Guide de déploiement DAP (Dynamic Access Policies) ASA 8.x

Contenu

Introduction

Les passerelles du réseau privé virtuel (VPN) fonctionnent dans les environnements dynamiques. Les plusieurs variables peuvent affecter chaque connexion VPN ; par exemple, configurations d'intranet qui changent fréquemment, les divers rôles que chaque utilisateur peut habiter dans une organisation, et procédures de connexion des sites d'Accès à distance avec différents configurations et niveaux de sécurité. La tâche d'autoriser des utilisateurs beaucoup davantage est compliquée dans un environnement dynamique VPN qu'elle est dans un réseau avec une configuration statique.

Les stratégies d'accès dynamique (DAP), une nouvelle fonctionnalité introduite en code de la version logicielle v8.0 de l'appliance de sécurité adaptable (ASA), te permettent de configurer l'autorisation qui adresse le dynamics des environnements VPN. Vous créez une stratégie d'accès dynamique en plaçant une collection d'attributs de contrôle d'accès que vous associez avec un tunnel ou une session spécifique d'utilisateur. Ces attributs abordent des questions de plusieurs adhésion à des associations et de Sécurité des terminaux.

Par exemple, l'accès de concessions de dispositifs de sécurité à un utilisateur particulier pour une session particulière basée sur les stratégies que vous définissez. Il génère un DAP pendant l'authentification de l'utilisateur en sélectionnant et/ou en agrégeant des attributs d'un ou plusieurs enregistrements DAP. Il sélectionne ces enregistrements DAP basés sur les informations de Sécurité des terminaux du périphérique distant et/ou les informations d'autorisation d'AAA pour l'utilisateur authentifié. Il applique alors l'enregistrement DAP au tunnel ou à la session d'utilisateur.

Remarque: *Le fichier dap.xml*, qui contient les attributs de sélection de stratégies DAP, est enregistré dans l'éclair de l'ASA. Bien que vous puissiez exporter la hors fonction-case de fichier dap.xml, éditez-la (si vous savez la syntaxe de xml), et réimportez-la de retour, fasse attention très, parce que vous pouvez faire cesser l'ASDM de traiter des enregistrements DAP si vous misconfigured quelque chose. Il n'y a aucun CLI pour manipuler la présente partie de la

configuration.

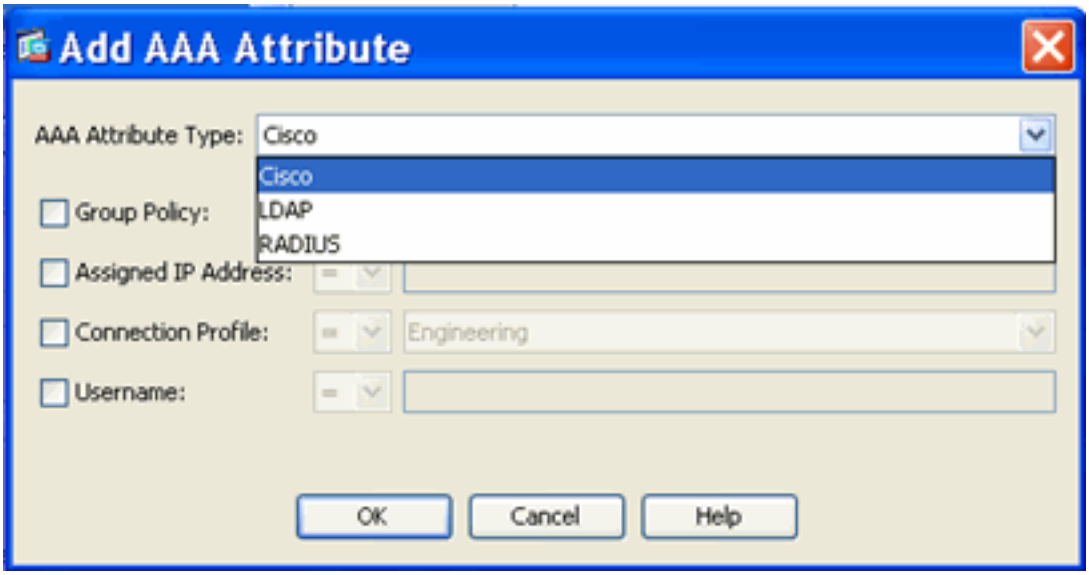
Remarque: Essayer pour configurer les paramètres d'*accès de dynamique-Access-stratégie-enregistrement* par l'intermédiaire du CLI peut faire cesser DAP de fonctionner bien que l'ASDM gère correctement la même chose. Évitez le CLI, et employez toujours l'ASDM pour gérer des stratégies DAP.

Attributs DAP et d'AAA

DAP complète des services d'AAA et fournit un ensemble limité d'attributs d'autorisation qui peuvent ignorer les attributs que l'AAA fournit. Les dispositifs de sécurité peuvent sélectionner des enregistrements DAP basés sur les informations d'autorisation d'AAA pour l'utilisateur. Les dispositifs de sécurité peuvent sélectionner des enregistrements du multiple DAP selon ces informations, qu'ils agrègent alors pour assigner à des attributs d'autorisation DAP.

Vous pouvez spécifier des attributs d'AAA de la hiérarchie d'aaa attribute de Cisco, ou de l'ensemble complet d'attributs de réponse que l'appliance de Sécurité reçoit d'un RAYON ou d'un serveur LDAP suivant les indications de la figure 1.

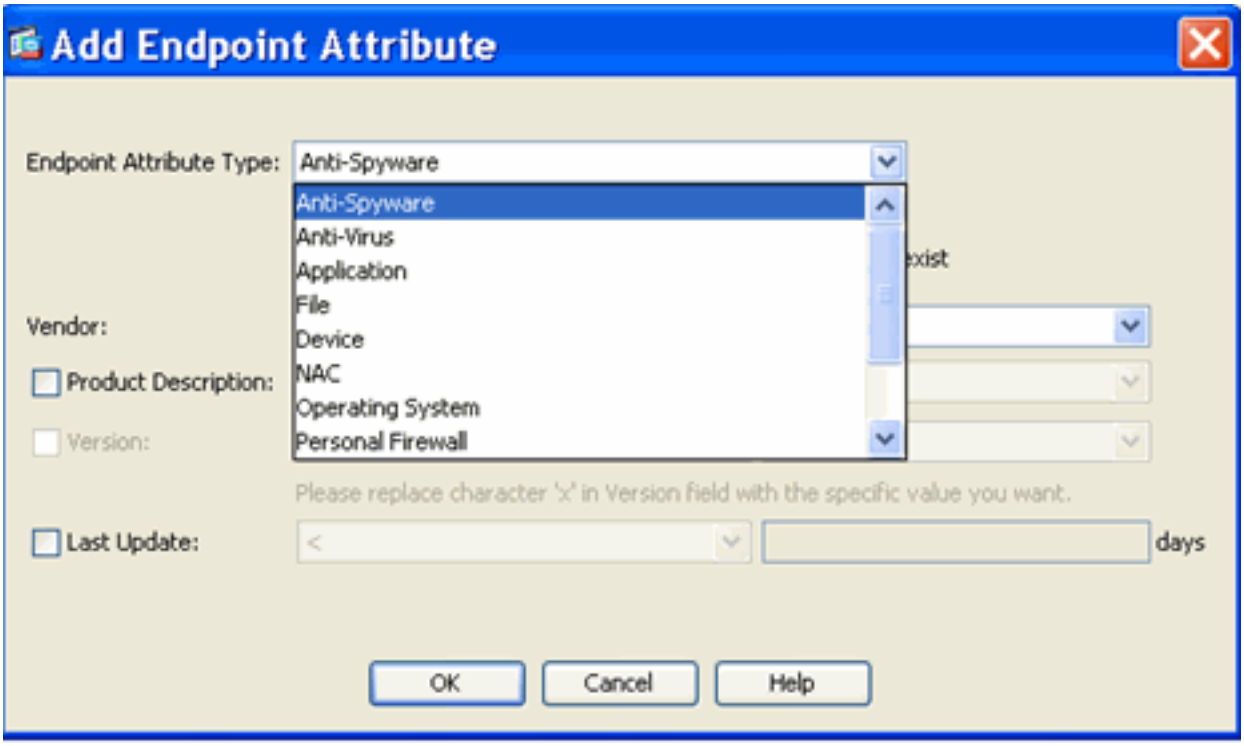
GUI d'aaa attribute du schéma 1. DAP



DAP et attributs de Sécurité des terminaux

En plus des attributs d'AAA, les dispositifs de sécurité peuvent également obtenir des attributs de Sécurité des terminaux à l'aide des méthodes d'estimation de posture que vous configurez. Ceux-ci incluent le balayage de base d'hôte, Secure Desktop, standard/a avancé l'estimation de point final et le NAC suivant les indications des attributs d'estimation de point final du schéma 2. sont obtenus et envoyés aux dispositifs de sécurité avant l'authentification de l'utilisateur. Cependant, des attributs d'AAA, y compris l'enregistrement global DAP, sont validés pendant l'authentification de l'utilisateur.

GUI d'attribut de point final du schéma 2.

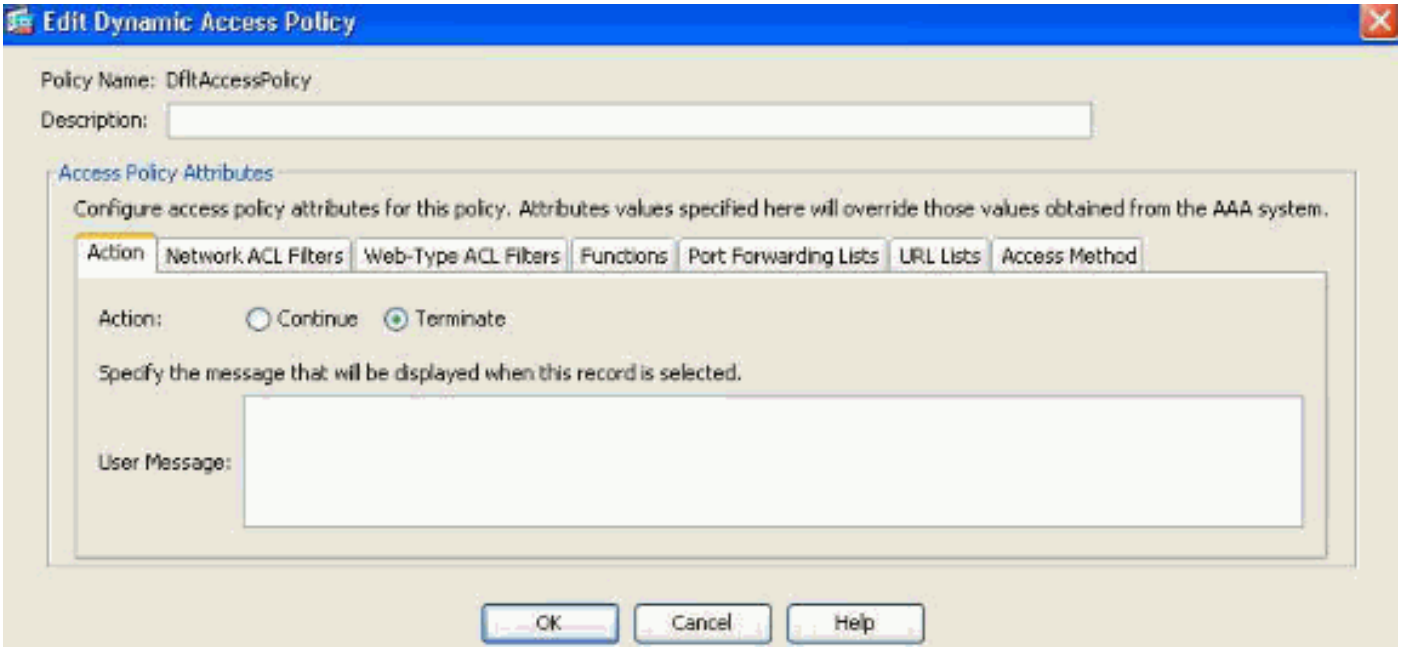


Stratégie par défaut d'accès dynamique

Avant l'introduction et l'implémentation de DAP, l'attribut de stratégie d'accès/paires de valeur qui ont été associées avec un tunnel ou une session spécifique d'utilisateur ont été définis localement sur l'ASA, c.-à-d., (des groupes et des stratégies de groupe de tunnel) ou tracés par l'intermédiaire des serveurs externes d'AAA. Cependant, dans la release v8.0, DAP peut être configuré pour compléter ou ignorer des stratégies locales et externes d'accès.

DAP est toujours imposé par défaut. Cependant, pour des administrateurs qui préfèrent la méthode existante d'application de stratégie, par exemple, imposant le contrôle d'accès par l'intermédiaire des groupes de tunnel, les stratégies de groupe et l'AAA sans application explicite de DAP peuvent encore obtenir ce comportement. Pour le comportement existant, aucune modification de configuration à la caractéristique DAP, y compris l'enregistrement du par défaut DAP, DfltAccessPolicy, n'est exigée suivant les indications de la figure 3.

Stratégie par défaut d'accès dynamique du schéma 3.



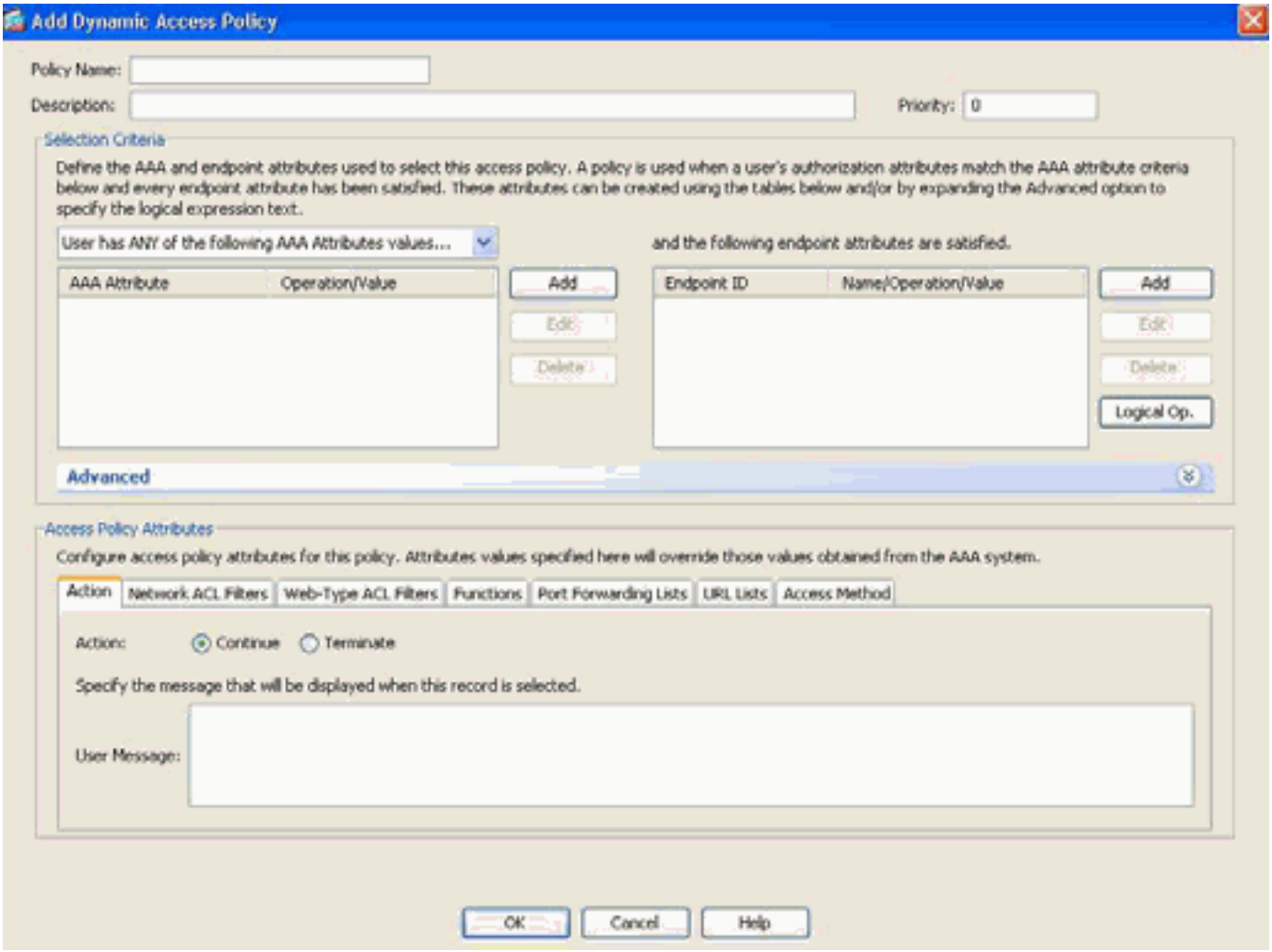
Néanmoins, si des valeurs par défaut l'unes des dans un enregistrement DAP sont changées, par exemple, l'action : le paramètre dans le DfltAccessPolicy est changé de sa valeur par défaut pour se terminer et des enregistrements supplémentaires DAP ne sont pas configurés, les utilisateurs authentifiés, par défaut, apparieront l'enregistrement de DfltAccessPolicy DAP et seront refusés l'accès VPN.

