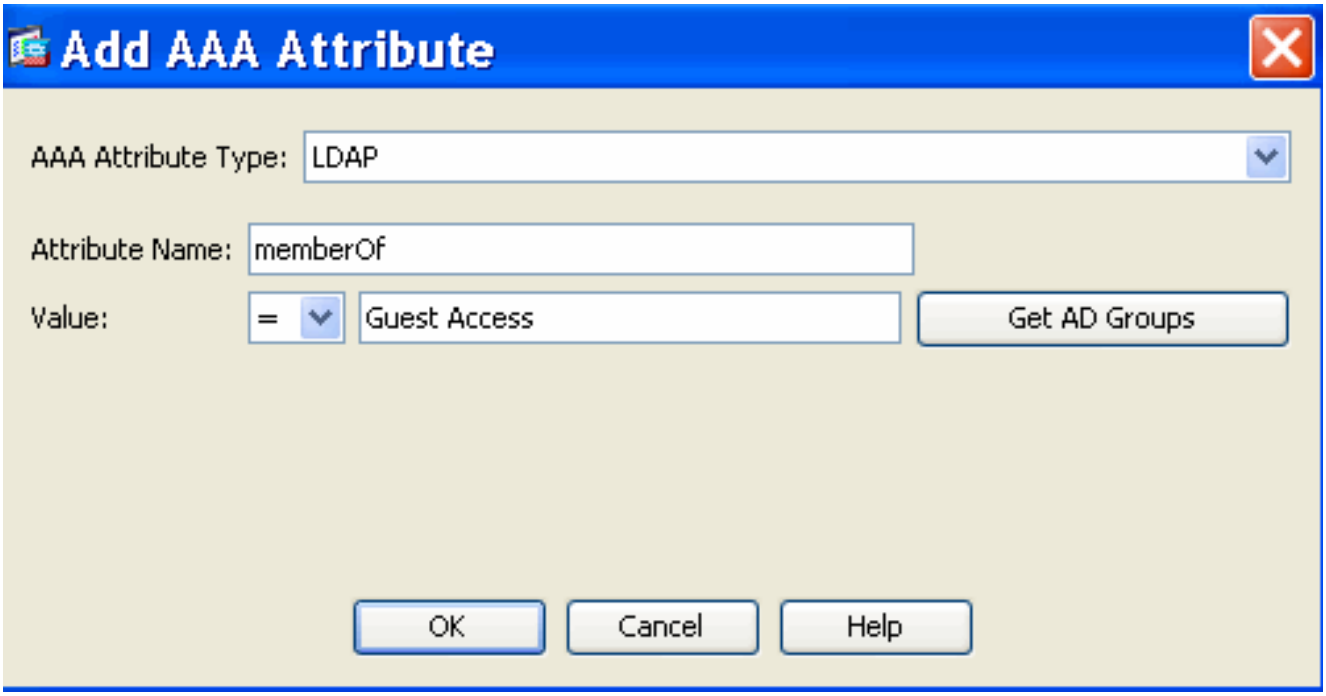
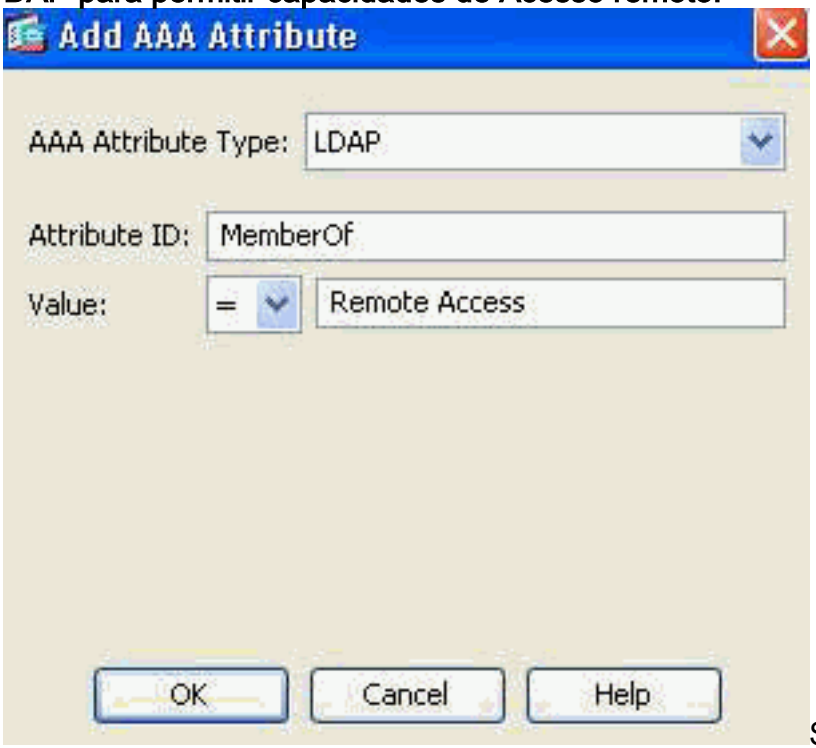



