Implantar políticas de acesso dinâmico (DAP) do ASA 9.X

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Informações de Apoio](#)

[Atributos DAP e AAA](#)

[Atributos de segurança de DAP e endpoint](#)

[Política de acesso dinâmico padrão](#)

[Configurar políticas de acesso dinâmico](#)

[Agregar várias políticas de acesso dinâmico](#)

[Implementação do DAP](#)

[Conclusão](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a implantação, os recursos e o uso das políticas de acesso dinâmico (DAP) do ASA 9.x.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Gateways de Rede Virtual Privada (VPN)
- Políticas de acesso dinâmico (DAP)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

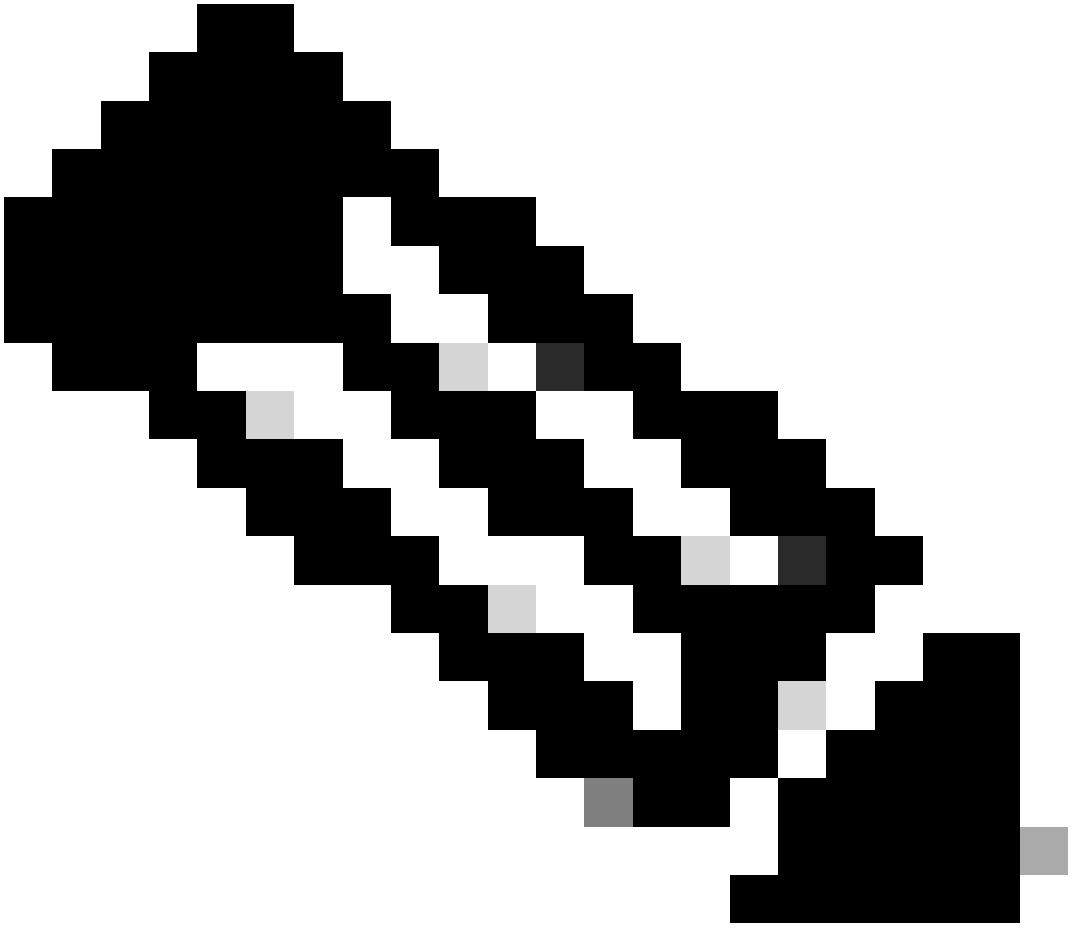
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

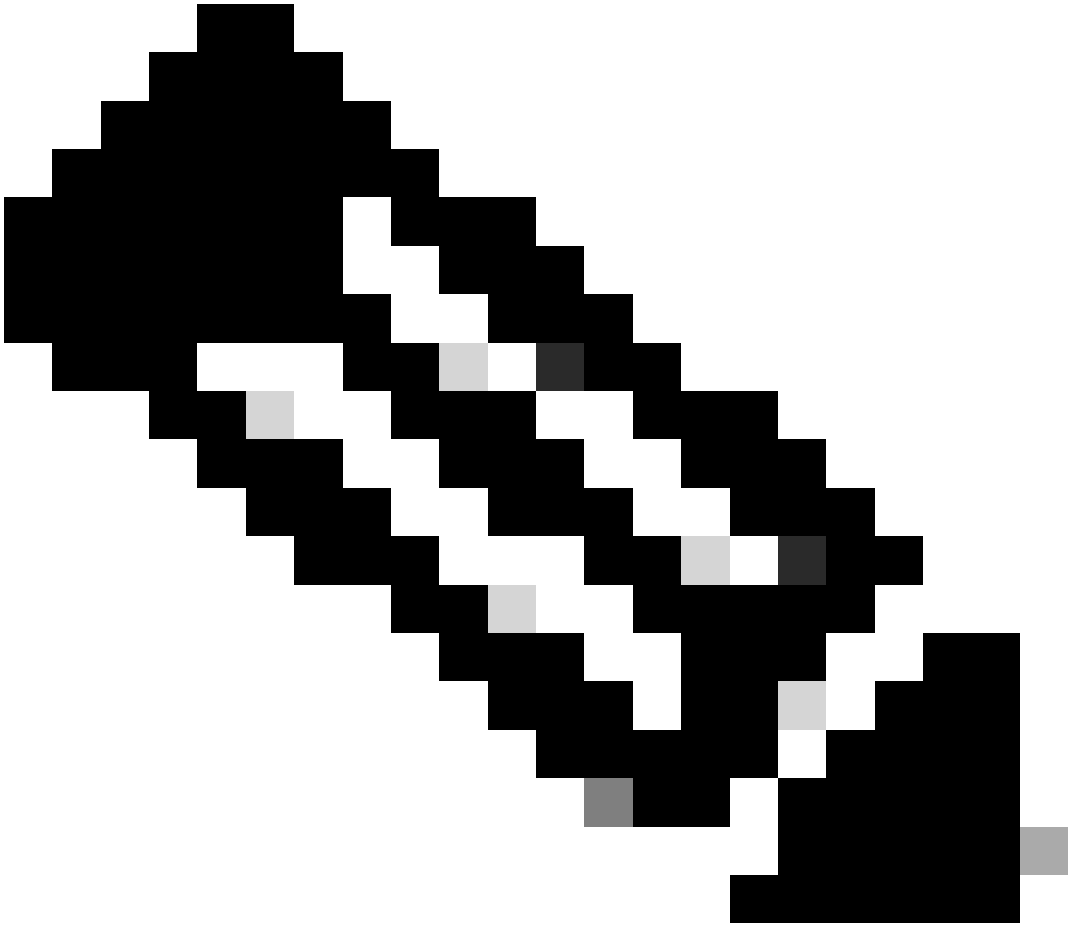
Os gateways de Rede Virtual Privada (VPN - Virtual Private Network) operam em ambientes dinâmicos. Várias variáveis podem afetar cada conexão VPN; por exemplo, configurações de intranet que mudam com frequência, as várias funções que cada usuário pode ocupar dentro de uma organização e logons de sites de acesso remoto com diferentes configurações e níveis de segurança. A tarefa de autorizar usuários é muito mais complicada em um ambiente de VPN dinâmico do que em uma rede com uma configuração estática.

Políticas de acesso dinâmico (DAP), um recurso que permite configurar a autorização que aborda a dinâmica de ambientes VPN. Você cria uma política de acesso dinâmico definindo uma coleção de atributos de controle de acesso que você associa a um túnel ou sessão de usuário específico. Esses atributos abordam questões de associação de vários grupos e segurança de endpoint.

Por exemplo, o Security Appliance concede acesso a um usuário específico para uma sessão específica com base nas políticas definidas. Gera um DAP através da autenticação de usuário selecionando e/ou agregando atributos de um ou mais registros DAP. Ele seleciona esses registros DAP com base nas informações de segurança do endpoint do dispositivo remoto e/ou nas informações de autorização AAA para o usuário autenticado. Em seguida, aplica o registro DAP ao túnel ou sessão do usuário.



Observação: o arquivo dap.xml, que contém os atributos de seleção de políticas DAP, é armazenado na flash do ASA. Embora seja possível exportar o arquivo dap.xml off-box, editá-lo (se você souber sobre a sintaxe XML) e reimportá-lo, tenha muito cuidado, pois você pode fazer com que o ASDM pare de processar registros DAP se tiver configurado algo incorretamente. Não há CLI para manipular esta parte da configuração.



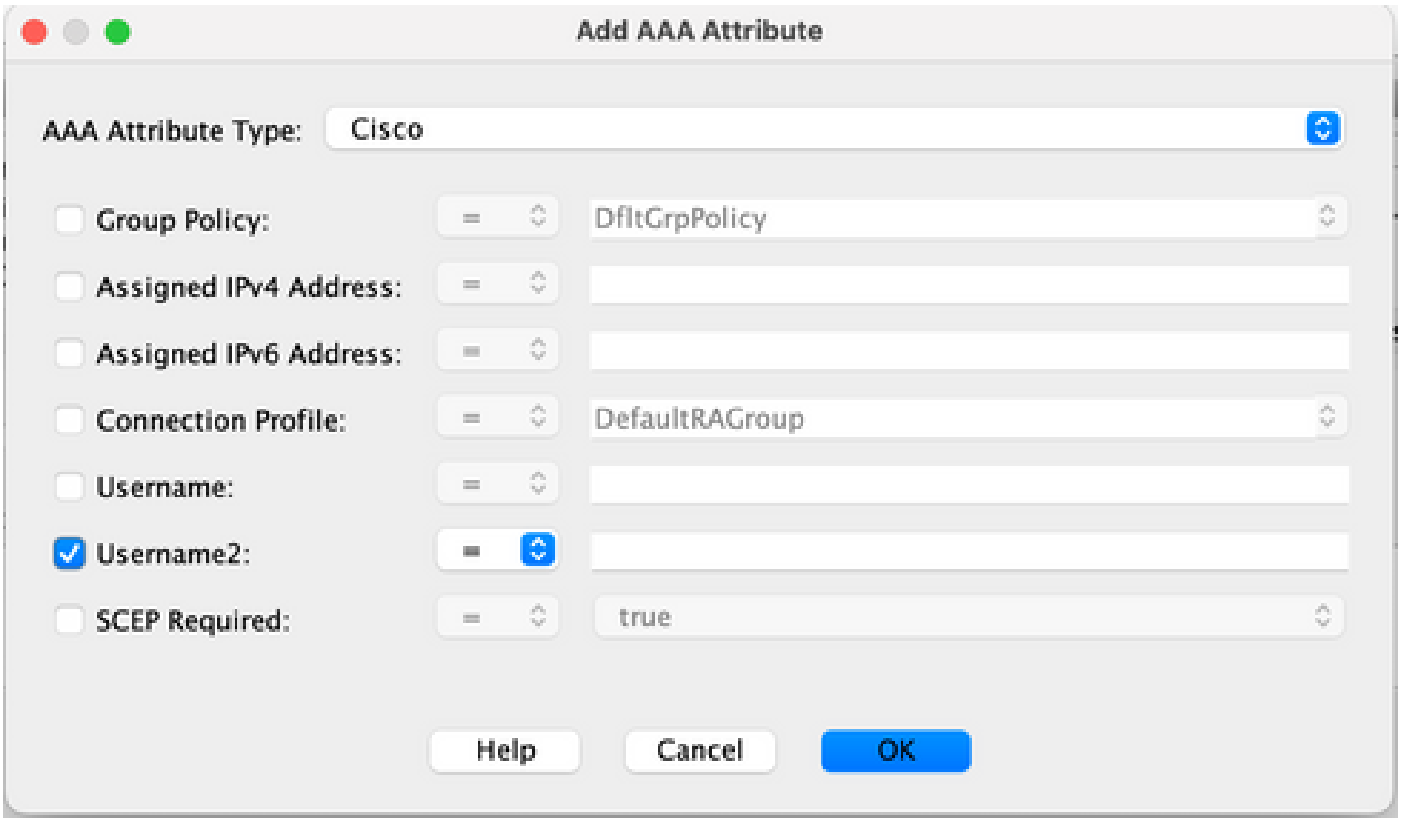
Observação: tentar configurar os parâmetros de acesso dynamic-access-policy-record via CLI pode fazer com que o DAP pare de funcionar, embora o ASDM gerencie corretamente o mesmo. Evite a CLI e sempre use o ASDM para gerenciar as políticas do DAP.

Atributos DAP e AAA

O DAP complementa os serviços AAA e fornece um conjunto limitado de atributos de autorização que podem substituir atributos que o AAA fornece. O Security Appliance pode selecionar registros LDAP com base nas informações de autorização AAA para o usuário. O Security Appliance pode selecionar vários registros de DAP dependendo dessas informações, que depois agrega para atribuir atributos de autorização de DAP.

Você pode especificar atributos AAA da hierarquia de atributos AAA da Cisco ou do conjunto completo de atributos de resposta que o Security Appliance recebe de um servidor RADIUS ou LDAP, como mostrado na Figura 1.

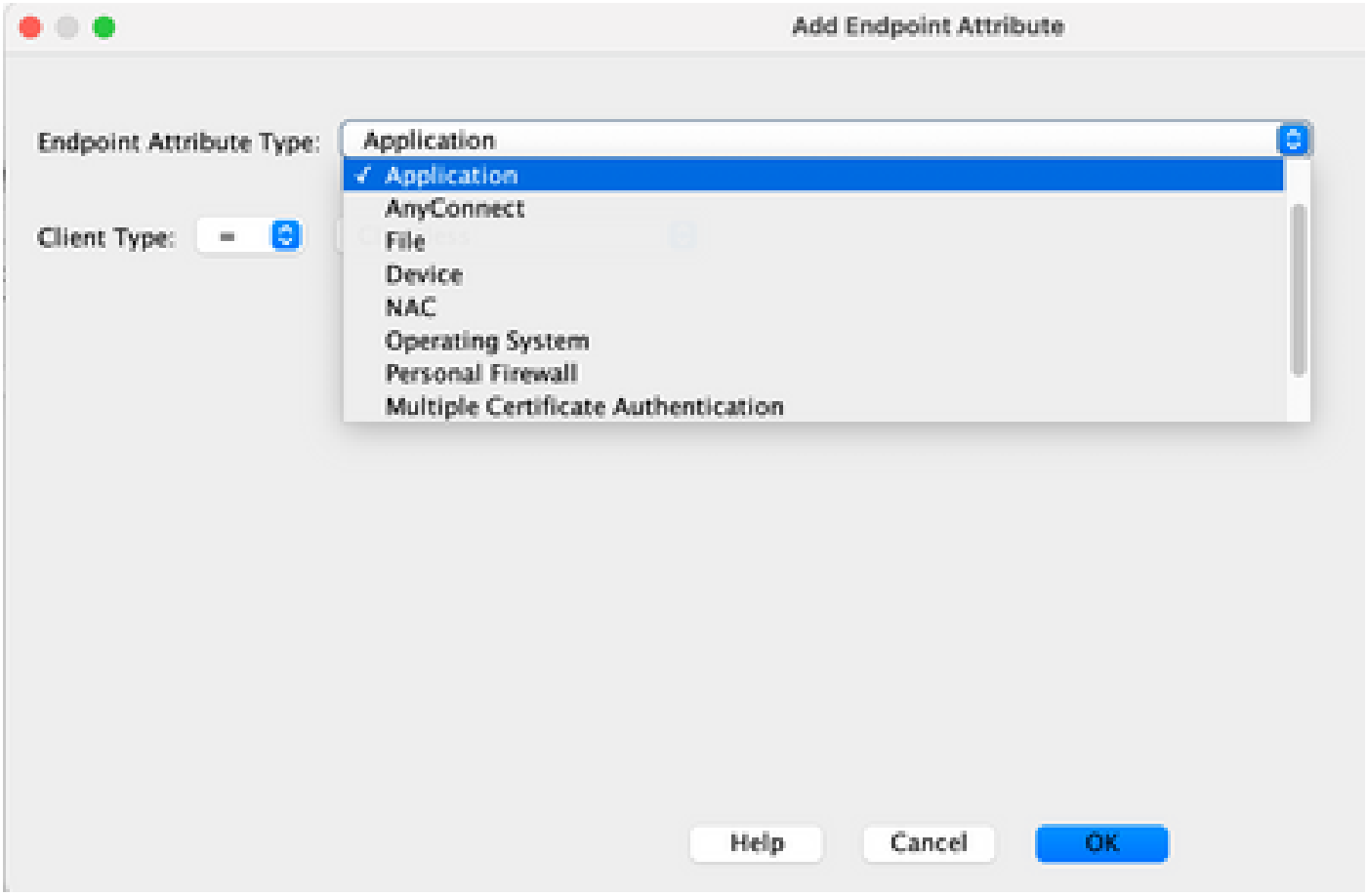
Figura 1. GUI de atributo AAA do DAP



Atributos de segurança de DAP e endpoint

Além dos atributos AAA, o Security Appliance também pode obter atributos de segurança de endpoint usando os métodos de avaliação de postura que você configura. Eles incluem verificação básica de host, desktop seguro, avaliação de endpoint padrão/avançado e NAC, como mostrado na Figura 2. Os atributos de avaliação de endpoint são obtidos e enviados ao Security Appliance antes da autenticação do usuário. No entanto, os atributos AAA, incluindo o registro DAP geral, são validados durante a autenticação do usuário.