En conséquence, un ou plusieurs enregistrements DAP devront être créés et configurés pour autoriser la connectivité VPN et pour la définir que des ressources de réseau un utilisateur authentifié est autorisé pour accéder à. Ainsi, DAP, si configuré, aura la priorité au-dessus de l'application existante de stratégie.

Configurer Dynamic Access Policies

En employant DAP pour définir au lequel les ressources de réseau un utilisateur a accès, il y a beaucoup de paramètres à considérer. Par exemple, identifier si le point final se connectant provient géré, non pris en charge ou environnement non approuvé, déterminant des critères de sélection nécessaires pour identifier le point final se connectant, et basé sur l'estimation de point final et/ou les qualifications d'AAA, que des ressources de réseau l'utilisateur se connectant seront autorisé pour accéder à. Pour accomplir ceci, vous devrez d'abord se familiariser avec des configurations et des fonctions DAP suivant les indications de la figure 4.

Stratégie d'accès dynamique du schéma 4.



En configurant un enregistrement DAP, il y a deux composants importants à considérer :

- Critères de sélection comprenant des options avancées
- Attributs de stratégie d'Access

La section de critères de sélection est où un administrateur configurerait l'AAA et les attributs de point final utilisés pour sélectionner un enregistrement de la particularité DAP. Un enregistrement DAP est utilisé quand l'autorisation d'un utilisateur attribue la correspondance les critères d'aaa attribute et chaque attribut de point final a été satisfait.

Par exemple, si le type d'aaa attribute : Le LDAP (Répertoire actif) est sélectionné, la chaîne de nom d'attribut est memberOf et la chaîne de valeur est des sous-traitants, suivant les indications de la figure 5a, l'utilisateur authentifiant doit être un membre des sous-traitants de groupe de Répertoire actif pour apparier les critères d'aaa attribute.

En plus de satisfaire les critères d'aaa attribute, l'utilisateur authentifiant sera également requis de répondre aux critères d'attribut de point final. Par exemple, si l'administrateur configurait le Cisco Secure Desktop (CSD) pour déterminer la posture du point final se connectant et basée sur cette estimation de posture, le point final a été placé dans le non pris en charge d'emplacement CSD, l'administrateur pourrait alors utiliser cette information sur l'évaluation pendant que les critères de sélection pour le point final attribuent représenté sur la figure 5b.

Figure 5a. Critères d'aaa attribute

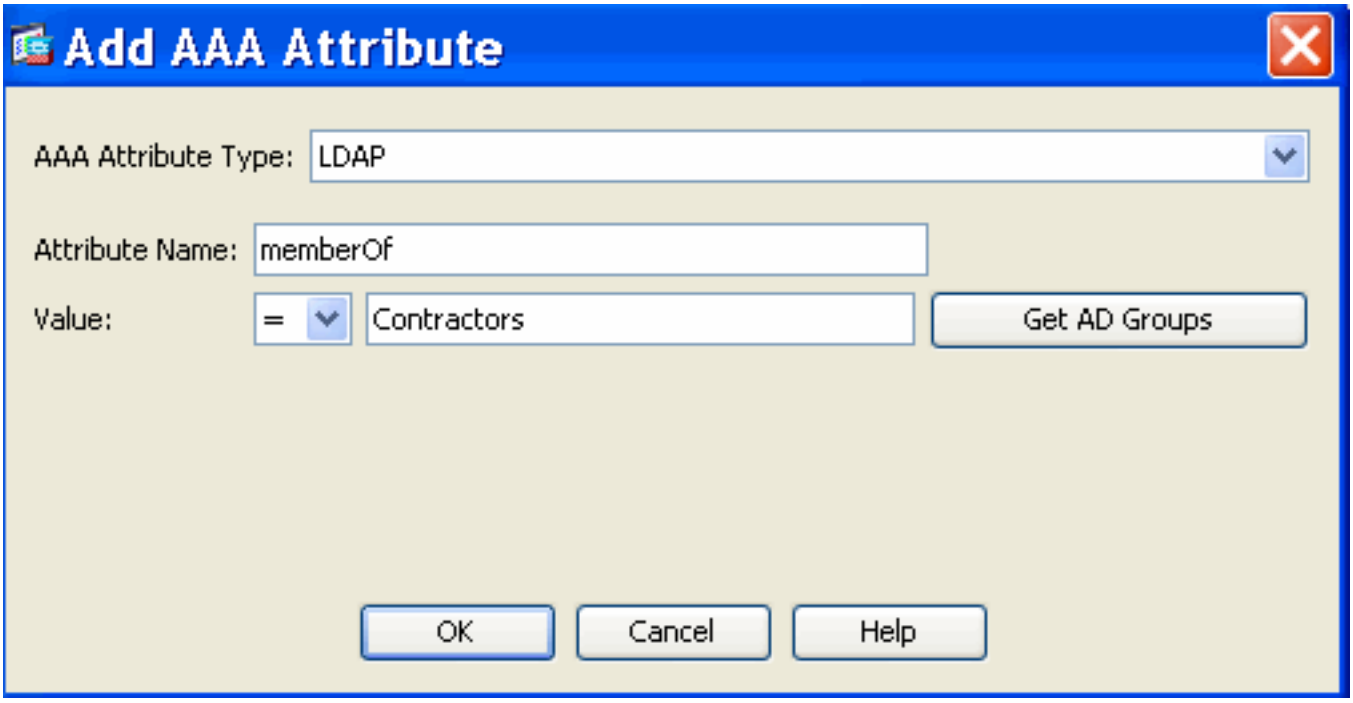
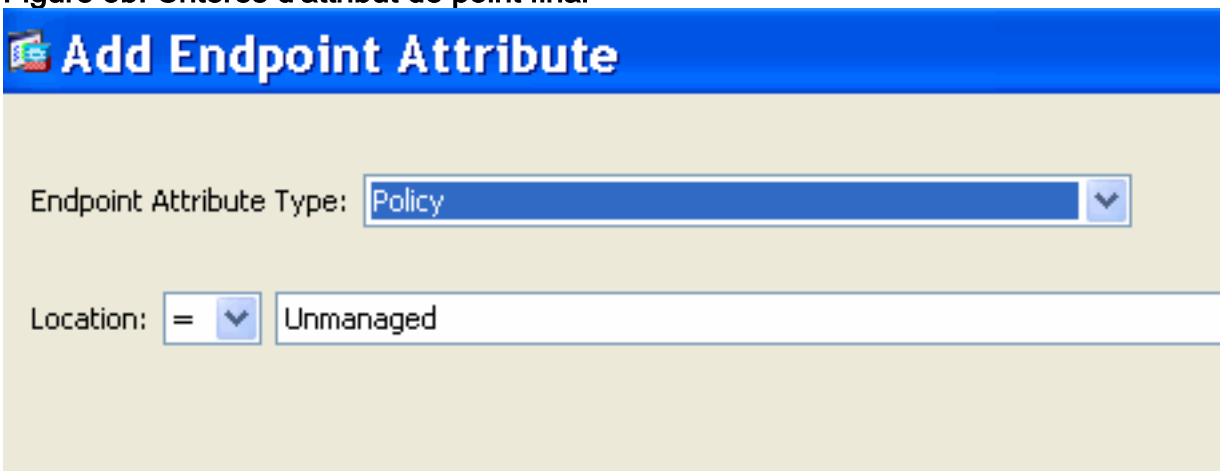
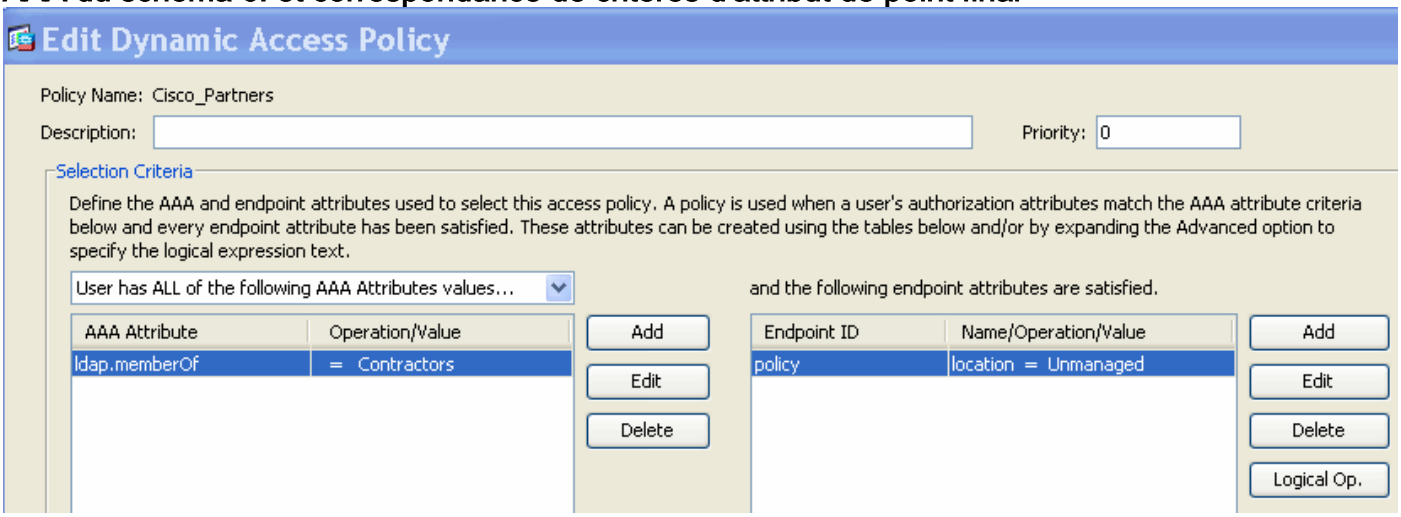


Figure 5b. Critères d'attribut de point final



Ainsi, pour apparier l'enregistrement DAP affiché dans la figure 6, l'utilisateur authentifiant doit être un membre du groupe actif de répertoire de sous-traitants et son point final se connectant doit satisfaire la valeur de stratégie CSD « sans changement, » pour être assigné l'enregistrement DAP.

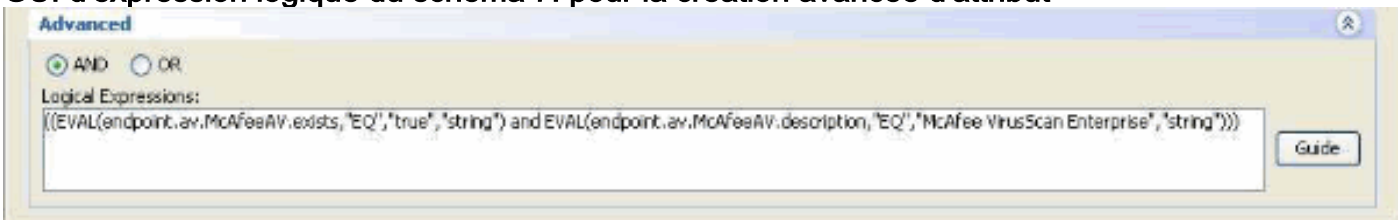
AAA du schéma 6. et correspondance de critères d'attribut de point final



L'AAA et les attributs de point final peuvent être créés utilisant les tables comme décrit dans la figure 6 et/ou en développant l'option avancée de spécifier une expression logique suivant les indications de la figure 7. Actuellement, l'expression logique est construite avec les fonctions d'ÉVAL, par exemple, l'ÉVAL (endpoint.av.McAfeeAV.exists, « EQ », « vrai », « chaîne ») et l'ÉVAL (endpoint.av.McAfeeAV.description, « EQ », « entreprise de McAfee VirusScan », « chaîne »), qui représentent l'AAA et/ou les opérations logiques de sélection de point final.

Les expressions logiques sont utiles pour ajouter des critères de sélection autres que ce qui est possible dans l'AAA et les zones d'attribut de point final ci-dessus. Par exemple, alors que vous pouvez configurer les dispositifs de sécurité pour utiliser les attributs d'AAA qui n'en satisfont n'importe lequel, tous les ou aucun critères spécifiés, les attributs de point final sont cumulatifs, et doivent tout être satisfaits. Pour permettre les dispositifs de sécurité d'utiliser un attribut ou des autres de point final, vous devez créer des expressions logiques appropriées sous la section avancée de l'enregistrement DAP.

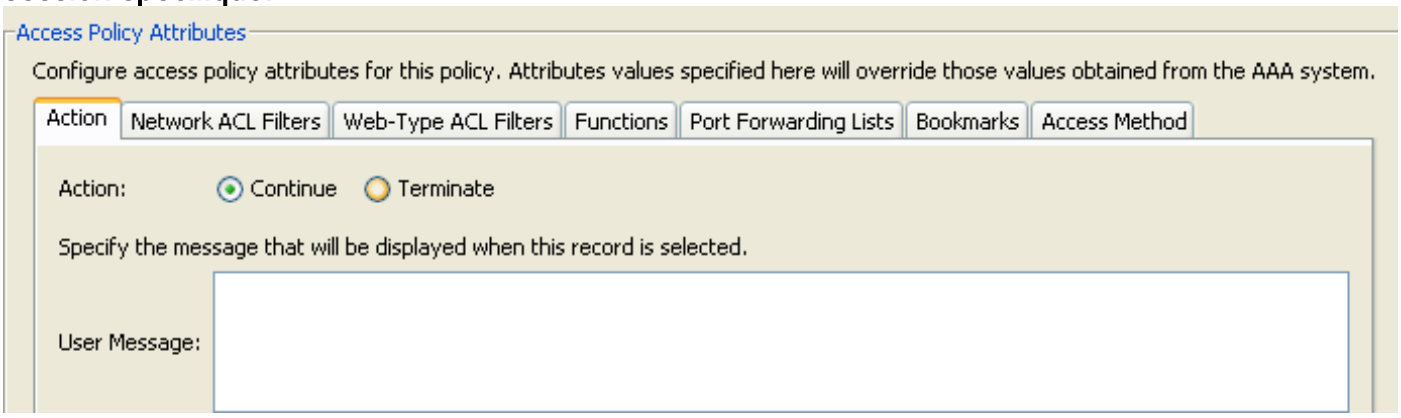
GUI d'expression logique du schéma 7. pour la création avancée d'attribut



La section d'attributs de stratégie d'accès suivant les indications de la figure 8 est où un administrateur configurerait des attributs d'accès VPN pour un enregistrement de la particularité DAP. Quand l'autorisation d'un utilisateur attribue la correspondance les critères d'AAA, de point final et/ou d'expression logique ; les valeurs d'attribut configurées de stratégie d'accès dans cette section seront imposées. Les valeurs d'attribut spécifiées ici ignoreront ces valeurs obtenues du système d'AAA, y compris ceux dans l'utilisateur, le groupe, le groupe de tunnel, et les enregistrements de groupe par défaut existants.

Un enregistrement DAP a un ensemble limité de valeurs d'attribut qui peuvent être configurées. Ces valeurs tombent sous les onglets suivants suivant les indications des figures 8 par 14 :

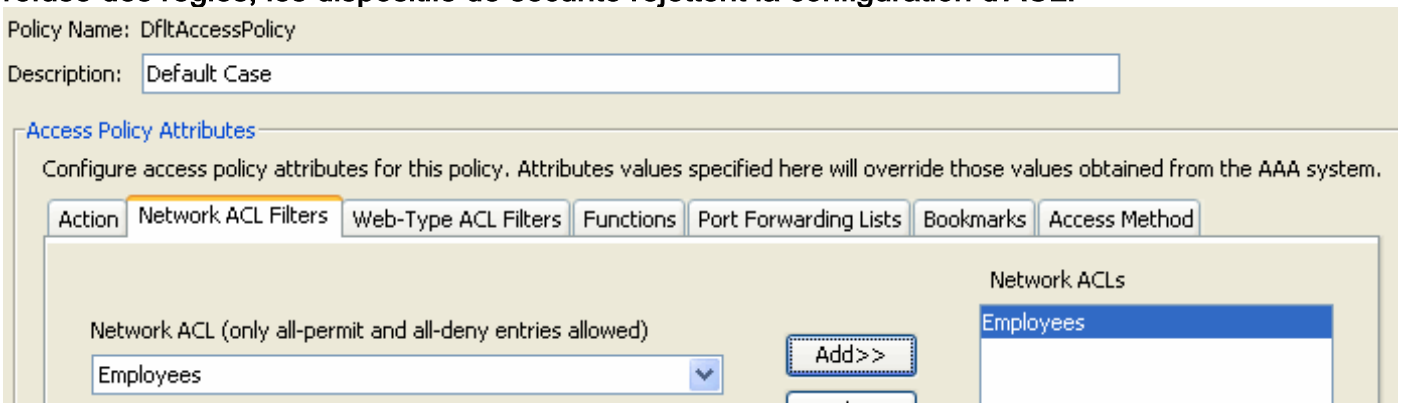
Action du schéma 8. — Spécifie le traitement spécial à s'appliquer à une connexion ou à une session spécifique.