**Figura 42. Atributo DAP AAA — A membrasia do clube AAA será usada como um critério DAP para permitir capacidades de Acesso remoto.**




Sob a aba da ação, verifique que a ação está ajustada **para continuar**. (Figura 35 da referência.)Sob os endereços da Internet catalogue, selecione os **contratantes do** nome de lista da gota-para baixo e clique-os então adicionam. Também, verifique que os **endereços da Internet da possibilidade** estão verificados. (Figura 40 da referência.)Sob a aba do método de acesso, selecione o **portal da web do** método de acesso. (Figura 36 da referência.)Clique a **APROVAÇÃO**, e **aplique-a** então.

**Critérios de seleção DAP — Baseado em procedimentos de configuração esse DAP acima, seus critérios de seleção para as 4 políticas DAP definidas, devem ser consistentes com figuras 43, 44, 45 e 46.**

**Figura 43. Valores-limite controlados — Se os critérios deste registro DAP são satisfeitos, os empregados terão o acesso aos recursos corporativos através de uma conexão do cliente/rede (cliente de AnyConnect).**

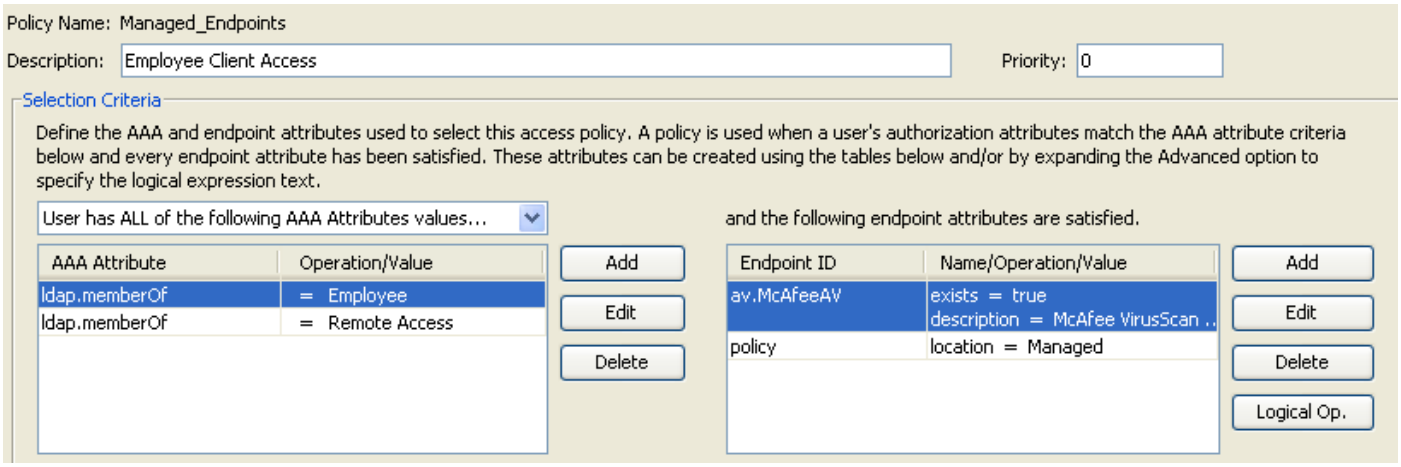



**Figura 44. Valores-limite Unmanaged — Se os critérios deste registro DAP são satisfeitos, os empregados terão o acesso aos recursos corporativos através de uma conexão dos sem clientes (portal). Uma lista URL para empregados é aplicada igualmente a esta política.**