Figura 2. GUI de atributo de endpoint

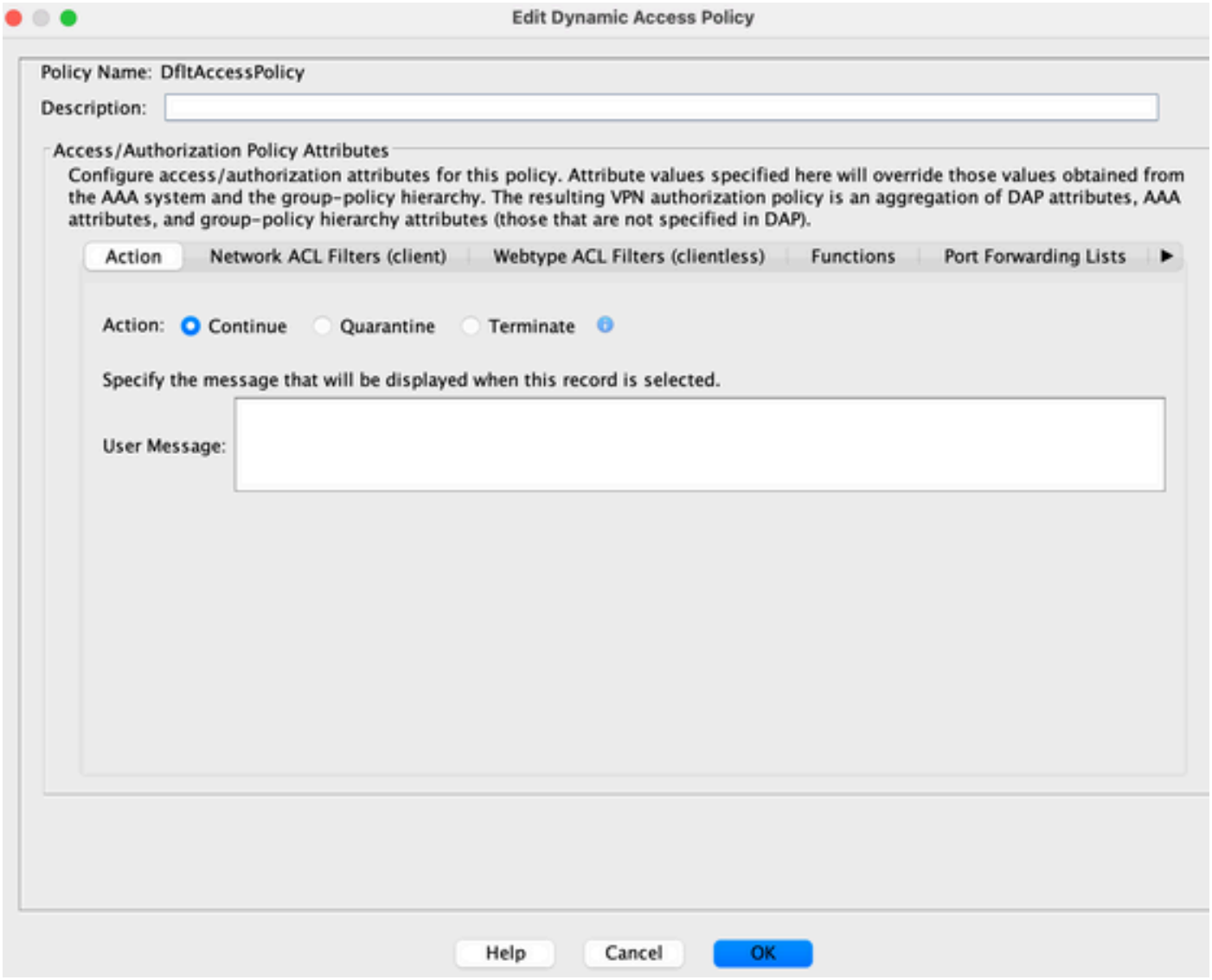


Política de acesso dinâmico padrão

Antes da introdução e implementação do DAP, os pares de atributo/valor da política de acesso que estavam associados a um túnel ou sessão de usuário específico eram definidos localmente no ASA, (isto é, Grupos de Túnel e Políticas de Grupo) ou mapeados através de servidores AAA externos.

O DAP é sempre aplicado por padrão. Por exemplo, a aplicação do controle de acesso através de grupos de túnel, políticas de grupo e AAA sem a aplicação explícita do DAP ainda pode obter esse comportamento. Para o comportamento legado, nenhuma alteração de configuração no recurso DAP, incluindo o registro DAP padrão, DfltAccessPolicy, é necessária, como mostrado na Figura 3.

Figura 3. Política de acesso dinâmico padrão



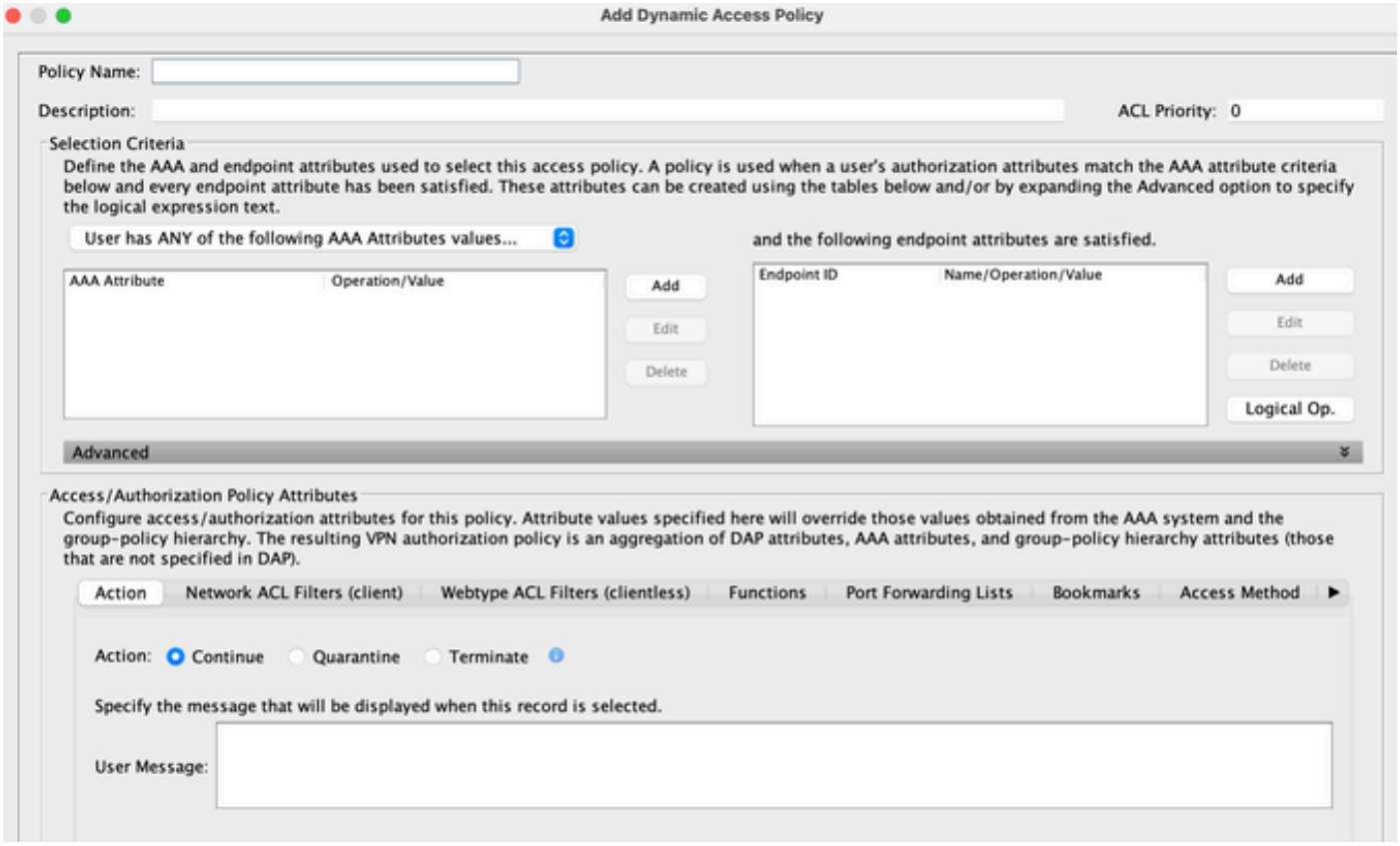
No entanto, se qualquer um dos valores padrão em um registro DAP for alterado, por exemplo, o parâmetro Action: em DfltAccessPolicy for alterado de seu valor padrão para Terminar e registros DAP adicionais não estiverem configurados, os usuários autenticados podem, por padrão, corresponder ao registro DfltAccessPolicy DAP e podem ter acesso VPN negado.

Consequentemente, um ou mais registros LDAP precisam ser criados e configurados para autorizar a conectividade VPN e definir quais recursos de rede um usuário autenticado está autorizado a acessar. Assim, o DAP, se configurado, pode ter precedência sobre a aplicação de políticas legadas.

Configurar políticas de acesso dinâmico

Quando você usa o DAP para definir a quais recursos de rede um usuário tem acesso, há muitos parâmetros a considerar. Por exemplo, se você identificar se o endpoint de conexão é de um ambiente gerenciado, não gerenciado ou não confiável, determine os critérios de seleção necessários para identificar o endpoint de conexão e, com base na avaliação do endpoint e/ou nas credenciais AAA, quais recursos de rede o usuário que se conecta está autorizado a acessar. Para fazer isso, você deve primeiro se familiarizar com os recursos e funções do DAP, como mostrado na Figura 4.

Figura 4. Política de acesso dinâmico



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

- Critérios de seleção incluindo opções avançadas
- Atributos da política de acesso

A seção Critérios de seleção é onde um administrador configura os atributos AAA e Endpoint usados para selecionar um registro DAP específico. Um registro DAP é usado quando os atributos de autorização de um usuário correspondem aos critérios do atributo AAA e cada atributo de ponto final foi satisfeito.

Por exemplo, se o Tipo de Atributo AAA LDAP (Ative Diretory) for selecionado, a string Nome do Atributo será memberOf e a string Valor será Contratados, como mostrado na Figura 5a, o usuário de autenticação deve ser um membro do grupo Contratados do Ative Diretory para corresponder aos critérios do atributo AAA.

Além de satisfazer os critérios de atributo AAA, o usuário de autenticação também pode ser solicitado a satisfazer os critérios de atributo de ponto final. Por exemplo, se o administrador configurou o para determinar a postura do ponto final de conexão e com base nessa avaliação de postura, o administrador pode usar essas informações de avaliação como critérios de seleção para o atributo de ponto final mostrado na Figura 5b.