- Continuez — (par défaut) cliquez sur pour s'appliquer des attributs de stratégie d'accès à la session.
- Terminez — Cliquez sur pour terminer la session.
- Message d'utilisateur — Entrez un message texte pour afficher sur la page du portail quand cet enregistrement DAP est sélectionné. Caractères du maximum 128. Affichages de

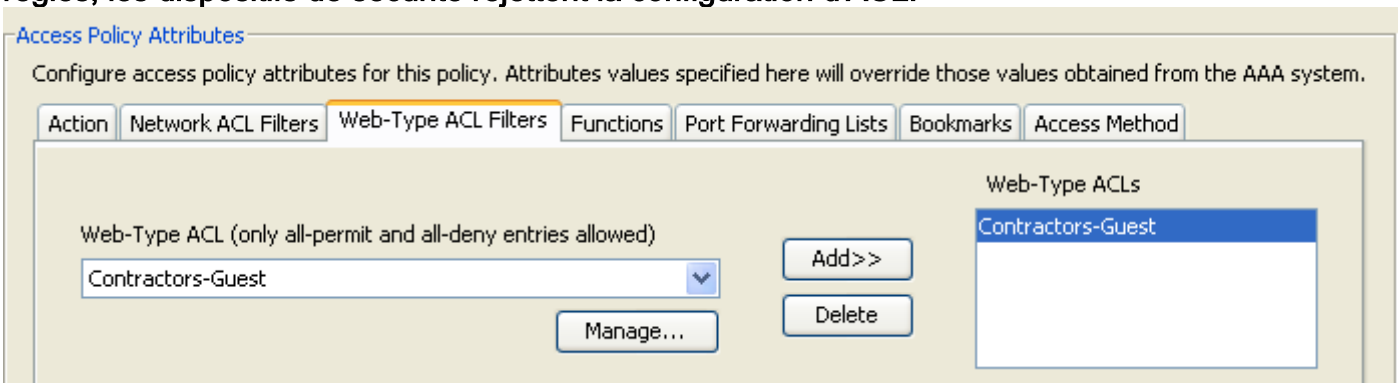
message d'utilisateur comme globe jaune. Quand un utilisateur ouvre une session, il clignote trois fois d'attirer l'attention, et alors il est toujours. Si plusieurs enregistrements DAP sont sélectionnés, et chacun d'eux a un message d'utilisateur, tout les affichage de messages d'utilisateur. Supplémentaire, vous pouvez inclure en de tels messages URLs ou tout autre texte inclus, qui exigent que vous utilisez les balises HTML correctes.

Onglet de filtres d'ACL de réseau du schéma 9. — Permet vous de sélectionner et la configure network ACLs à s'appliquer à cet enregistrement DAP. Un ACL pour DAP peut contenir l'autorisation ou refuser des règles, mais pas chacun des deux. Si un ACL contient l'autorisation et refuse des règles, les dispositifs de sécurité rejettent la configuration d'ACL.



- Liste déroulante d'ACL de réseau — Sélectionnez le réseau déjà configuré ACLs pour ajouter à cet enregistrement DAP. Seulement ACLs ayant toute l'autorisation ou tous refusent des règles sont éligibles, et ce sont le seul ACLs qui affichent ici.
- Gérez — Cliquez sur pour ajouter, éditer, et supprimer le réseau ACLs.
- Liste d'ACL de réseau — Affiche le réseau ACLs pour cet enregistrement DAP.
- Ajoutez — Cliquez sur pour ajouter l'ACL de réseau sélectionné de la liste déroulante à la liste d'ACLs de réseau du côté droit.
- Effacement — Clic pour supprimer un ACL mis en valeur de réseau de la liste d'ACLs de réseau. Vous ne pouvez pas supprimer un ACL s'il est assigné à un DAP ou à autre enregistrement.

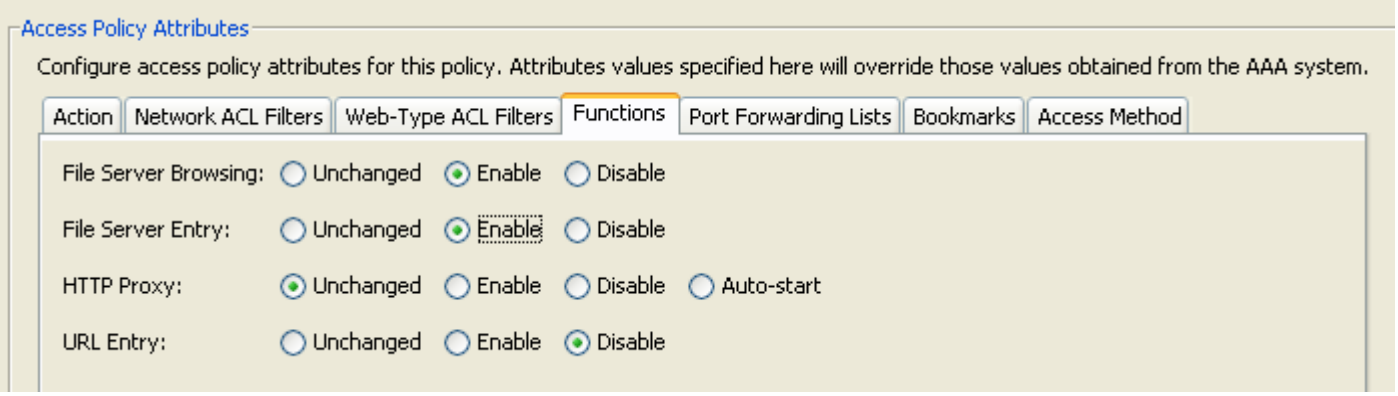
Onglet de filtres d'ACL de Web-type du schéma 10. — Vous permet de sélectionner et configurer le Web-type ACLs pour s'appliquer à cet enregistrement DAP. Un ACL pour DAP peut contenir seulement l'autorisation ou refuser des règles. Si un ACL contient l'autorisation et refuse des règles, les dispositifs de sécurité rejettent la configuration d'ACL.



- Liste déroulante d'ACL de Web-type — Sélectionnez le Web-type déjà configuré ACLs pour ajouter à cet enregistrement DAP. Seulement ACLs ayant toute l'autorisation ou tous refusent des règles sont éligibles, et ce sont le seul ACLs qui affichent ici.
- Gérez… — Cliquez sur pour ajouter, éditer, et supprimer le Web-type ACLs.

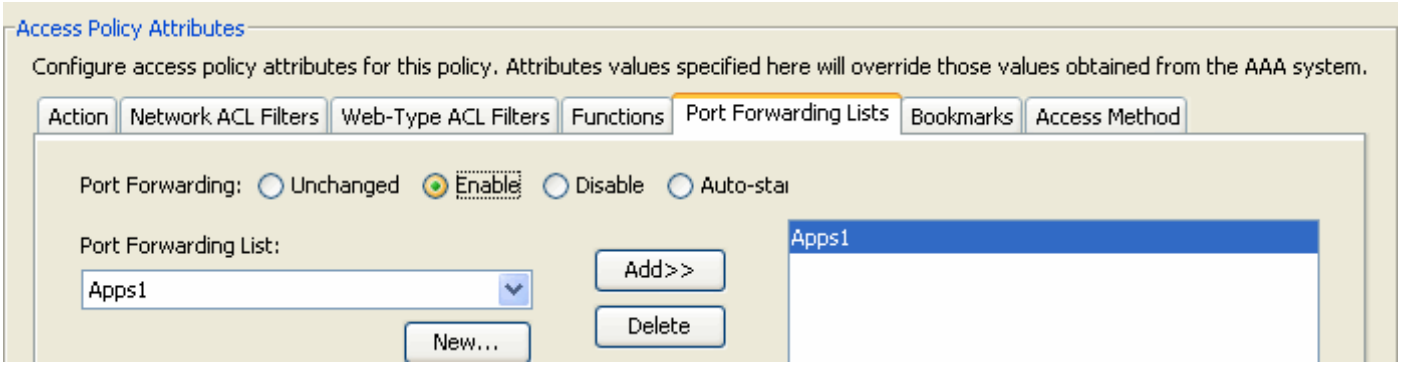
- Liste d'ACL de Web-type — Affiche le Web-type ACLs pour cet enregistrement DAP.
- Ajoutez — Cliquez sur pour ajouter l'ACL sélectionné de Web-type de la liste déroulante à la liste d'ACLs de Web-type du côté droit.
- Effacement — Clic pour supprimer un ACL de Web-type de la liste d'ACLs de Web-type. Vous ne pouvez pas supprimer un ACL s'il est assigné à un DAP ou à autre enregistrement.

Onglet de fonctions du schéma 11. — Vous permet de configurer l'entrée et furetage de serveur de fichiers, le proxy HTTP, et l'entrée URL pour l'enregistrement DAP.



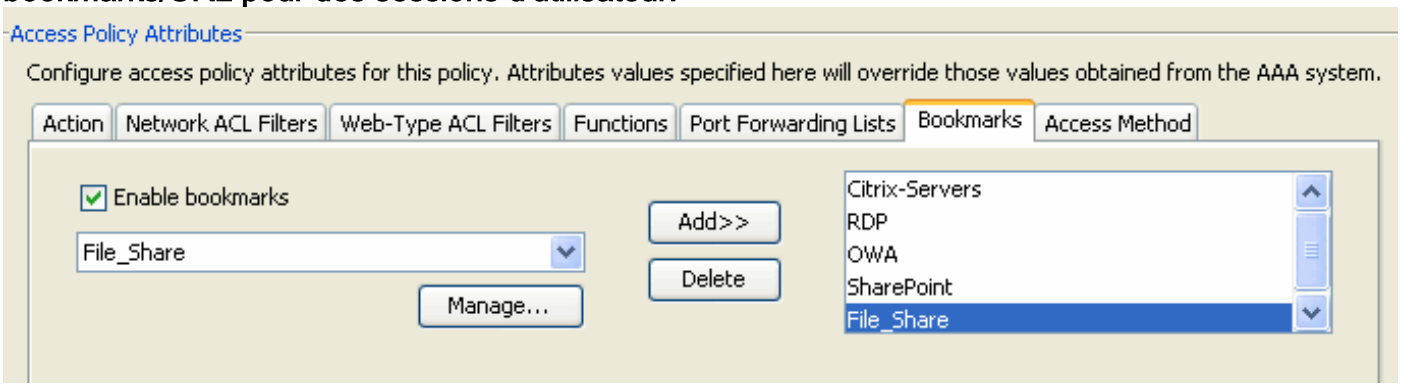
- Serveur de fichiers parcourant — Enables ou protocole CIFS de débronchements recherchant des serveurs de fichiers ou des caractéristiques de partage.
- Entrée de serveur de fichiers — Permet ou refuse un utilisateur d'écrire des chemins et des noms de serveur de fichiers sur la page du portail. Une fois activé, place le tiroir d'entrée de serveur de fichiers sur la page du portail. Les utilisateurs peuvent écrire des noms de chemin aux fichiers Windows directement. Ils peuvent télécharger, éditer, supprimer, renommer, et déplacer des fichiers. Ils peuvent également ajouter des fichiers et dossiers. Des partages doivent également être configurés pour l'accès client sur les serveurs applicables de Microsoft Windows. Des utilisateurs pourraient devoir être authentifiés avant d'accéder à des fichiers, selon des spécifications du réseau.
- Proxy HTTP — Affecte l'expédition d'un proxy d'applet de HTTP au client. Le proxy est utile pour les Technologies qui gênent la transformation satisfaite appropriée, telle que Javas, ActiveX, et éclair. Il saute mutiler/processus de réécriture tout en assurant l'utilisation continue des dispositifs de sécurité. Le proxy expédié modifie la vieille configuration de proxy du navigateur automatiquement et réoriente toutes les demandes de HTTP et HTTPS à la nouvelle configuration de proxy. Il prend en charge pratiquement toutes les Technologies de côté client, y compris le HTML, le CSS, le Javascript, le VBScript, l'ActiveX, et Javas. Le seul navigateur qu'il le prend en charge est Microsoft Internet Explorer.
- Entrée URL — Permet ou empêche un utilisateur d'écrire HTTP/HTTPS URLs sur la page du portail. Si cette caractéristique est activée, les utilisateurs peuvent introduire des adresses Web dans la case d'entrée URL, et emploient le VPN SSL sans client pour accéder à ces sites Web.
- Sans changement — (par défaut) cliquez sur pour utiliser des valeurs de la stratégie de groupe qui s'applique à cette session.
- Enable/disable — Cliquez sur pour activer ou désactiver la caractéristique.
- Démarrage automatique — Clic pour activer le proxy HTTP et pour faire commencer l'enregistrement DAP automatiquement les applet associés avec ces configurations.

Figure 12. Onglet de listes de transmission du port — Vous permet de sélectionner et configurer des listes de transmission du port pour des sessions d'utilisateur.



- Transmission du port — Sélectionnez une option pour les listes de transmission du port qui s'appliquent à cet enregistrement DAP. Les autres attributs dans ce domaine sont activés seulement quand vous placez la transmission du port pour activer ou le démarrage automatique.
- Sans changement — Cliquez sur pour utiliser des valeurs de la stratégie de groupe qui s'applique à cette session.
- Enable/disable — Clic pour activer ou désactiver la transmission du port.
- Démarrage automatique — Le clic pour activer la transmission du port, et pour faire commencer l'enregistrement DAP automatiquement les applet de transmission du port associés avec sa transmission du port le répertorie.
- Liste déroulante de liste de transmission du port — Sélectionnez les listes déjà configurées de transmission du port pour ajouter à l'enregistrement DAP.
- Nouveau — Cliquez sur pour configurer de nouvelles listes de transmission du port.
- Listes de transmission du port — Affiche la liste de transmission du port pour l'enregistrement DAP.
- Ajoutez — Cliquez sur pour ajouter la liste sélectionnée de transmission du port de la liste déroulante à la liste de transmission du port du côté droit.
- Effacement — Clic pour supprimer la liste sélectionnée de transmission du port de la liste de transmission du port. Vous ne pouvez pas supprimer un ACL s'il est assigné à un DAP ou à autre enregistrement.

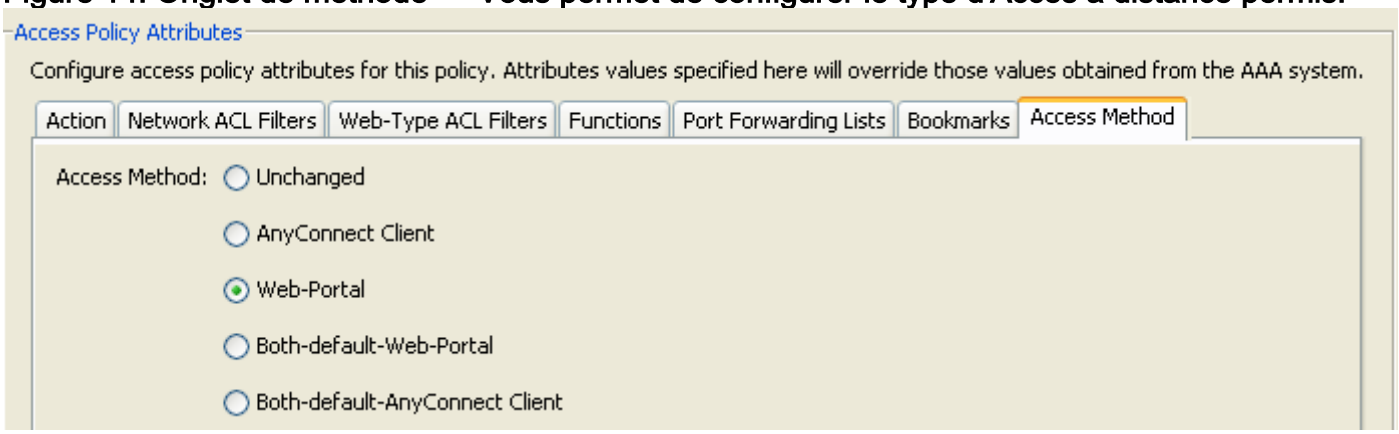
Figure 13. Onglet de signets — Vous permet de sélectionner et configurer des listes bookmarks/URL pour des sessions d'utilisateur.



- Signets d'enable — Clic à activer. quand cette case n'est pas sélectionnée, aucun affichage de listes de signet sur la page du portail pour la connexion
- Gérez — Cliquez sur pour ajouter, importer, exporter, et supprimer des listes de signet.
- Listes de signets (déroulant) — Affiche les listes de signet pour l'enregistrement DAP.
- Ajoutez — Cliquez sur pour ajouter la liste sélectionnée de signet de la liste déroulante à la liste déroulante de signet du côté droit.