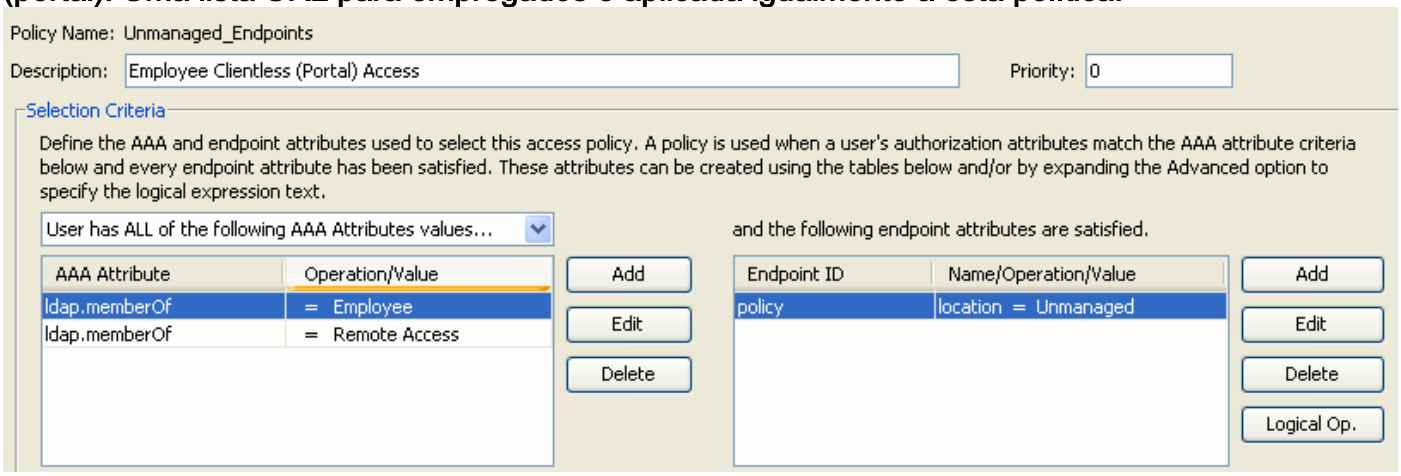



**Figura 45. Acesso do convidado — Se os critérios deste registro DAP são satisfeitos, os contratantes terão o acesso aos recursos corporativos através de uma conexão dos sem clientes (portal). Uma lista URL para contratantes é aplicada igualmente a esta política.**