Figura 5a. Critérios de Atributo AAA

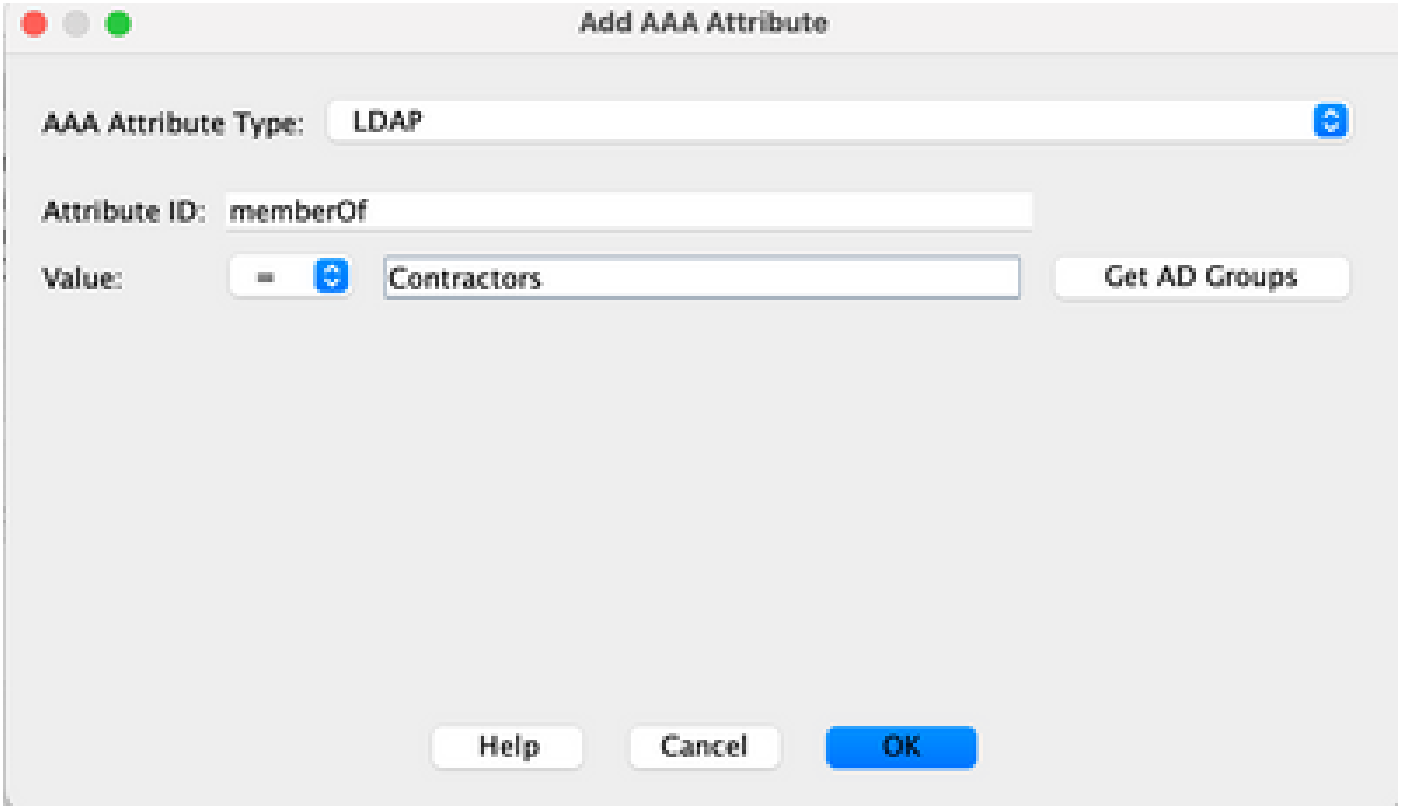


Figura 5b. Critérios de Atributo de Ponto Final

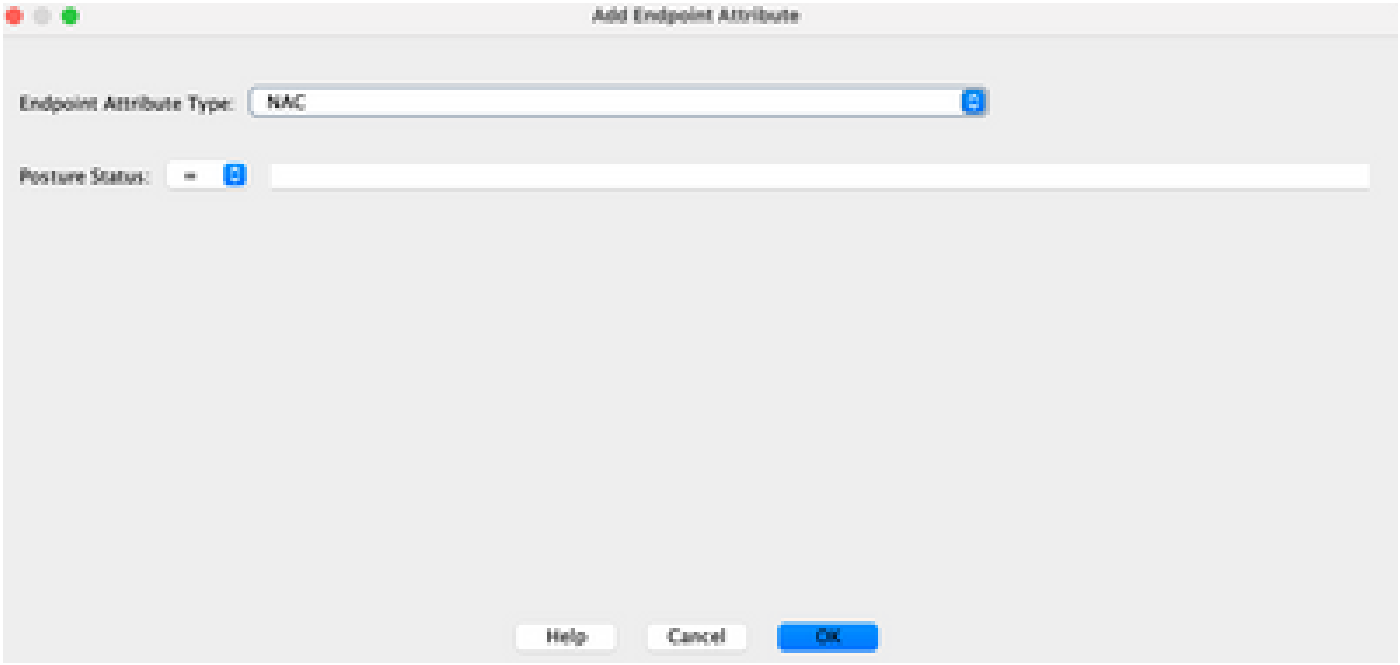
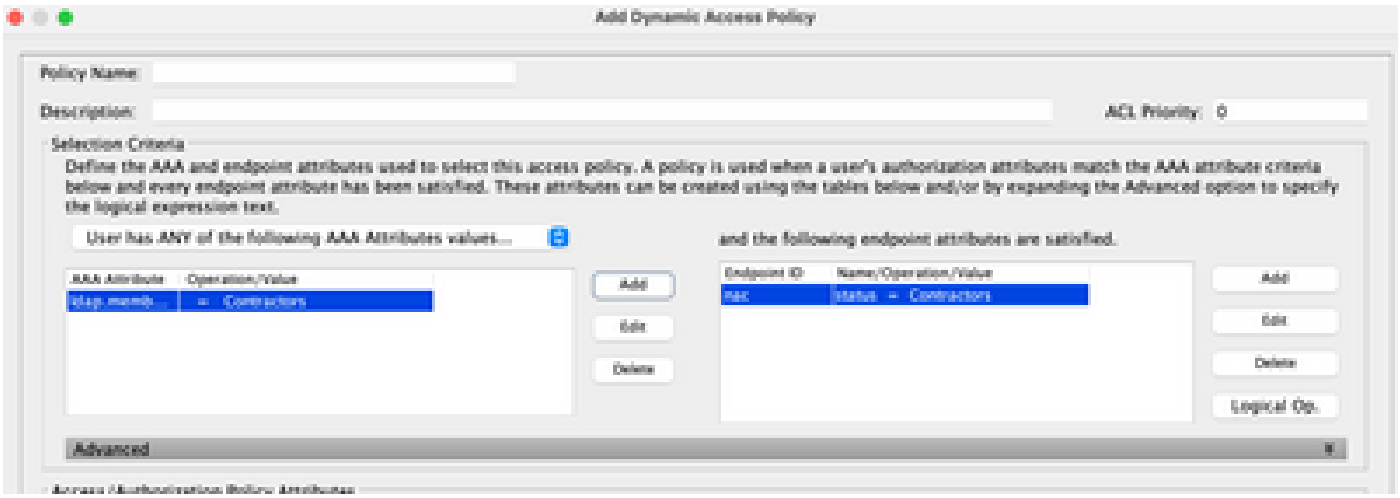


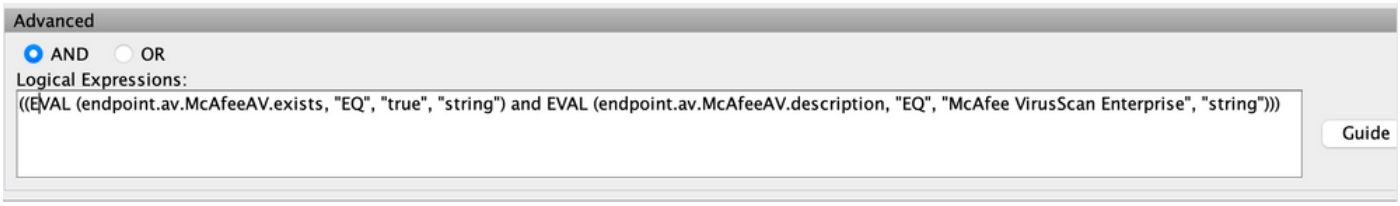
Figura 6. Correspondência de Critérios de Atributo de AAA e Endpoint



Os atributos AAA e Endpoint podem ser criados usando as tabelas conforme descrito na Figura 6 e/ou expandindo a opção Advanced para especificar uma expressão lógica conforme mostrado na Figura 7. Atualmente, a expressão lógica é construída com funções EVAL, por exemplo, EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") e EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"), que representam AAA e/ou operações lógicas de seleção de endpoint.

As expressões lógicas são úteis se você precisar adicionar critérios de seleção diferentes do que é possível nas áreas de atributo AAA e endpoint, como mostrado anteriormente. Por exemplo, embora você possa configurar os Security Appliances para usar atributos AAA que satisfaçam qualquer, todos ou nenhum dos critérios especificados, os atributos de ponto final são cumulativos e devem ser todos satisfeitos. Para permitir que o Security Appliance empregue um atributo de endpoint ou outro, é necessário criar expressões lógicas apropriadas na seção Avançado do registro DAP.

Figura 7. GUI de expressão lógica para criação de atributos avançados

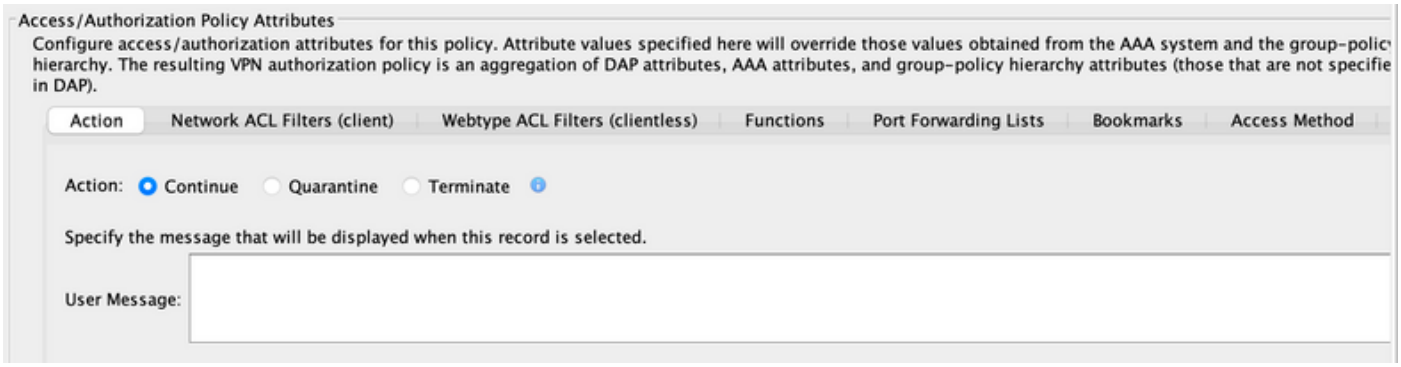


A seção Access Policy Attributes (Atributos da política de acesso), como mostrado na Figura 8, é onde um administrador configuraria os atributos de acesso de VPN para um registro LDAP específico. Quando os atributos de autorização de um usuário correspondem aos critérios de AAA, Endpoint e/ou Expressão Lógica; os valores configurados do atributo da política de acesso nesta seção podem ser aplicados. Os valores de atributo especificados aqui podem substituir os valores obtidos do sistema AAA, incluindo aqueles nos registros de usuário, grupo, grupo de túneis e grupo padrão existentes.

Um registro DAP tem um conjunto limitado de valores de atributos que podem ser configurados. Esses valores estão sob as guias, como mostrado nas Figuras 8 a 14:

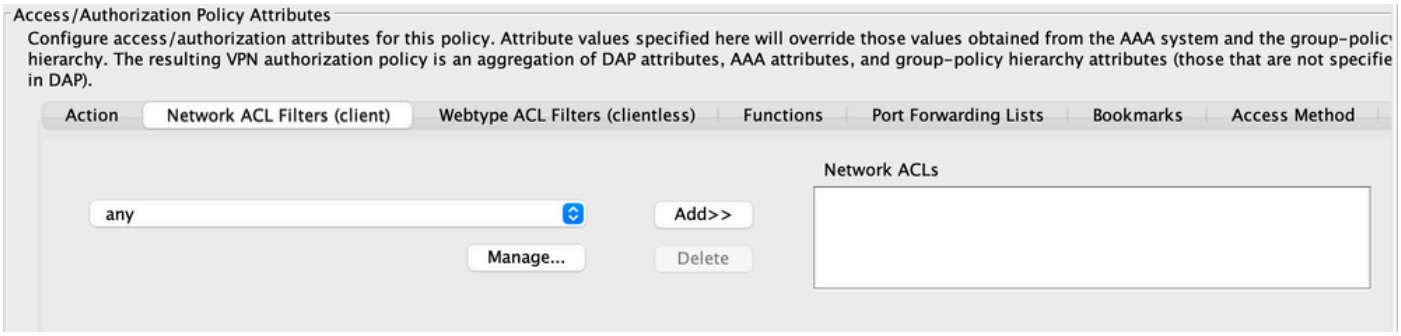
Figura 8. Ação — Especifica o processamento especial a ser aplicado a uma conexão ou sessão

específica.



- Continuar—(padrão) Clique para aplicar os atributos da política de acesso à sessão.
- Encerrar—Clique para encerrar a sessão.
- Mensagem do usuário — Insira uma mensagem de texto a ser exibida na página do portal quando este registro LDAP for selecionado. Máximo de 128 caracteres. Uma mensagem de usuário é exibida como uma orbe amarela. Quando um usuário faz logon, ele pisca três vezes para chamar a atenção e, em seguida, permanece. Se vários registros LDAP forem selecionados e cada um deles tiver uma mensagem de usuário, todas as mensagens de usuário serão exibidas. Além disso, você pode incluir nessas mensagens URLs ou outros textos incorporados, que exigem o uso das tags HTML corretas.

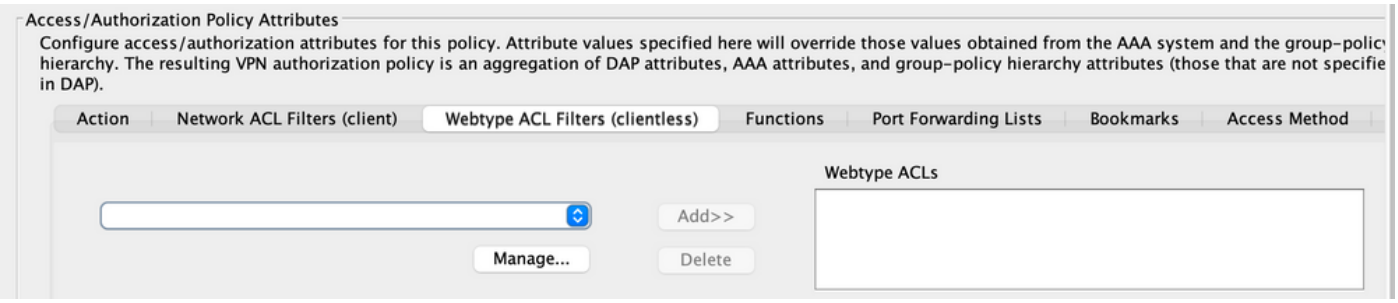
Figura 9. Guia Filtros de ACL de rede — Permite selecionar e configurar ACLs de rede para aplicar a esse registro LDAP. Uma ACL para DAP pode conter regras de permissão ou negação, mas não ambas. Se uma ACL contiver regras de permissão e de negação, o Security Appliance rejeitará a configuração da ACL.



- A caixa suspensa de ACL de rede já configurou as ACLs de rede para adicionar a este registro LDAP. Somente as ACLs que têm todas as regras de permissão ou negação são elegíveis, e essas são as únicas ACLs exibidas aqui.
- Gerenciar—Clique para adicionar, editar e excluir ACLs de rede.
- A ACL de rede lista as ACLs de rede para este registro LDAP.
- Adicionar—Clique para adicionar a ACL de rede selecionada na caixa suspensa à lista ACL de rede à direita.

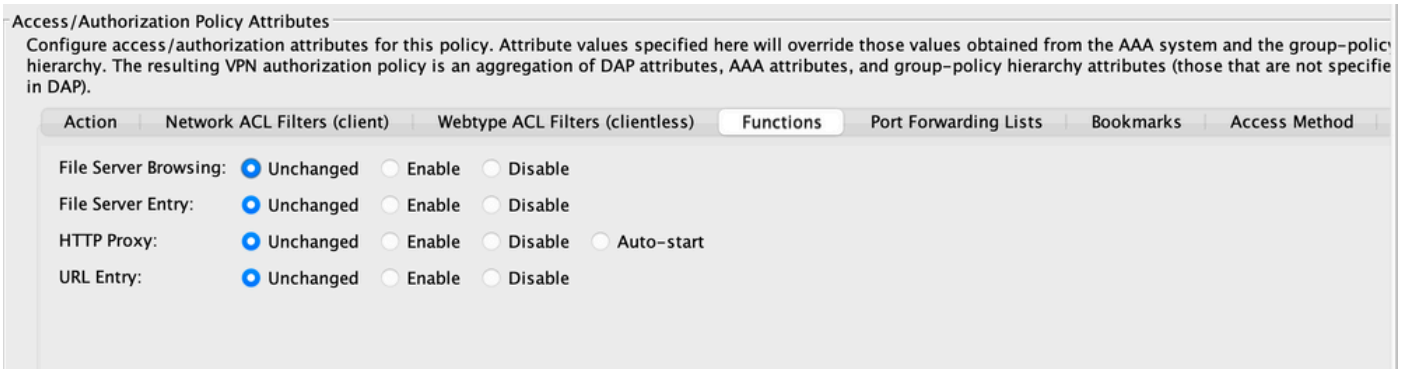
- Excluir—Clique para excluir uma ACL de rede destacada da lista ACLs de rede. Não é possível excluir uma ACL se ela estiver atribuída a um DAP ou outro registro.

Figura 10. Guia Filtros ACL do tipo Web — Permite selecionar e configurar ACLs do tipo Web para aplicar a esse registro LDAP. Uma ACL para DAP pode conter apenas regras de permissão ou negação. Se uma ACL contiver regras de permissão e de negação, o Security Appliance rejeitará a configuração da ACL.



- Caixa suspensa ACL do tipo Web — Selecione as ACLs do tipo Web já configuradas para adicionar a esse registro LDAP. Somente as ACLs com todas as regras de permissão ou todas as regras de negação são elegíveis, e essas são as únicas ACLs exibidas aqui.
- Gerenciar... — Clique para adicionar, editar e excluir ACLs do tipo Web.
- Lista de ACLs do tipo Web — Exibe as ACLs do tipo Web para esse registro LDAP.
- Adicionar — Clique para adicionar a ACL do tipo Web selecionada na caixa suspensa à lista ACLs do tipo Web à direita.
- Excluir — Clique para excluir uma ACL do tipo Web da lista ACLs do tipo Web. Não é possível excluir uma ACL se ela estiver atribuída a um DAP ou outro registro.

Figura 11. Guia Funções — Permite configurar a entrada e a navegação do servidor de arquivos, o proxy HTTP e a entrada de URL para o registro LDAP.

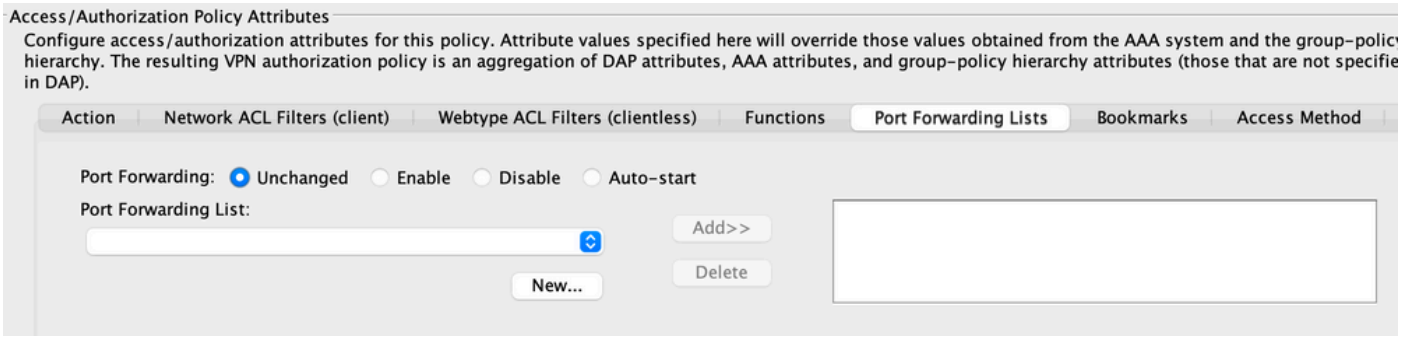


- Navegação no servidor de arquivos: habilita ou desabilita a navegação no CIFS para servidores de arquivos ou recursos de compartilhamento.
- Entrada do servidor de arquivos — Permite ou impede que um usuário insira caminhos e nomes de servidores de arquivos na página do portal. Quando habilitado, coloca a alça de entrada do servidor de arquivos na página do portal. Os usuários podem inserir nomes de

caminho para arquivos do Windows diretamente. Eles podem baixar, editar, excluir, renomear e mover arquivos. Eles também podem adicionar arquivos e pastas. Os compartilhamentos também devem ser configurados para acesso do usuário nos servidores Microsoft Windows aplicáveis. Os usuários podem ser solicitados a fazer a autenticação antes de acessar os arquivos, dependendo dos requisitos de rede.

- Proxy HTTP — Afeta o encaminhamento de um proxy de applet HTTP para o cliente. O proxy é útil para tecnologias que interferem na transformação adequada de conteúdo, como Java, AtiveX e Flash. Ele ignora o processo de manuseio/regravação e garante o uso contínuo do dispositivo de segurança. O proxy encaminhado modifica automaticamente a configuração de proxy antiga do navegador e redireciona todas as solicitações HTTP e HTTPS para a nova configuração de proxy. Ele suporta virtualmente todas as tecnologias do cliente, incluindo HTML, CSS, JavaScript, VBScript, AtiveX e Java. O único navegador que ele suporta é o Microsoft Internet Explorer.
- Entrada de URL—Permite ou impede que um usuário insira URLs HTTP/HTTPS na página do portal. Se esse recurso estiver habilitado, os usuários poderão inserir endereços da Web na caixa de entrada de URL e usar VPN SSL sem cliente para acessar esses sites.
- Inalterado—(padrão) Clique para usar valores da política de grupo que se aplica a esta sessão.
- Habilitar/Desabilitar—Clique para habilitar ou desabilitar o recurso.
- Início automático—Clique para ativar o proxy HTTP e para que o registro DAP inicie automaticamente os applets associados a estes recursos.

Figura 12. Guia Listas de encaminhamento de portas — Permite selecionar e configurar listas de encaminhamento de portas para sessões do usuário.

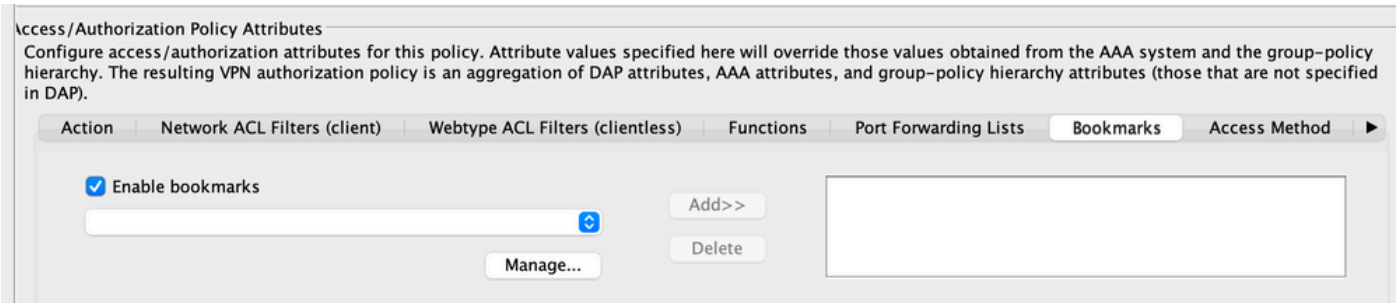


- Encaminhamento de portas—Selecione uma opção para as listas de encaminhamento de portas que se aplicam a este registro LDAP. Os outros atributos neste campo são ativados somente quando você define o Encaminhamento de portas como Ativado ou Início automático.
- Inalterado— Clique para usar valores da política de grupo que se aplica a esta sessão.
- Habilitar/Desabilitar—Clique para habilitar ou desabilitar o encaminhamento de portas.
- Início automático—Clique para ativar o encaminhamento de portas e para que o registro

DAP inicie automaticamente os miniaplicativos de encaminhamento de portas associados às suas listas de encaminhamento de portas.

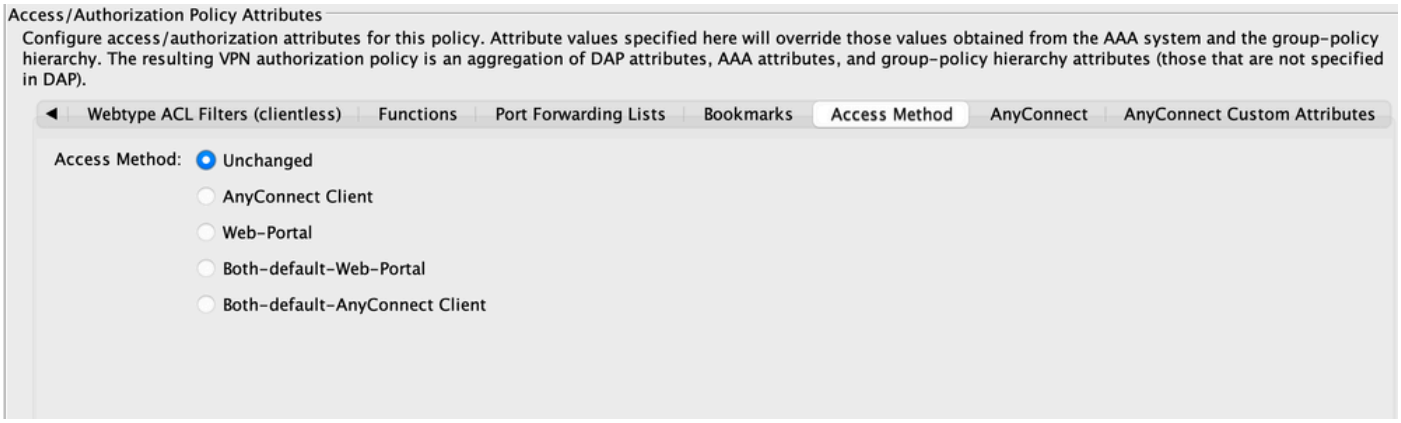
- Caixa suspensa Lista de encaminhamento de portas—Selecione as listas de encaminhamento de portas já configuradas para adicionar ao registro LDAP.
- Novo—Clique para configurar novas listas de encaminhamento de portas.
- Listas de encaminhamento de portas—Exibe a lista de encaminhamento de portas para o registro DAP.
- Adicionar—Clique para adicionar a lista de encaminhamento de portas selecionada da caixa suspensa à lista Encaminhamento de portas à direita.
- Excluir—Clique para excluir a lista de encaminhamento de portas selecionada da lista Encaminhamento de portas. Não é possível excluir uma ACL se ela estiver atribuída a um DAP ou outro registro.

Figura 13. Guia Marcadores — permite selecionar e configurar marcadores/listas de URLs para sessões de usuário.



- Habilitar indicadores—Clique para habilitar. quando esta caixa não está selecionada, nenhuma Lista de indicadores é exibida na página do portal para a conexão
- Gerenciar—Clique para adicionar, importar, exportar e excluir listas de favoritos.
- Listas de marcadores (drop-down) — Exibe as listas de marcadores para o registro DAP.
- Adicionar—Clique para adicionar a lista de marcadores selecionada na caixa suspensa à caixa da lista de marcadores à direita.
- Excluir—Clique para excluir a lista de marcadores selecionada da caixa da lista de marcadores. Você não pode excluir uma lista de marcadores do Security Appliance, a menos que primeiro a exclua dos registros LDAP.

Figura 14. Guia Método — Permite configurar o tipo de acesso remoto permitido.



- Inalterado — Continua com o método de acesso remoto atual definido na política de grupo para a sessão.
- AnyConnect Client—Conecta-se usando o Cisco AnyConnect VPN Client.
- Portal da Web—Conecte-se com uma VPN sem cliente.
- Both-default-Web-Portal — Conecte-se via cliente ou AnyConnect, com um padrão de sem cliente.
- Both-default-AnyConnect Client — Conecte-se via cliente sem cliente ou AnyConnect, com um padrão do AnyConnect.

Como mencionado anteriormente, um registro DAP tem um conjunto limitado de valores de atributos padrão, somente se forem modificados, terão precedência sobre os registros AAA, usuário, grupo, grupo de túneis e grupo padrão atuais. Se forem necessários valores de atributo adicionais fora do escopo do DAP, por exemplo, Listas de túneis divididas, Banners, Túneis inteligentes, Personalizações de portal, etc., eles precisarão ser aplicados via AAA, usuário, grupo, grupo de túneis e registros de grupo padrão. Nesse caso, esses valores de atributo específicos podem complementar o DAP e não podem ser substituídos. Assim, o usuário obtém um conjunto cumulativo de valores de atributo em todos os registros.

Agregar várias políticas de acesso dinâmico

Um administrador pode configurar vários registros LDAP para lidar com muitas variáveis. Como resultado, um usuário de autenticação pode satisfazer os critérios de atributos AAA e Endpoint de vários registros DAP. Consequentemente, os Atributos da política de acesso podem ser consistentes ou conflitantes em todas essas políticas. Nesse caso, o usuário autorizado pode obter o resultado cumulativo em todos os registros LDAP correspondentes.

Isso também inclui valores de atributo exclusivos impostos por meio de autenticação, autorização, usuário, grupo, grupo de túneis e registros de grupo padrão. O resultado cumulativo de Atributos de política de acesso cria a política de acesso dinâmica. Exemplos de Atributos de Política de Acesso combinados são listados nas próximas Tabelas. Esses exemplos retratam os resultados de 3 registros DAP combinados.

O atributo de ação mostrado na Tabela 1 tem um valor que é Terminar ou Continuar. O valor do

atributo agregado será Finalizar se o valor Finalizar estiver configurado em qualquer um dos registros LDAP selecionados e será Continuar se o valor Continuar estiver configurado em todos os registros DAP selecionados.

Tabela 1. Atributo de Ação

Nome do atributo	DAP#1	DAP#2	DAP#3	DAP
Ação (Exemplo 1)	continuar	continuar	continuar	continuar
Ação (Exemplo 2)	Terminar	continuar	continuar	terminar

O atributo de mensagem de usuário mostrado na Tabela 2 contém um valor de string. O valor de atributo agregado pode ser uma string separada de alimentação de linha (valor hexadecimal 0x0A) criada pela vinculação dos valores de atributo dos registros DAP selecionados. A ordem dos valores de atributo na sequência combinada é insignificante.

Tabela 2. Atributo de mensagem do usuário

Nome do atributo	DAP#1	DAP#2	DAP#3	DAP
mensagem do usuário	o rápido	raposa marrom	Salta para cima	a ágil<LF>raposa marrom<LF>salta

Os atributos de ativação do recurso sem cliente (Funções) mostrados na Tabela 3 contêm valores que são Início automático, Habilitar ou Desabilitar. O valor do atributo agregado poderá ser Início automático se o valor de Início automático estiver configurado em qualquer um dos registros LDAP selecionados.

O valor de atributo agregado pode ser Habilitado se não houver um valor de Início automático configurado em nenhum dos registros LDAP selecionados e o valor de Habilitar estiver configurado em pelo menos um dos registros DAP selecionados.

O valor do atributo agregado pode ser desativado se não houver nenhum valor AutoStart ou Enable configurado em qualquer um dos registros DAP selecionados, e o valor "disable" estiver configurado em pelo menos um dos registros DAP selecionados.

Tabela 3. Atributos de Ativação de Recursos sem Cliente (Funções)

Nome do atributo	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable	disable		enable
navegação de arquivos	disable	enable	disable	enable
entrada de arquivo			disable	disable
proxy HTTP	disable	início automático	disable	início automático
entrada de URL	disable		enable	enable

Os atributos URL list e port-forward mostrados na Tabela 4 contêm um valor que é uma string ou uma string separada por vírgulas. O valor de atributo agregado pode ser uma string separada por

vírgulas criada pelo ao vincular os valores de atributo dos registros DAP selecionados. Qualquer valor de atributo duplicado na string combinada pode ser removido. O modo como os valores de atributo são ordenados na sequência combinada é insignificante.

Tabela 4. Atributo de Lista de URL e Lista de encaminhamento de portas

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

Os atributos de Método de Acesso especificam o método de acesso do cliente permitido para conexões VPN SSL. O método de acesso do cliente pode ser acesso somente ao AnyConnect Client, acesso somente ao portal da Web, acesso ao AnyConnect Client ou portal da Web com acesso ao portal da Web como padrão ou acesso ao AnyConnect Client ou portal da Web com acesso ao AnyConnect Client como padrão. O valor agregado do atributo está resumido na Tabela 5.

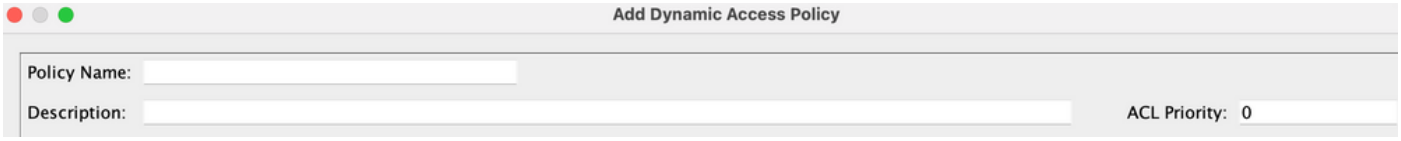
Tabela 5. Atributos do Método de Acesso

Valores de Atributo Selecionados				Resultado da agregação
Cliente AnyConnect	Portal da Web	Both-default-Web- Portal	Cliente AnyConnect padrão de ambos	
			X	Cliente AnyConnect padrão de ambos
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Portal da Web
	X		X	Cliente AnyConnect padrão de ambos
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
X				Cliente AnyConnect
X			X	Cliente AnyConnect padrão de ambos
X		X		Both-default-Web-Portal
X		X	X	Both-default-Web-Portal
X	X			Both-default-Web-Portal
X	X		X	Cliente AnyConnect padrão de ambos
X	X	X		Both-default-Web-Portal
X	X	X	X	Both-default-Web-Portal

Quando você combina os atributos Network (Firewall) e Web-Type (Clientless) ACL Filter, a Prioridade do DAP e a ACL do DAP são dois componentes principais a serem considerados.

O atributo Priority, como mostrado na figura 15, não é agregado. O Security Appliance usa esse valor para sequenciar logicamente as listas de acesso ao agregar as ACLs de rede e tipo Web de vários registros LDAP. O Security Appliance ordena os registros do número de prioridade mais alto para o mais baixo, 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. Não é possível classificá-los manualmente.

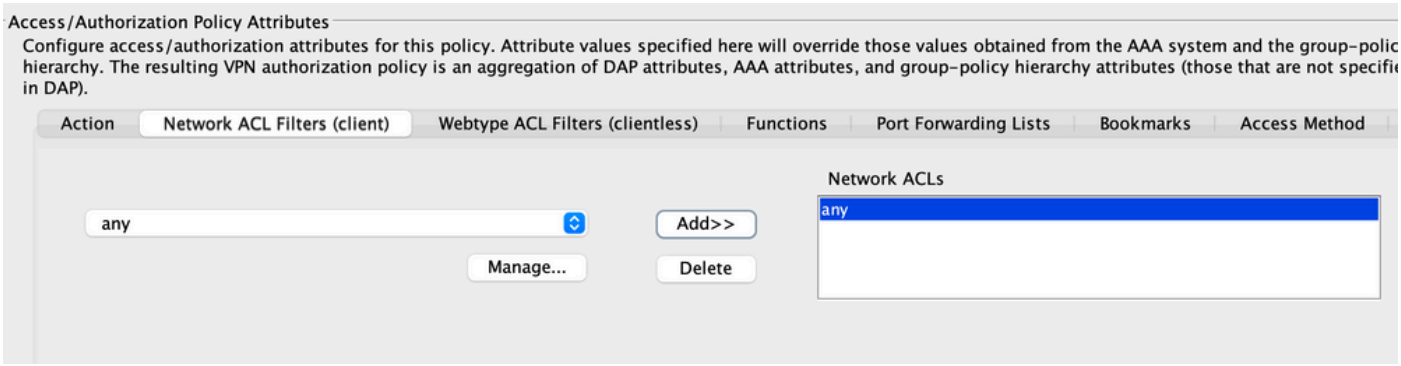
Figura 15. Priority — Exibe a prioridade do registro DAP.



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

O atributo de ACL do DAP só suporta listas de acesso que estejam em conformidade com um modelo de ACL Allow-List ou Block-List estrito. Em um modelo Allow-List ACL, as entradas da lista de acesso especificam regras que "Permitem" o acesso a redes ou hosts especificados. No modo Block-List ACL, as entradas da lista de acesso especificam regras que negam o acesso a redes ou hosts especificados. Uma lista de acesso não compatível contém entradas de lista de acesso com uma mistura de regras de permitir e negar . Se uma lista de acesso não conforme for configurada para um registro LDAP, ela poderá ser rejeitada como um erro de configuração quando o administrador tentar adicionar o registro. Se uma lista de acesso em conformidade for atribuída a um registro LDAP, qualquer modificação na lista de acesso que altera a característica de conformidade poderá ser rejeitada como um erro de configuração.

Figura 16. DAP ACL— Permite selecionar e configurar ACLs de rede para aplicar a este registro DAP.



Quando vários registros DAP são selecionados, os atributos das listas de acesso especificados na ACL de Rede (Firewall) são agregados para criar uma Lista de Acesso Dinâmica para a ACL de Firewall DAP. Da mesma forma, os atributos das listas de acesso especificados na ACL de Tipo Web (Sem Clientes) são agregados para criar uma Lista de Acesso Dinâmica para a ACL

sem Clientes DAP. O próximo exemplo focaliza como uma lista de acesso de firewall DAP dinâmica é criada especificamente. No entanto, uma lista de acesso sem cliente LDAP dinâmica também pode fazer o mesmo processo.

Primeiro, o ASA cria dinamicamente um nome exclusivo para o DAP Network-ACL como mostrado na Tabela 6.

Tabela 6. Nome da ACL de rede dinâmica

Nome da ACL de rede DAP
DAP-Network-ACL-X (onde X é um inteiro que pode incrementar para garantir exclusividade)

Em segundo lugar, o ASA recupera o atributo Network-ACL dos registros DAP selecionados, conforme mostrado na Tabela 7.

Tabela 7. ACLs de rede

Registros DAP selecionados	Prioridade	ACLs de rede	Entradas de ACL de rede
DAP 1	1	101 e 102	A ACL 101 tem 4 regras de negação e a ACL 102 tem 4 regras de permissão
DAP 2	2	201 e 202	A ACL 201 tem 3 regras de permissão e a ACL 202 tem 3 regras de negação
DAP 3	2	101 e 102	A ACL 101 tem 4 regras de negação e a ACL 102 tem 4 regras de permissão

Em terceiro lugar, o ASA reorganiza a rede ACL primeiro pelo número de prioridade do registro DAP e, em seguida, pela lista de bloqueio primeiro se o valor de prioridade para 2 ou mais registros DAP selecionados for o mesmo. Depois disso, o ASA pode recuperar as entradas de Network-ACL de cada Network-ACL, como mostrado na Tabela 8.

Tabela 8. Prioridade de registro DAP

ACLs de rede	Prioridade	Modelo de lista de acesso branco/preto	Entradas de ACL de rede
101	2	Lista Negra	4 Regras de Negação (DDDD)
202	2	Lista Negra	3 Regras de Negação (DDD)
102	2	Lista branca	4 Regras de permissão (PPP)
202	2	Lista branca	3 regras de permissão (PPP)
101	1	Lista Negra	4 Regras de Negação (DDDD)
102	1	Lista branca	4 Regras de permissão (PPP)

Por fim, o ASA mescla as entradas Network-ACL na Network-ACL gerada dinamicamente e retorna o nome da Network-ACL dinâmica como a nova Network-ACL a ser aplicada, como mostrado na Tabela 9.

Tabela 9. Rede DAP dinâmica-ACL

Nome da ACL de rede DAP	Entrada de ACL de rede
DAP-Network-ACL-1	DDDD DDD PPP PPP DDDD PPP

Implementação do DAP

Há vários motivos pelos quais um administrador deve considerar a implementação do DAP. Algumas razões subjacentes são quando a avaliação de postura em um endpoint deve ser aplicada e/ou quando atributos AAA ou de política mais granulares devem ser considerados ao autorizar o acesso do usuário aos recursos de rede. No próximo exemplo, você pode configurar o DAP e seus componentes para identificar um endpoint de conexão e autorizar o acesso do usuário a vários recursos de rede.

Caso de Teste - Um cliente solicitou uma Prova de Conceito com estes requisitos de Acesso VPN:

- A capacidade de detectar e identificar um endpoint de funcionário como Gerenciado ou Não Gerenciado. — Se o endpoint for identificado como gerenciado (PC de trabalho), mas falhar nos requisitos de postura, o acesso a ele deverá ser negado. Por outro lado, se o endpoint do funcionário for identificado como não gerenciado (PC residencial), esse endpoint deverá receber acesso sem cliente.
- A capacidade de chamar a limpeza de cookies de sessão e cache quando uma conexão sem cliente é encerrada.
- A capacidade de detectar e aplicar aplicativos em execução em endpoints gerenciados de funcionários, como o McAfee AntiVirus. Se o aplicativo não existir, o acesso a esse ponto final deverá ser negado.
- A capacidade de usar autenticação AAA para determinar a quais recursos de rede os usuários autorizados devem ter acesso. O Security Appliance deve oferecer suporte à autenticação Nativa do MS LDAP e a várias funções de associação de grupo LDAP.
- A capacidade de permitir o acesso de LAN local a recursos de rede, como faxes e impressoras de rede, quando conectado através de uma conexão baseada em cliente/rede.
- A capacidade de fornecer acesso de convidado autorizado aos contratados. Os prestadores de serviços e seus endpoints devem obter acesso sem cliente, e o acesso do portal aos aplicativos deve limitar o acesso dos funcionários.

Neste exemplo, você pode executar uma série de etapas de configuração para atender aos requisitos de acesso VPN do cliente. Pode haver etapas de configuração necessárias, mas não diretamente relacionadas ao DAP, enquanto outras configurações podem ser diretamente relacionadas ao DAP. O ASA é muito dinâmico e pode se adaptar a muitos ambientes de rede. Como resultado, as soluções de VPN podem ser definidas de várias maneiras e, em alguns casos, fornecem a mesma solução final. A abordagem adotada, no entanto, é orientada pelas

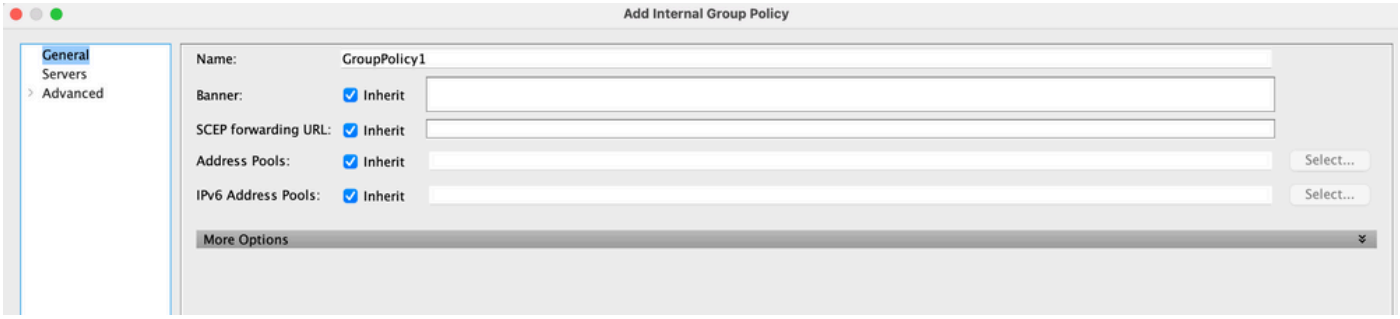
necessidades do cliente e seus ambientes.

Com base na natureza deste documento e nos requisitos do cliente definidos, você pode usar o Adaptive Security Device Manager (ASDM) e concentrar a maioria de nossas configurações no DAP. No entanto, você também pode configurar Políticas de grupo locais para mostrar como o DAP pode complementar e/ou substituir atributos de política local. Para a base deste caso de teste, você pode supor que um Grupo de servidores LDAP, a Lista de redes com tunelamento dividido e a conectividade IP básica, incluindo Pools de IP e o Grupo de servidores DNS padrão, estão pré-configurados.

Definir uma Política de Grupo— esta configuração é necessária para definir Atributos de Política Local. Alguns atributos definidos aqui não são configuráveis no DAP (por exemplo, Local LAN Access). (Essa política também pode ser usada para definir atributos baseados em Clientless e Client).

Navegue para Configuration > Remote Access VPN > Network (Client) Access > Group Policies e adicione uma Internal Group Policy como mostrado:

Figura 17. Group Policy —Define atributos específicos de VPN local.

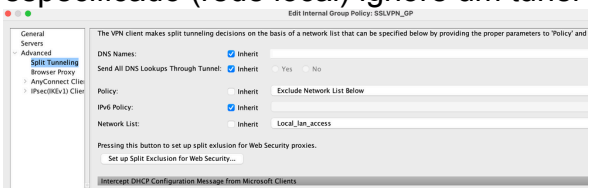


a. No link General (Geral), configure o nomeSSLVPN_GP para Group Policy (Política de grupo).

b. Também no link General, clique em More Options e configure apenas o Tunneling Protocol:Clientless SSLVPN. (Você pode configurar o DAP para substituir e gerenciar o Access Method.)

c. No link Advanced > Split Tunneling, configure as próximas etapas:

Figura 18. Split Tunneling — Permite que o tráfego especificado (rede local) ignore um túnel não criptografado durante uma conexão de cliente.

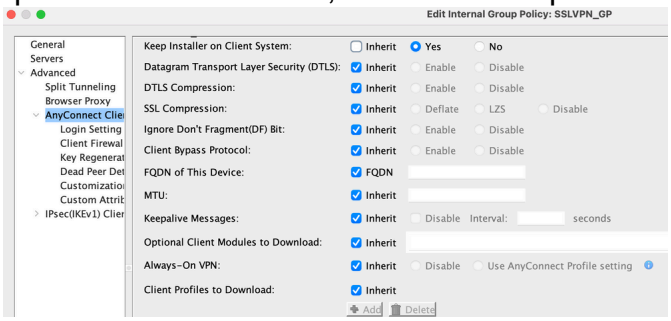


a. Política: UncheckInheritand selectExclude Network List.

b. Network List: UncheckInherite selecione o nomeLocal_Lan_Access da lista. (Suponha que esteja pré-configurado.)

d. No link Advanced > ANYCONNECT Client, configure estas próximas etapas:

Figura 19. Instalador de Cliente VPN SSL — Após o término da VPN, o Cliente SSL pode permanecer no endpoint ou ser desinstalado.



e. Mantenha o instalador no sistema cliente: DesmarqueHerdar e selecioneSim.

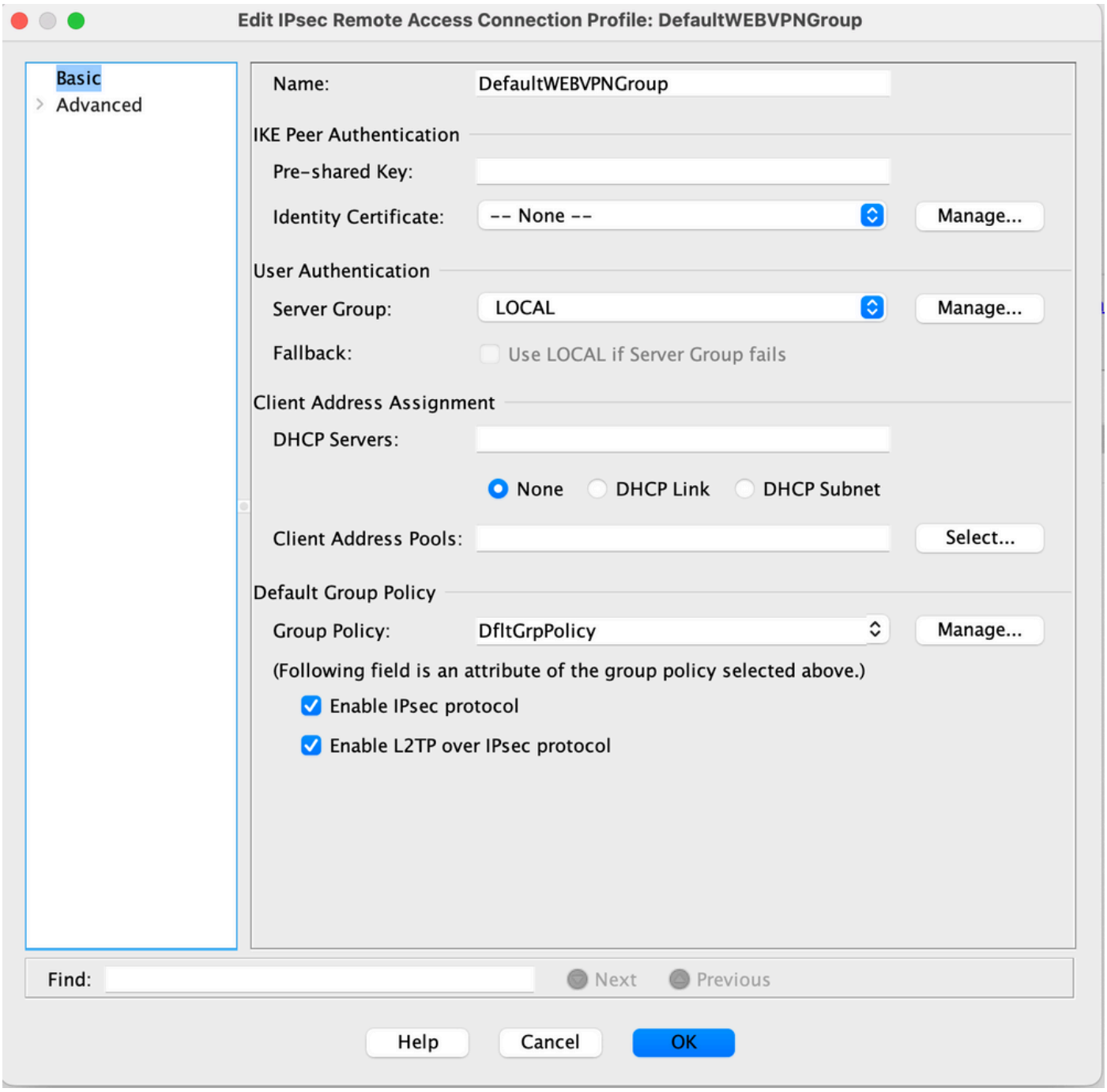
f. Clique emOKe emAplicar.

g. Aplique suas alterações de configuração.

Definindo um Perfil de Conexão—esta configuração é necessária para definir nosso método de autenticação AAA, por exemplo, LDAP, e aplicar a Política de Grupo previamente configurada (SSLVPN_GP) a este Perfil de Conexão. Os usuários que se conectam por meio desse Perfil de Conexão podem estar sujeitos aos atributos definidos aqui, bem como aos atributos definidos na Política de Grupo SSLVPN_GP. (Este perfil também pode ser usado para definir atributos baseados em Cliente e Sem Cliente).

Navegue até Configuration > Remote Access VPN > Network (Client) Access >IPsec Remote Access Connection Profile e configure:

Figura 20. Perfil de conexão — Define localmente os atributos específicos de VPN.



a. Na seção Perfis de conexão, edite o DefaultWEBVPNGroup e, no link Básico, configure as próximas etapas:

   a. Autenticação — Método:AAA

   b. Autenticação — Grupo de servidores AAA:LDAP(Presumido pré-configurado)

   c. Atribuição de endereço de cliente — Pools de endereços de cliente:IP_Pool(Presumido pré-configurado)

   d. Política de grupo padrão — Política de grupo: SelectSSLVPN_GP

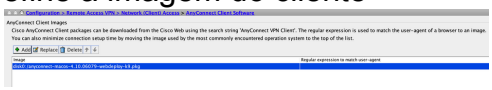
b. Aplique suas alterações de configuração.

Definir uma interface IP para conectividade VPN SSL — Esta configuração é necessária para

encerrar conexões SSL Cliente e Sem Cliente em uma interface especificada.

Antes de habilitar o acesso de Cliente/Rede em uma interface, você deve primeiro definir uma imagem de Cliente VPN SSL.

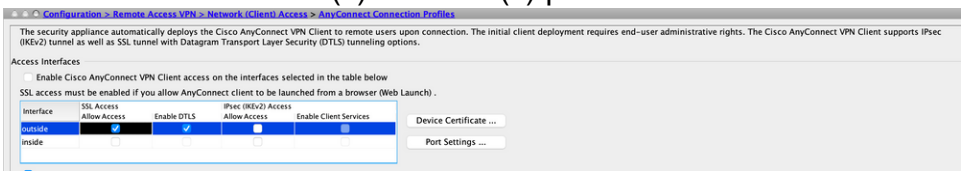
1. Navegue para Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software e adicione a próxima imagem, a imagem do SSL VPN Client do sistema de arquivos ASA Flash: (Esta imagem pode ser baixada do CCO, https://www.cisco.com)

   Figura 21. Instalação da imagem do cliente VPN SSL — Define a imagem do cliente AnyConnect a ser enviada para os endpoints de conexão. 

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

   b. Clique em OK,OKnovamente e em Aplicar.

2. Navegue para Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles e use as próximas etapas para ativar isso:

   Figura 22. SSL VPN Access Interface—Define a(s) interface(s) para terminar a conectividade VPN SSL. 

   a. Na seção Interface de acesso, habilite:Habilite o Cisco AnyConnect VPN Client ou o acesso ao SSL VPN Client legado nas interfaces selecionadas na tabela abaixo.

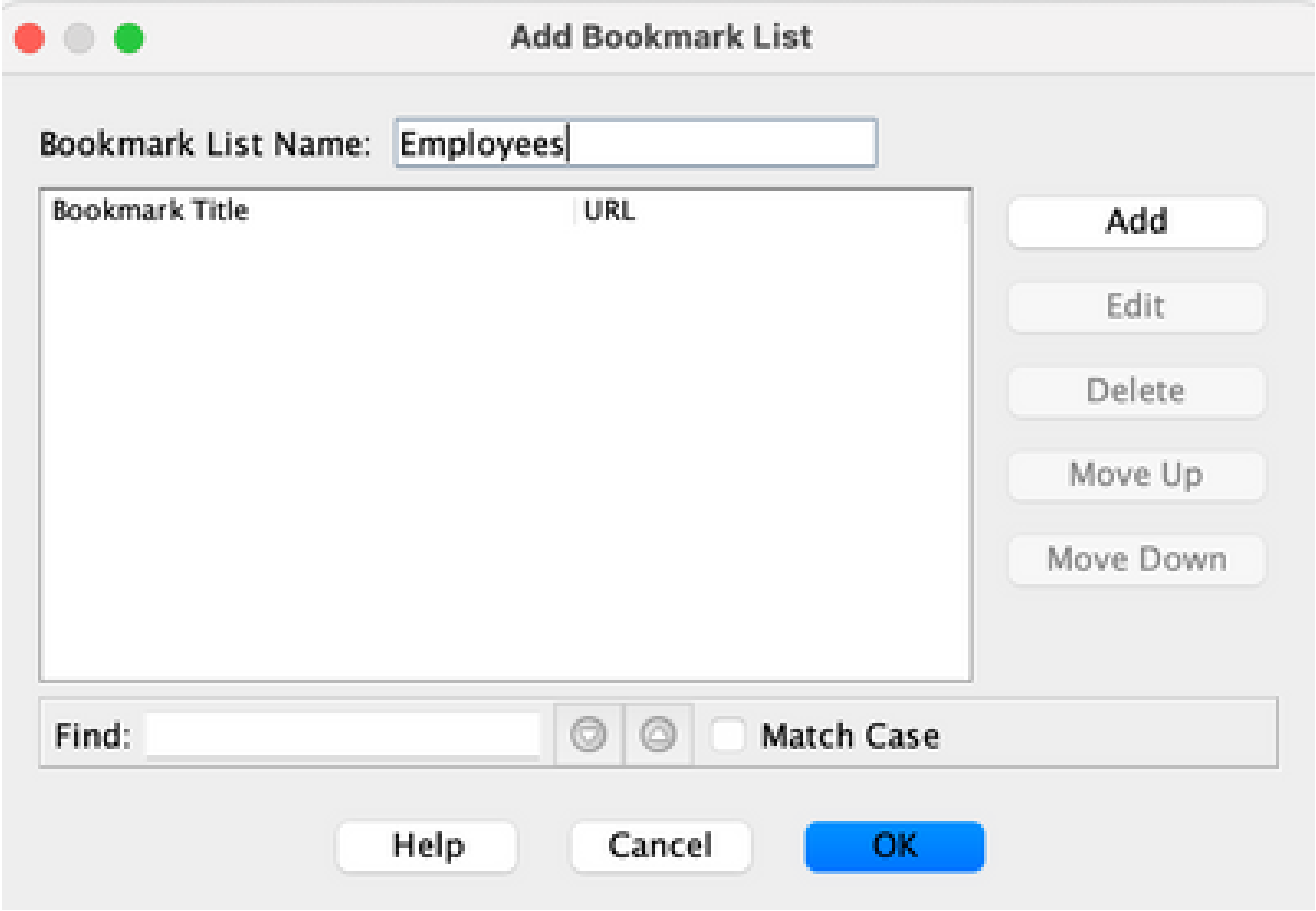
   b. Também na seção Access Interfaces (Interfaces de acesso), marque Allow Access (Permitir acesso) na interface externa. (Essa configuração também pode habilitar o acesso sem cliente VPN SSL na interface externa.)

   c. Clique em Aplicar.

Definição de Listas de Indicadores (Listas de URLs) para Acesso sem Cliente — Essa configuração é necessária para definir um aplicativo baseado na Web a ser publicado no Portal. Você pode definir duas Listas de URLs, uma para Funcionários e outra para Contratantes.

1. Navegue até Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks, clique em+ Addand configure as próximas etapas:

   Figura 23. Lista de marcadores — Define URLs a serem publicados e acessados no portal da Web. (Personalizado para acesso de funcionários).



a. Nome da lista de favoritos:Funcionários e, em seguida, clique em Adicionar.

b. Título do indicador:Intranet da empresa

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

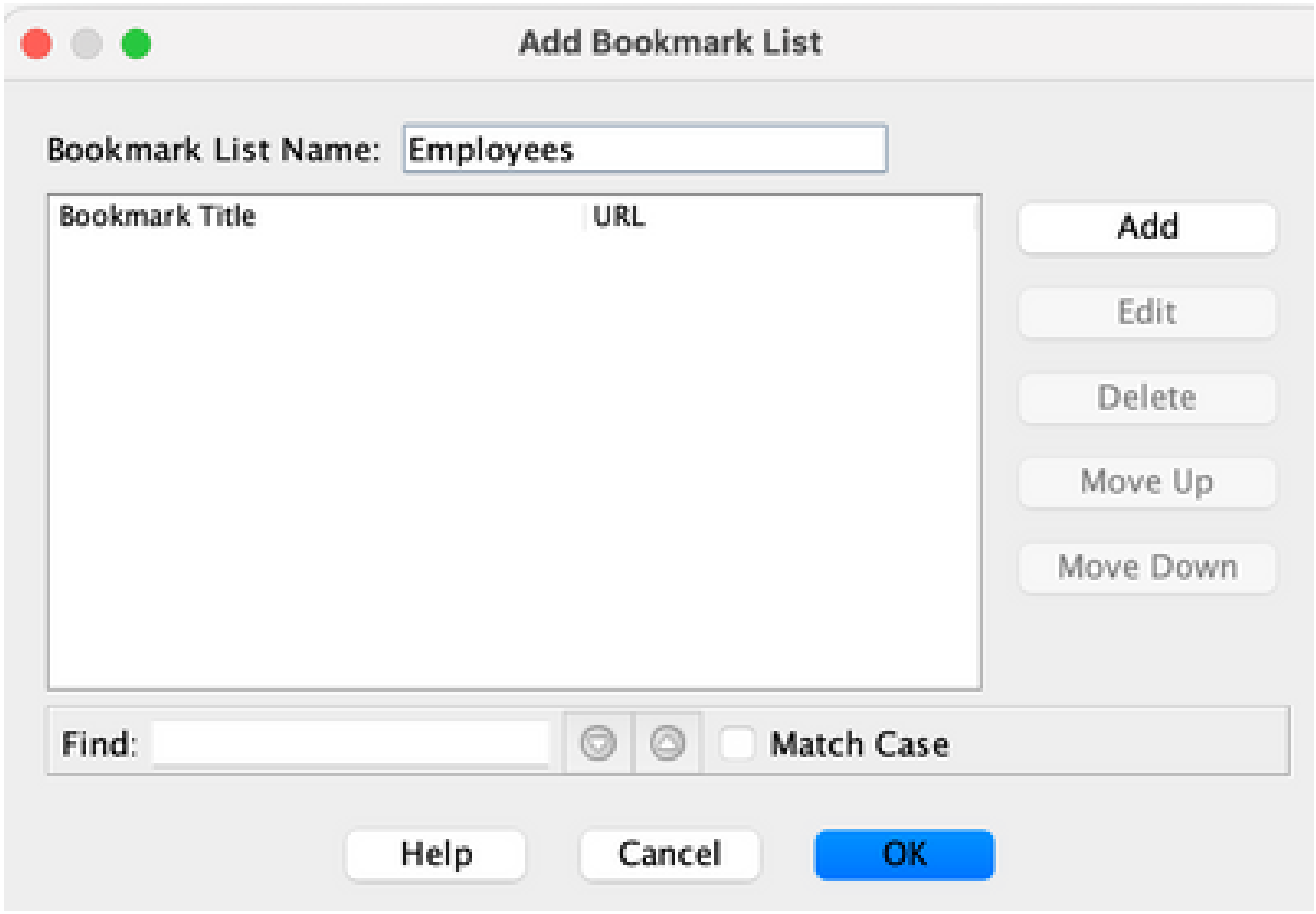
-

Clique em OK e em OK novamente.

-

Clique em+ Adicionar e configure uma segunda Lista de favoritos (Lista de URLs) da seguinte maneira:

Figura 24. Lista de favoritos — Personalizada para acesso de convidados.



a.

Nome da lista de favoritos:**Contratantes** e, em seguida, **clique em Adicionar**.

b.

Título do indicador:**Acesso para convidado**

c.

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

-

Clique em OK e em OK novamente.

-

Clique em Aplicar.

Configurar o Hostscan:

- Navegue até **Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image** e configure as próximas etapas:

Figura 25. Instalação da Imagem do HostScan — Define a imagem do HostScan a ser enviada aos endpoints de conexão. 

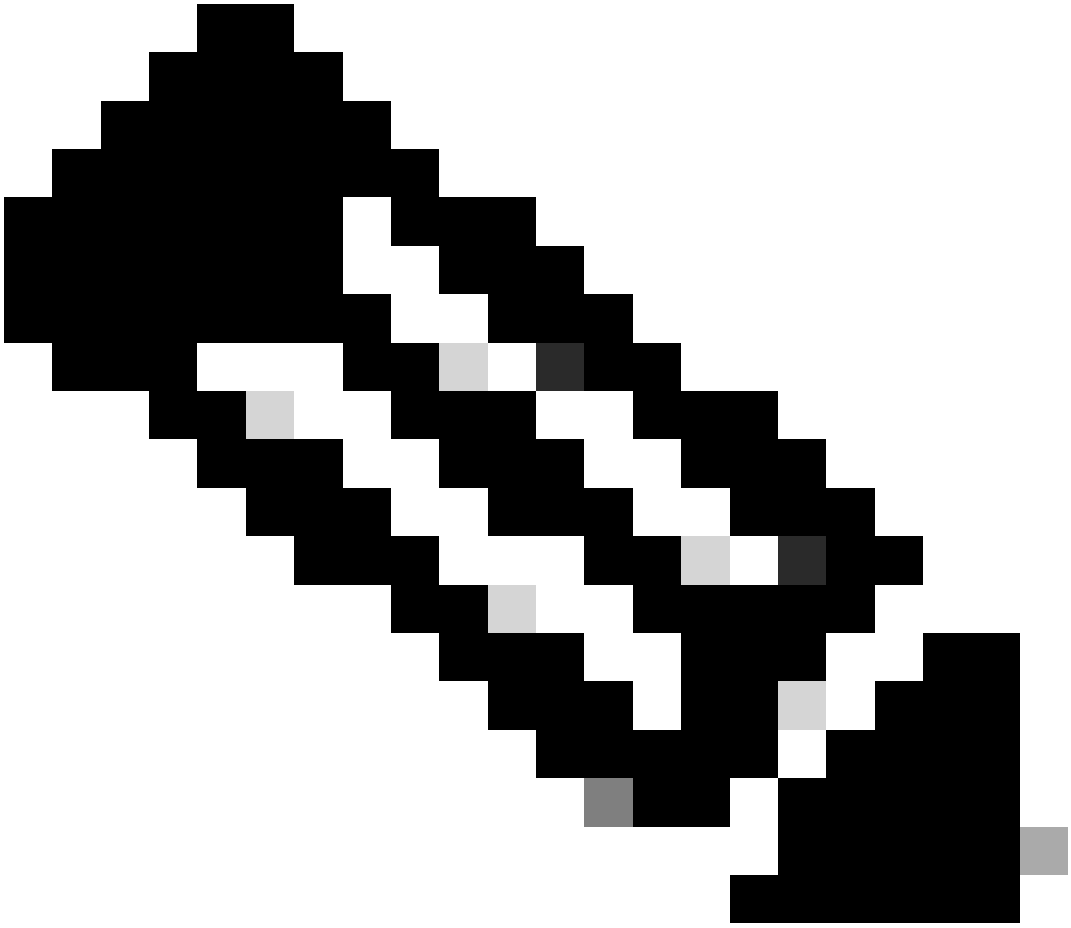
a. Instale **o disk0:/hostscan_4.xx.xxxxx-k9.**pkgimage a partir do sistema de arquivos Flash ASA.

b. **Marque Ativar HostScan**.

c. **Clique em Aplicar**.