- Effacement — Clic pour supprimer la liste sélectionnée de signet de la liste déroulante de signet. Vous ne pouvez pas supprimer une liste de signet des dispositifs de sécurité à moins que vous les supprimiez d'abord des enregistrements DAP.

Figure 14. Onglet de méthode — Vous permet de configurer le type d'Accès à distance permis.



- Sans changement — Continuez la méthode en cours d'Accès à distance réglée dans la stratégie de groupe pour la session.
- Client d'AnyConnect — Connectez utilisant le Cisco AnyConnect VPN Client.
- Portail web — Connectez au VPN sans client.
- Les Deux-par défaut-Web-portail — Connectez par l'intermédiaire de sans client ou du client d'AnyConnect, à un par défaut de sans client.
- client de Les deux-par défaut-AnyConnect — Connectez par l'intermédiaire de sans client ou du client d'AnyConnect, à un par défaut d'AnyConnect.

Comme mentionné précédemment, un enregistrement DAP a un ensemble limité de valeurs d'attribut par défaut, seulement s'ils sont modifiés ils auront la priorité au-dessus de l'AAA, de l'utilisateur, du groupe, du groupe de tunnel, et des enregistrements de groupe par défaut existants. Si des valeurs d'attribut supplémentaires hors de portée de DAP est exigées, par exemple, des listes de Segmentation de tunnel, des bannières, les tunnels intelligents, des personnalisations portailes,… etc., devront alors être imposées par l'intermédiaire de l'AAA, de l'utilisateur, du groupe, du groupe de tunnel, et des enregistrements de groupe par défaut. Dans ce cas, ces valeurs d'attribut spécifiques compléteront DAP et ne l'ignoreront pas. Ainsi, l'utilisateur obtiendra un ensemble cumulatif de valeurs d'attribut à travers tous les enregistrements.

Agréger plusieurs Dynamic Access Policies

Un administrateur peut configurer des enregistrements du multiple DAP pour adresser beaucoup de variables. En conséquence, il est possible que un utilisateur authentifiant réponde à l'AAA et aux critères d'attribut de point final des enregistrements du multiple DAP. En conséquence, les attributs de stratégie d'Access seront cohérents ou seront en conflit dans toutes ces stratégies. Dans ce cas, l'utilisateur autorisé obtiendra le résultat cumulatif à travers tous les enregistrements appariés DAP.

Ceci inclut également de seules valeurs d'attribut imposées par l'intermédiaire de l'authentification, de l'autorisation, de l'utilisateur, du groupe, du groupe de tunnel, et des enregistrements de groupe par défaut. Le résultat cumulatif des attributs de stratégie d'Access crée la stratégie d'accès dynamique. Des exemples des attributs combinés de stratégie d'Access sont répertoriés dans les Tableaux ci-dessous. Ces exemples dépeignent les résultats de 3 enregistrements combinés DAP.

L'attribut d'action affiché dans le tableau 1 a une valeur qui est se terminent ou continuent. La valeur d'attribut agrégée sera se terminent si la valeur de terminaison est configurée dans les enregistrements sélectionnés l'uns des DAP et continuer si la valeur de continuation est configurée dans tous les enregistrements sélectionnés DAP.

Attribut d'action du tableau 1.

Nom d'attribut	DAP#1	DAP#2	DAP#3	DAP
Action (exemple 1)	continuez	continuez	continuez	continuez
Action (exemple 2)	Terminez	continuez	continuez	terminez

L'attribut d'utilisateur-message affiché dans le tableau 2 contient une valeur de chaîne. La valeur d'attribut agrégée sera une chaîne séparée de retour à la ligne (valeur hexadécimale 0x0A) créée en joignant ensemble les valeurs d'attribut des enregistrements sélectionnés DAP. La commande des valeurs d'attribut dans la chaîne combinée est non significative.

Attribut d'Utilisateur-message du tableau 2.

Nom d'attribut	DAP#1	DAP#2	DAP#3	DAP
utilisateur-message	le rapide	renard brun	Accès plus de	les fox<LF>jumps de quick<LF>brown plus de

La caractéristique sans client activant des attributs (fonctions) affichés dans le tableau 3 contiennent les valeurs qui sont démarrage automatique, activent ou désactivent. La valeur d'attribut agrégée sera démarrage automatique si la valeur de démarrage automatique est configurée dans les enregistrements sélectionnés l'uns des DAP.

La valeur d'attribut agrégée sera enable s'il n'y a aucune valeur de démarrage automatique configurée dans les enregistrements sélectionnés l'uns des DAP, et la valeur d'enable est configurée dans au moins un des enregistrements sélectionnés DAP.

La valeur d'attribut agrégée sera débronchement s'il n'y a aucune valeur de démarrage automatique ou d'enable configurée dans les enregistrements sélectionnés l'uns des DAP, et la valeur de « débronchement » est configurée dans au moins un des enregistrements sélectionnés DAP.

Caractéristique sans client du tableau 3. activant des attributs (fonctions)

Nom d'attribut	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable	débronchement		enable
FILE-furetage	débronchement	enable	débronchement	enable

entrée de fichier			débronchement	débronchement
proxy HTTP	débronchement	démarrage automatique	débronchement	démarrage automatique
URL-entrée	débronchement		enable	enable

L'url-list et le port-forward attribue affiché dans le tableau 4 contiennent une valeur qui est une chaîne ou une chaîne séparée par virgule. La valeur d'attribut agrégée sera une chaîne séparée par virgule créée en joignant ensemble les valeurs d'attribut des enregistrements sélectionnés DAP. Valeur d'attribut en double dans la chaîne combinée en seront retirés. La commande des valeurs d'attributs dans la chaîne combinée est non significative.

Liste URL du tableau 4. et attribut en avant de liste de port

Nom d'attribut	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

Les attributs de méthode d'accès spécifie la méthode d'accès client permise pour des connexions de VPN SSL. La méthode d'accès client peut être accès client d'AnyConnect seulement, de portail web d'accès accès seulement, de client d'AnyConnect ou de portail web avec l'accès de portail web comme accès de par défaut ou de client ou de portail web d'AnyConnect avec l'accès client d'AnyConnect comme par défaut. La valeur d'attribut agrégée est récapitulée dans le tableau 5.

Attributs de méthode d'accès du tableau 5.

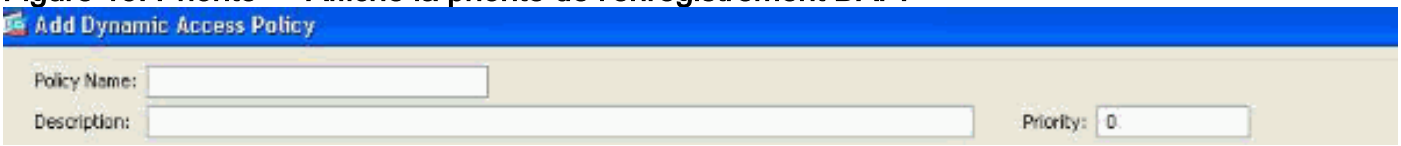
Valeurs d'attribut sélectionnées				Résultat d'agrégation
Client d'AnyConnect	Portail web	Portail de Les deux-par défaut-Web	client de Les deux-par défaut-AnyConnect	
			X	client de Les deux-par défaut-AnyConnect
		X		Les Deux-par défaut-Web-portail
		X	X	Les Deux-par défaut-Web-portail
	X			Portail web
	X		X	client de Les deux-par défaut-AnyConnect

	X	X		Les Deux-par défaut-Web-portail
	X	X	X	Les Deux-par défaut-Web-portail
X				Client d'AnyConnect
X			X	client de Les deux-par défaut-AnyConnect
X		X		Les Deux-par défaut-Web-portail
X		X	X	Les Deux-par défaut-Web-portail
X	X			Les Deux-par défaut-Web-portail
X	X		X	client de Les deux-par défaut-AnyConnect
X	X	X		Les Deux-par défaut-Web-portail
X	X	X	X	Les Deux-par défaut-Web-portail

En agrégeant des attributs (sans client) de filtre d'ACL de réseau (Pare-feu) et de Web-type, la priorité DAP et l'ACL DAP soyez deux composants importants à considérer.

La prise en compte de la priorité d'exécution suivant les indications de la figure 15 n'est pas agrégée. Les dispositifs de sécurité emploient cette valeur pour ordonnancer logiquement les Listes d'accès en agrégeant le réseau et le Web-type ACLs des enregistrements du multiple DAP. Les dispositifs de sécurité commandent les enregistrements de plus élevé au plus bas numéro prioritaire, avec le plus bas au bas de la table. Par exemple, un enregistrement DAP avec une valeur de 4 a une haute priorité qu'un enregistrement avec une valeur de 2. Vous ne pouvez pas manuellement les trier.

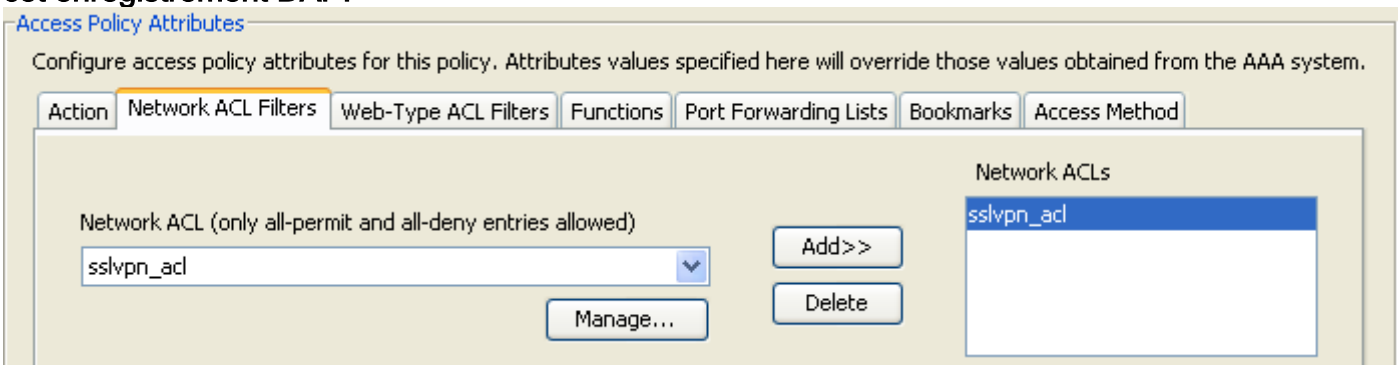
Figure 15. Priorité — Affiche la priorité de l'enregistrement DAP.



- Nom de stratégie — Affiche le nom de l'enregistrement DAP.
- Description — Décrit le but de l'enregistrement DAP.

L'attribut d'ACL DAP prend en charge seulement les Listes d'accès qui se conforment à « Blanc-liste » ou à un modèle strict stricte d'ACL de « liste noire ». Dans un modèle d'ACL de « Blanc-liste », les entrées de liste d'accès spécifient les règles que « permettez » à accès aux réseaux spécifiés ou aux hôtes. En mode d'ACL de « liste noire », les entrées de liste d'accès spécifient les règles que « refusez » à accès aux réseaux spécifiés ou aux hôtes. Une liste d'accès non conforme contient des entrées de liste d'accès avec une combinaison de « autorisation » et « refusez » les règles. Si une liste d'accès non conforme est configurée pour un enregistrement DAP, elle sera rejetée comme erreur de configuration quand les essais d'administrateur pour ajouter l'enregistrement. Si une liste d'accès de conformation est assignée à un enregistrement DAP, alors n'importe quelle modification à la liste d'accès qui change la caractéristique de conformité sera rejetée comme erreur de configuration.

Figure 16. ACL DAP — Permet vous de sélectionner et la configure network ACLs à s'appliquer à cet enregistrement DAP.



Quand des enregistrements du multiple DAP sont sélectionnés, les attributs de Listes d'accès spécifiés dans l'ACL de réseau (Pare-feu) sont agrégés pour créer une liste d'accès dynamique pour l'ACL de Pare-feu DAP. De la même manière, les attributs de Listes d'accès spécifiés dans l'ACL (sans client) de Web-type sont agrégés pour créer une liste d'accès dynamique pour l'ACL sans client DAP. L'exemple ci-dessous se concentrera sur la façon dont une liste d'accès dynamique de Pare-feu DAP est créée spécifiquement. Cependant, une liste d'accès sans client dynamique DAP suivra le même processus.

D'abord, l'ASA créera dynamiquement un nom unique pour le Réseau-ACL DAP suivant les indications du tableau 6.

Nom dynamique de Réseau-ACL du tableau 6. DAP

Nom de Réseau-ACL DAP
DAP-Réseau-ACL-x (où X est un entier qui incrémentera pour assurer l'unicité)

En second lieu, l'ASA récupèrera l'attribut de Réseau-ACL des enregistrements sélectionnés DAP suivant les indications du tableau 7.

Réseau ACLs du tableau 7.

Enregistrements sélectionnés DAP	Priorité	Réseau-ACLs	Entrées de Réseau-ACL
DAP 1	1	101 et 102	L'ACL 101 fait refuser 4 des règles et l'ACL 102 a 4 règles d'autorisation

DAP 2	2	201 et 202	L'ACL 201 a 3 règles d'autorisation et l'ACL 202 fait refuser 3 des règles
DAP 3	2	101 et 102	L'ACL 101 fait refuser 4 des règles et l'ACL 102 a 4 règles d'autorisation

Troisièmement, l'ASA commandera à nouveau le réseau-ACLs d'abord par le numéro prioritaire d'enregistrement DAP, et puis par la liste noire d'abord si la valeur prioritaire pour 2 enregistrements sélectionnés ou plus DAP sont les mêmes. Après ceci, l'ASA récupèrera alors les entrées de Réseau-ACL de chaque Réseau-ACL suivant les indications du tableau 8.

Priorité d'enregistrement du tableau 8. DAP

Réseau-ACLs	Priorité	Modèle blanc/de noir liste d'accès	Entrées de Réseau-ACL
101	2	Liste noire	4 refusez les règles (DDDD)
202	2	Liste noire	3 refusez les règles (le DDD)
102	2	Blanc-liste	4 règles d'autorisation (PPPP)
202	2	Blanc-liste	3 règles d'autorisation (PPP)
101	1	Liste noire	4 refusez les règles (DDDD)
102	1	Blanc-liste	4 règles d'autorisation (PPPP)

Pour finir, l'ASA fusionnera les entrées de Réseau-ACL dans le Réseau-ACL dynamiquement généré et puis renverra le nom du Réseau-ACL dynamique comme nouvel Réseau-ACL à imposer suivant les indications du tableau 9.

Réseau-ACL dynamique du tableau 9. DAP

Nom de Réseau-ACL DAP	Entrée de Réseau-ACL
DAP-Network-ACL-1	PPP DDDD PPPP DU DDD PPPP DDDD

Implémentation DAP

Il y a une foule de raisons pour lesquelles un administrateur devrait envisager de mettre en application DAP. Quelques raisons sous-jacentes sont quand l'estimation de posture sur un point final doit être imposée, et/ou quand un AAA ou des attributs plus granulaires de stratégie doivent être considérés quand autorisant l'accès client aux ressources de réseau. Dans l'exemple ci-

dessous, nous configurerons DAP et ses composants pour identifier un point final se connectant et pour autoriser l'accès client à de diverses ressources de réseau.

Cas de test – Un client a demandé un Preuve-de-concept avec les conditions requises suivantes d'accès VPN :

- La capacité de détecter et identifier un point final des employés comme géré ou non pris en charge. — Si le point final est identifié en tant que géré (PC de travail) mais échoue les conditions requises de posture, ce point final doit alors être refusé l'accès. D'autre part, si le point final des employés est identifié comme non pris en charge (pc home), on doit alors accorder ce point final l'accès sans client.
- La capacité d'appeler le nettoyage des Témoins et du cache de session quand une connexion sans client se termine.
- La capacité de détecter et imposer des applications en cours d'exécution sur les points finaux des employés gérés, tels que l'antivirus de McAfee. Si l'application n'existe pas, ce point final doit alors être refusé Access.
- La capacité d'employer l'authentification d'AAA pour déterminer à quels utilisateurs autorisés de ressources de réseau devrait avoir accès. Les dispositifs de sécurité doivent prendre en charge l'authentification LDAP indigène de MS et prendre en charge de plusieurs rôles d'adhésion à des associations de LDAP.
- La capacité de permettre l'accès local au LAN aux ressources de réseau telles que des télécopies et des imprimantes de réseau une fois connectée par l'intermédiaire d'un « client/de réseau » a basé la connexion.
- La capacité de fournir a autorisé l'accès invité aux sous-traitants. Les sous-traitants et leurs points finaux doivent obtenir l'accès sans client, et leur accès portail aux applications doit limité par rapport à un employé.