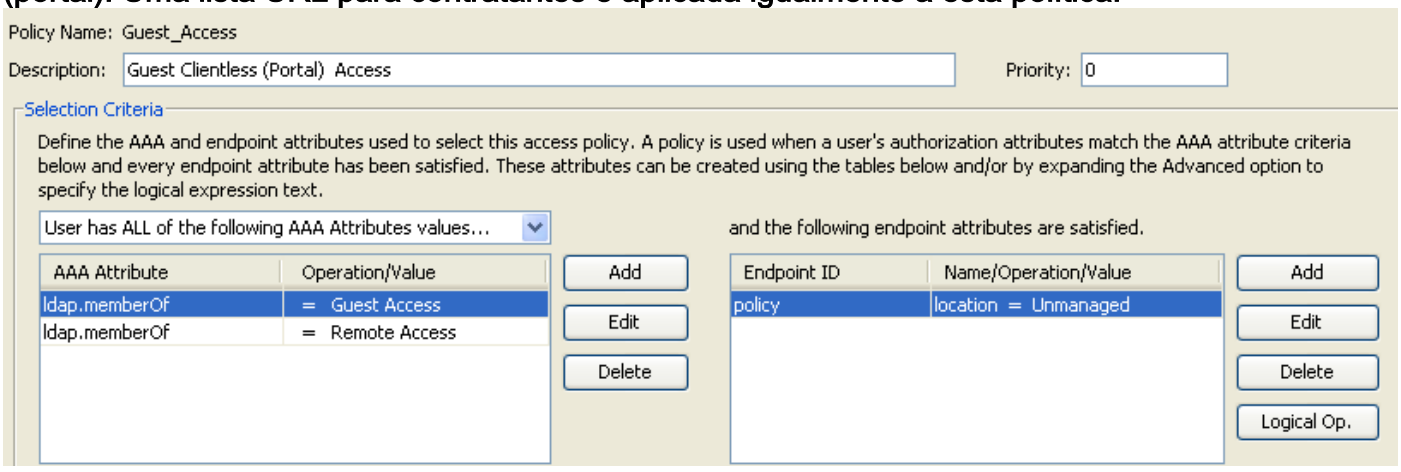
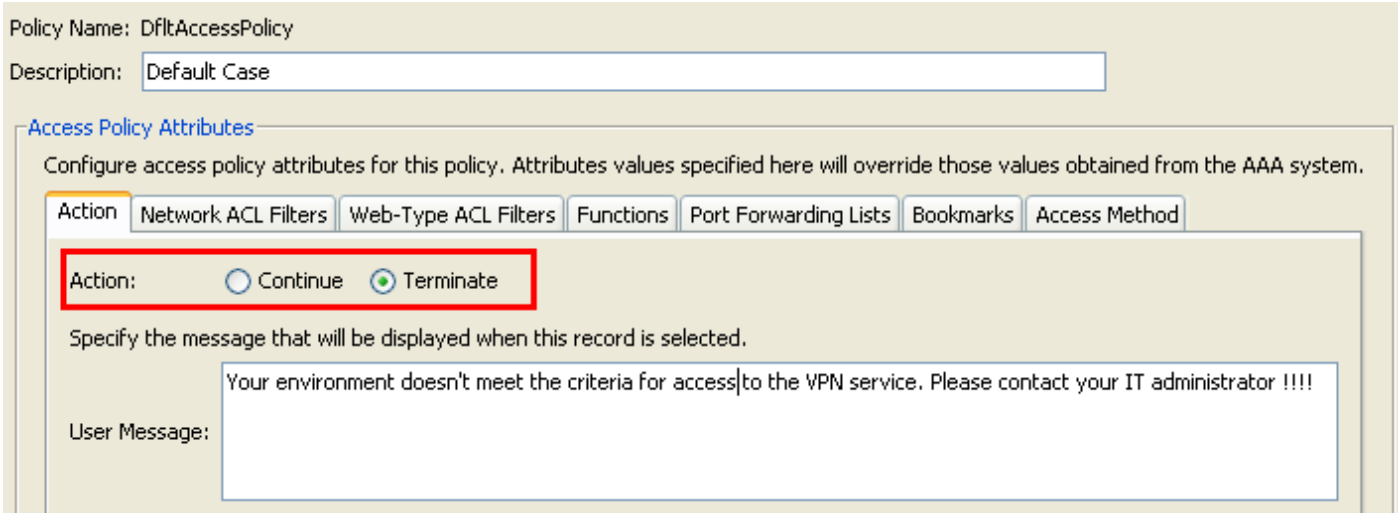



**Figura 46. Política do padrão DAP — Se os critérios para todo o DAP gravam acima não são satisfeitos, empregados e os contratantes, estarão negados à revelia o acesso.**




## Conclusão

Baseado nas exigências do Acesso remoto SSL VPN do cliente notáveis neste exemplo, esta solução satisfará suas exigências do acesso remoto VPN.

Com ambientes VPN em desenvolvimento e dinâmicos na fusão, as políticas do acesso dinâmico podem adaptar-se e para escalar para frequentar alterações de configuração do Internet, vários papéis que cada usuário pode habitar dentro de uma organização, e inícios de uma sessão dos locais controlados e unmanaged do Acesso remoto com configurações e níveis de segurança diferentes.

As políticas do acesso dinâmico são complementadas pelas Tecnologias novas e provadas do legado que incluem, por avaliação avançada do valor-limite, por varredura do host, por Secure Desktop, por AAA e por políticas do acesso local. Em consequência, as organizações podem seguramente entregar o acesso do VPN seguro a todos os recursos de rede de qualquer lugar.

## Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems