ASA 9.X Dynamic Access Policies (DAP) implementeren

Inhoud

Inleiding

In dit document worden de implementatie, functies en het gebruik van ASA 9.x Dynamic Access Policy (DAP) beschreven.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Virtual Private Network (VPN)-gateways
- Dynamisch toegangsbeleid (DAP)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

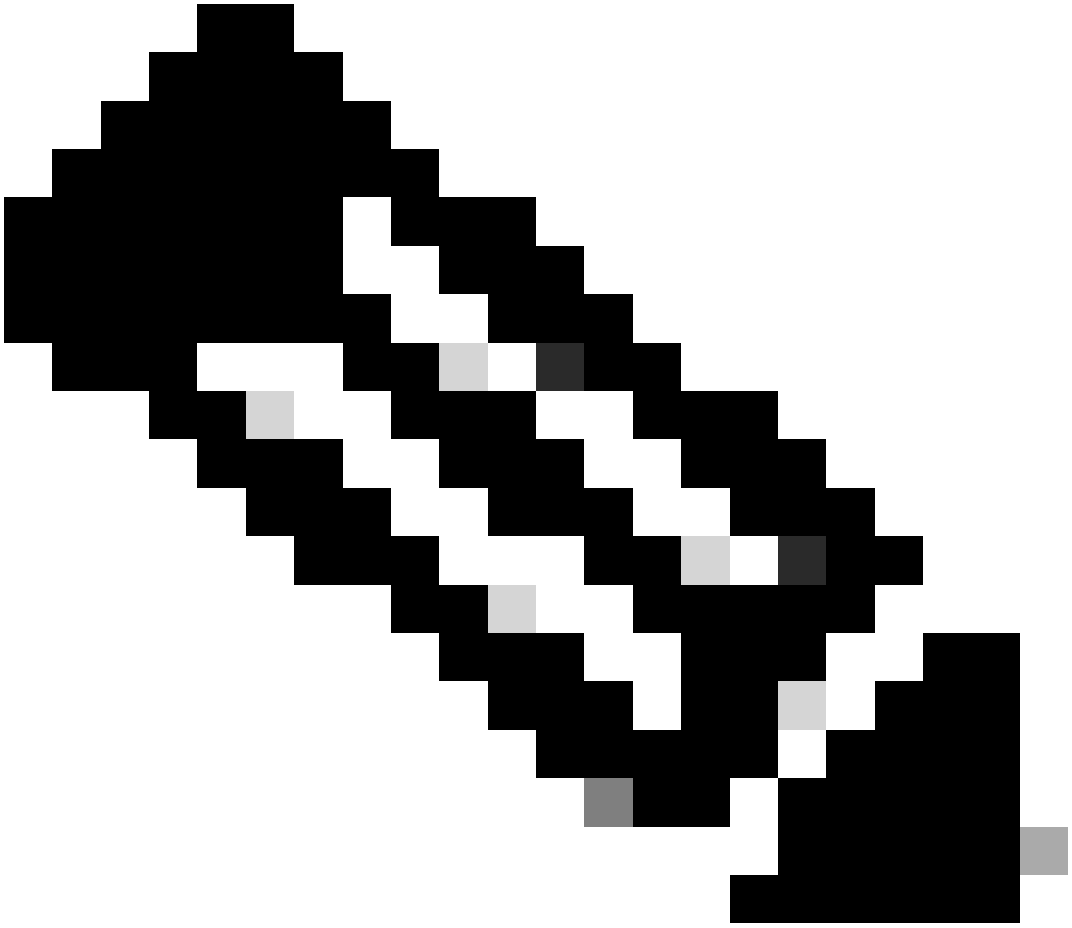
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

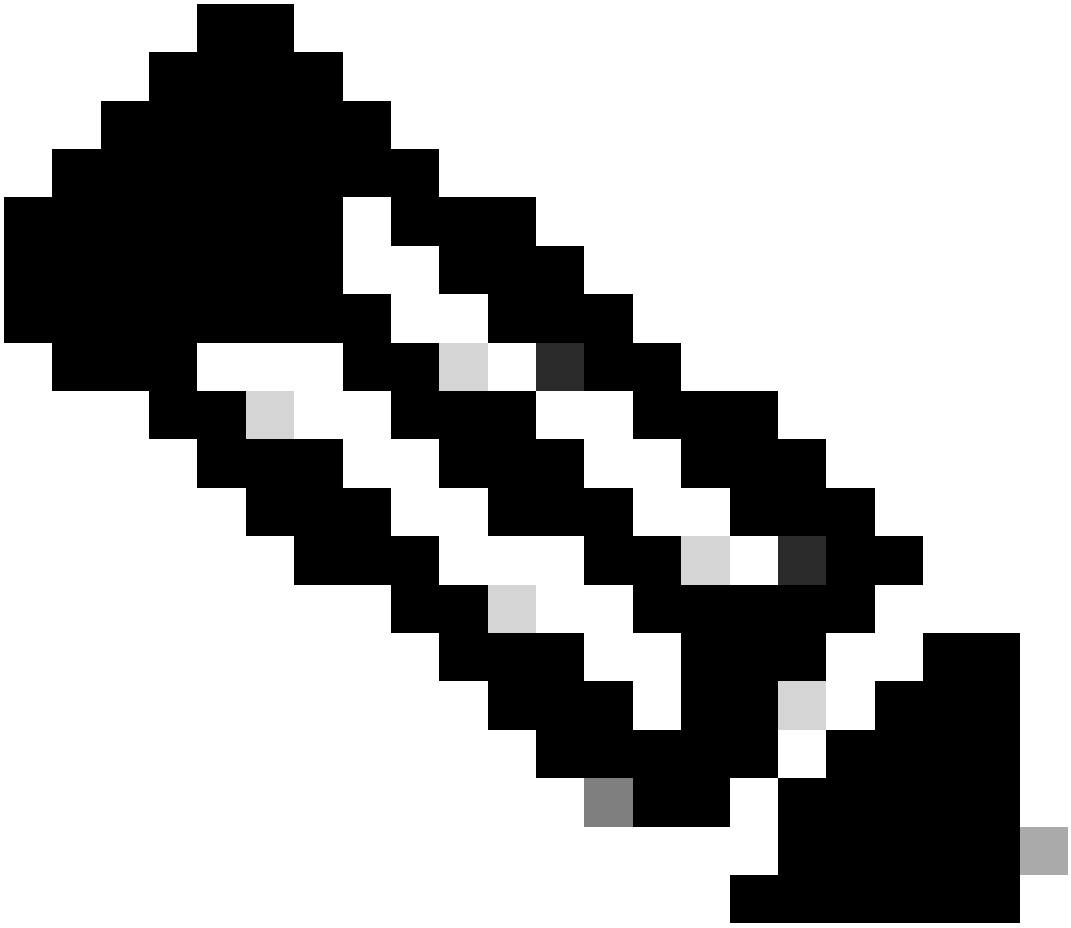
Virtual Private Network (VPN)-gateways werken in dynamische omgevingen. Meervoudige variabelen kunnen van invloed zijn op elke VPN-verbinding; bijvoorbeeld intranetconfiguraties die vaak veranderen, de verschillende rollen die elke gebruiker binnen een organisatie kan innemen, en inloggegevens van externe toegangssites met verschillende configuraties en beveiligingsniveaus. De taak van het autoriseren van gebruikers is veel gecompliceerder in een dynamische VPN-omgeving dan in een netwerk met een statische configuratie.

Dynamic Access Policy (DAP), is een functie die u in staat stelt om een autorisatie te configureren die zich richt op de dynamiek van VPN-omgevingen. U maakt een dynamisch toegangsbeleid door een verzameling toegangscontrolekenmerken in te stellen die u aan een specifieke gebruikerstunnel of -sessie koppelt. Deze eigenschappen behandelen kwesties van veelvoudig groepslidmaatschap en eindpuntveiligheid.

Het beveiligingstoestel verleent bijvoorbeeld toegang tot een bepaalde gebruiker voor een bepaalde sessie op basis van het beleid dat u definieert. Het genereert een DAP tijdens de gehele gebruikersverificatie door kenmerken uit een of meer DAP-records te selecteren en/of te aggregeren. Het selecteert deze DAP-records op basis van de endpointbeveiligingsinformatie van het externe apparaat en/of AAA-autorisatieinformatie voor de geverifieerde gebruiker. Het past dan de DAP record toe op de gebruikerstunnel of sessie.



Opmerking: het bestand dap.xml, dat de selectiekenmerken voor het DAP-beleid bevat, wordt opgeslagen in de ASA-flitser. Hoewel u het dap.xml-bestand kunt exporteren, het kunt bewerken (als u weet van de XML-syntaxis) en opnieuw importeren, moet u zeer voorzichtig zijn omdat u ASDM kunt veroorzaken dat de verwerking van DAP-records stopt als u iets verkeerd hebt geconfigureerd. Er is geen CLI om dit deel van de configuratie te manipuleren.



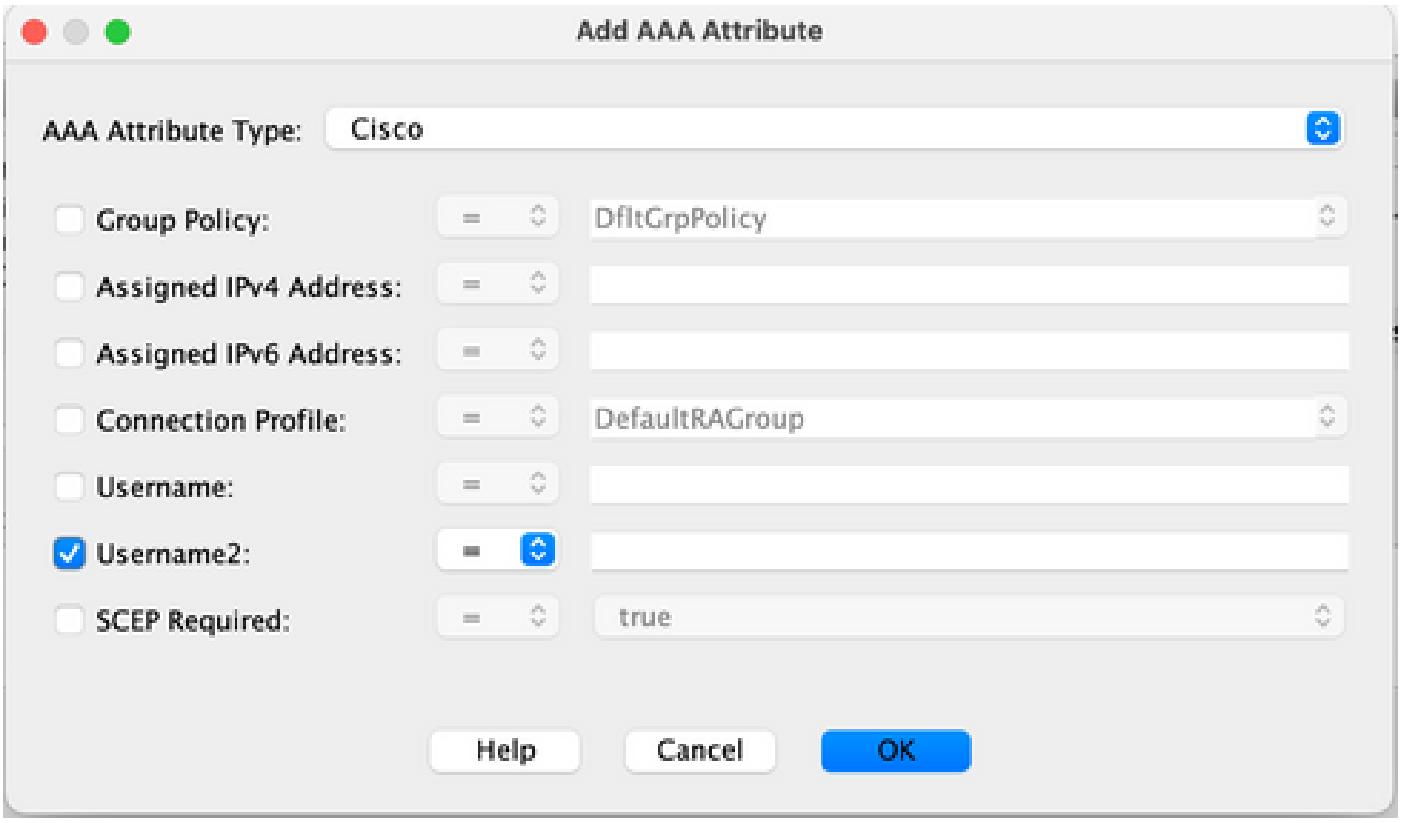
Opmerking: Het proberen om de toegangsparameters voor dynamische toegangsbeleid via de CLI te configureren kan ervoor zorgen dat DAP stopt met werken, hoewel ASDM juist hetzelfde zou beheren. Vermijd de CLI en gebruik altijd ASDM om DAP-beleid te beheren.

DAP- en AAA-kenmerken

DAP vult AAA-services aan en biedt een beperkte set autorisatiekenmerken die de kenmerken die AAA biedt, kunnen negeren. Het beveiligingstoestel kan DAP-records selecteren op basis van de AAA-autorisatiegegevens voor de gebruiker. Het beveiligingstoestel kan meerdere DAP-records selecteren afhankelijk van deze informatie, die vervolgens worden samengevoegd om DAP-autorisatiekenmerken toe te wijzen.

U kunt AAA-kenmerken specificeren in de hiërarchie van Cisco AAA-kenmerken of in de volledige set responskenmerken die het security apparaat ontvangt van een RADIUS- of LDAP-server zoals in afbeelding 1.