Políticas de acesso dinâmico — Esta configuração é necessária para validar a conexão de usuários e seus endpoints com base em critérios de avaliação de AAA e/ou endpoint definidos. Se os critérios definidos de um registro LDAP forem atendidos, os usuários que se conectarem poderão receber acesso aos recursos de rede associados a esse registro ou registros DAP. A autorização do DAP é executada durante o processo de autenticação.

Para garantir que uma conexão VPN SSL possa terminar no caso padrão (por exemplo, quando o ponto final não corresponder a nenhuma política de acesso dinâmico configurada), você pode configurá-lo com estas etapas:

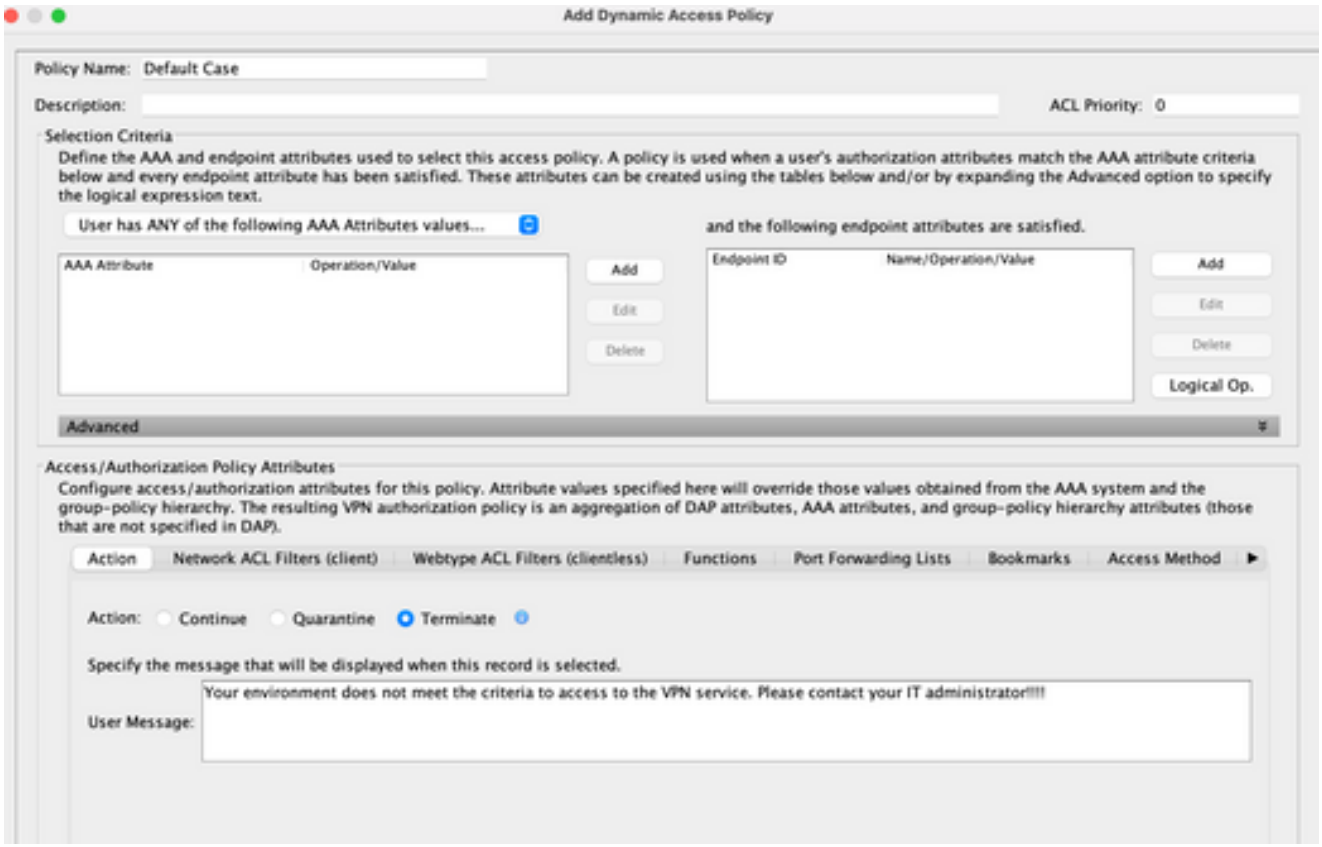


Observação: ao configurar políticas de acesso dinâmico pela primeira vez, uma mensagem de erro DAP.xml é exibida indicando que um arquivo de configuração DAP (DAP.XML) não existe. Depois que a configuração inicial do DAP for modificada e salva, esta mensagem não poderá mais ser exibida.

•

Navegue até **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** e configure as próximas etapas:

Figura 30. Política de acesso dinâmico padrão — se nenhum registro LDAP predefinido for correspondido, esse registro LDAP poderá ser aplicado. Assim, o acesso VPN SSL pode ser negado.



a.

Edite aDfltAccessPolicy e defina a Ação **como Encerrar**.

b.

Clique em OK.

•

Adicione uma nova Política de acesso dinâmico **chamadaManaged_Endpoints**, da seguinte maneira:

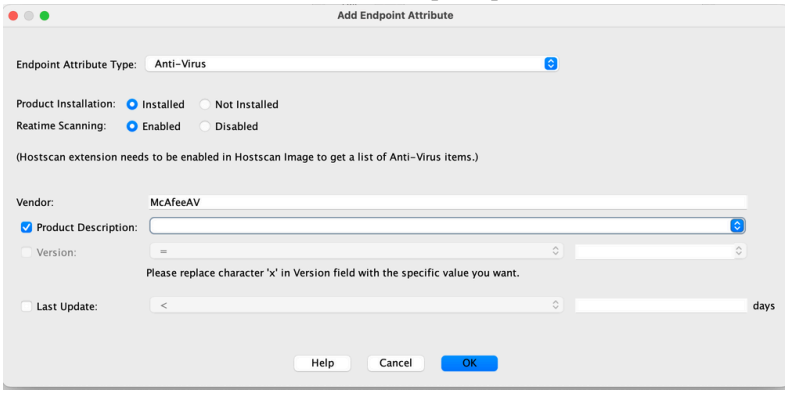
a.

Descrição:**Employee Client Access**

b.

Adicione um tipo de atributo de ponto final (antivírus) como mostrado na Figura 31. Clique em OK quando terminar.

Figura 31. Atributo de endpoint do DAP — O antivírus de avaliação avançada de endpoint pode ser usado como um critério do DAP para acesso de cliente/rede.



c.

Como mostrado na imagem anterior, na lista suspensa da seção AAA Attribute, selecione User has ALL of the following AAA Attributes Values.

•

Adicione (localizado à direita da caixa AAA Attribute) um AAA Attribute Type (LDAP), conforme mostrado nas Figuras 33 e 34. Clique em OK quando terminar.

Figura 33. Atributo AAA do DAP — A associação ao grupo AAA pode ser usada como critério DAP para identificar um Funcionário.

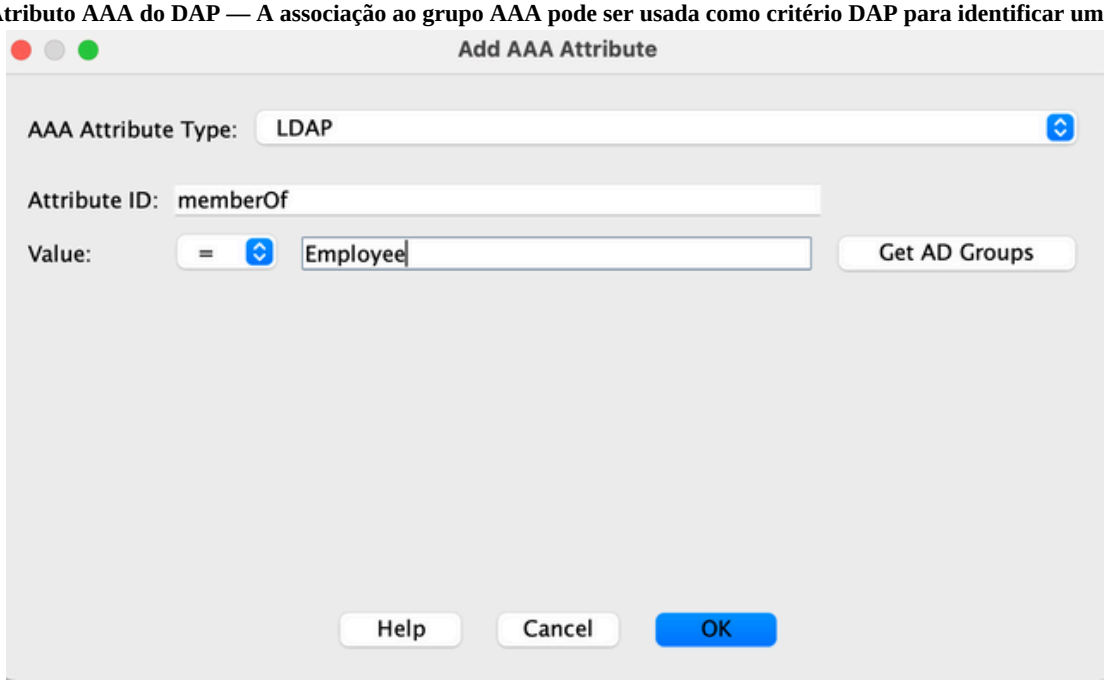
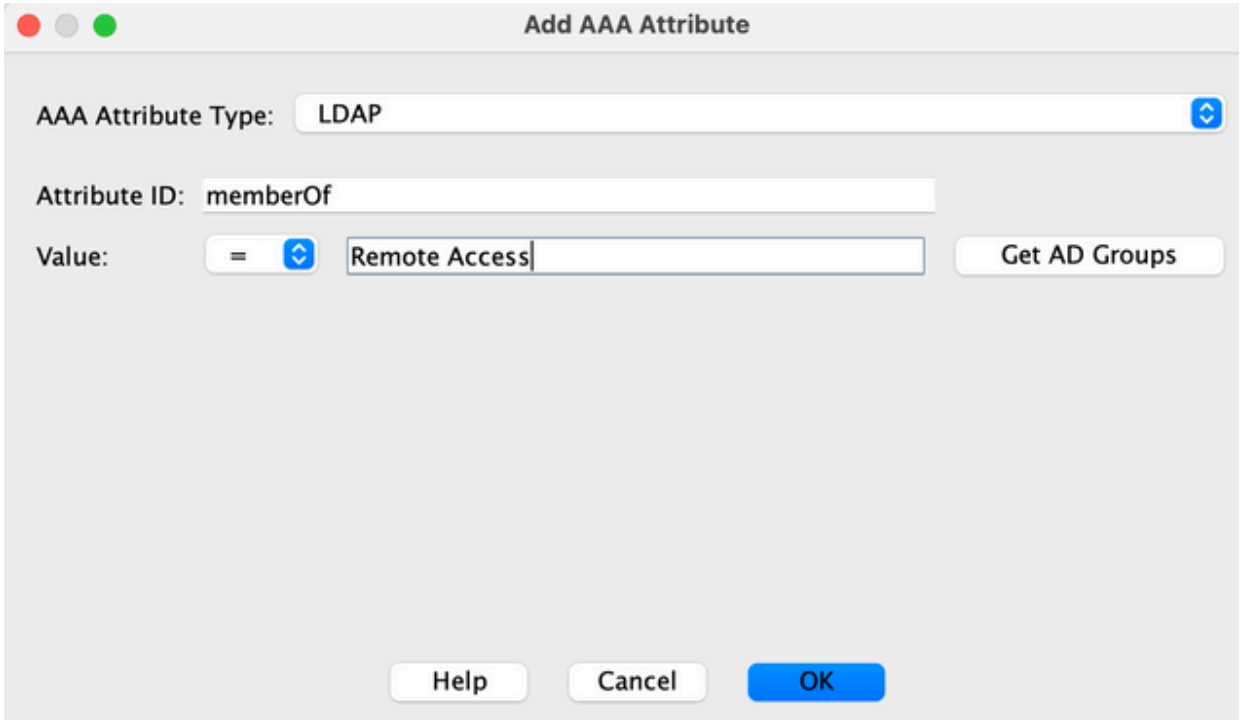


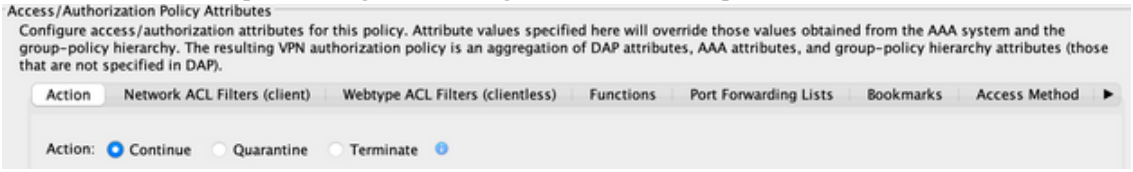
Figura 34. Atributo de AAA do DAP — A associação ao grupo AAA pode ser usada como um critério de DAP para permitir capacidades de Acesso Remoto.



-

Na guia Action (Ação), verifique se a Ação está definida **como Continue**, como mostrado na Figura 35.

Figura 35. Guia Ação—Esta configuração é necessária para definir o processamento especial para uma conexão ou sessão específica. O acesso à VPN pode ser negado se um registro DAP for correspondido e a Ação estiver definida como Encerrar.



-

Na guia Access Method (Método de acesso), selecione o Access **MethodAnyConnect Client**, como mostrado na Figura 36.

Figura 36. Guia Método de acesso—Esta configuração é necessária para definir os tipos de conexão do cliente VPN SSL.

-

Clique em OK e **em Aplicar**.

-

Adicione uma segunda Política de acesso dinâmico **chamadaUnmanaged_Endpoints**, conforme descrito:

a.

Descrição:**Employee Clientless Access**.

b.

Na lista suspensa na imagem anterior da seção AAA Attribute, selecione User has ALL of the following AAA Attributes Values .

-

Adicione (localizado à direita do Tipo de Atributo AAA) um Tipo de Atributo AAA (LDAP) como mostrado nas Figuras 38 e 39. Clique em OK quando terminar.

Figura 38. Atributo AAA do DAP — A associação ao grupo AAA pode ser usada como critério DAP para identificar um Funcionário.