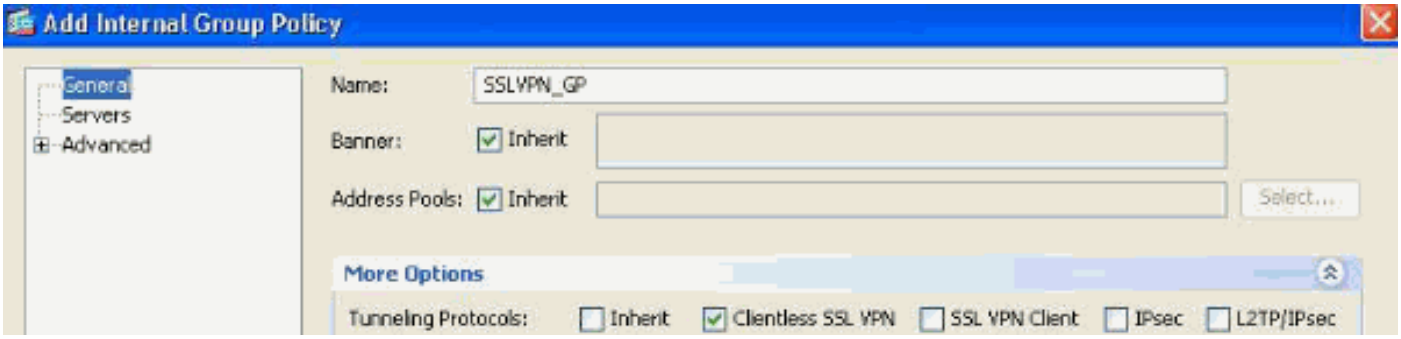
Dans cet exemple, nous exécuterons une gamme d'étapes de configuration dans un effort de répondre aux exigences de l'accès VPN du client. Il y aura des étapes de configuration qui sont nécessaires mais pas directement associées à DAP tandis que d'autres configurations seront directement liées à DAP. L'ASA est très dynamique et peut s'adapter dans beaucoup d'environnements de réseau. En conséquence, des solutions VPN peuvent être définies dans diverses manières et fournir dans certains cas la même chose finissez la solution. L'approche adoptée cependant est pilotée par les besoins et leurs environnements des clients.

Basé sur la nature de ce document et des exigences de client définies, nous utiliserons Adaptive Security Device Manager (ASDM) 6.0(x) et focaliserons la plupart de nos configurations autour de DAP. Cependant, nous configurerons également des stratégies de groupe locales pour afficher comment DAP peut compléter et/ou ignorer des attributs locaux de stratégie. Pour la base de ce cas de test, nous assumerons un groupe de serveur LDAP, liste des réseaux de Segmentation de tunnel et la connectivité IP de base, y compris les groupes IP et le groupe de serveurs de DefaultDNS, sont préconfigurées.

Définissant une stratégie de groupe — cette configuration est nécessaire pour définir des attributs locaux de stratégie. Quelques attributs définis ici ne sont pas configurables dans DAP pour (exemple, accès local au LAN). (Cette stratégie sera également utilisée pour définir des attributs sans client et par client basés).

Naviguez vers le **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, et ajoutez une stratégie de groupe interne en faisant ce qui suit :

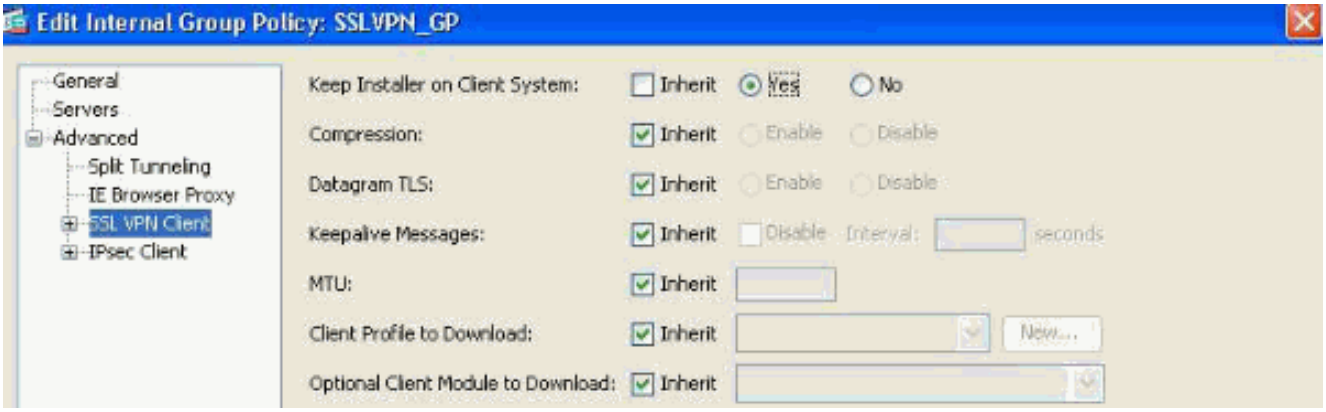
Figure 17. Stratégie de groupe — Définit des attributs spécifiques locaux VPN.



1. Sous le lien général, configurez le nom **SSLVPN_GP** pour la stratégie de groupe.
2. Également sous le lien général, cliquez sur **plus d'options** et configurez seulement le perçage d'un tunnel Protocol : **SSLVPN sans client**. (Nous configurerons DAP pour ignorer et gérer la méthode d'accès.)
3. Sous l'avancé > le lien de Segmentation de tunnel, configurent ce qui suit :**Figure 18. Segmentation de tunnel — Permet au trafic indiqué (réseau local) pour sauter un tunnel décrypté pendant une connexion client.**

Stratégie : Décochez **héritent** et choisi **excluez la liste des réseaux ci-dessous**.Liste des réseaux : Décochez **héritent** et sélectionnent du nom de liste **Local_Lan_Access**. (Assumé préconfiguré.)

4. Sous l'avancé > le lien de client de VPN SSL, configurent ce qui suit :**Figure 19. Installateur de client de VPN SSL — Sur l'arrêt VPN, le client SSL peut rester sur le point final ou être désinstallé.**



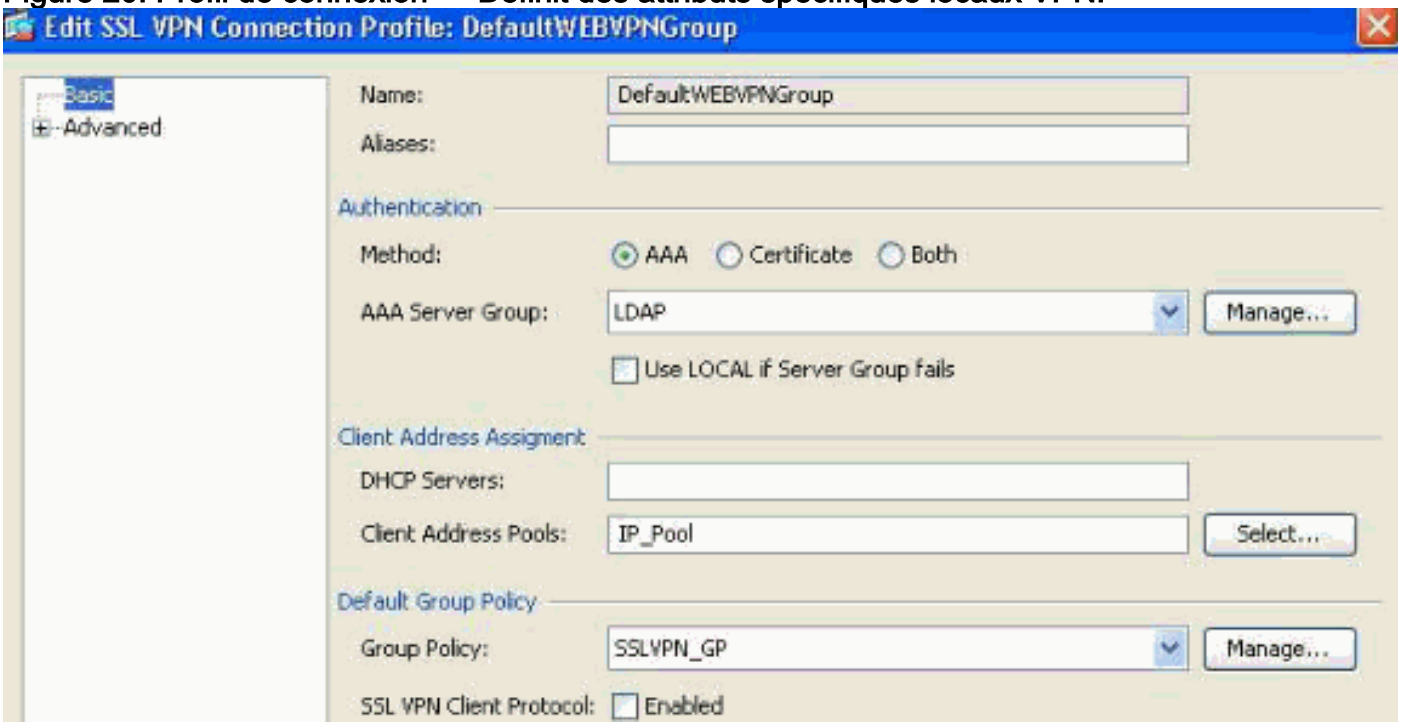
5. Keep Installer on Client System : Décochez **héritent** et sélectionnent alors **oui**.
6. Cliquez sur OK **s'appliquent** alors.
7. Appliquez vos modifications de configuration.

Définissant un profil de connexion — cette configuration est nécessaire pour définir notre méthode d'authentification d'AAA, par exemple LDAP et application de la stratégie de groupe précédemment configurée (SSLVPN_GP) à ce profil de connexion. Des utilisateurs se connectant

par l'intermédiaire de ce profil de connexion seront soumis aux attributs définis ici aussi bien qu'aux attributs définis dans la stratégie de groupe SSLVPN_GP. (Ce profil sera également utilisé pour définir des attributs sans client et par client basés).

Naviguez vers la **configuration > l'Accès à distance VPN > profils de connexion VPN d'Access >SSL de réseau (client)** et configurez ce qui suit :

Figure 20. Profil de connexion — Définit des attributs spécifiques locaux VPN.

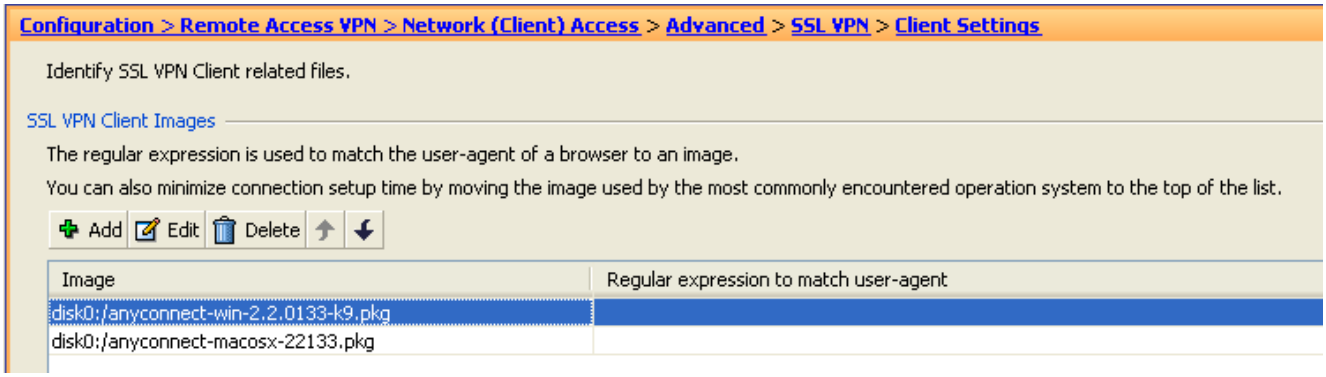


1. Sous la connexion les profils sectionnent, éditent le DefaultWEBVPNGroup et sous le lien de base configurez ce qui suit :Authentification — Méthode : **AAA**Authentification — Groupe de serveurs AAA : **LDAP** (assumé préconfiguré)Affectation d'adresse du client — Groupes d'adresse du client : **IP_Pool** (assumé préconfiguré)Stratégie de policy group de groupe par défaut : **SSLVPN_GP** choisi
2. Appliquez vos modifications de configurations.

Définissant une interface IP pour la Connectivité de VPN SSL — Cette configuration est nécessaire pour terminer le client et les connexions sans client SSL sur une interface spécifiée.

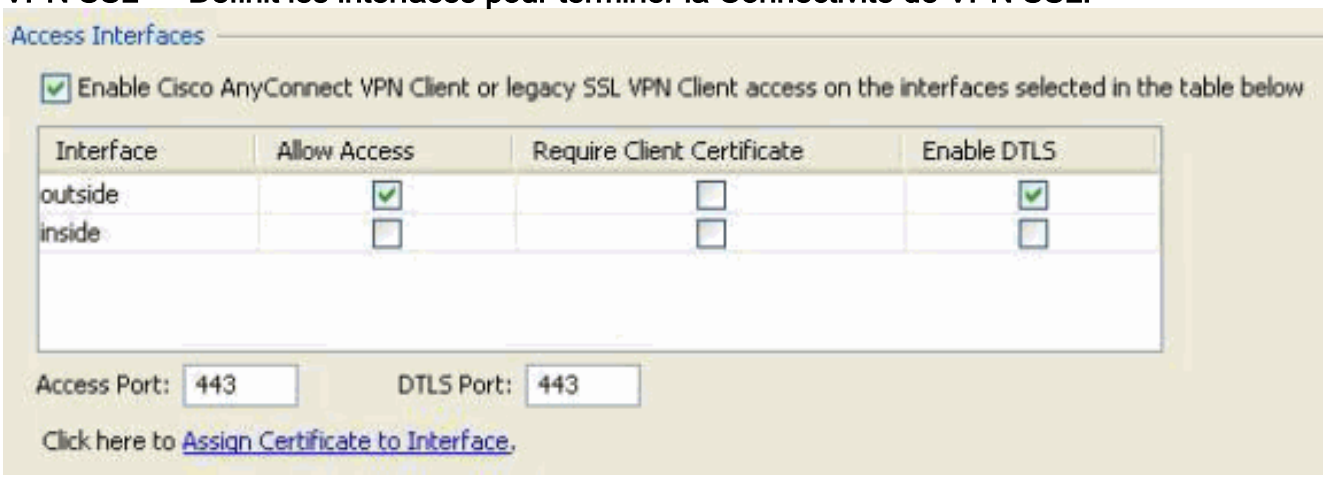
Avant d'activer le client/accès au réseau sur une interface, vous devez d'abord définir une image de client de VPN SSL.

1. Naviguez vers la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > des configurations de VPN SSL > de client**, et ajoute l'image suivante de client de VPN SSL du système de fichiers Flash ASA : (Cette image peut être téléchargée de CCO, www.cisco.com)**Figure 21. L'image de client de VPN SSL installent — Définit l'image de client SSLVPN (AnyConnect) à pousser aux points finaux se connectants.**



anyconnect-win-2.x.xxx-k9.pkg Cliquez sur OK, **APPROUVEZ** de nouveau, et **appliquez** alors.