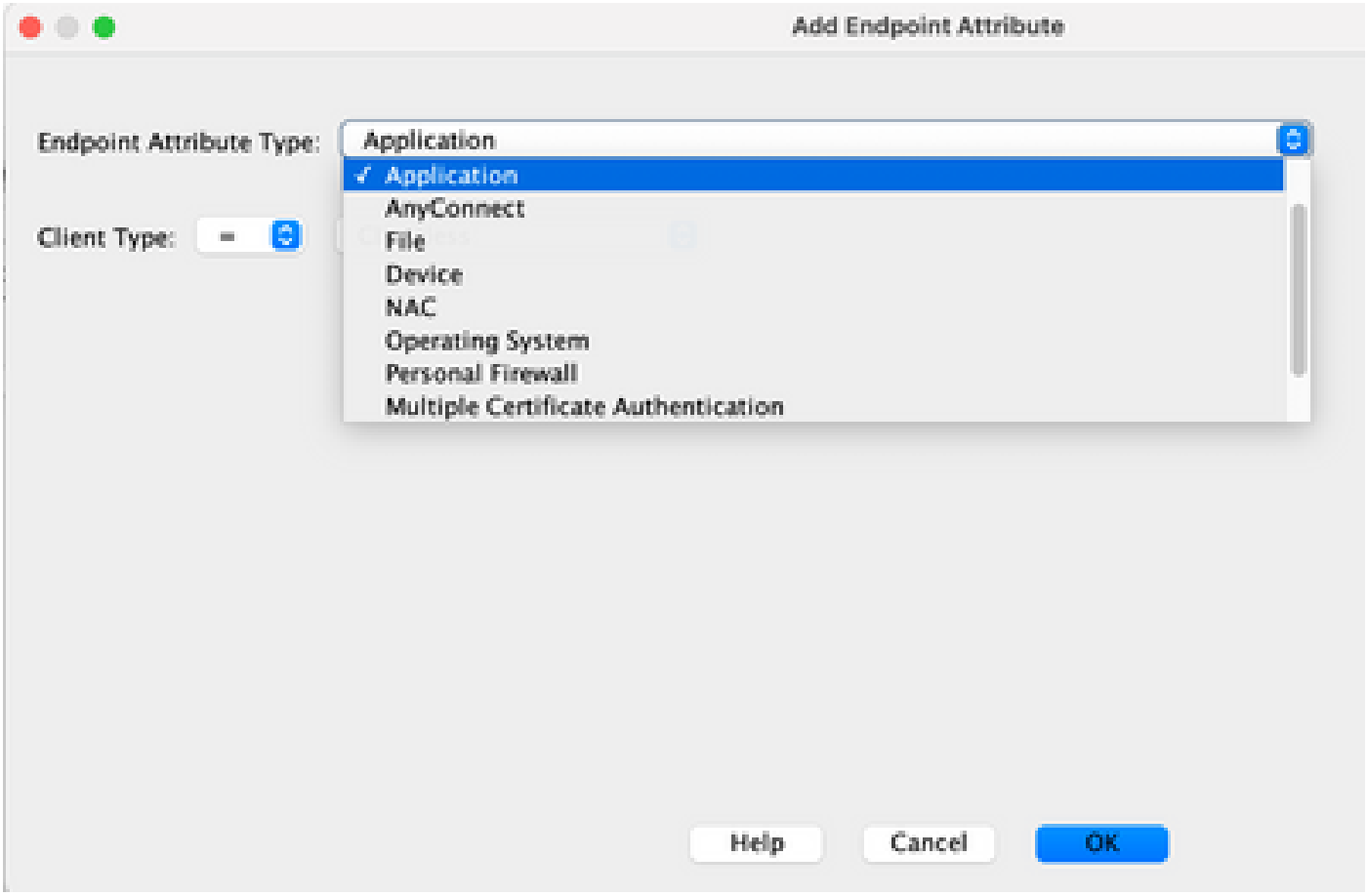
Afbeelding 1. DAP AAA-kenmerk GUI



Kenmerken DAP- en endpointbeveiliging

Naast de AAA-kenmerken kan het security apparaat ook endpointbeveiligingskenmerken verkrijgen door de postuur-evaluatiemethoden te gebruiken die u configureert. Deze omvatten Basic Host Scan, Secure Desktop, Standard/Advanced Endpoint Assessment, en NAC zoals in afbeelding 2. Endpoint Assessment Attributes worden verkregen en naar het security applicatie verzonden voordat de gebruikersverificatie plaatsvindt. AAA-kenmerken, inclusief de algemene DAP-record, worden echter gevalideerd tijdens gebruikersverificatie.

Afbeelding 2. GUI van endpointkenmerken

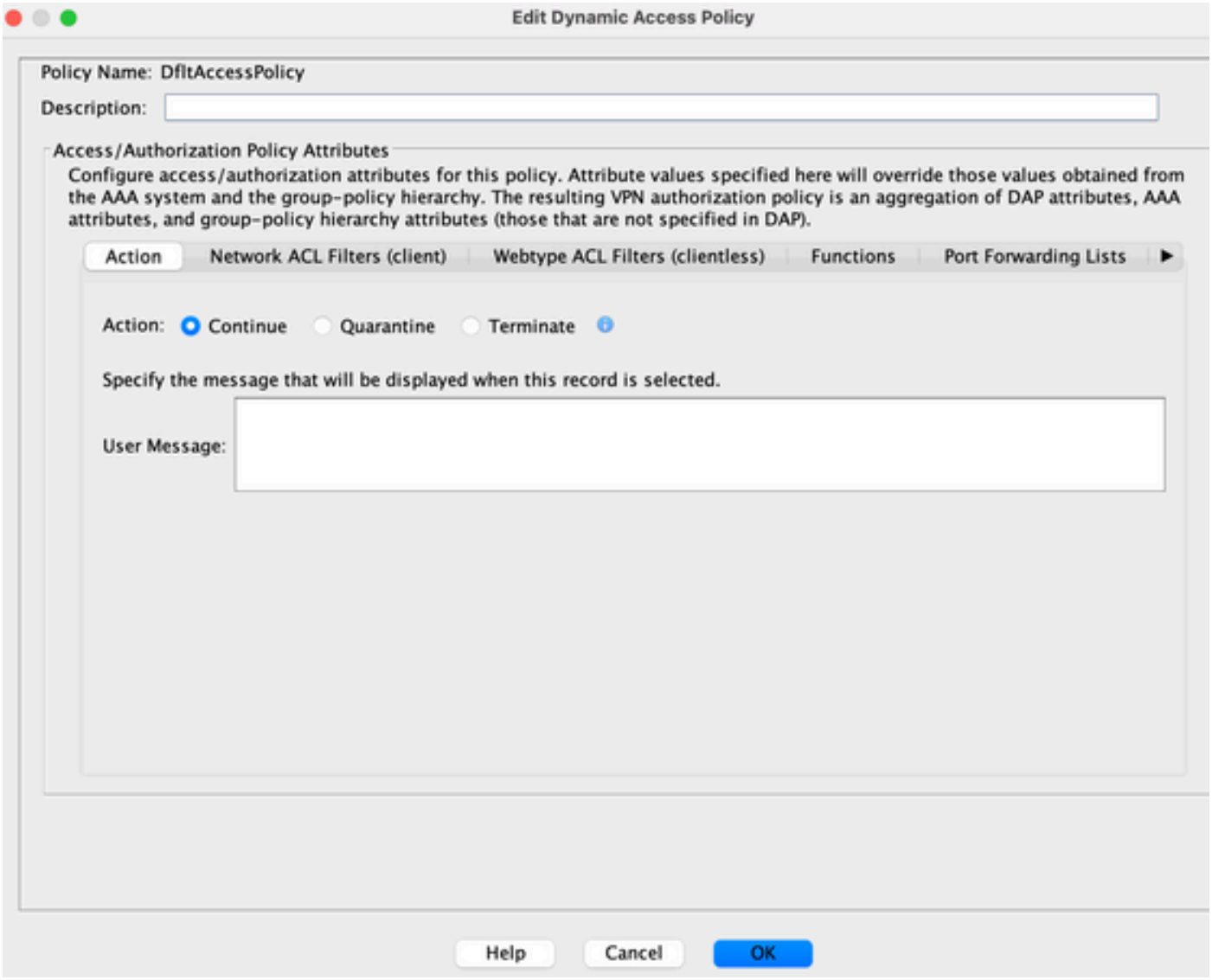


Standaard dynamisch toegangsbeleid

Vóór de introductie en implementatie van DAP, werden attributen/waardeparen van het toegangsbeleid die met een specifieke gebruikerstunnel of een zitting werden geassocieerd of plaatselijk op ASA, (d.w.z., de Groepen en het Beleid van de Tunnel) bepaald of via externe AAA servers in kaart gebracht.

DAP wordt altijd standaard afgedwongen. Zo kan het afdwingen van toegangscontrole via Tunnelgroepen, Groepsbeleid en AAA zonder de expliciete afdwinging van DAP nog steeds dit gedrag opleveren. Voor ouder gedrag zijn geen configuratiewijzigingen in de DAP-functie, inclusief de standaard DAP-record DfltAccess Policy, vereist zoals in afbeelding 3.

Afbeelding 3. Standaard dynamisch toegangsbeleid



Desalniettemin, als een van de standaardwaarden in een DAP-record wordt gewijzigd, bijvoorbeeld de Action: parameter in het DfltAccessPolicy wordt gewijzigd van de standaardwaarde naar Terminate en er worden geen extra DAP-records geconfigureerd, kunnen geverifieerde gebruikers standaard overeenkomen met de DfltAccessPolicy DAP-record en kan VPN-toegang worden geweigerd.

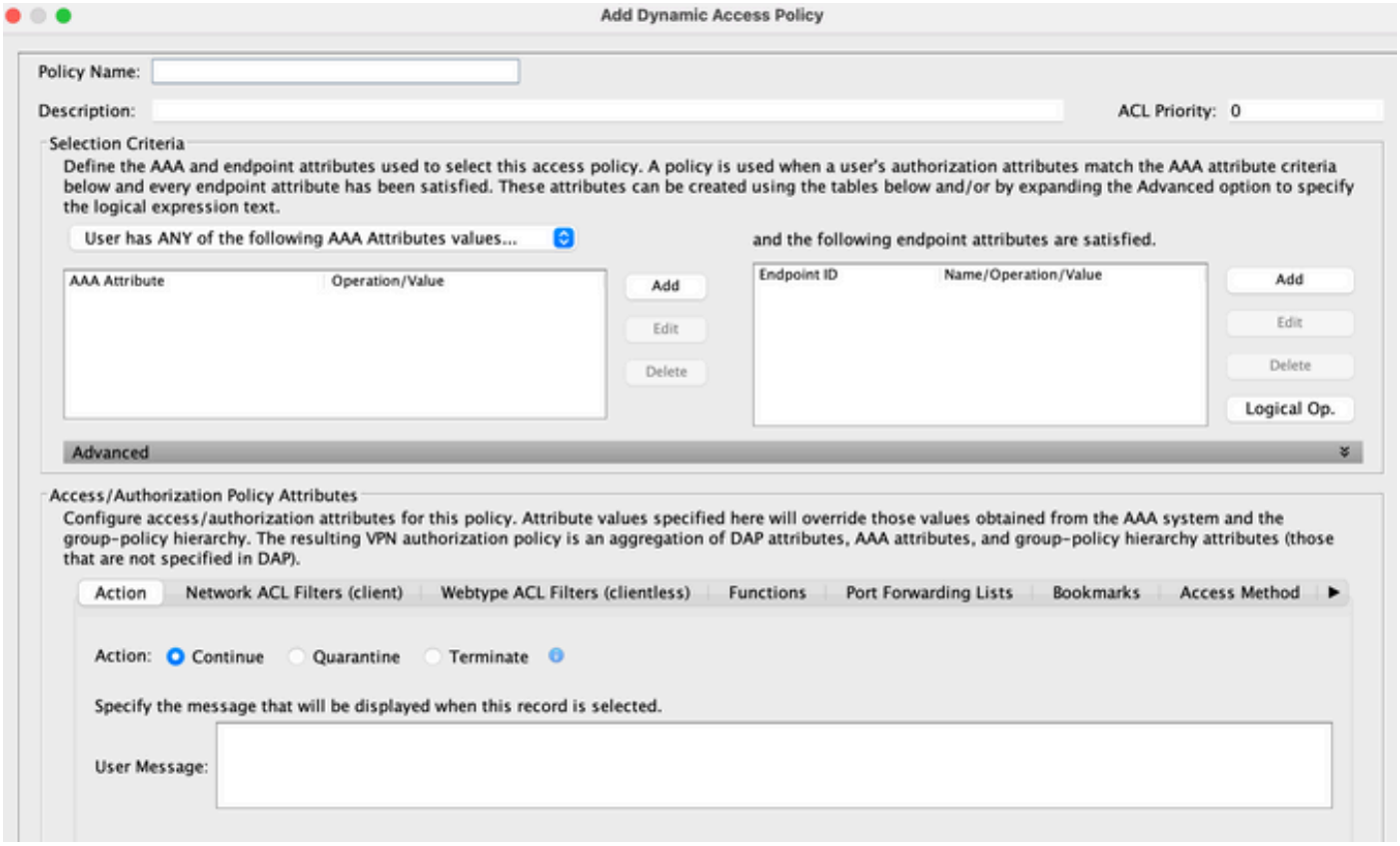
Daarom moeten een of meer DAP-records worden gemaakt en geconfigureerd om VPN-connectiviteit te autoriseren en te definiëren welke netwerkbronnen een geverifieerde gebruiker mag gebruiken. Zo kan DAP, indien geconfigureerd, voorrang krijgen op legacy policy enforcement.

Dynamisch toegangsbeleid configureren

Wanneer u DAP gebruikt om te definiëren welke netwerkbronnen een gebruiker toegang heeft tot, zijn er veel parameters om te overwegen. Als u bijvoorbeeld identificeert of het verbindende eindpunt afkomstig is van een beheerde, onbeheerde of onbetrouwbare omgeving, dan bepaalt u de selectiecriteria die nodig zijn om het verbindende eindpunt te identificeren, en gebaseerd op endpointbeoordeling en/of AAA-referenties, waartoe de netwerkbronnen die verbinding maken, geautoriseerd zijn om toegang te krijgen. Om dit te bereiken, moet u eerst vertrouwd worden met

DAP-functies en -functies zoals in afbeelding 4.

Afbeelding 4. Dynamisch toegangsbeleid



Bij het configureren van een DAP-record zijn er twee belangrijke onderdelen die in overweging moeten worden genomen:

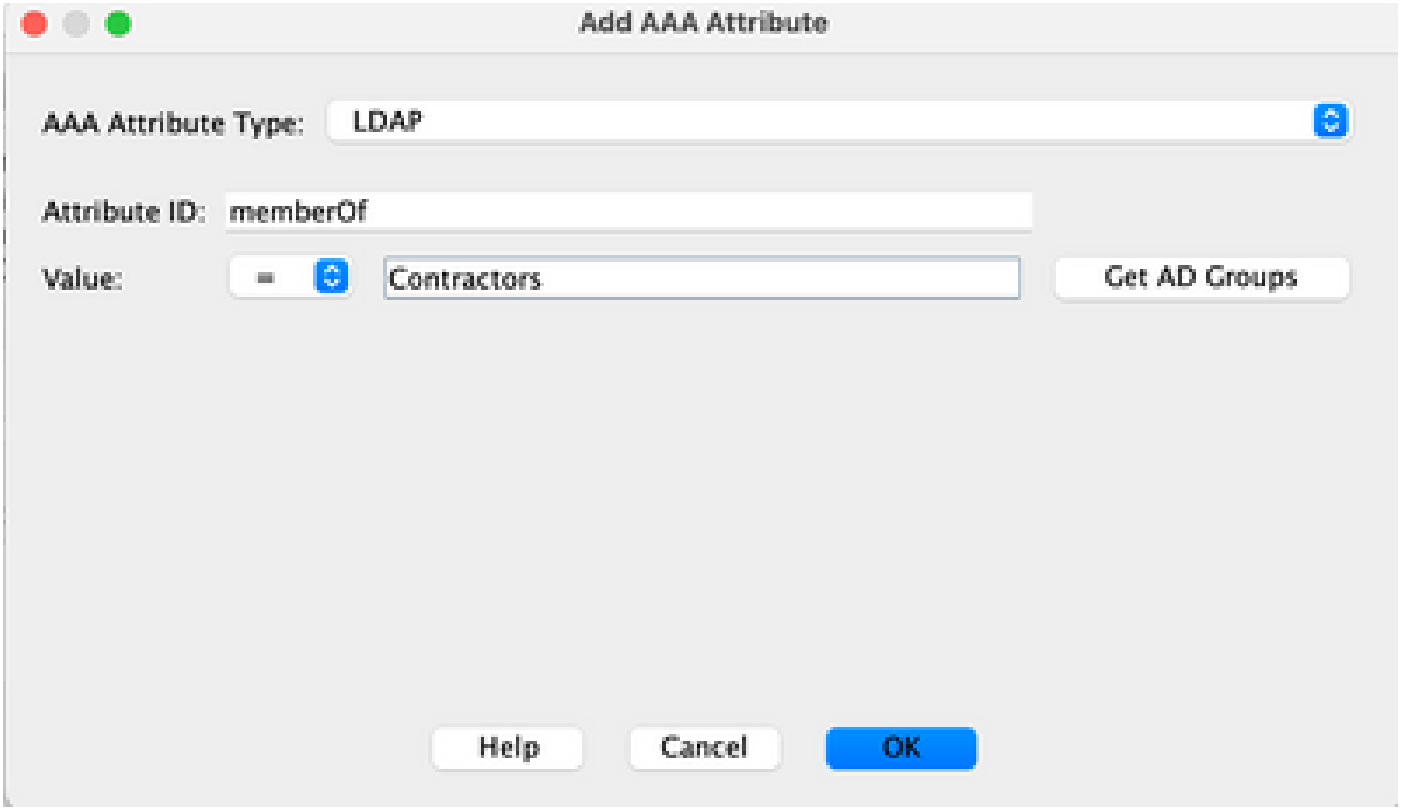
- Selectiecriteria, inclusief geavanceerde opties
- Kenmerken toegangsbeleid

In het gedeelte Selectiecriteria kan een beheerder AAA- en endpointkenmerken configureren die worden gebruikt om een specifieke DAP-record te selecteren. Er wordt een DAP-record gebruikt wanneer de autorisatiekenmerken van een gebruiker overeenkomen met de AAA-kenmerkcriteria en elk endpointkenmerk is vervuld.

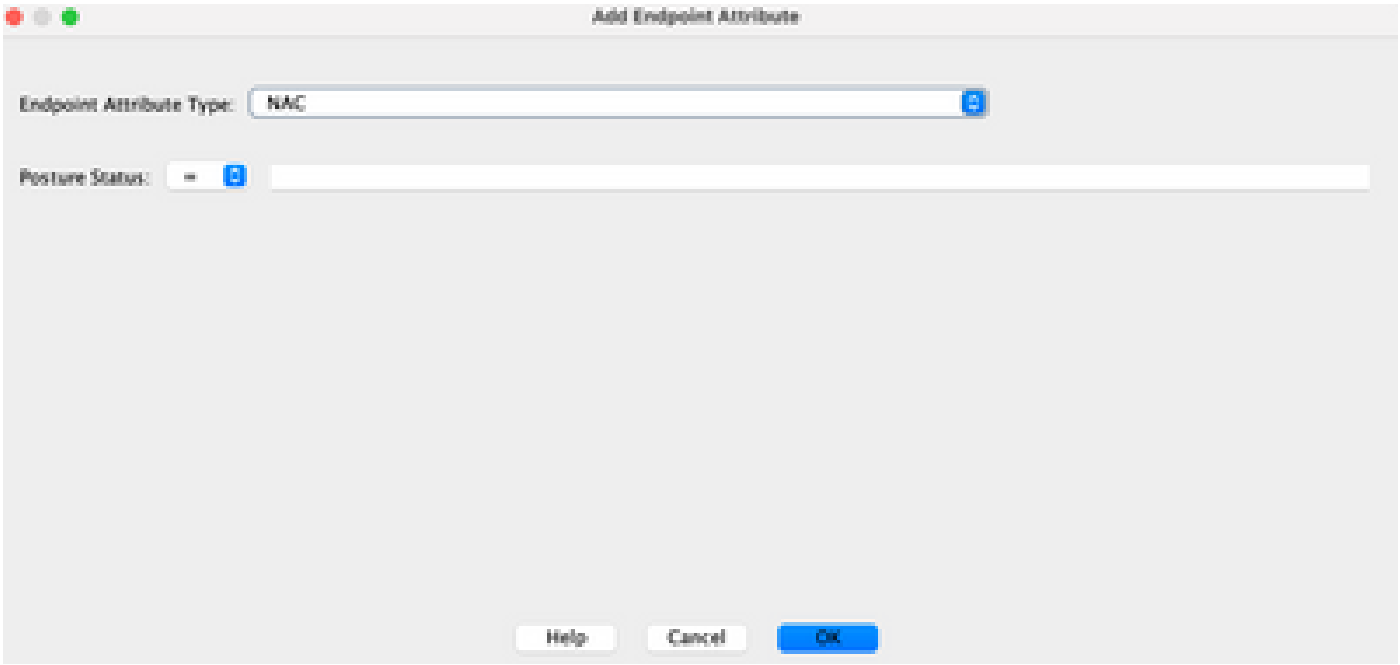
Als bijvoorbeeld AAA Attribute Type LDAP (Active Directory) is geselecteerd, is de Attribute Name string memberOf en is de Value string Contractors, zoals in afbeelding 5a, moet de verificerende gebruiker lid zijn van de Active Directory group Contractors om aan de AAA attributen criteria te voldoen.

Naast het voldoen aan de AAA attribuut criteria, kan de authenticerende gebruiker ook worden vereist om te voldoen aan de endpoint attribuut criteria. Als de beheerder bijvoorbeeld is ingesteld om de houding van het verbindende eindpunt te bepalen en op basis van die standpuntbeoordeling, kan de beheerder deze beoordelingsinformatie gebruiken als selectiecriteria voor de in afbeelding 5b weergegeven endpointkenmerken.

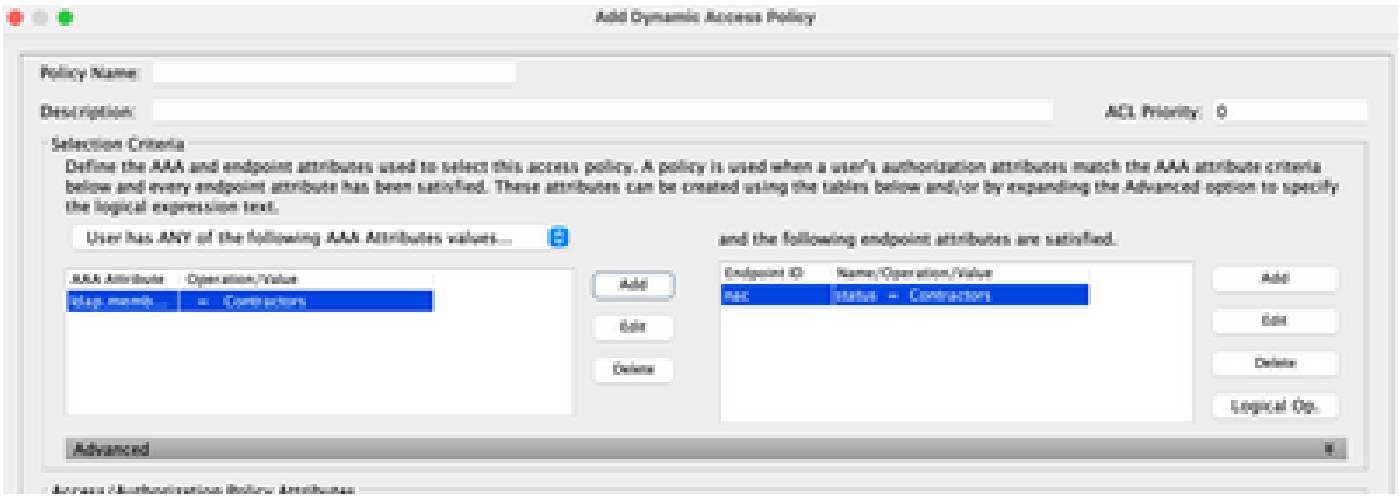
Afbeelding 5a. Criteria voor AAA-kenmerken



Afbeelding 5b. Criteria voor endpointkenmerken



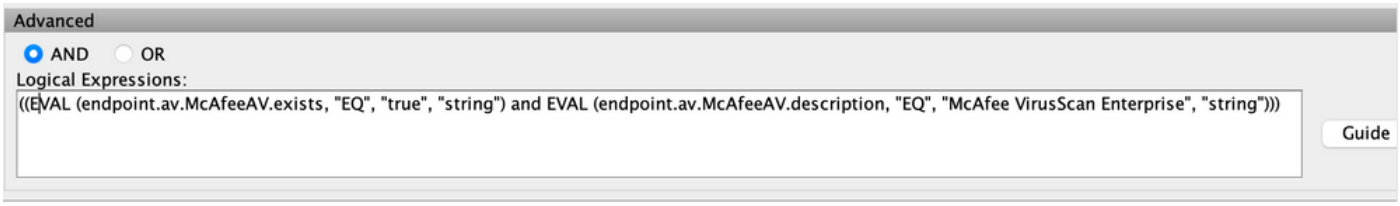
Afbeelding 6. Criteria voor AAA- en endpointkenmerken overeenkomen



De eigenschappen AAA en Endpoint kunnen worden gecreëerd met behulp van de tabellen zoals beschreven in afbeelding 6 en/of door de optie Advanced uit te breiden om een logische expressie te specificeren zoals in afbeelding 7. Momenteel is de logische expressie geconstrueerd met EVAL-functies, bijvoorbeeld EVAL (endpoint.av.McAfeeAV.existent, "EQ", "true", "string") en EVAL (endpoint.av.McAfeeAV.Description, "EQ", "McAfee VirusScan Enterprise", "string"), die de logische bewerkingen van de AAA en/of endpointselectie vertegenwoordigen.

Logische expressies zijn handig als u andere selectiecriteria wilt toevoegen dan wat mogelijk is in de gebieden met AAA- en endpointkenmerken zoals eerder getoond. Terwijl u bijvoorbeeld de beveiligingsapparaten kunt configureren om AAA-kenmerken te gebruiken die voldoen aan alle, alle of geen van de opgegeven criteria, zijn endpointkenmerken cumulatief en moeten ze allemaal worden vervuld. Om het security apparaat te laten gebruik maken van een of ander endpointkenmerk, moet u de juiste logische expressies aanmaken onder de sectie Geavanceerd van de DAP-record.

Afbeelding 7. GUI voor logische expressie voor geavanceerde attributen

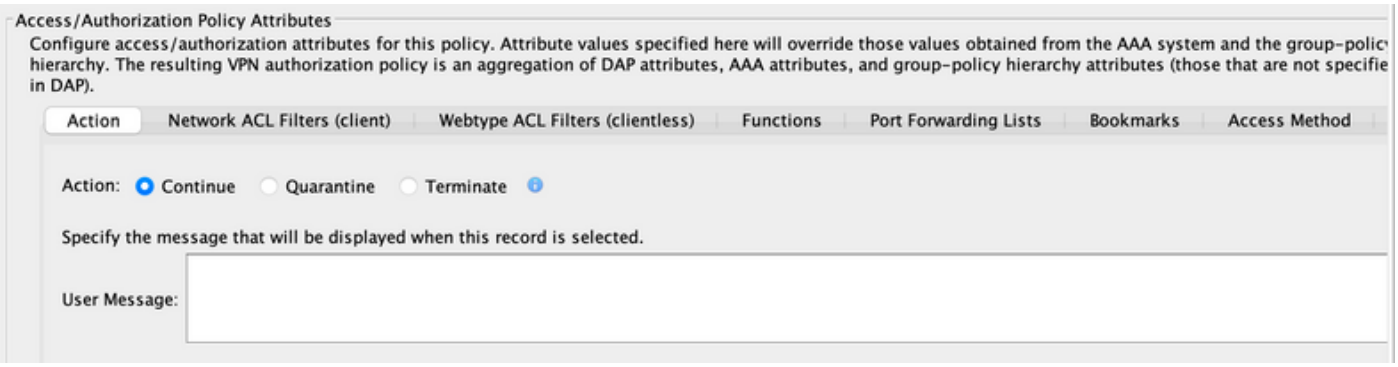


De sectie Access Policy Attributes zoals in afbeelding 8 wordt getoond, is waar een beheerder VPN-toegangskenmerken voor een specifieke DAP-record zou configureren. Wanneer de kenmerken van een gebruikersautorisatie overeenkomen met de criteria AAA, Endpoint en/of Logical Expression; kunnen de in deze sectie ingestelde waarden voor de kenmerken van het toegangsbeleid worden afgedwongen. De hier gespecificeerde attributenwaarden kunnen die waarden met voeten treden die uit het systeem AAA worden verkregen, met inbegrip van die in bestaande gebruiker, groep, tunnelgroep, en standaardgroepsverslagen.

Een DAP-record heeft een beperkte set attribuutwaarden die kunnen worden geconfigureerd. Deze waarden vallen onder de tabbladen zoals weergegeven in de figuren 8 tot en met 14:

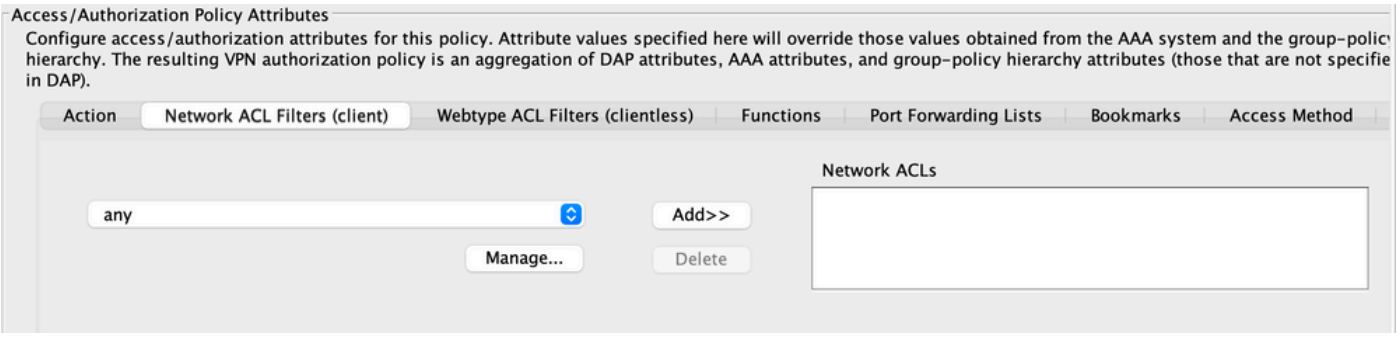
Afbeelding 8. Actie — Specificeert speciale verwerking die moet worden toegepast op een

specifieke verbinding of sessie.



- Doorgaan—(standaard) Klik om de eigenschappen van het toegangsbeleid op de sessie toe te passen.
- Beëindigen-Klik op om de sessie te beëindigen.
- Gebruikersbericht — Voer een tekstbericht in dat op de portaalpagina moet worden weergegeven wanneer deze DAP-record is geselecteerd. Maximaal 128 tekens. Een gebruikersbericht wordt weergegeven in de vorm van een gele bol. Als een gebruiker zich aanmeldt, knippert hij drie keer om aandacht te trekken, en dat is hij nog steeds. Als verschillende DAP-records zijn geselecteerd en elk ervan een gebruikersbericht heeft, worden alle gebruikersberichten weergegeven. Daarnaast kunt u in dergelijke berichten URL's of andere ingesloten tekst opnemen, waarvoor u de juiste HTML-tags moet gebruiken.

Afbeelding 9. Tabblad ACL-filters voor netwerk — Hiermee kunt u netwerk-ACL's selecteren en configureren die op deze DAP-record van toepassing zijn. Een ACL voor DAP kan vergunning bevatten of regels ontkennen, maar niet allebei. Als een ACL zowel regel voor vergunningen als regels voor weigering bevat, wijst het security apparaat de ACL-configuratie af.

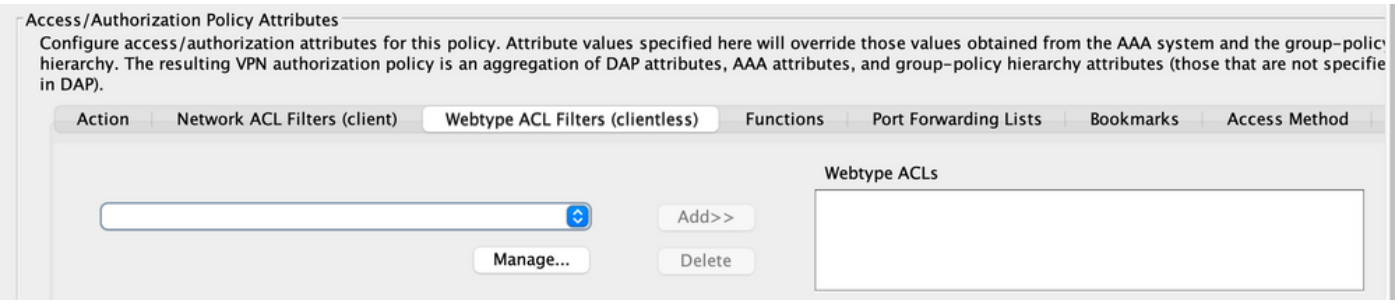


- Vervolgkeuzelijst voor netwerktoegangsrechten die al zijn geconfigureerd voor netwerk-ACL's om aan deze DAP-record toe te voegen. Alleen ACL's die alle vergunningen hebben of regels ontkennen komen in aanmerking, en dit zijn de enige ACL's die hier worden weergegeven.
- Beheer—Klik op om netwerk-ACL's toe te voegen, te bewerken en te verwijderen.
- ACL-netwerken van netwerk maakt een lijst van de netwerk-ACL's voor deze DAP-record.
- Toevoegen—Klik om de geselecteerde netwerk ACL toe te voegen uit het

vervolgkeuzevenster aan de netwerk ACL's lijst aan de rechterkant.

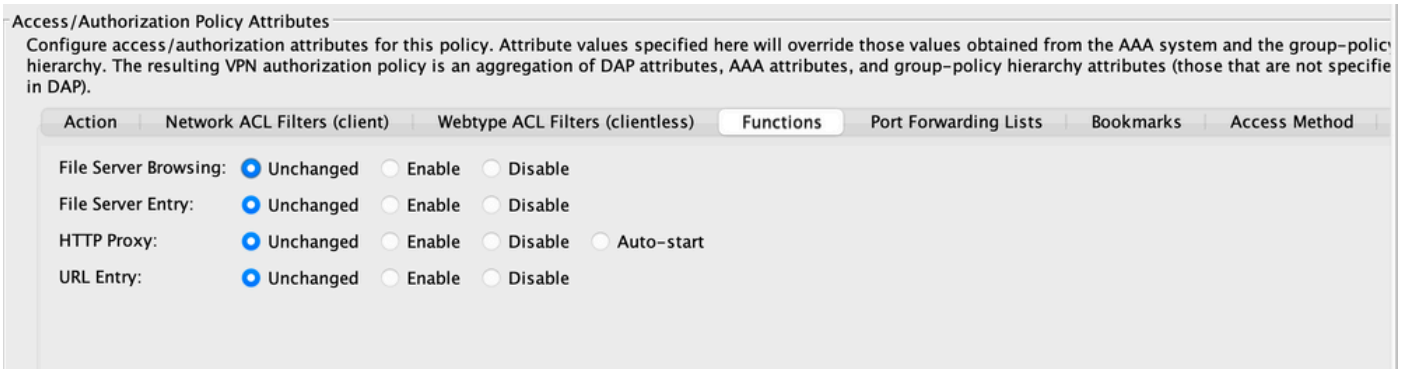
- Verwijderen-Klik om een gemarkeerd netwerk ACL te verwijderen uit de lijst van netwerk ACL's. U kunt geen ACL verwijderen als deze is toegewezen aan een DAP- of ander record.

Afbeelding 10. Web-type ACL Filters Tab — Hiermee kunt u webtype ACL's selecteren en configureren om toe te passen op deze DAP-record. Een ACL voor DAP kan alleen toestemming bevatten of regels weigeren. Als een ACL zowel regel voor vergunningen als regels voor weigering bevat, wijst het security apparaat de ACL-configuratie af.



- Vervolgkeuzelijst Web-Type ACL — Selecteer reeds geconfigureerde webtype ACL's om aan deze DAP-record toe te voegen. Alleen ACL's met alle vergunningen of alle ontkennen regels zijn in aanmerking komend, en dit zijn de enige ACL's die hier worden weergegeven.
- Beheer... — Klik om webtype ACL's toe te voegen, te bewerken en te verwijderen.
- Web-type ACL-lijst —Hier worden de webtype ACL's voor deze DAP-record weergegeven.
- Toevoegen —Klik om de geselecteerde webtype ACL toe te voegen uit het vervolgkeuzevenster aan de lijst van webtype ACL's rechts.
- Verwijderen —Klik om een webtype ACL te verwijderen uit de lijst van webtype ACL's. U kunt geen ACL verwijderen als deze is toegewezen aan een DAP- of ander record.

Afbeelding 11. Tabblad Functies — Hiermee kunt u de invoer en het bladeren van bestandsservers, HTTP-proxy en URL-vermeldingen configureren voor de DAP-record.



- Bestandsserver bladeren—maakt het bladeren door CIFS naar bestandsservers of gedeelde functies mogelijk of onmogelijk.
- File Server Entry-staat toe of ontkent een gebruiker van het invoeren van de paden en

namen van de bestandsserver op de portal pagina. Als deze optie is ingeschakeld, plaatst u de invoerlade voor de bestandsserver op de portal-pagina. De gebruikers kunnen pathnames aan de dossiers van Windows direct ingaan. Ze kunnen bestanden downloaden, bewerken, verwijderen, hernoemen en verplaatsen. Ze kunnen ook bestanden en mappen toevoegen. Delen moeten ook worden geconfigureerd voor gebruikerstoegang op de toepasselijke Microsoft Windows-servers. Afhankelijk van netwerkvereisten kan van gebruikers worden verlangd dat ze hun verificatie uitvoeren voordat ze toegang krijgen tot bestanden.

- HTTP proxy-beïnvloedt het doorsturen van een HTTP-applet proxy naar de client. De proxy is handig voor technologieën die interfereren met de juiste contenttransformatie, zoals Java, ActiveX en Flash. Hiermee wordt het proces van mangelen/herschrijven omzeild en wordt ervoor gezorgd dat het beveiligingsapparaat blijvend wordt gebruikt. De doorgestuurde proxy wijzigt automatisch de oude proxyconfiguratie van de browser en leidt alle HTTP- en HTTPS-verzoeken om naar de nieuwe proxyconfiguratie. Het ondersteunt vrijwel alle client-side technologieën, waaronder HTML, CSS, JavaScript, VBScript, ActiveX en Java. De enige browser die het ondersteunt is Microsoft Internet Explorer.

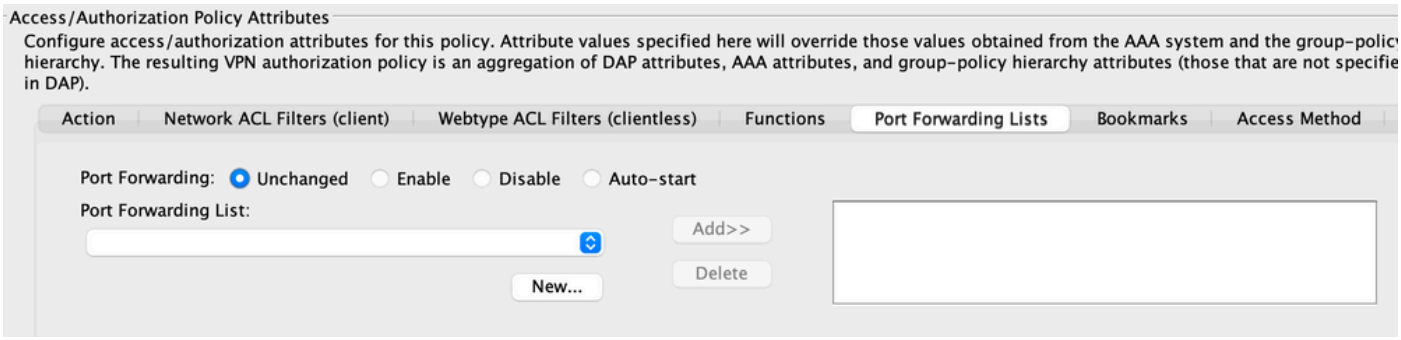
- URL-vermeldingen: hiermee kan een gebruiker HTTP/HTTPS-URL's op de portal-pagina invoeren of voorkomen. Als deze functie is ingeschakeld, kunnen gebruikers webadressen invoeren in het veld voor URL-vermeldingen en clientloze SSL VPN gebruiken om toegang te krijgen tot die websites.

- Ongewijzigd—(standaard) Klik om waarden te gebruiken uit het groepsbeleid dat van toepassing is op deze sessie.

- In-/uitschakelen—Klik om de optie in of uit te schakelen.

- Auto-start-Klik om HTTP proxy in te schakelen en om de DAP-record automatisch te laten starten de applets die aan deze functies zijn gekoppeld.

Afbeelding 12. Tabblad Port Forwarding Lists - Hiermee kunt u lijsten voor poortdoorsturen selecteren en configureren voor gebruikerssessies.



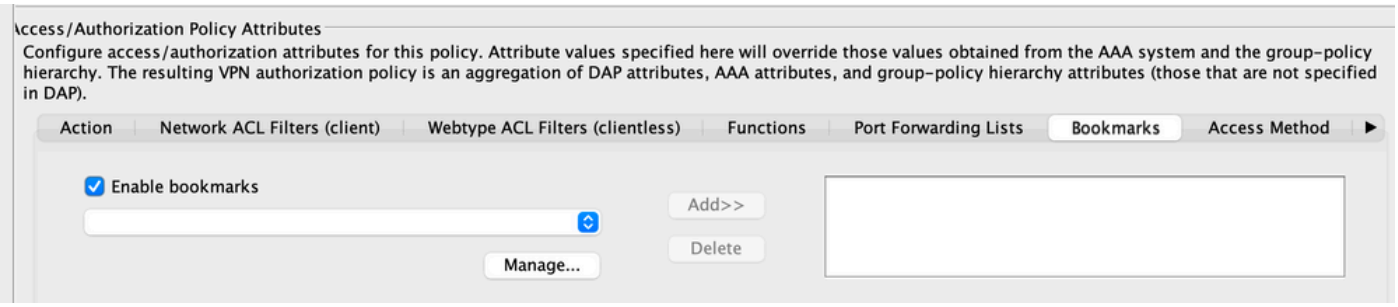
- Port Forwarding: selecteer een optie voor de lijsten voor het doorsturen van poorten die van toepassing zijn op deze DAP-record. De andere kenmerken in dit veld worden alleen ingeschakeld wanneer u Port Forwarding instelt op Inschakelen of Automatisch starten.

- Ongewijzigd - Klik om waarden te gebruiken uit het groepsbeleid dat van toepassing is op

deze sessie.

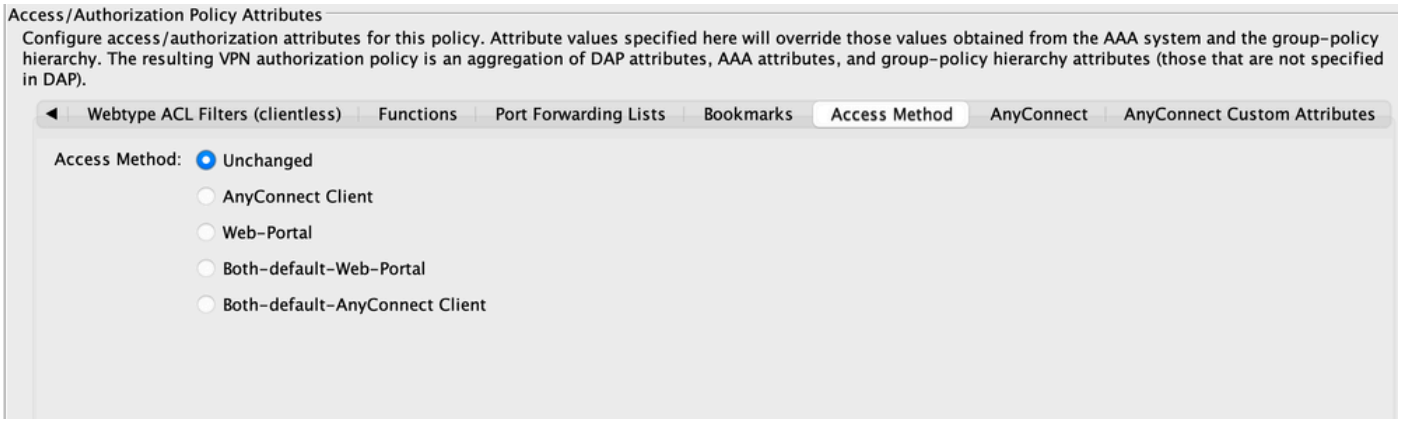
- In- en uitschakelen—Klik om het doorsturen van poorten in of uit te schakelen.
- Auto-start-Klik om het doorsturen van poorten in te schakelen en om de DAP-record automatisch te laten starten van de poortdoorsturen applets die gekoppeld zijn aan de poortdoorsturen lijsten.
- Vervolgkeuzelijst Port Forwarding List—Selecteer reeds geconfigureerde lijsten voor doorsturen van poorten om toe te voegen aan de DAP-record.
- Nieuw-Klik om nieuwe haven het door:sturen lijsten te vormen.
- Port Forwarding Lists—Hier wordt de lijst met poortdoorsturen voor de DAP-record weergegeven.
- Voeg toe-klik om de geselecteerde poort door:sturen lijst toe te voegen van het vervolgkeuzevenster aan de Port Forwarding lijst aan de rechterkant.
- Verwijderen-Klik om de geselecteerde poort te verwijderen door:sturen lijst uit de Port Forwarding lijst. U kunt geen ACL verwijderen als deze is toegewezen aan een DAP- of ander record.

Afbeelding 13. Bladwijzers tabblad — hiermee kunt u bladwijzers/URL-lijsten voor gebruikerssessies selecteren en configureren.



- Bladwijzers inschakelen—Klik om deze in te schakelen. Als dit vakje niet is geselecteerd, wordt er geen bladwijzer weergegeven op de portaalpagina voor de verbinding
- Beheer—Klik om Bladwijzerlijsten toe te voegen, te importeren, te exporteren en te verwijderen.
- Bladwijzerlijsten (Drop-down) —Hier worden de bladwijzerlijsten voor de DAP-record weergegeven.
- Toevoegen—Klik om de geselecteerde bladwijzerlijst toe te voegen vanuit de vervolgkeuzelijst naar het vak met bladwijzerlijst rechts.
- Verwijderen-Klik om de geselecteerde bladwijzerlijst uit het vak bladwijzerlijst te verwijderen. U kunt geen bladwijzerlijst uit het security apparaat verwijderen tenzij u het eerst verwijdert uit DAP-records.

Afbeelding 14. Tabblad Methode — hiermee kunt u het toegestane type externe toegang configureren.



- Ongewijzigd-Ga verder met de huidige methode voor externe toegang die is ingesteld in het groepsbeleid voor de sessie.
- AnyConnect client-Connect met de Cisco AnyConnect VPN-client.
- Web portal-Connect met een clientloze VPN.
- Beide-standaard-Web-Portal-Connect via clientloze of de AnyConnect-client, met een standaard van clientloze.
- Standaard-AnyConnect-client—Verbinding maken via clientloze client of AnyConnect-client, met standaard AnyConnect.

Zoals eerder vermeld, heeft een DAP-record een beperkte set standaardattribuutwaarden, alleen als ze worden aangepast krijgen ze voorrang op huidige AAA, gebruiker, groep, tunnelgroep en standaard groepsrecords. Als extra attribuutwaarden buiten het bereik van DAP vereist zijn, bijvoorbeeld Split Tunneling Lists, Banners, Smart Tunnels, Portal Personalisations, enzovoort, dan moeten ze worden afgedwongen via AAA, gebruiker, groep, tunnelgroep en standaard groepsrecords. In dit geval kunnen deze specifieke attribuutwaarden een aanvulling vormen op DAP en kunnen zij niet worden overschreven. Aldus, krijgt de gebruiker een cumulatieve reeks attributenwaarden over alle verslagen.

Meervoudig dynamisch toegangsbeleid aggregeren

Een beheerder kan meerdere DAP records configureren om vele variabelen aan te pakken. Hierdoor kan een verificerende gebruiker voldoen aan de AAA en Endpoint attribuutcriteria van meerdere DAP records. Dientengevolge, kunnen de Attributen van het Toegangsbeleid of verenigbaar of conflict door dit beleid zijn. In dit geval kan de geautoriseerde gebruiker het cumulatieve resultaat in alle overeenkomende DAP-records verkrijgen.

Dit omvat ook unieke attribuutwaarden die worden afgedwongen via verificatie, autorisatie, gebruiker, groep, tunnelgroep en standaard groepsrecords. Het cumulatieve resultaat van de Kenmerken van het Toegangsbeleid leidt tot het Dynamische Toegangsbeleid. In de volgende tabellen worden voorbeelden gegeven van gecombineerde kenmerken van toegangsbeleid. Deze

voorbeelden geven de resultaten weer van 3 gecombineerde DAP records.

Het actiekenmerk in tabel 1 heeft een waarde die is Afsluiten of Doorgaan. De geaggregeerde attribuutwaarde wordt beëindigd als de eindwaarde in om het even welke geselecteerde DAP verslagen wordt gevormd en verdergaat als de Doorgaan waarde in alle geselecteerde DAP verslagen wordt gevormd.

Tabel 1. Handelingskenmerk

Naam kenmerk	DAP#1	DAP#2	DAP#3	DAP
Actie (voorbeeld 1)	voortzetten	voortzetten	voortzetten	voortzetten
Actie (voorbeeld 2)	Beëindigen	voortzetten	voortzetten	eindigen

Het user-message attribuut in tabel 2 bevat een string waarde. De geaggregeerde attributenwaarde kan een lijn-feed (hex waarde 0x0A) gescheiden string zijn die gemaakt wordt door de attribuutwaarden van de geselecteerde DAP records aan elkaar te koppelen. De volgorde van de attribuutwaarden in de gecombineerde string is onbelangrijk.

Tabel 2. User-Message Attribute

Naam kenmerk	DAP#1	DAP#2	DAP#3	DAP
gebruikersbericht	vlug	vos	Opnieuw beginnen	de snelle<LF>bruine vos<LF>springt over

De clientloze eigenschap die eigenschappen (functies) in tabel 3 inschakelt, bevat waarden die automatisch starten, inschakelen of uitschakelen zijn. De geaggregeerde attribuutwaarde kan Auto-start zijn als de Auto-Start waarde in om het even welke geselecteerde DAP verslagen wordt gevormd.

De geaggregeerde attribuutwaarde kan worden ingeschakeld als er geen Auto-start waarde is ingesteld in een van de geselecteerde DAP-records en de Enable waarde is ingesteld in ten minste een van de geselecteerde DAP-records.

De geaggregeerde attribuutwaarde kan worden uitgeschakeld als er geen Auto-start is of waarde inschakelen die is ingesteld in een van de geselecteerde DAP-records, en de waarde "deactiveren" is ingesteld in ten minste een van de geselecteerde DAP-records.

Tabel 3. Clientloze kenmerken die kenmerken inschakelen (functies)

Naam kenmerk	DAP#1	DAP#2	DAP#3	DAP
voorwaarts	inschakelen	disable		inschakelen
bladeren door bestanden	disable	inschakelen	disable	inschakelen
bestandsindeling			disable	disable
HTTP-proxy	disable	automatisch starten	disable	automatisch starten
URL-vermelding	disable		inschakelen	inschakelen

De URL-lijst en poortvoorwaartse kenmerken in tabel 4 bevatten een waarde die een string of een

door komma's gescheiden string is. De geaggregeerde attributenwaarde kan een komma-gescheiden string zijn die gemaakt is door wanneer u de attribuutwaarden uit de geselecteerde DAP records koppelt. Elke dubbele attribuutwaarde in de gecombineerde string kan verwijderd worden. Hoe de attribuutwaarden in de gecombineerde string worden geordend is niet significant.

Tabel 4. Kenmerk URL-lijst en poortvoorwaartse lijst

Naam kenmerk	DAP#1	DAP#3	DAP#3	DAP
url-list	a	b,c	a	a,b,c
voorwaarts		d,e	e,f	d,e,f

De attributen Access Method specificeren de methode voor clienttoegang die is toegestaan voor SSL VPN-verbindingen. De methode voor clienttoegang kan bestaan uit AnyConnect-clienttoegang, alleen webportaaltoegang, AnyConnect-client of webportaaltoegang met standaardtoegang tot webportaal, of AnyConnect-clienttoegang of webportaaltoegang met AnyConnect-clienttoegang als standaardtoegang. De geaggregeerde waarde van eigenschappen wordt samengevat in tabel 5.

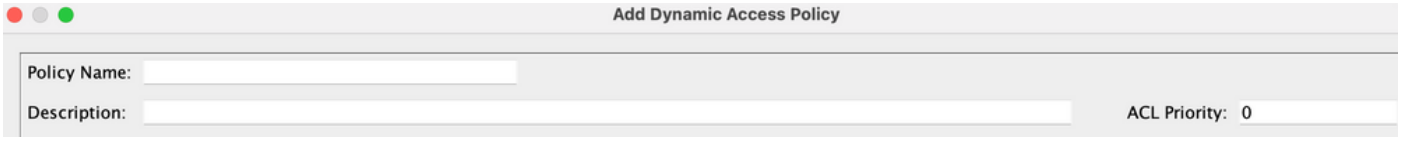
Tabel 5. Kenmerken toegangsmethode

Waarden kenmerken geselecteerd				Aggregatieresultaat
AnyConnect-client	Web-portal	Beide-standaard-web-portal	Standaard beide AnyConnect-client	
			X	Standaard beide AnyConnect-client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			webportal
	X		X	Standaard beide AnyConnect-client
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
X				AnyConnect-client
X			X	Standaard beide AnyConnect-client
X		X		Both-default-Web-Portal
X		X	X	Both-default-Web-Portal
X	X			Both-default-Web-Portal
X	X		X	Standaard beide AnyConnect-client
X	X	X		Both-default-Web-Portal
X	X	X	X	Both-default-Web-Portal

Wanneer u attributen voor netwerk (firewall) en webtype (clientloze) ACL-filter combineert, zijn de DAP-prioriteit en DAP-ACL twee belangrijke componenten die u in overweging moet nemen.

De prioriteitsklasse zoals weergegeven in figuur 15 wordt niet samengevoegd. Het beveiligingstoestel gebruikt deze waarde om logische sequenties van de toegangslijsten te bepalen bij het aggregeren van netwerk- en webtype-ACL's uit meerdere DAP-records. Het beveiligingsapparaat bestelt de records van het hoogste naar het laagste prioriteitsnummer, met het laagste aan de onderkant van de tabel. Een DAP-record met een waarde van 4 heeft bijvoorbeeld een hogere prioriteit dan een record met een waarde van 2. U kunt deze niet handmatig sorteren.

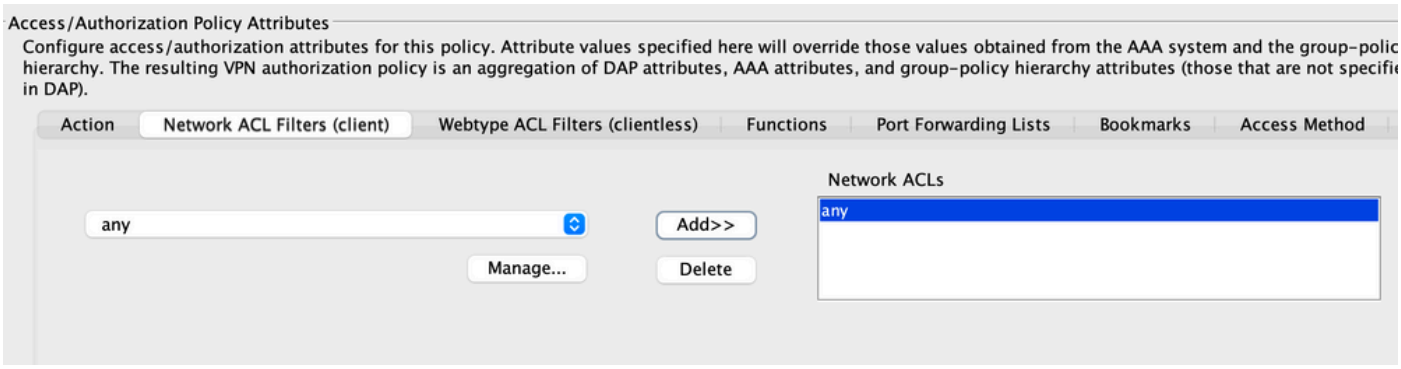
Afbeelding 15. Prioriteit — Hier wordt de prioriteit van de DAP-record weergegeven.



- Beleidsnaam—Hier wordt de naam van de DAP-record weergegeven.
- Beschrijving—Beschrijft het doel van de DAP-record.

Het DAP ACL-kenmerk ondersteunt alleen toegangslijsten die in overeenstemming zijn met een strikt ACL-model of een strikt ACL-model met een blokkeringslijst. In een ACL-model met toegangslijsten worden regels gespecificeerd die toegang tot opgegeven netwerken of hosts "toestaan". In een blok-lijst ACL-modus specificeren de toegangslijsten regels die toegang tot gespecificeerde netwerken of hosts weigeren. Een niet-conforme toegangslijst bevat toegangslijsten met een combinatie van vergunningen en regels weigeren. Als een niet-conforme toegangslijst is geconfigureerd voor een DAP-record, kan deze worden afgewezen als een configuratiefout wanneer de beheerder de record probeert toe te voegen. Als een toegangslijst die voldoet aan een DAP-record wordt toegewezen, kan elke wijziging in de toegangslijst die de conformiteitskenmerken wijzigt, worden afgewezen als een configuratiefout.

Afbeelding 16. DAP ACL - Hiermee kunt u netwerk-ACL's selecteren en configureren die op deze DAP-record van toepassing zijn.



Wanneer meerdere DAP-records zijn geselecteerd, worden de toegangslijsten die in de ACL voor het netwerk (firewall) zijn gespecificeerd, samengevoegd om een dynamische toegangslijst voor de DAP-firewall-ACL te maken. Op dezelfde manier worden de toegangslijsten-kenmerken die in

de ACL voor webtypen (clientloze) zijn gespecificeerd, samengevoegd om een dynamische toegangslijst voor de DAP-clientloze ACL te maken. Het volgende voorbeeld concentreert zich op hoe een dynamische DAP Firewall Access-List specifiek wordt gemaakt. Een dynamische DAP Clientless Access List kan echter hetzelfde proces doen.

Eerst maakt de ASA dynamisch een unieke naam voor de DAP Network-ACL zoals in tabel 6 is weergegeven.

Tabel 6. Dynamische DAP netwerk-ACL-naam

DAP netwerk-ACL naam
DAP-Network-ACL-X (waarin X een integer is dat kan worden verhoogd om uniciteit te garanderen)

Ten tweede haalt de ASA het Network-ACL-kenmerk uit de geselecteerde DAP-records zoals in tabel 7.

Tabel 7. Netwerk ACL's

Geselecteerde DAP-records	Prioriteit	Netwerk-ACL's	Netwerk-ACL-vermeldingen
DAP 1	1	101 en 102	ACL 101 heeft 4 regels voor ontkennen en ACL 102 heeft 4 regels voor toegangsrechten
DAP 2	2	201 en 202	ACL 201 heeft 3 vergunningsregels en ACL 202 heeft 3 ontkenningsregels
DAP 3	2	101 en 102	ACL 101 heeft 4 regels voor ontkennen en ACL 102 heeft 4 regels voor toegangsrechten

In de derde plaats herstelt de ASA Network-ACL eerst bij het DAP record Priority number en vervolgens bij Block-List eerst als de Priority value voor 2 of meer geselecteerde DAP records hetzelfde is. Daarna kan de ASA de netwerk-ACL-vermeldingen ophalen van elke netwerk-ACL zoals in tabel 8.

Tabel 8. DAP-recordprioriteit

Netwerk-ACL's	Prioriteit	Wit/zwart-toegangslijstmodel	Netwerk-ACL-vermeldingen
101	2	Zwarte lijst	4 Regels voor weigeren (DDD)
202	2	Zwarte lijst	3 Regels voor weigeren (DD)
102	2	Witlijst	4 Vergunningsregels (PPP)
202	2	Witlijst	3 Vergunningsregels (PPP)
101	1	Zwarte lijst	4 Regels voor weigeren (DDD)
102	1	Witlijst	4 Vergunningsregels (PPP)

Tot slot voegt de ASA de netwerk-ACL-vermeldingen samen in de dynamisch gegenereerde netwerk-ACL en retourneert vervolgens de naam van de dynamische netwerk-ACL als de nieuwe

netwerk-ACL die moet worden afgedwongen zoals in tabel 9 is weergegeven.

Tabel 9. Dynamische DAP-netwerk - ACL

DAP netwerk-ACL naam	Netwerk-ACL-vermeldingen
DAP-Network-ACL-1	DD DD DD DD PPP PPP DDD PPP

DAP-implementatie

Er zijn tal van redenen waarom een beheerder moet overwegen DAP uit te voeren. Sommige onderliggende redenen zijn wanneer een beoordeling van de houding op een eindpunt moet worden afgedwongen, en/of wanneer meer gedetailleerde AAA- of beleidskenmerken moeten worden overwogen bij het toestaan van gebruikerstoegang tot netwerkbronnen. In het volgende voorbeeld, kunt u DAP en zijn componenten vormen om een verbindend eindpunt te identificeren en gebruikerstoegang tot diverse netwerkmiddelen te machtigen.

Testcase - een client heeft een concepttest aangevraagd met deze VPN-toegangsvereisten:

- De mogelijkheid om een werknemer-endpoint te detecteren en te identificeren als beheerd of onbeheerd. —Als het eindpunt wordt geïdentificeerd als beheerd (werk-PC) maar niet aan de postuur-eisen voldoet, moet dat eindpunt dan de toegang worden geweigerd. Aan de andere kant, als het eindpunt van de werknemer wordt geïdentificeerd als onbeheerd (thuis PC), moet dat eindpunt dan clientloze toegang worden verleend.
- De mogelijkheid om het opschonen van sessiecookies en cache aan te roepen wanneer een clientloze verbinding wordt beëindigd.
- De mogelijkheid om actieve toepassingen te detecteren en af te dwingen op beheerde eindpunten van werknemers, zoals McAfee AntiVirus. Als de applicatie niet bestaat, moet dat eindpunt dan de toegang geweigerd worden.
- De mogelijkheid om AAA-verificatie te gebruiken om te bepalen tot welke netwerkbronnen geautoriseerde gebruikers toegang moeten hebben. De security applicatie moet Native MS LDAP-verificatie ondersteunen en meerdere LDAP-groepslidmaatschapsrollen ondersteunen.
- De mogelijkheid om lokale LAN-toegang te verlenen tot netwerkbronnen zoals netwerkfaxen en printers wanneer deze zijn aangesloten via een client/netwerkgebaseerde verbinding.
- De mogelijkheid om geautoriseerde gast toegang te verlenen aan aannemers. Contractanten en hun endpoints moeten clientloze toegang krijgen en hun portal-toegang tot toepassingen moet worden beperkt in vergelijking met de toegang van werknemers.

In dit voorbeeld, kunt u een reeks configuratiestappen uitvoeren om aan de de toegangsvereisten van VPN van de cliënt te voldoen. Er kunnen noodzakelijke configuratiestappen zijn, maar niet direct gerelateerd aan DAP, terwijl andere configuraties direct gerelateerd kunnen zijn aan DAP. ASA is zeer dynamisch en kan zich aan vele netwerkmilieu's aanpassen. Dientengevolge, kunnen

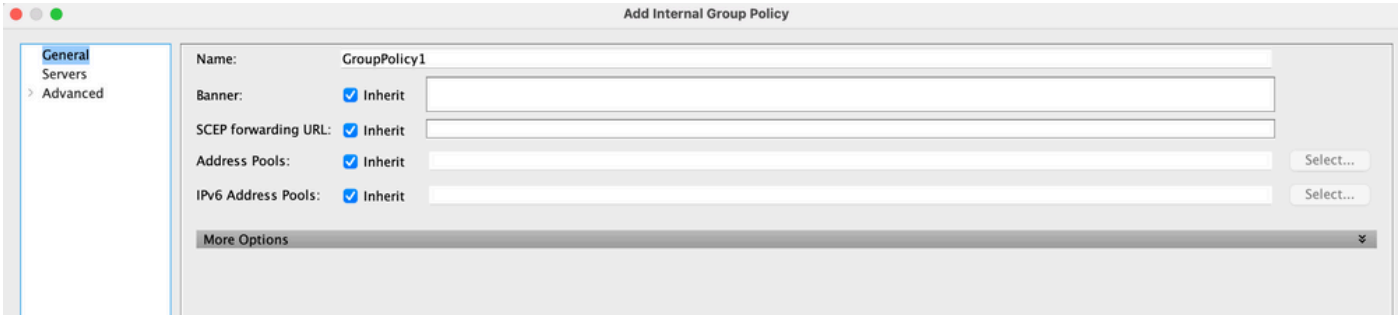
de oplossingen van VPN op diverse manieren worden bepaald en in sommige gevallen de zelfde eindoplossing verstrekken. De gekozen benadering is echter gebaseerd op de behoeften van de klant en zijn omgeving.

Gebaseerd op de aard van dit document en de gedefinieerde clientvereisten, kunt u Adaptive Security Device Manager (ASDM) gebruiken en de meeste van onze configuraties op DAP richten. U kunt echter ook lokaal groepsbeleid configureren om aan te tonen hoe DAP de lokale beleidskenmerken kan aanvullen en/of negeren. Op basis van deze testcase kunt u ervan uitgaan dat een LDAP-servergroep, een Split Tunneling Network List en een basis IP-verbinding, inclusief IP-pools en de Default DNS Server Group, vooraf zijn geconfigureerd.

Het definiëren van een groepsbeleid— deze configuratie is nodig voor het definiëren van lokale beleidskenmerken. Sommige hier gedefinieerde kenmerken zijn niet configureerbaar in DAP (bijvoorbeeld Local LAN Access). (Dit beleid kan ook worden gebruikt om Clientless en Clientgebaseerde eigenschappen te definiëren).

Navigeer naar Configuration > Remote Access VPN > Network (Client) Access > Group Policies en voeg een intern groepsbeleid toe zoals hieronder wordt getoond:

Afbeelding 17. Groepsbeleid — definieert lokale VPN-specifieke kenmerken.

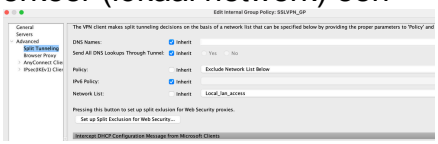


a. Configureer onder de koppeling Algemeen de naam SSLVPN_GP voor het groepsbeleid.

b. Ook onder de Algemene link klikt u op Meer opties en configureert u alleen het Tunneling Protocol:Clientless SSL VPN. (U kunt DAP configureren om de toegangsmethode te overschrijven en te beheren.)

c. Voer onder de link Advanced > Split Tunneling de volgende stappen uit:

Afbeelding 18. Split-tunneling — hiermee kan gespecificeerd verkeer (lokaal netwerk) een niet-versleutelde tunnel passeren tijdens een clientverbinding.

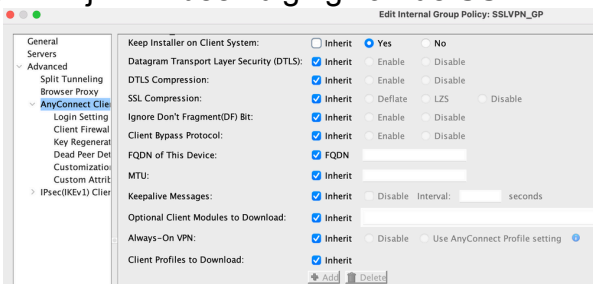


a. Beleid: UncheckInheriten selecteer Netwerklijst uitsluiten.

b. Netwerklijst: UncheckInheriten selecteer de naamLocal_LAN_Access. (Aangenomen dat dit vooraf is ingesteld.)

d. Configureer de volgende stappen onder de link Geavanceerd > ANYCONNECT-client:

Afbeelding 19. SSL VPN-clientinstallatieprogramma — Bij VPN-beëindiging kan de SSL-client op het eindpunt blijven of worden verwijderd.



e. Houd Installateur op Clientsysteem: UncheckInheriten selecteerJa.

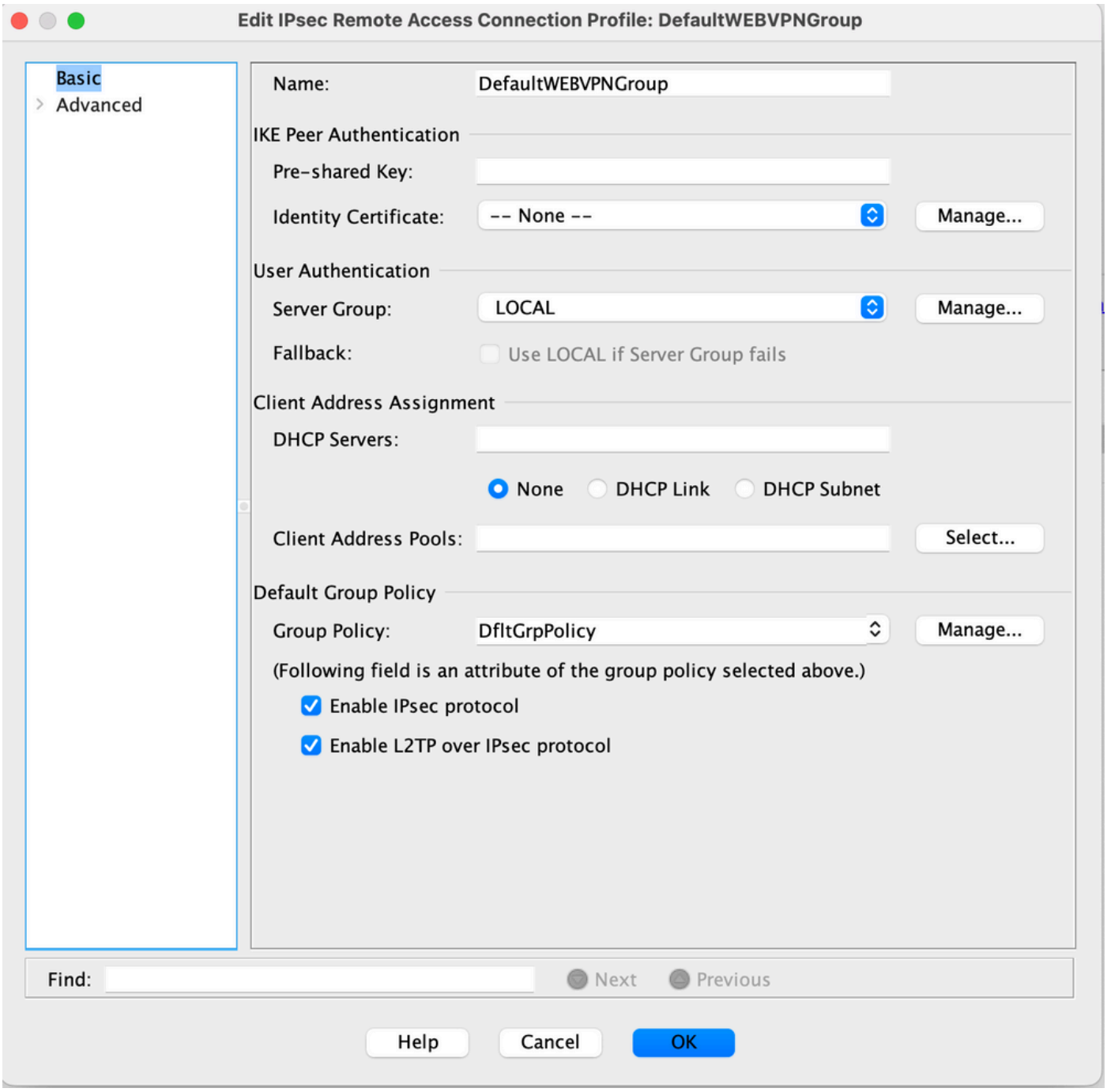
f. Klik op OKen vervolgens op Toepassen.

g. Pas uw configuratieveranderingen toe.

Een verbindingsprofiel definiëren—deze configuratie is nodig om onze AAA-verificatiemethode te definiëren, bijvoorbeeld LDAP, en het eerder geconfigureerde groepsbeleid (SLVPN_GP) toe te passen op dit verbindingsprofiel. Gebruikers die verbinding maken via dit verbindingsprofiel kunnen worden onderworpen aan de hier gedefinieerde eigenschappen en aan de eigenschappen die zijn gedefinieerd in het SSLVPN_GP Group Policy. (Dit profiel kan ook worden gebruikt om zowel Clientless als Clientgebaseerde kenmerken te definiëren).

Navigeren naar configuratie > Externe toegang > VPN > Netwerktoegang (client) >IPsec Remote Access Connection Profile en configureren:

Afbeelding 20. Verbindingsprofiel — definieert lokale VPN-specifieke kenmerken.



a. Bewerk onder de sectie Verbindingsprofielen de DefaultWEBVPNGgroup en configureer onder de Basis link de volgende stappen:

   a. Verificatie—Methode:AAA

   b. Verificatie—AAA-servergroep:LDAP (aangenomen, vooraf geconfigureerd)

   c. Toewijzing van clientadres—Clientadrespools:IP_Pool (verondersteld pregeconfigureerd)

   d. Standaardgroepbeleid—groepsbeleid: SelectSSL VPN_GP

b. Pas uw configuratieveranderingen toe.

Definieer een IP-interface voor SSL VPN-connectiviteit — Deze configuratie is nodig voor het

beëindigen van client- en clientloze SSL-verbindingen op een gespecificeerde interface.

Alvorens de toegang van de Cliënt/van het Netwerk op een interface toe te laten, moet u eerst een SSL VPN cliëntbeeld bepalen.

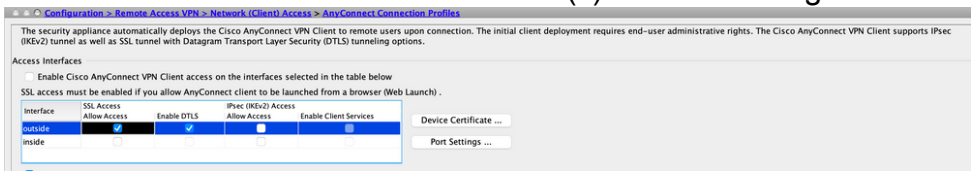
1. Navigeren naar configuratie > Externe toegang VPN > Netwerktoegang (client) > AnyConnect-clientsoftware, en het volgende beeld toevoegen, de SSL VPN-clientafbeelding van het ASA Flash-bestandssysteem: (Deze afbeelding kan worden gedownload van CCO, https://www.cisco.com)

   Afbeelding 21. SSL VPN Client Image Install: hiermee wordt de AnyConnect-clientafbeelding gedefinieerd die moet worden gedrukt om eindpunten te verbinden. 

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

   b. KlikOK, OKnogmaals, en danToepassen.

2. Navigeer naar Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles en gebruik de volgende stappen om dit in te schakelen:

   Afbeelding 22. SSL VPN Access interface-definieert de interface(s) voor het eindigen van SSL VPN-connectiviteit. 

   a. Schakel onder het gedeelte Access Interface in:Cisco AnyConnect VPN-client of oudere SSL VPN-clienttoegang inschakelen op de interfaces die in de onderstaande tabel zijn geselecteerd.

   b. Controleer ook onder het gedeelte Access Interfaces of Toegang toestaan op de buiteninterface. (Deze configuratie kan ook SSL VPN Clientloze toegang op de buiteninterface mogelijk maken.)

   c. Klik op Toepassen.

Het definiëren van Bladwijzerlijsten (URL Lists) voor Clientless Access-Deze configuratie is noodzakelijk voor het definiëren van een webgebaseerde toepassing die op de Portal moet worden gepubliceerd. u kunt 2 URL-lijsten definiëren, één voor Werknemers en de andere voor Contractors.

1. Navigeer naar Configuration > Remote Access VPN > Clientloze SSL VPN Access > Portal > Bladwijzers, klik op+ Add en configureer de volgende stappen:

   Afbeelding 23. De lijst van de referentie-bepaalt URLs die van het Webportaal moeten worden gepubliceerd en worden betreden. (Aangepast voor toegang van werknemers). 

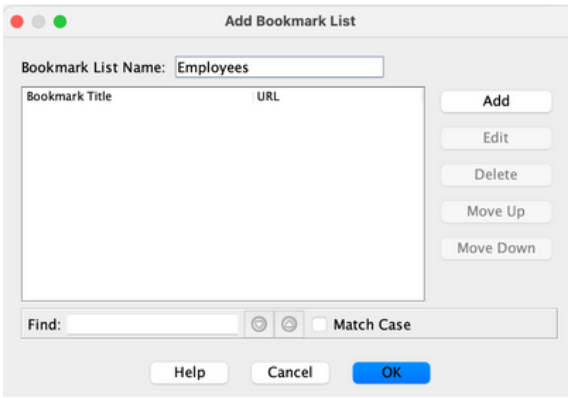
   a. Naam bladwijzerlijst:Werknemers, klik vervolgens op Toevoegen.

b. Bladwijzertitel:Intranet van bedrijf

c. URL-waarde: https://company.resource.com

- Klik nogmaals op OK en vervolgens op OK.

- Klik op + Toevoegen en vorm als volgt een tweede bladwijzerlijst (URL-lijst):



Afbeelding 24. Bladwijzerlijst —Aangepast voor de toegang van de gast.

a. Naam bladwijzerlijst:**Contractors**, **klik** vervolgens **op Toevoegen**.

b. Bladwijzertitel:**Gasttoegang**

c. URL-waarde: https://company.contractors.com

- Klik nogmaals op OK en vervolgens op OK.

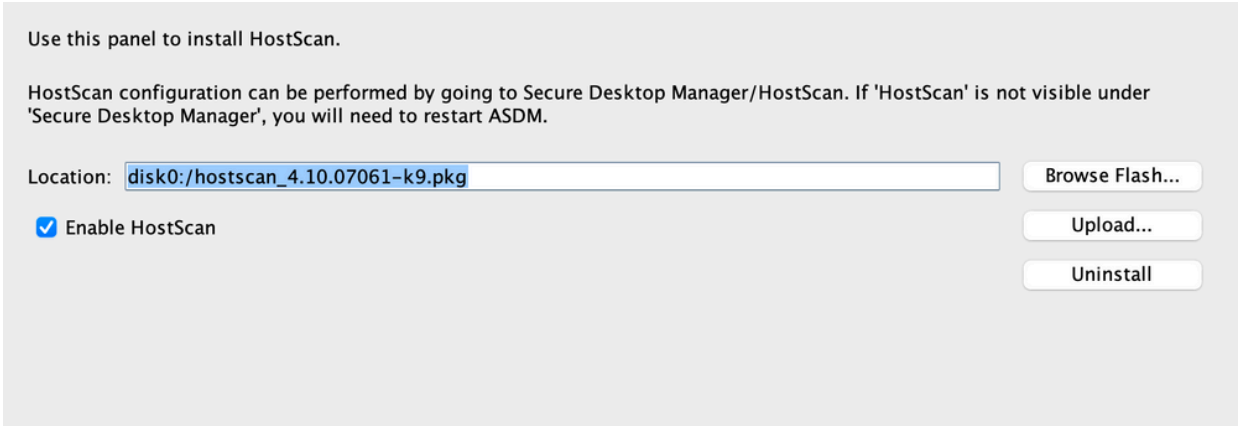
-

Klik op Toepassen.

Hostscan configureren:

- Navigeer **naar Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image**, en configureer de volgende stappen:

Afbeelding 25. HostScan Image Install: hiermee wordt het te drukken HostScan-beeld gedefinieerd om eindpunten aan te sluiten.



a. Installeer **de disk0:/hostscan_4.xx.xxxxx-k9.**pkgimage vanuit het ASA Flash-bestandssysteem.

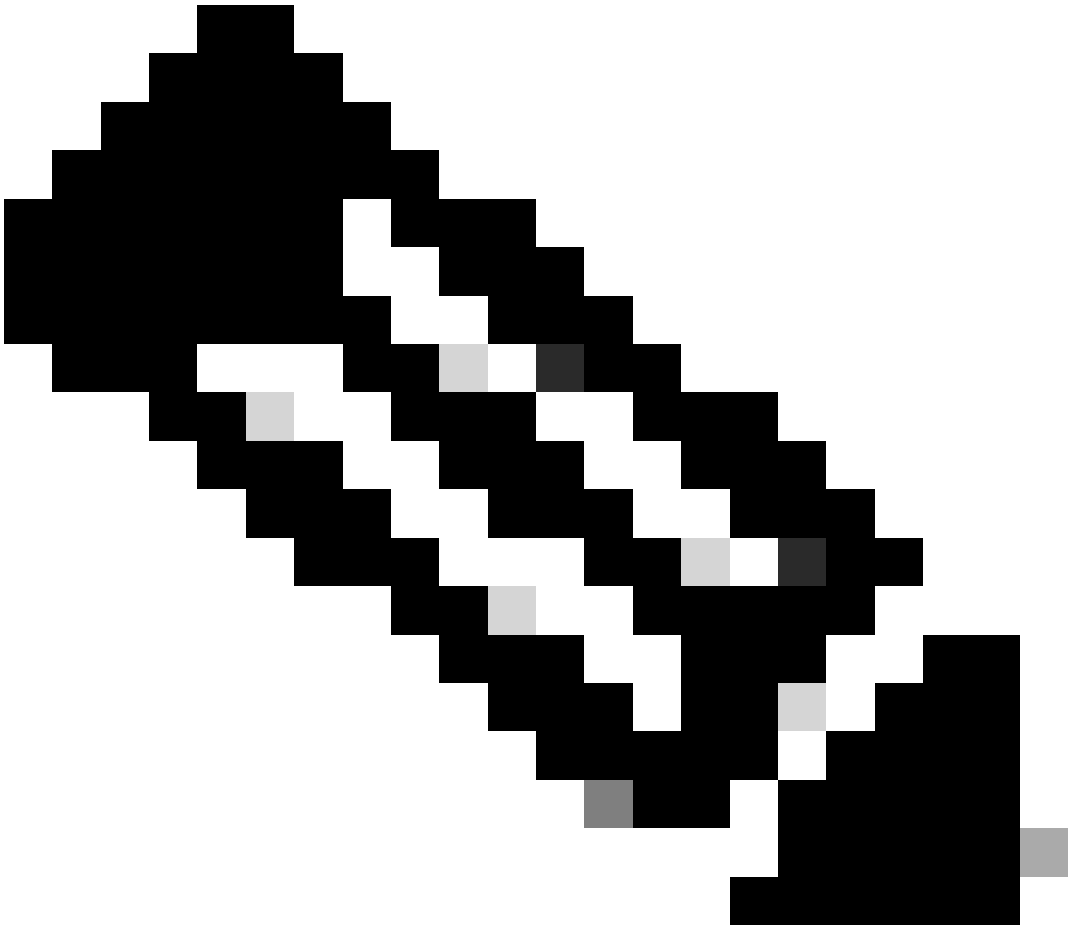
b. **Controleer of HostScan inschakelen**.

c. **Klik op Toepassen**.

Dynamisch toegangsbeleid — Deze configuratie is nodig voor de validatie van verbindende gebruikers en hun endpoints op basis van gedefinieerde AAA- en/of endpointbeoordelingscriteria. Als aan de gedefinieerde criteria voor een DAP-record is voldaan, kunnen verbindende gebruikers toegang krijgen tot netwerkbronnen die aan die DAP-record(s) zijn gekoppeld. De DAP-autorisatie wordt uitgevoerd tijdens het

verificatieproces.

Om ervoor te zorgen dat een SSL VPN verbinding in het standaardgeval kan eindigen, bijvoorbeeld, wanneer het eindpunt niet overeenkomt met een geconfigureerd beleid voor dynamische toegang), kunt u het met deze stappen configureren:

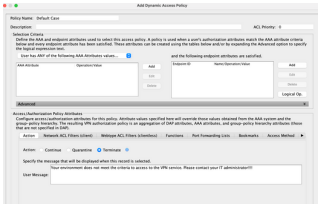


Opmerking: bij het voor het eerst configureren van Dynamic Access Policies wordt er een DAP.xml foutmelding weergegeven die aangeeft dat er geen DAP-configuratiebestand (DAP.XML) bestaat. Zodra uw oorspronkelijke DAP-configuratie is gewijzigd en vervolgens is opgeslagen, kan dit bericht niet meer verschijnen.

-

Navigeer **naar Configuration > Remote Access VPN > Clientloze SSL VPN-toegang > Dynamisch toegangsbeleid** en configureer de volgende stappen:

Afbeelding 30. Standaard Dynamisch Toegangsbeleid — indien er geen vooraf gedefinieerde DAP-records worden gekoppeld, kan deze DAP-record worden afgedwongen. Zodoende kan SSL VPN-toegang worden geweigerd.



a.

Bewerk het DFLTAccess Policy en stel de actie in **op Terminate**.

b.

Klik op OK.

•

Voeg als volgt een nieuw Dynamisch Toegangsbeleid **toe met de naam Managed_Endpoints**:

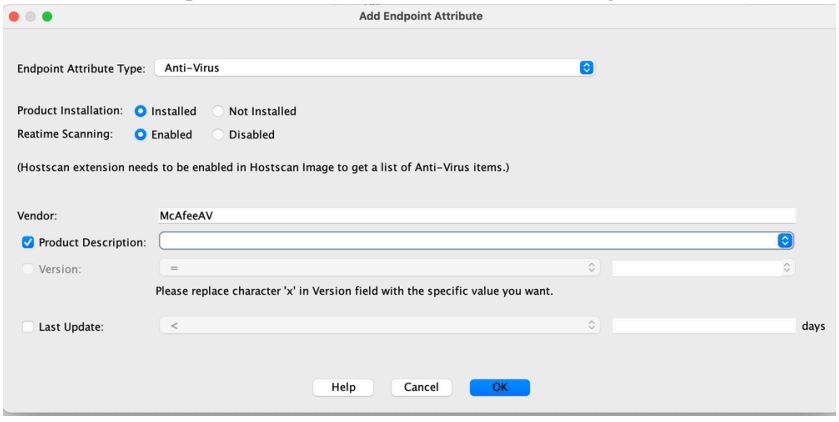
a.

Beschrijving:**Client Access voor werknemers**

b.

Voeg een type endpointkenmerk (antivirus) toe zoals in afbeelding 31. Klik op OK wanneer u klaar bent.

Afbeelding 31. DAP Endpoint Attribute - Advanced Endpoint Assessment AntiVirus kan worden gebruikt als een DAP-criterium voor client-/netwerktoegang.



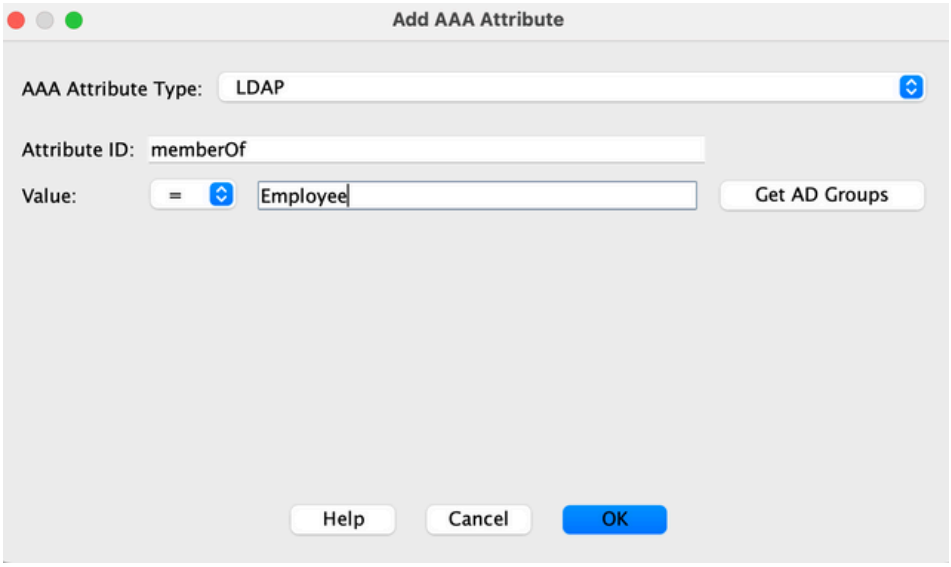
c.

Zoals in de vorige afbeelding is aangegeven, selecteert u in de vervolgkeuzelijst de optie AAA-kenmerken User has ALL of the following AAA Attributes Values.

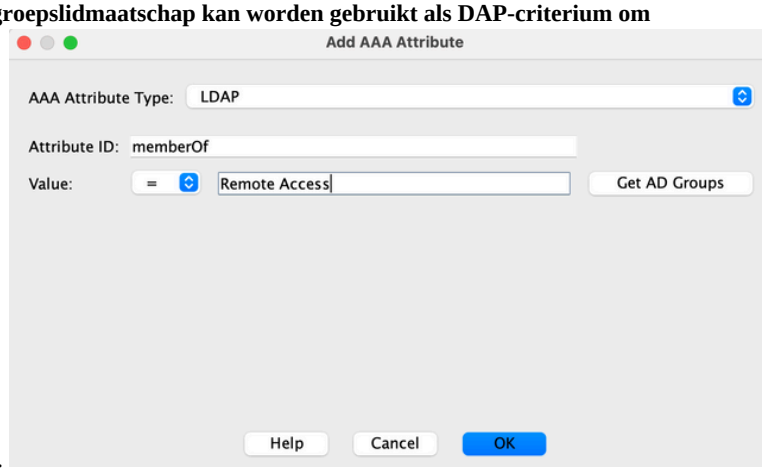
-

Voeg (rechts van het vak AAA-kenmerken) een AAA-type kenmerken toe (LDAP) zoals in de figuren 33 en 34. Klik op OK wanneer u klaar bent.

Afbeelding 33. DAP AAA Attribute - AAA Group Membership kan worden gebruikt als een DAP-criterium om een werknemer te identificeren.



Afbeelding 34. DAP AAA-kenmerk — AAA-groepslidmaatschap kan worden gebruikt als DAP-criterium om mogelijkheden voor externe toegang te bieden.



-

Controleer onder het tabblad Actie of de actie is ingesteld **op Doorgaan**, zoals in afbeelding 35.

Afbeelding 35. Handeling tabblad—Deze configuratie is nodig voor het definiëren van een speciale verwerking voor een specifieke verbinding of sessie. VPN-toegang kan worden geweigerd als een DAP-record wordt gekoppeld en de actie wordt ingesteld op Beëindigen.

-

Selecteer onder het tabblad Toegangsmethode de **client voor** toegangsmethode **AnyConnect**, zoals in afbeelding 36.

Afbeelding 36. Tab-Deze configuratie is nodig voor het definiëren van de SSL VPN-clientverbindingstypen. 

- **Klik op OK** en **pas het vervolgens toe**.

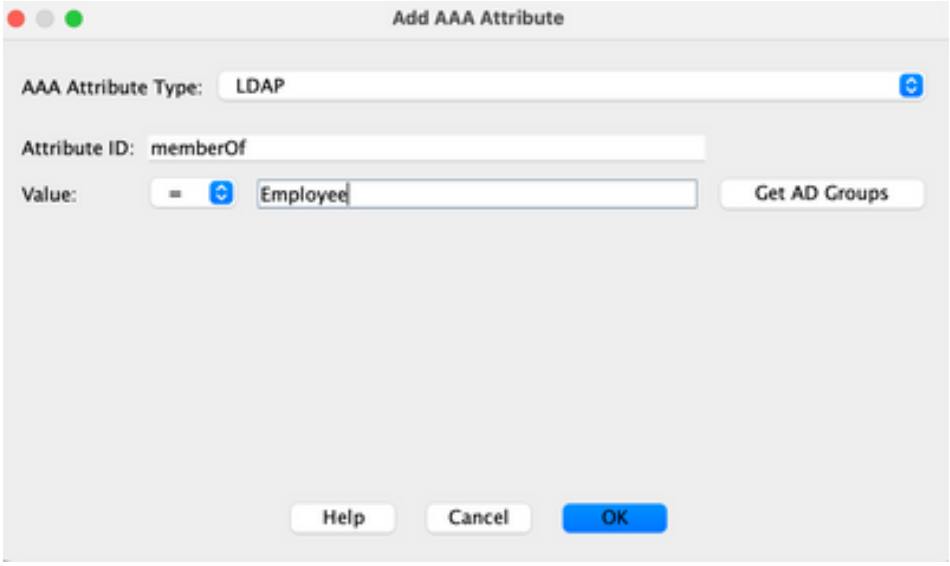
- Voeg een tweede Dynamisch Toegangsbeleid **toe**, **genaamdUnmanaged_Endpoints**, zoals beschreven:

a. Beschrijving:**Werknemersclientloze toegang**.