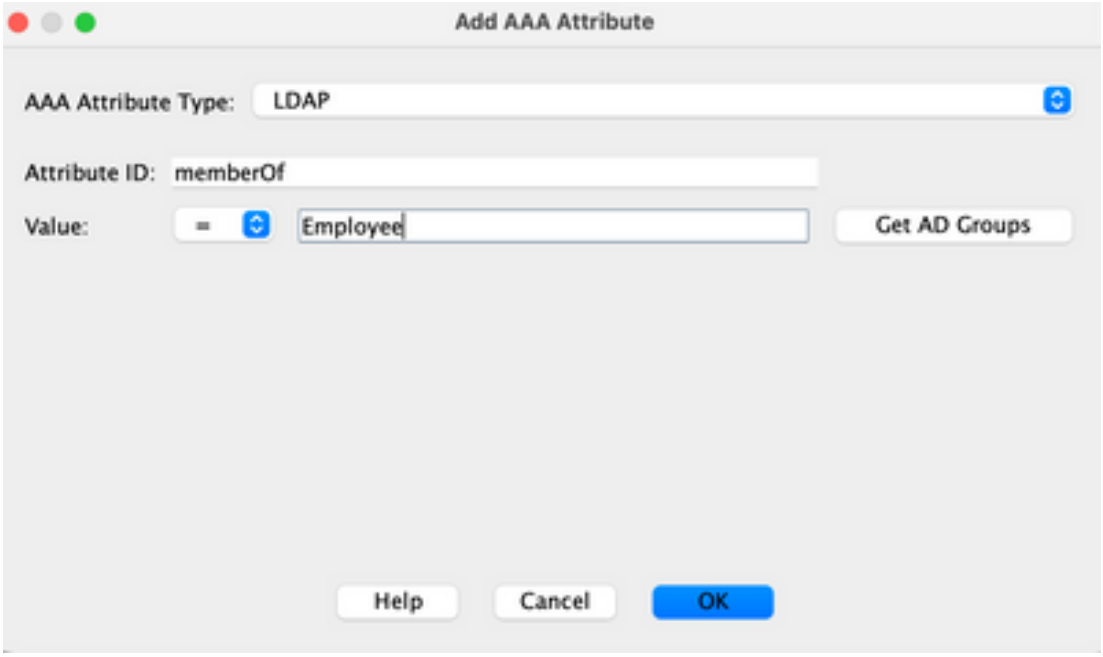
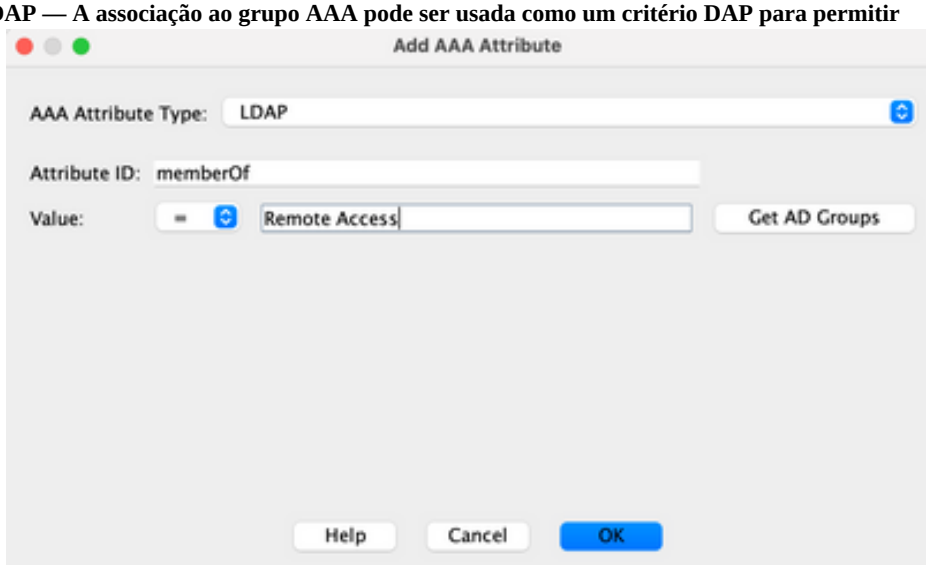


Figura 39. Atributo AAA do DAP — A associação ao grupo AAA pode ser usada como um critério DAP para permitir capacidades de acesso remoto.



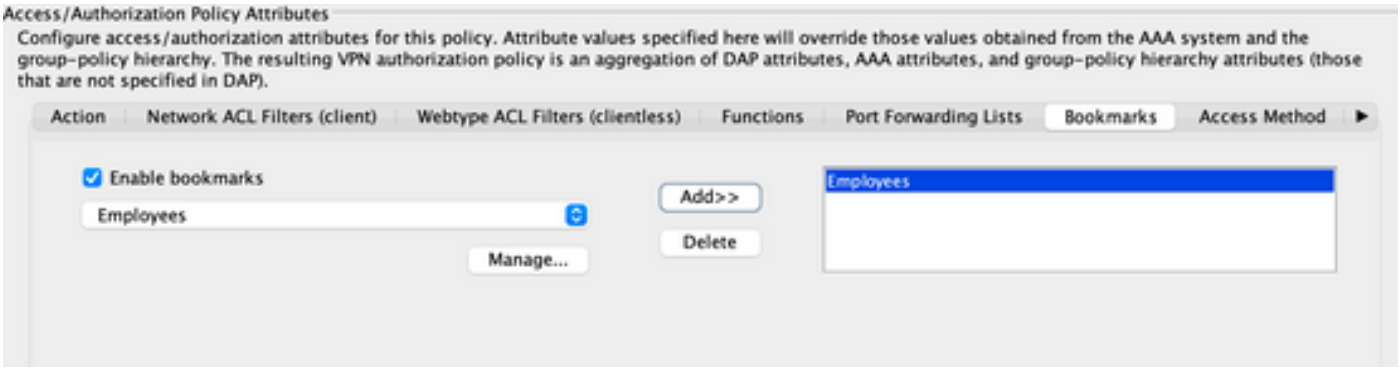
-

Na guia Ação, verifique se a Ação está definida **como Continuar**. (Figura 35)

-

  Na guia Bookmarks, selecione o nome da lista Employeesna lista suspensa e, em seguida, **clique em Add**. Além disso, verifique se os marcadores Enable estão marcados, como mostrado na Figura 40.

Figura 40. Guia Bookmarks — Permite selecionar e configurar listas de URL para sessões de usuário.



-

  a.

  Na guia Método de acesso, selecione o **Portal da Web** Método de acesso. (Figura 36)

- **Clique em OK** e **em Aplicar**.

1. Os contratados podem ser identificados somente pelos atributos AAA do DAP. Como resultado, o Tipo de Atributos de Ponto Final: (Política) não pode ser configurado na Etapa 4. Essa abordagem serve apenas para mostrar versatilidade dentro do DAP.

3. Adicione uma terceira Política de Acesso Dinâmico **chamadaGuest_Access** com o seguinte:

-

  Descrição:**Guest Clientless Access**.

-

Adicione (localizado à direita da caixa Endpoint Attribute) um Endpoint Attribute Type (Policy), como mostrado na Figura 37. Clique em OK quando terminar.

-

Na Figura 40, na lista suspensa na seção AAA Attribute, selecione User has ALL of the following AAA Attributes Values.

-

Adicione (localizado à direita da caixa AAA Attribute) um AAA Attribute Type (LDAP), conforme mostrado nas Figuras 41 e 42. Clique em OK quando terminar.

Figura 41. Você pode usar o Atributo AAA do DAP — Associação ao Grupo AAA como um Critério DAP para Identificar um Contratante

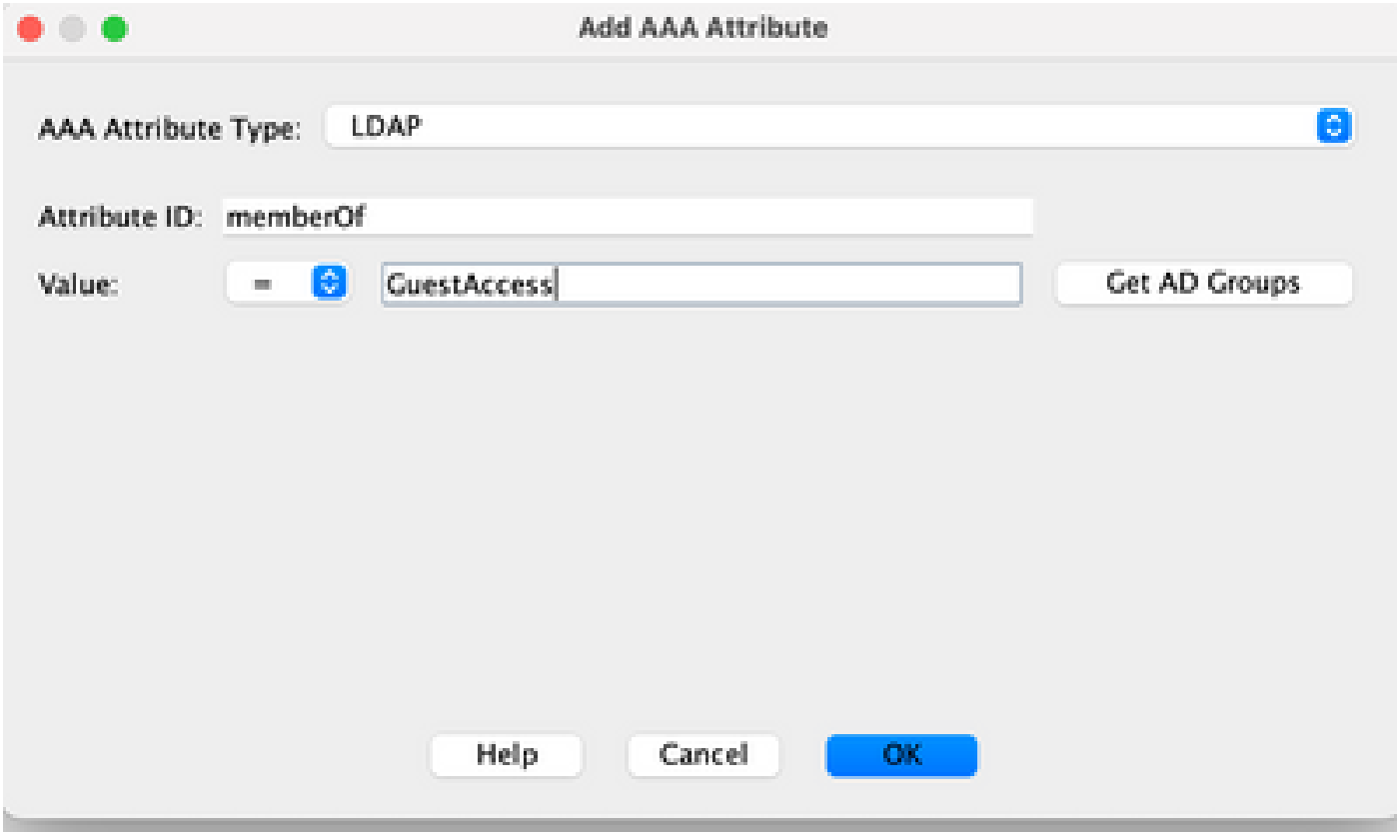
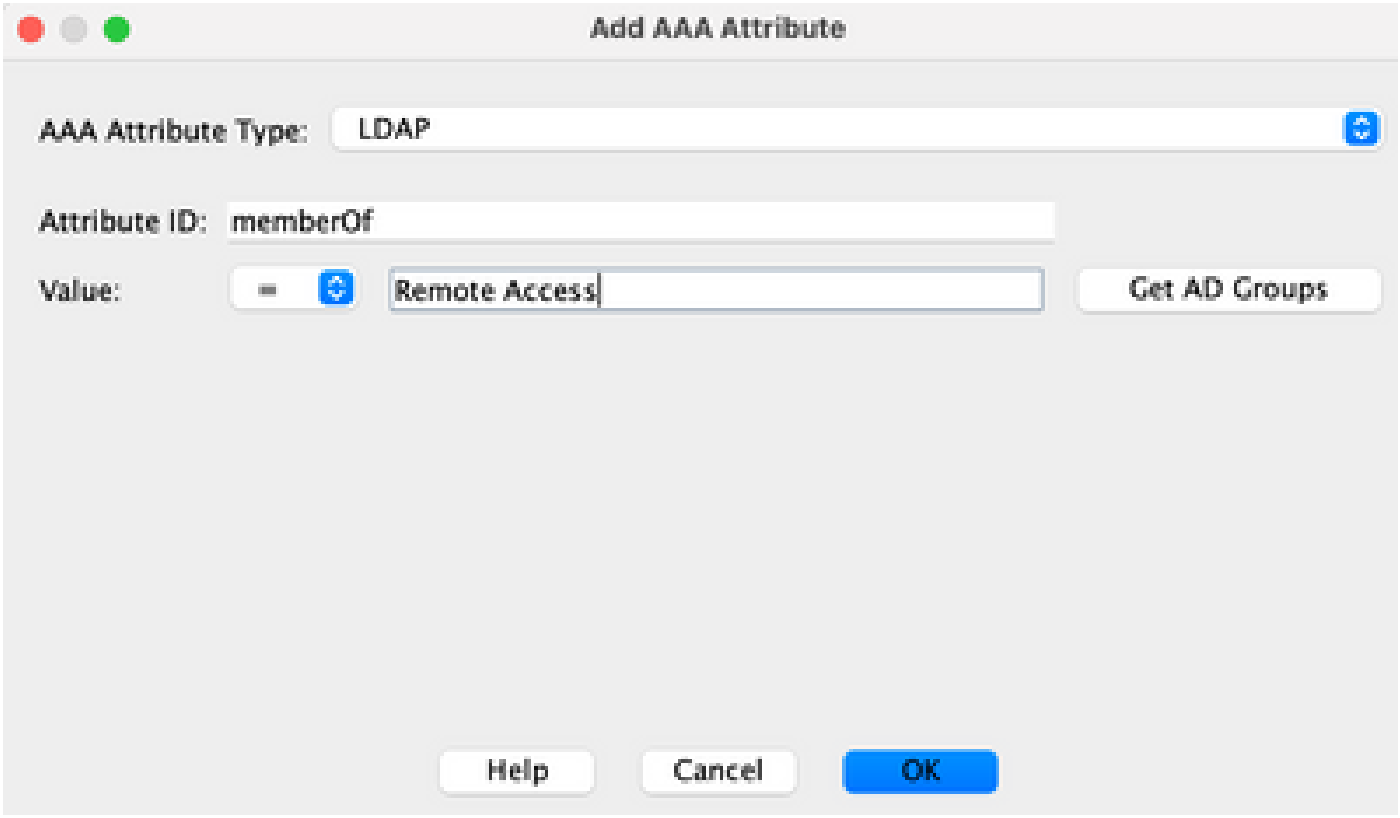


Figura 42. Atributo de AAA do DAP—Você pode usar a associação ao grupo de AAA como um critério de DAP para permitir capacidades de acesso remoto



-

a.

Na guia Ação, verifique se a Ação está definida como **Continuar**. (Figura 35)

b.

Na guia Bookmarks, selecione o nome da lista **Contractors** na lista suspensa e clique em Add. Além disso, verifique se a opção **Ativar marcadores** está marcada. (Consulte a Figura 40.)

c.

Na guia Método de acesso, selecione o Portal da Web Método de acesso. (Figura 36)

d.

Clique em **OK** e em **Apply**.

Conclusão

Com base nos requisitos de VPN SSL de Acesso Remoto do cliente observados neste exemplo, esta solução satisfaz os requisitos de VPN de Acesso Remoto do cliente.

Com a fusão de ambientes de VPN dinâmicos e em evolução, as políticas de acesso dinâmico podem se adaptar e escalar para alterações frequentes na configuração da Internet, várias funções que cada usuário pode ocupar dentro de uma organização e logins de sites de acesso remoto gerenciados e não gerenciados com diferentes configurações e níveis de segurança.

As políticas de acesso dinâmico são complementadas por tecnologias legadas novas e comprovadas, incluindo Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA e políticas de acesso local. Como resultado, as organizações podem fornecer acesso seguro à VPN para qualquer recurso de rede de qualquer local.

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.