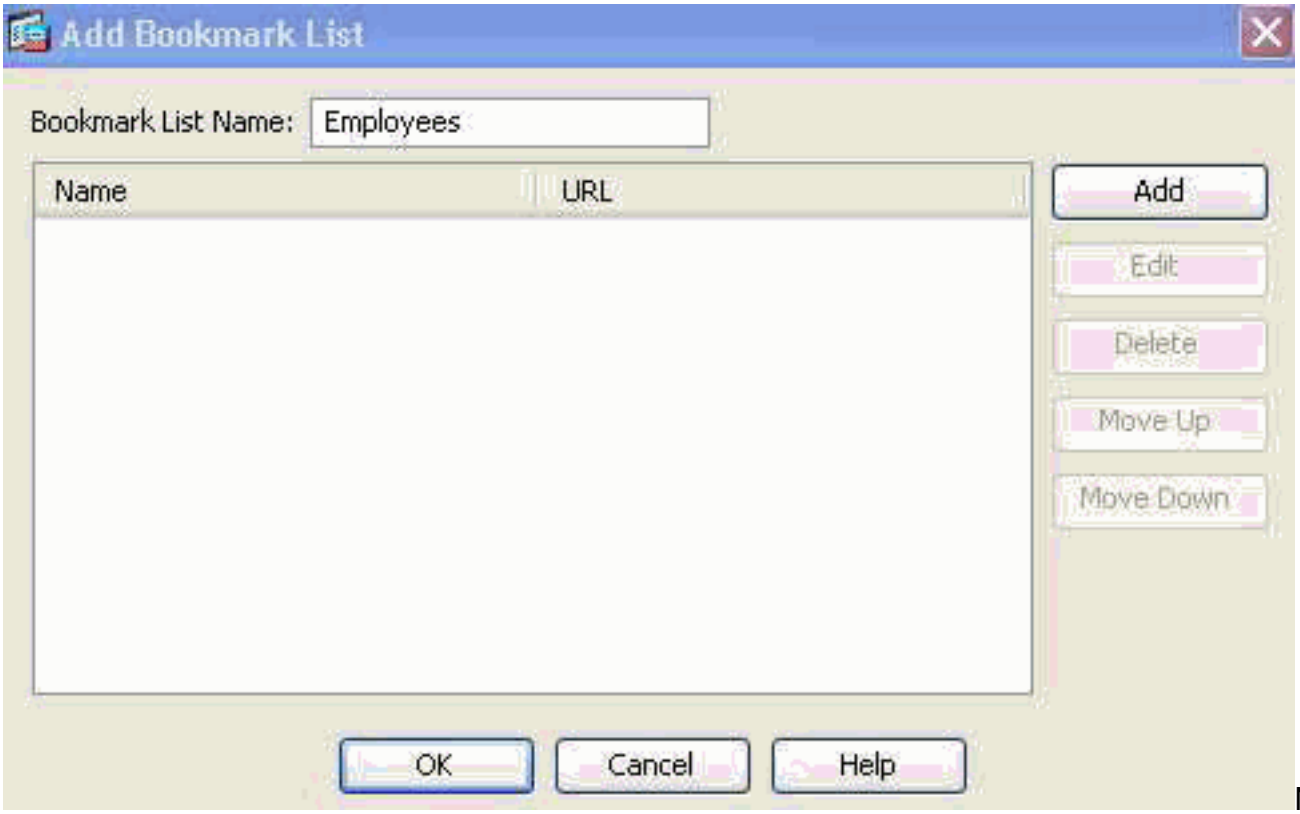
2. **Naviguez vers la configuration > l'Accès à distance VPN > réseau (client) Access > des profils de connexion de VPN SSL**, et activez ce qui suit :**Figure 22. Interface d'Access de VPN SSL — Définit les interfaces pour terminer la Connectivité de VPN SSL.**



Sous la section d'interface d'Access, enable : **« Activez l'accès client de VPN SSL de Cisco AnyConnect VPN Client ou de legs sur les interfaces sélectionnées dans la table ci-dessous. »**Également sous les interfaces d'Access sectionnez, contrôle **permettent Access** sur l'interface extérieure. (Cette configuration activera également l'accès sans client de VPN SSL sur l'interface extérieure.)Cliquez sur **Apply**.

Définissant le signet le répertorie (des listes URL) pour Access sans client — cette configuration est nécessaire pour définir une application basée sur le WEB à éditer sur le portail. Nous définirons 2 listes URL, une pour des employés et l'autre pour des sous-traitants.

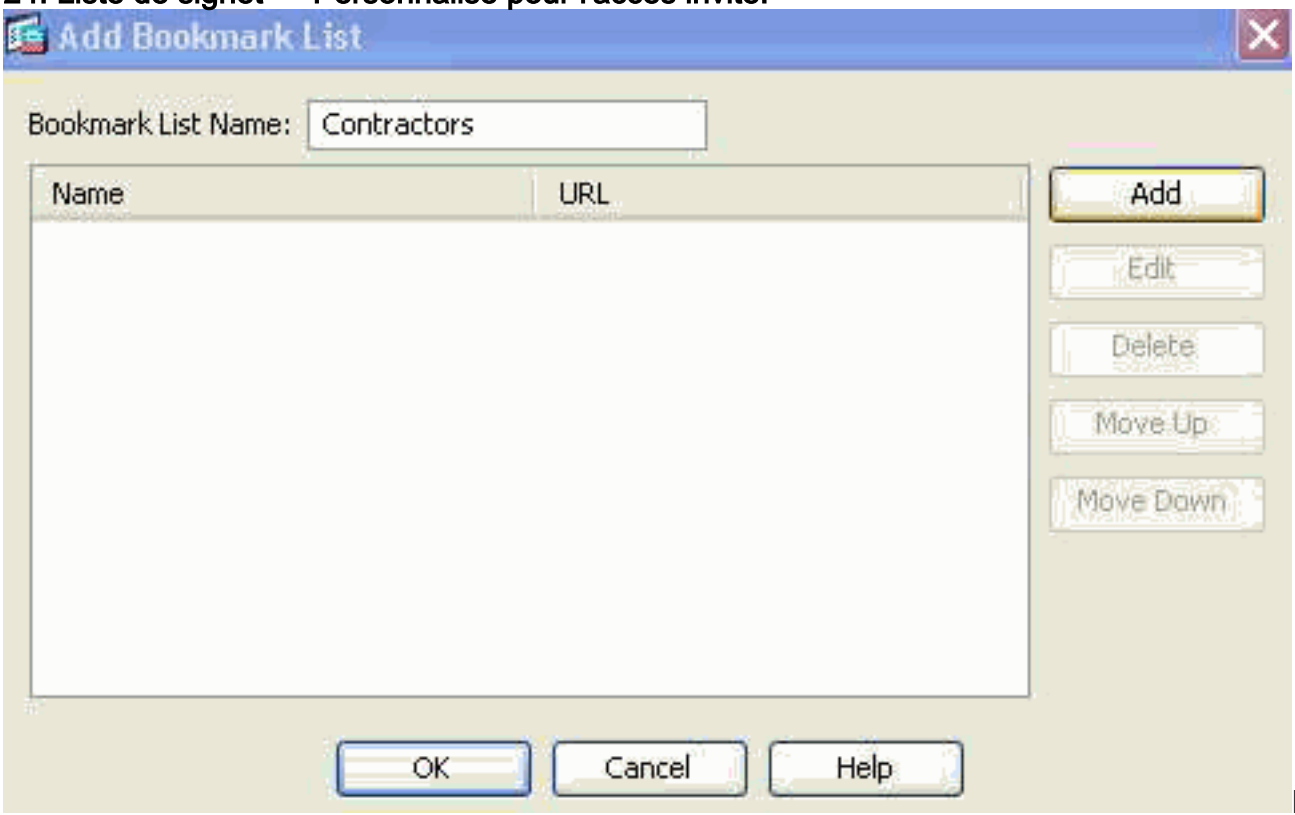
1. Naviguez vers la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > portail > signets**, le clic **+ ajoutent** et configurent ce qui suit :**Figure 23. Liste de signet — Définit l'URLs à éditer et être accédé à du portail web. (Personnalisé pour l'accès des employés).**



N

om de liste de signet : **Les employés**, cliquent sur Add alors.Titre de signet : **Intranet d'une entreprise**Valeur URL : **http://company.resource.com**Cliquez sur OK et **APPROUVEZ** alors de nouveau.

2. Le clic **+ ajoutent** et configurent une deuxième liste de signet (liste URL) comme suit :**Figure 24. Liste de signet — Personnalisé pour l'accès invité.**



N

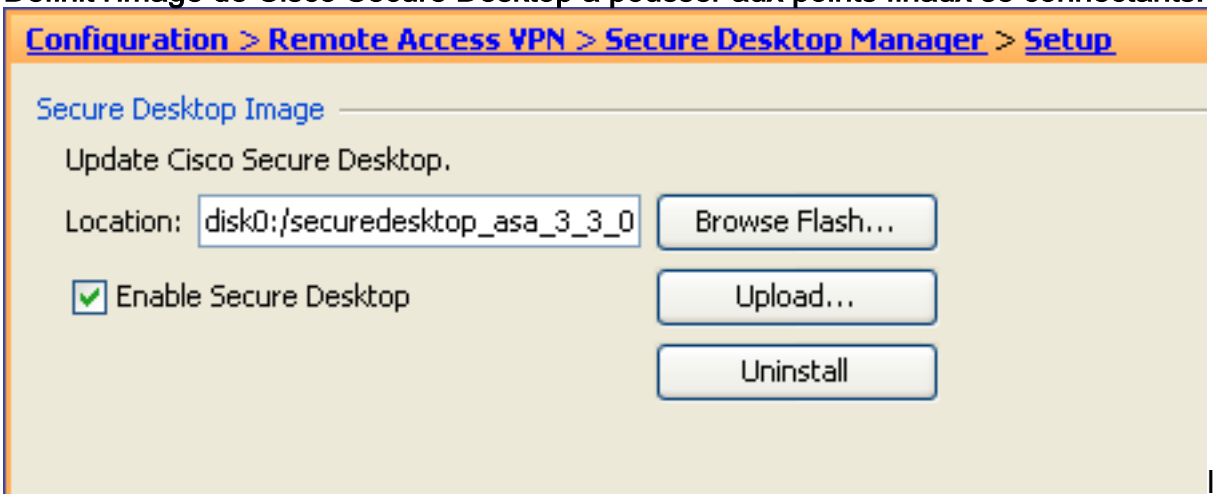
om de liste de signet : **Les sous-traitants**, cliquent sur Add alors.Titre de signet : **Accès invité**Valeur URL : **http://company.contractors.com**Cliquez sur OK et **APPROUVEZ** alors de nouveau.Cliquez sur **Apply**.

Cisco Secure Desktop — cette configuration est nécessaire pour définir des attributs d'estimation de point final. Basé sur les critères à satisfaire, des points finaux se connectants seront classifiés

comme géré ou non pris en charge. Des estimations de Cisco Secure Desktop sont exécutées avant la procédure d'authentification.

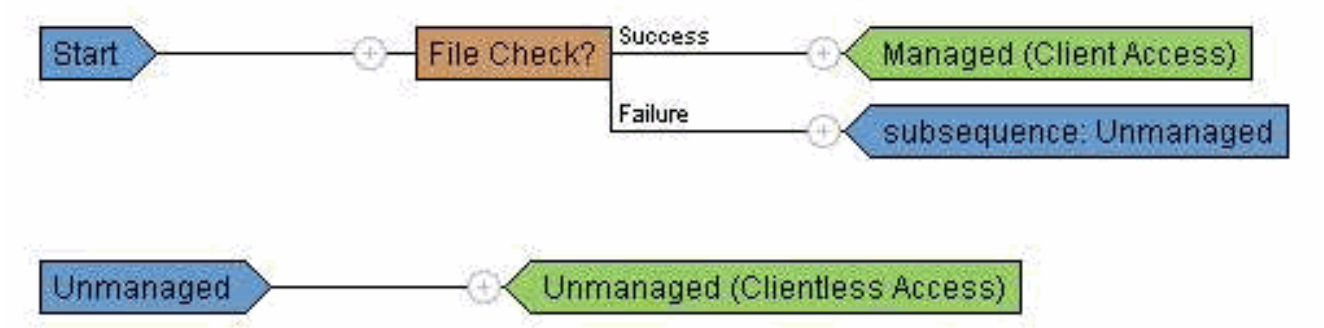
Configurer le Cisco Secure Desktop et pré une arborescence de décision de procédure de connexion pour des emplacements de Windows :

1. Naviguez vers la **configuration > l'Accès à distance VPN > gestionnaire de Secure Desktop > installé**, et configurez ce qui suit :**Figure 25. L'image de Cisco Secure Desktop installent — Définit l'image de Cisco Secure Desktop à pousser aux points finaux se connectants.**



Installez l'image **disk0:/securedesktop-asa-3.3.-xxx-k9.pkg du** système de fichiers Flash ASA.**Secure Desktop d'enable de** contrôle.Cliquez sur **Apply**.

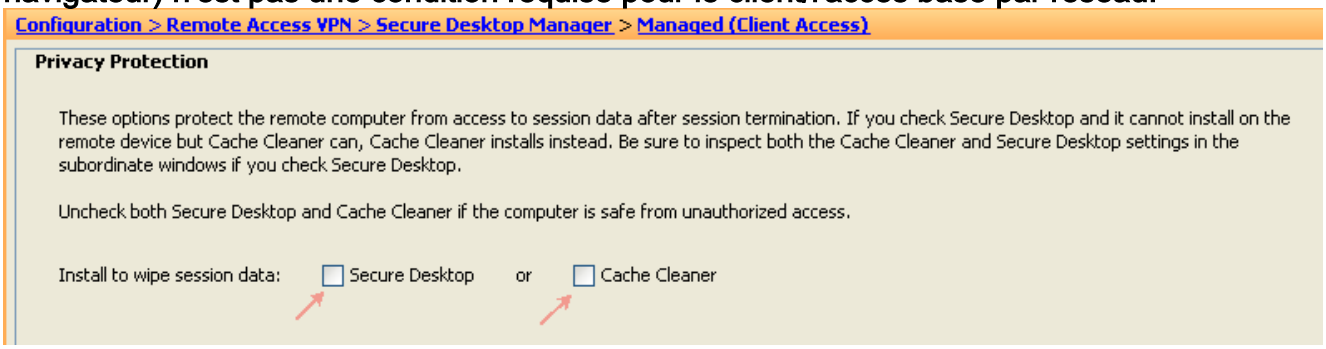
2. Naviguez vers la **configuration > l'Accès à distance VPN > gestionnaire de Secure Desktop > stratégie de Prelogin**, et configurez ce qui suit :**Figure 26. arborescence de décision de Pré-connexion — Personnalisé par l'intermédiaire du contrôle de fichier pour distinguer un point final géré et un point final de non pris en charge.**



Cliquez sur le noeud **par défaut** et renommez l'étiquette **gérée (accès client)** et puis cliquez sur la **mise à jour**.Cliquez sur « + » le symbole au début du noeud géré.Pour le contrôle, sélectionnez et ajoutez le **contrôle de fichier** à insérer.Entrez dans **C:\managed.txt** pour le chemin de fichier à « existe » et clique sur la **mise à jour**.Cliquez sur la **procédure de connexion a refusé le** noeud et puis sélectionne **Subsequence**.Entrez dans le **non pris en charge** pour l'étiquette et puis cliquez sur la **mise à jour**.Cliquez sur la **procédure de connexion a refusé le** noeud et puis sélectionne l'**emplacement**.Entrez dans le **non pris en charge (Access sans client)** pour l'étiquette et puis cliquez sur la **mise à jour**.Cliquez sur Apply **tous**.

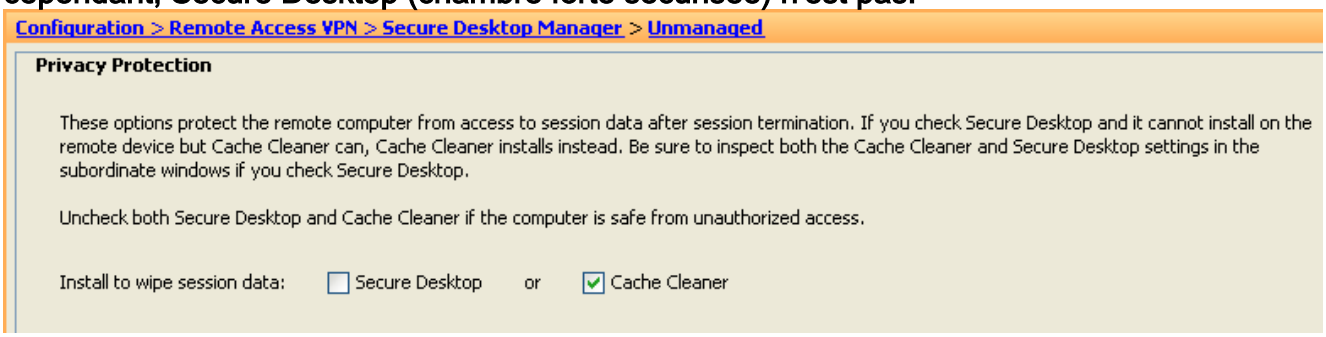
3. Naviguez vers la **configuration > l'Accès à distance VPN > gestionnaire de Secure Desktop >Managed (accès client)**, et configurez le suivant sous la section de configurations d'emplacement :**Figure 27. Configurations d'emplacement/protection de la vie privée — Le Secure Desktop (chambre forte sécurisée) et le décapant de cache (nettoyage de**

navigateur) n'est pas une condition requise pour le client/l'accès basé par réseau.



Module d'emplacement : Décochez le **Secure Desktop** et le **décapant de cache** si activé.Cliquez sur Apply **tous** si nécessaire.