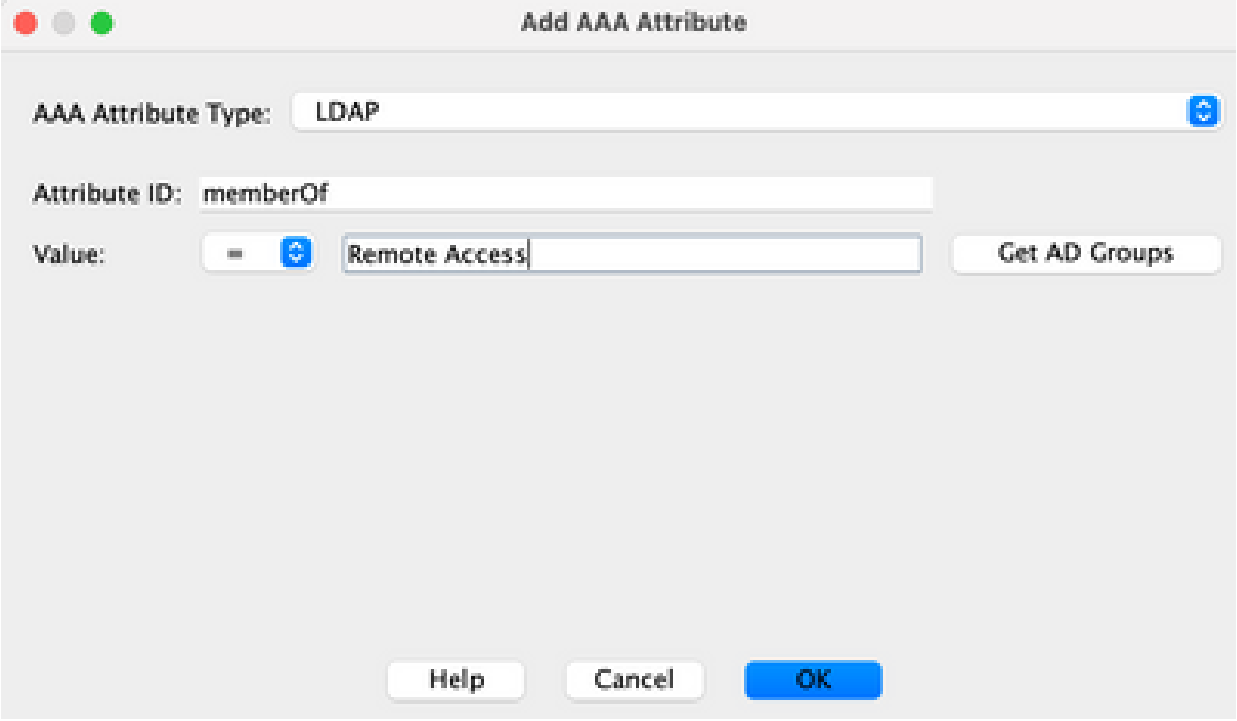
b. Selecteer in de vervolgkeuzelijst in de vorige afbeelding van de sectie AAA-kenmerken de optie User has ALL of the following AAA Attributes Values.

- Voeg (rechts van het type AAA-kenmerk) een type AAA-kenmerk (LDAP) toe zoals in de figuren 38 en 39. Klik op OK wanneer u klaar bent.

Afbeelding 38. DAP AAA-kenmerk — AAA-groepslidmaatschap kan worden gebruikt als DAP-criteria om een werknemer te identificeren.



Afbeelding 39. DAP AAA-kenmerk - AAA-groepslidmaatschap kan worden gebruikt als een DAP-criterium voor de mogelijkheid van externe toegang.



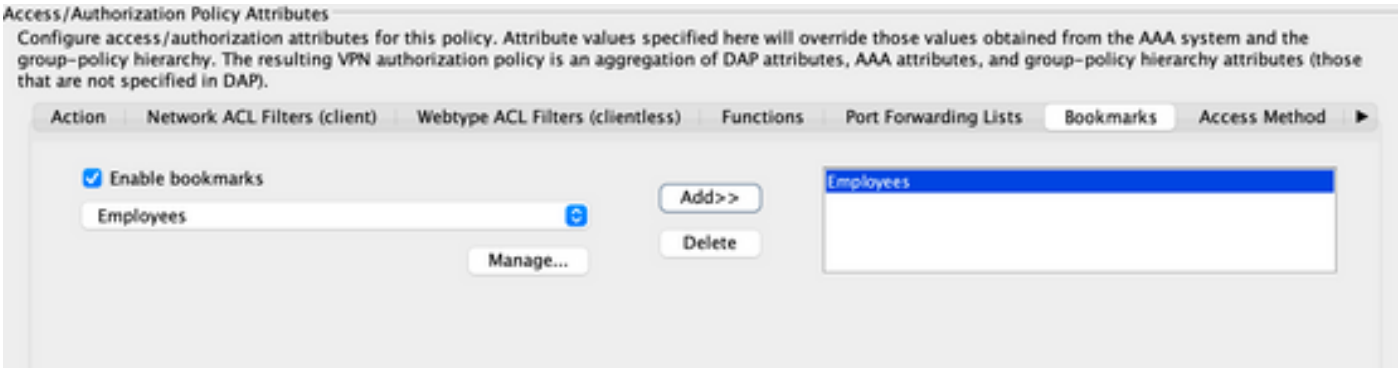
-

Controleer onder het tabblad Actie of de actie is ingesteld **op Doorgaan**. (Afbeelding 35)

-

Selecteer onder het tabblad Bladwijzers de lijst nameWerknemers in de vervolgkeuzelijst en **klik** vervolgens **op Toevoegen**. Controleer ook dat de optie Bladwijzers inschakelen is ingeschakeld zoals in afbeelding 40.

Afbeelding 40. Tabblad Bladwijzers—Hiermee kunt u URL-lijsten voor gebruikerssessies selecteren en configureren.



-

a.

Selecteer onder het tabblad Toegangsmethode het **webportaal** voor toegangsmethoden. (Afbeelding 36)

- **Klik op OK** en **pas het vervolgens toe**.

1. Contractors kunnen alleen worden geïdentificeerd door DAP AAA-kenmerken. Dientengevolge, kan het Type van Endpoint Attributen: (Beleid) niet in Stap 4 worden gevormd. Deze benadering is alleen bedoeld om veelzijdigheid te tonen binnen DAP.

3. Voeg een derde Dynamic Access Policy **genaamdGuest_Access toe** met de volgende informatie:

•

Beschrijving:**Guest Clientless Access**.

•

Voeg (rechts van het vak Endpoint Attribute) een Endpoint Attribute Type (Beleid) toe zoals in afbeelding 37. Klik op OK wanneer u klaar bent.

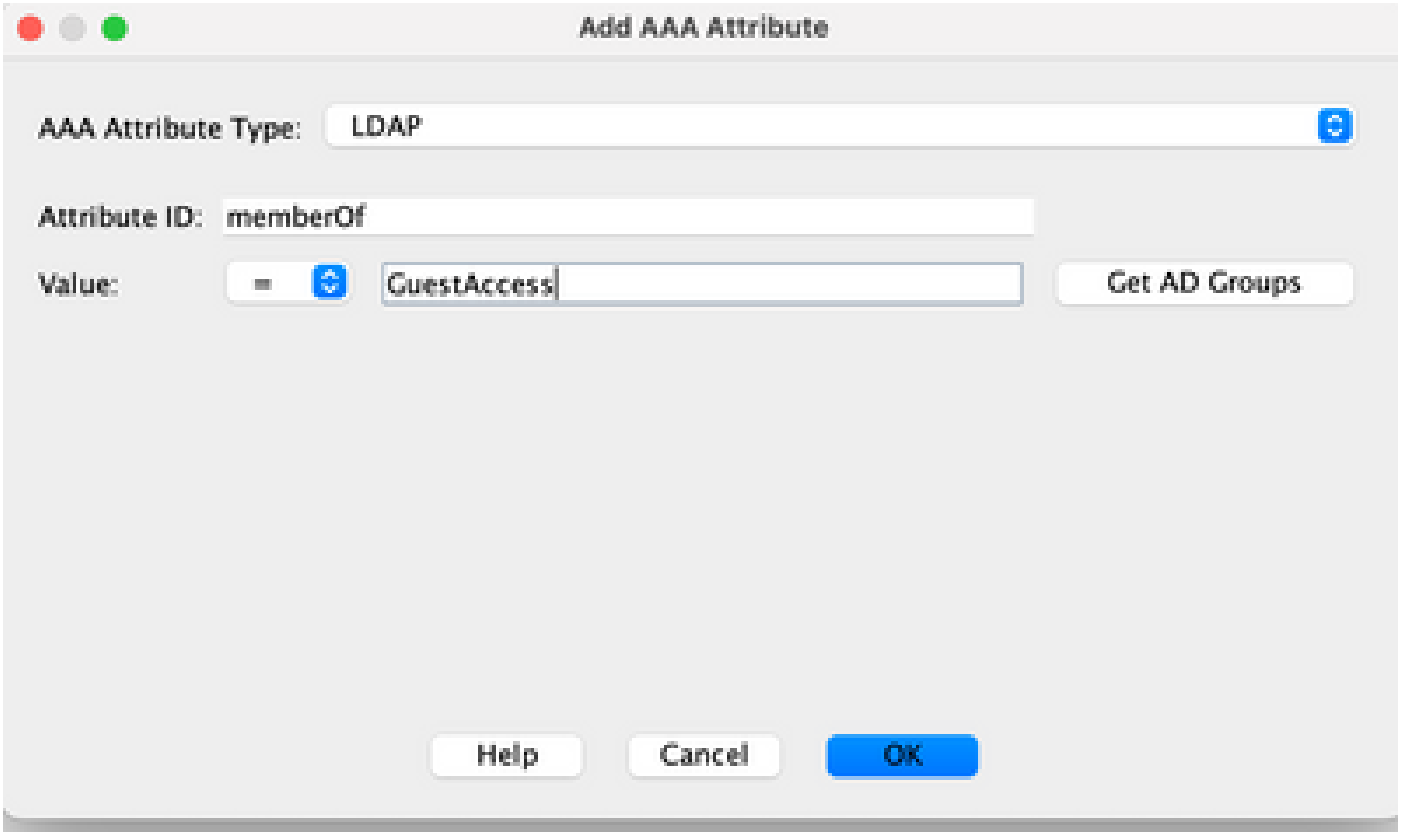
•

Selecteer in afbeelding 40 de optie in de vervolgkeuzelijst in het gedeelte AAA-kenmerken User has ALL of the following AAA Attributes Values.

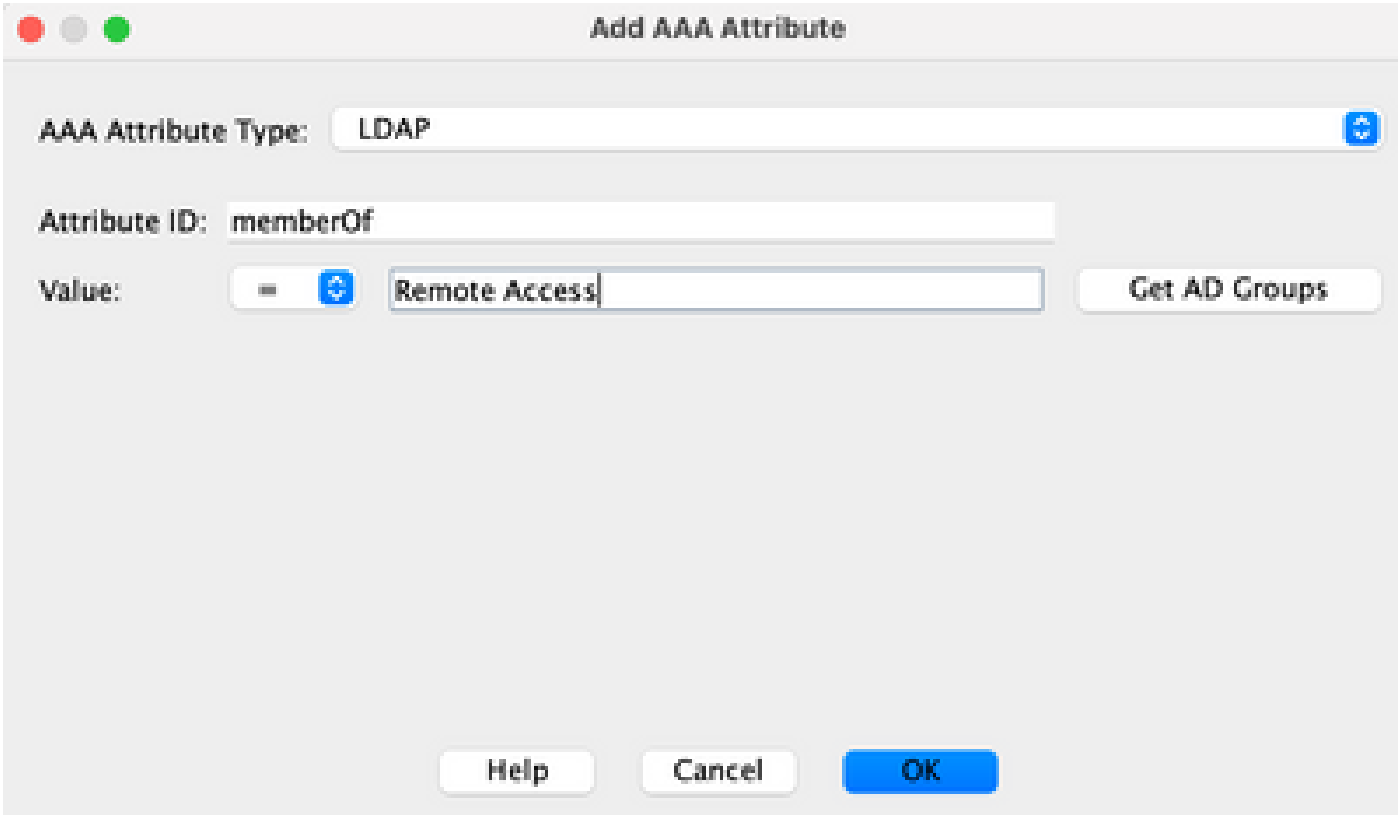
•

Voeg (rechts van het vak AAA-kenmerken) een AAA-type kenmerken toe (LDAP) zoals in de figuren 41 en 42. Klik op OK wanneer u klaar bent.

Afbeelding 41. U kunt DAP AAA-kenmerk—AAA-groepslidmaatschap als DAP-criterium gebruiken om een contractor te identificeren



Afbeelding 42. DAP AAA-kenmerk—U kunt AAA-groepslidmaatschap gebruiken als DAP-criterium voor toegang op afstand



-

a.

Controleer onder het tabblad Actie of de actie is ingesteld op **Doorgaan**. (Afbeelding 35)

b.

Selecteer onder het tabblad Bladwijzers de lijstnaam **Contractors** uit de vervolgkeuzelijst en klik vervolgens op Toevoegen. Controleer ook of de **optie Bladwijzers inschakelen** is ingeschakeld. (Referentiefiguur 40.)

c.

Selecteer onder het tabblad Toegangsmethode het webportaal voor toegangsmethoden. (Afbeelding 36)

d.

Klik op **OK** en **pas** het vervolgens toe.

Conclusie

Gebaseerd op de client Remote Access SSL VPN-vereisten die in dit voorbeeld zijn aangegeven, voldoet deze oplossing aan de client Remote Access VPN-vereisten.

Met de evoluerende en dynamische VPN-omgevingen bij de samenvoeging, kan Dynamic Access Policies zich aanpassen en schalen aan frequente wijzigingen in de internetconfiguratie, verschillende rollen die elke gebruiker binnen een organisatie kan bewonen, en logins van beheerde en onbeheerde externe toegangssites met verschillende configuraties en niveaus van beveiliging.

Dynamic Access Policies worden aangevuld door nieuwe en beproefde legacy-technologieën, zoals geavanceerde endpointbeoordeling, hostscan, beveiligde desktop, AAA en lokaal toegangsbeleid. Als gevolg daarvan kunnen organisaties met vertrouwen beveiligde VPN-toegang leveren aan elke netwerkbron vanaf elke locatie.

Gerelateerde informatie

- **Cisco Technical Support en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.