4. Naviguez vers la **configuration > l'Accès à distance VPN > gestionnaire de Secure Desktop > non pris en charge (Access sans client)**, et configurez le suivant sous la section de configurations d'emplacement :**Figure 28. Configurations d'emplacement — Le décapant de cache (nettoyage de navigateur) est une condition requise pour l'accès basé sans client, cependant, Secure Desktop (chambre forte sécurisée) n'est pas.**

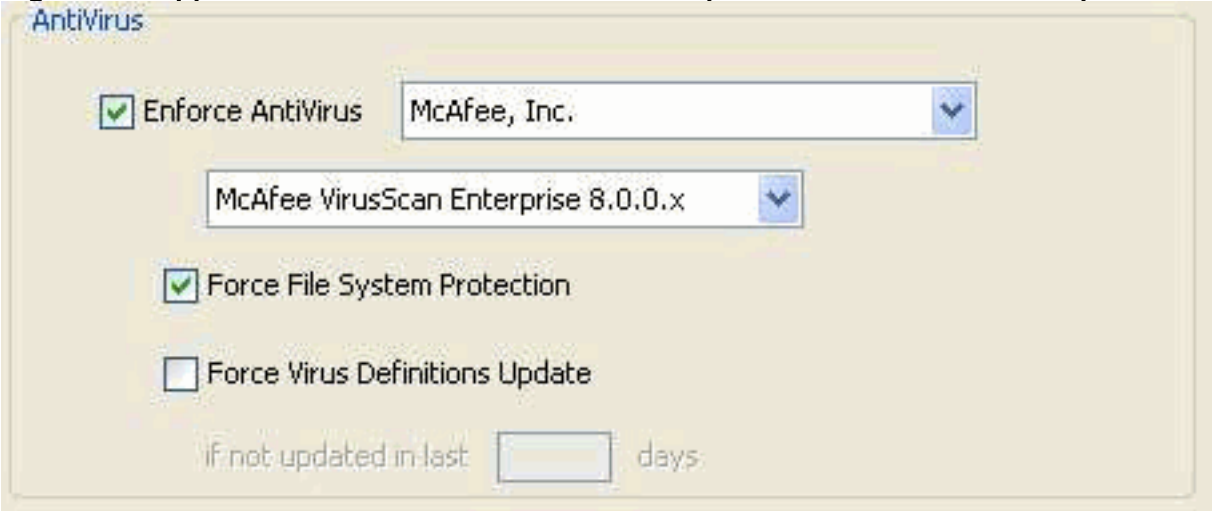


Module d'emplacement : Décochez le **Secure Desktop** et vérifiez le **décapant de cache**.Cliquez sur Apply **tous**.

Estimation avancée de point final — Cette configuration est nécessaire pour imposer l'antivirus, l'AntiSpyware et le pare-feu personnel sur un point final. Par exemple, cette estimation vérifiera si McAfee s'exécute sur le point final se connectant. (L'estimation avancée de point final est une caractéristique autorisée et n'est pas configurable si la caractéristique de Cisco Secure Desktop est désactivée).

Naviguez vers la **configuration > l'Accès à distance VPN > balayage de gestionnaire > d'hôte de Secure Desktop**, et configurez le suivant sous la section d'extensions de balayage d'hôte :

Figure 29. Application d'antivirus — Personnalisé pour le client/l'accès basé par réseau.



Sous l'hôte que les extensions de balayage sectionnent, configurent ce qui suit :

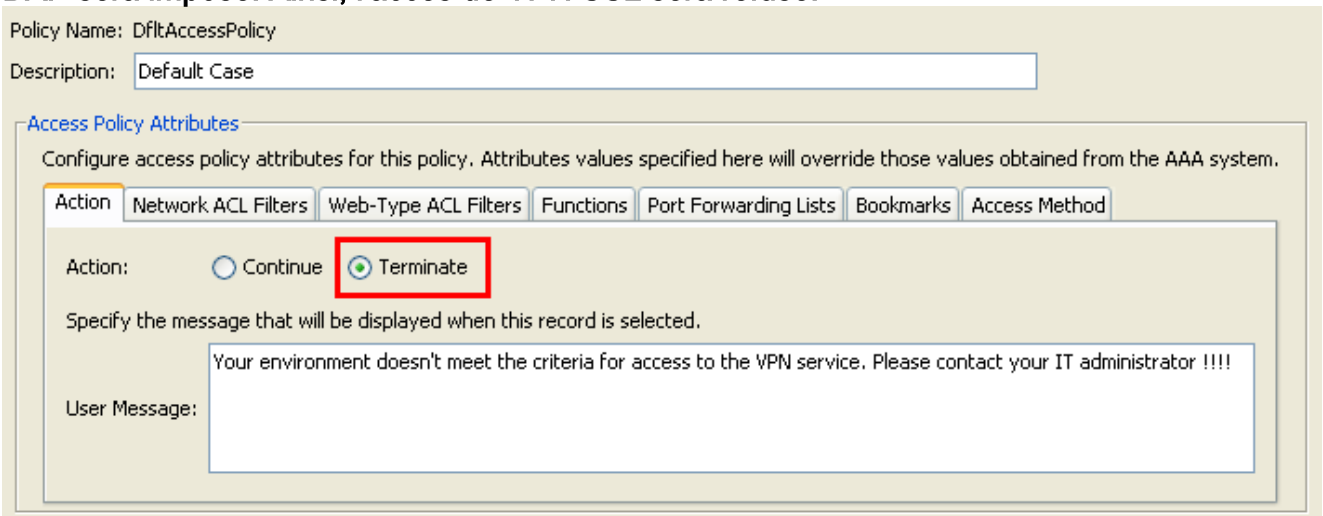
1. Sélectionnez le **ver avancé 2.3.3.1 d'estimation de point final** et puis **le configurez**.
2. Choisi **imposez l'antivirus**.
3. De la liste déroulante d'antivirus d'exécution, **McAfee, Inc.** choisi
4. **De l'entreprise** choisie **8.0.0.x de McAfee VirusScan de** liste déroulante de version d'antivirus.
5. Sélectionnez la **protection de système de fichiers de force** et puis cliquez sur Apply **tous**.

Dynamic Access Policies — Cette configuration est nécessaire pour valider les utilisateurs se connectants et leurs points finaux contre l'AAA et/ou les critères d'estimation définis de point final. Si les critères définis d'un enregistrement DAP sont satisfaits, on accordera des utilisateurs se connectants alors l'accès aux ressources de réseau qui sont associées avec celle enregistrement ou enregistrements DAP. L'autorisation DAP est exécutée pendant la procédure d'authentification.

Pour s'assurer qu'une connexion de VPN SSL se terminera dans le cas par défaut, par exemple quand le point final ne fait pas des stratégies d'accès dynamique configurées par match any), nous configurerons ce qui suit :

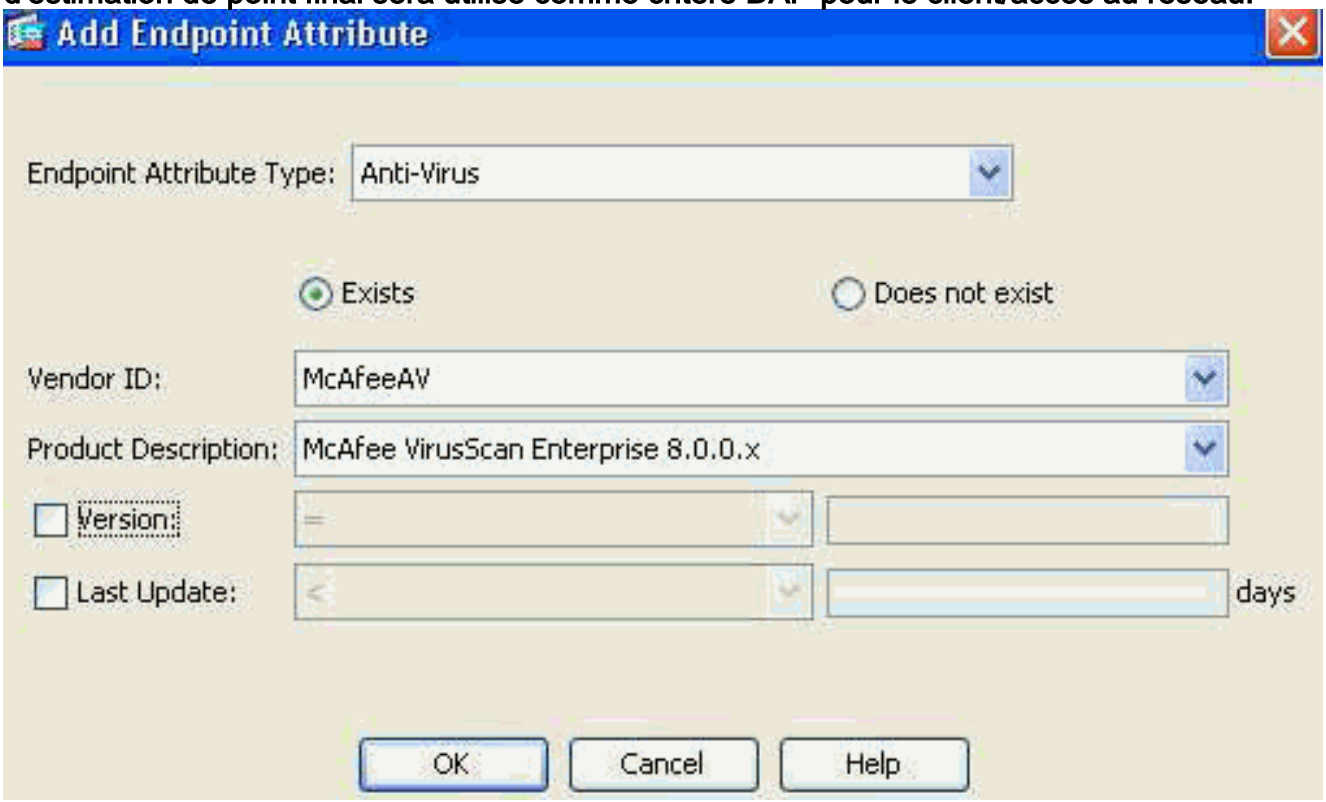
Remarque: En configurant Dynamic Access Policies pour la première fois, un message d'erreur DAP.xml est affiché indiquant qu'un fichier de configuration DAP (DAP.XML) n'existe pas. Une fois que votre configuration de l'initiale DAP est modifiée et puis enregistrée, ce message n'apparaîtra plus.

1. Naviguez vers la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > Dynamic Access Policies**, et configurez ce qui suit :**Figure 30. Stratégie par défaut d'accès dynamique — si aucun enregistrement des prédéfinis DAP n'est apparié, cet enregistrement DAP sera imposé. Ainsi, l'accès de VPN SSL sera refusé.**



   Éditez le **DfltAccessPolicy** et placez l'action **de se terminer**.Cliquez sur **OK**.
2. Ajoutez une nouvelle stratégie d'accès dynamique nommée **Managed_Endpoints**, comme suit :Description : **Accès client des employés**Ajoutez (situé à la droite du type d'attribut de point final) un type d'attribut de point final (stratégie) suivant les indications de la figure 31. Cliquez sur OK si complet.**Figure 31. Attribut de point final DAP — L'emplacement de Cisco Secure Desktop sera utilisé comme critère DAP pour le client/accès au réseau.**

Ajoutez un deuxième type d'attribut de point final (antivirus) suivant les indications de la figure 32. Cliquez sur OK si complet.**Figure 32. Attribut de point final DAP — L'antivirus avancé d'estimation de point final sera utilisé comme critère DAP pour le client/accès au réseau.**



De la liste déroulante au-dessus de la section d'aaa attribute, l'**utilisateur** choisi **a toutes les valeurs d'attributs suivantes d'AAA…**Ajoutez (situé à la droite de la case d'aaa attribute) un type d'aaa attribute (LDAP) suivant les indications de la figure 33 et de 34. Cliquez sur OK si complet.**Figure 33. Aaa attribute DAP — L'adhésion à des associations d'AAA sera utilisée comme critère DAP pour identifier un employé.**

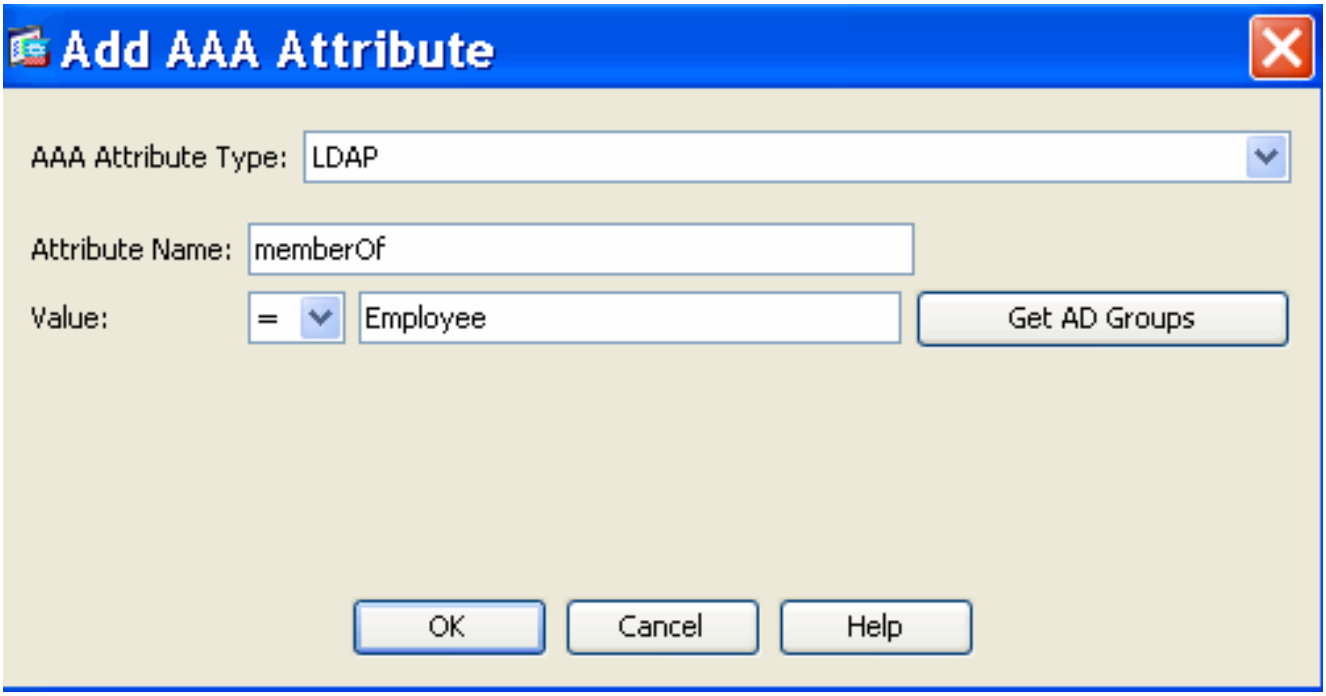
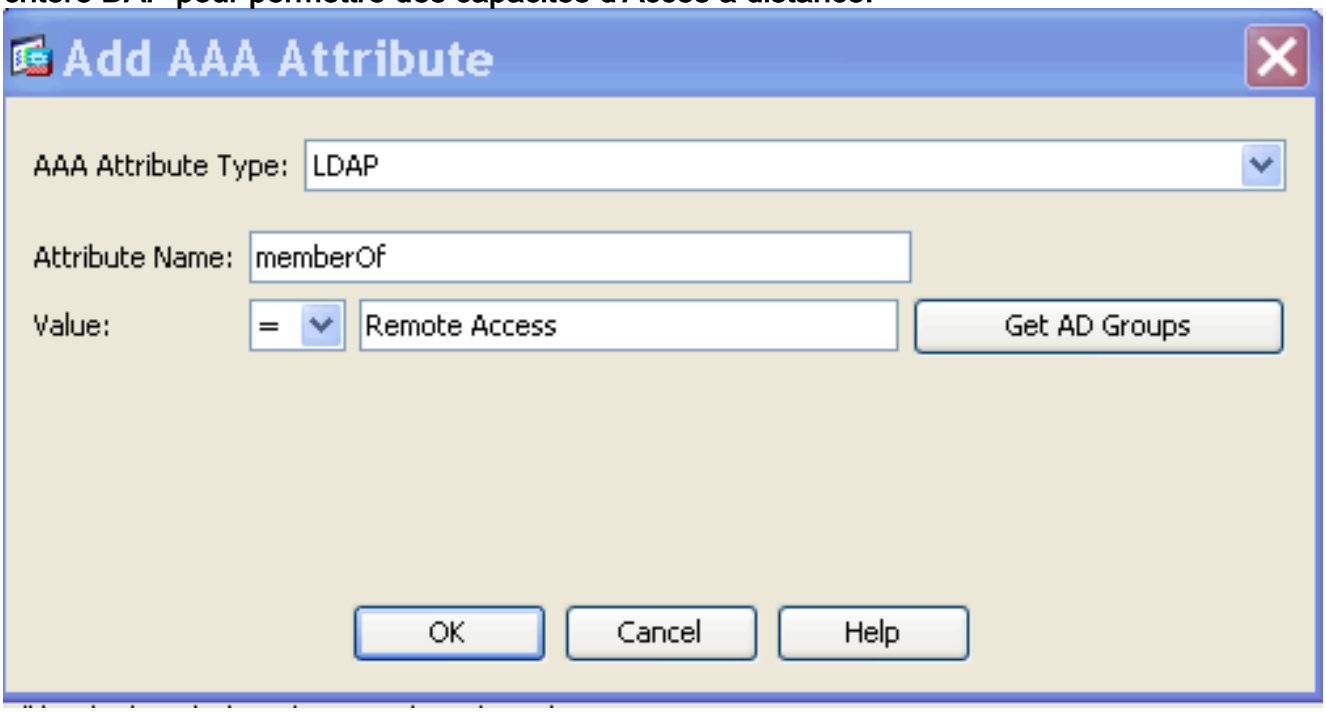
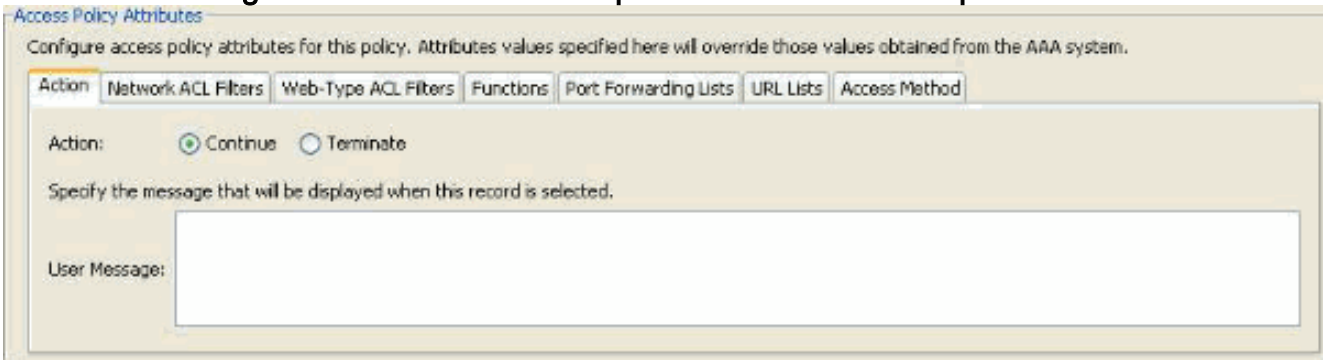


Figure 34. Aaa attribute DAP — L'adhésion à des associations d'AAA sera utilisée comme critère DAP pour permettre des capacités d'Accès à distance.

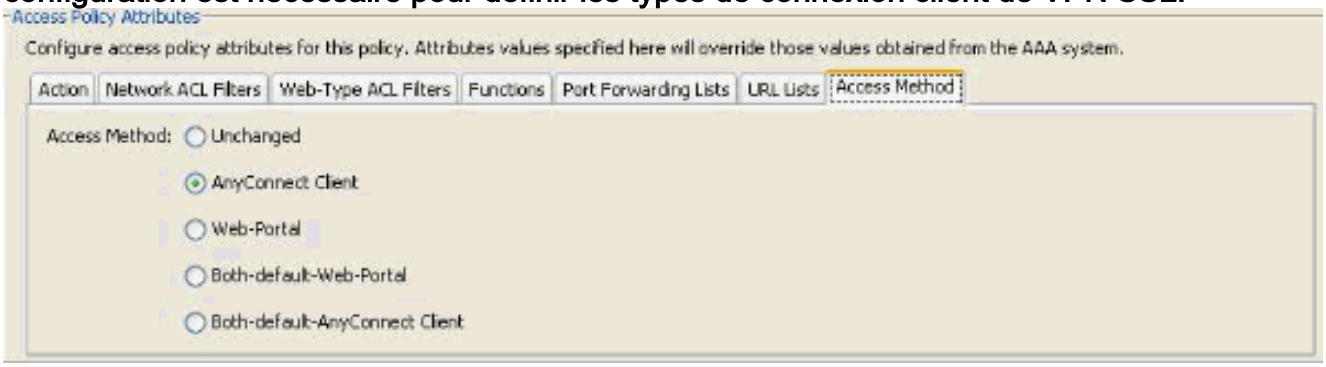


Sous l'onglet d'action, vérifiez que l'action est placée **de continuer**, suivant les indications de la figure 35.**Figure 35. Onglet d'action — Cette configuration est nécessaire pour définir l'offre spéciale traitant pour une connexion ou une session spécifique. L'accès VPN sera refusé si un enregistrement DAP est correspondance et l'action est placée de se terminer.**



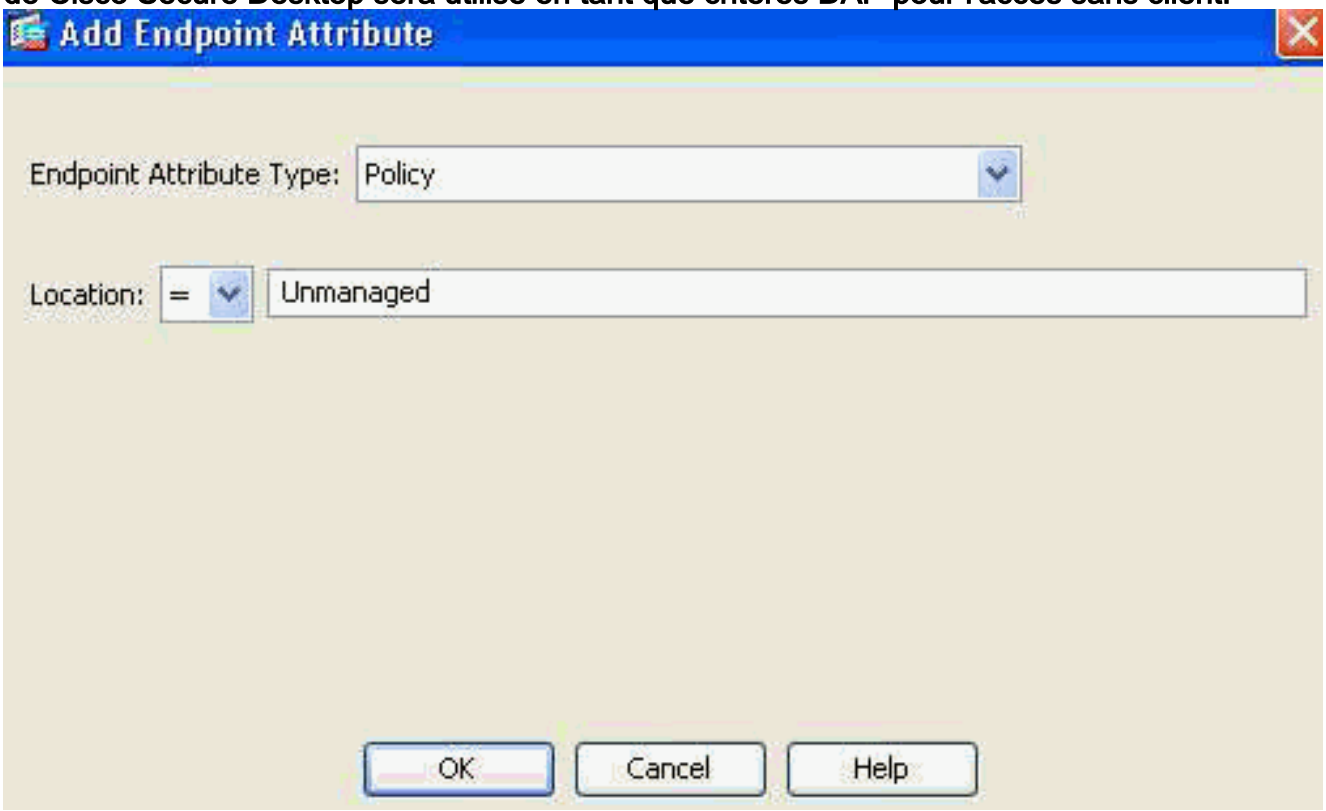
Sous l'onglet de méthode d'accès, sélectionnez le **client d'AnyConnect de** méthode d'accès,

suivant les indications de la figure 36.**Figure 36. Onglet de méthode d'accès — Cette configuration est nécessaire pour définir les types de connexion client de VPN SSL.**



Cliquez sur OK, et puis **appliquez**.

3. Ajoutez un deuxième accès dynamique **Unmanaged_Endpoints** nommé par stratégie, comme suit :Description : **Employé Access sans client**.Ajoutez (situé à la droite de la case d'attribut de point final) un type d'attribut de point final (stratégie) suivant les indications de la figure 37. Cliquez sur OK si complet.**Figure 37. Attribut de point final DAP — L'emplacement de Cisco Secure Desktop sera utilisé en tant que critères DAP pour l'accès sans client.**



De la liste déroulante au-dessus de la section d'aaa attribute, l'**utilisateur** choisi **a toutes les valeurs d'attributs suivantes d'AAA…**Ajoutez (situé à la droite du type d'aaa attribute) un type d'aaa attribute (LDAP) suivant les indications de la figure 38 et de 39. Cliquez sur OK si complet.**Figure 38. Aaa attribute DAP — L'adhésion à des associations d'AAA sera utilisée en tant que critères DAP pour identifier un employé.**

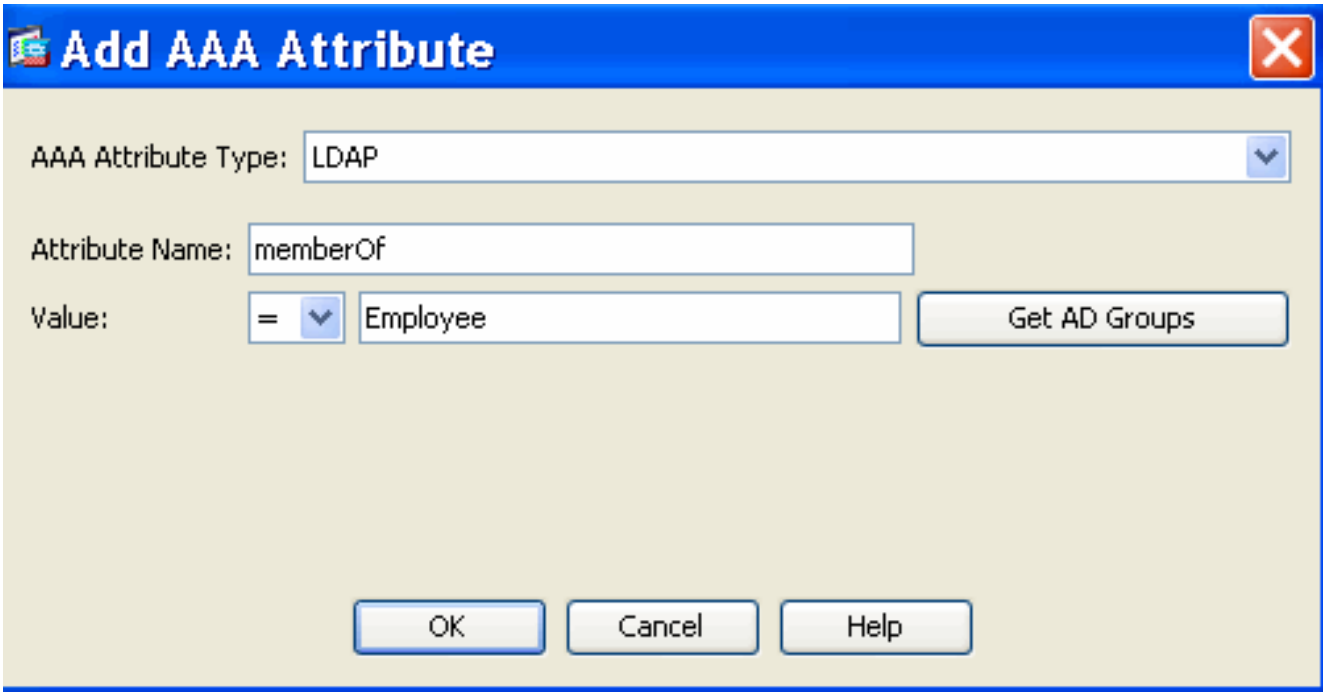
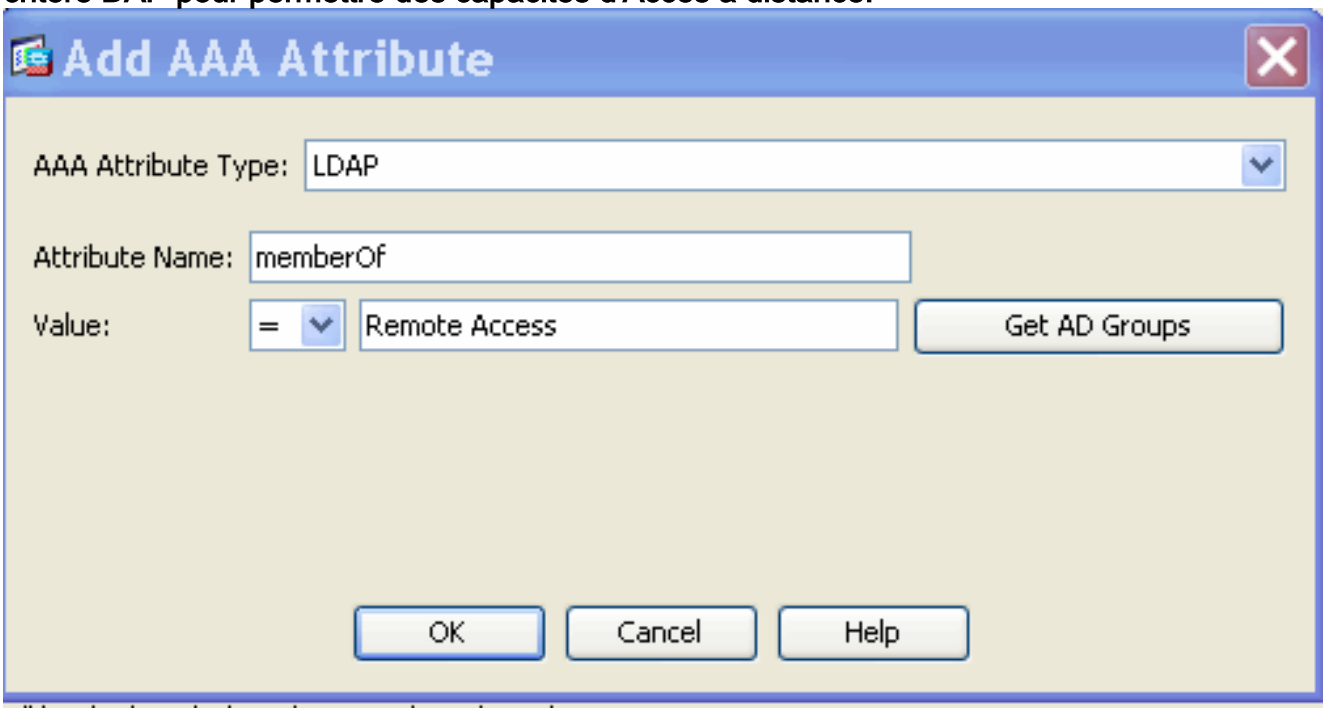
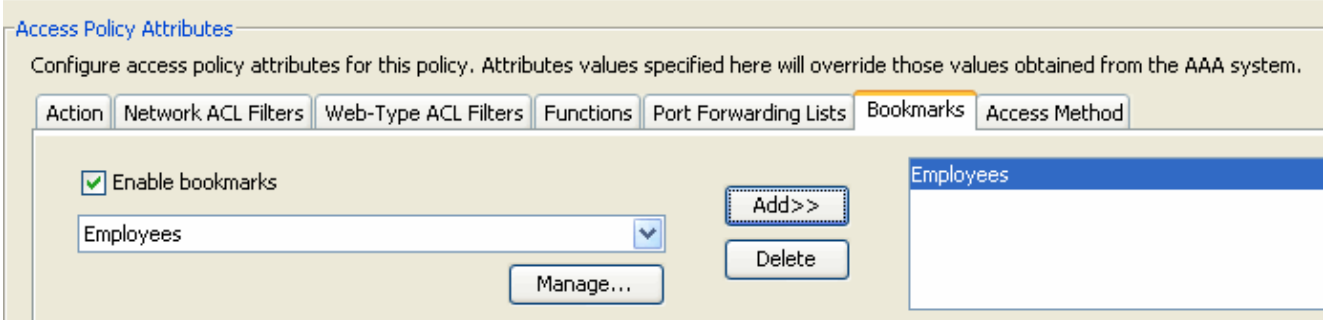


Figure 39. Aaa attribute DAP — L'adhésion à des associations d'AAA sera utilisée comme critère DAP pour permettre des capacités d'Accès à distance.



Sous l'onglet d'action, vérifiez que l'action est placée **de continuer**. (Figure 35 de référence.)Sous les signets tabulez, sélectionnez les **employés de** nom de liste du déroulant et puis cliquez sur Add. En outre, vérifiez que les signets d'enable est vérifiés suivant les indications de la figure 40.**Figure 40. Onglet de signets — Vous permet de sélectionner et configurer des listes URL pour des sessions d'utilisateur.**



Sous l'onglet de méthode d'accès, sélectionnez le **portail web de** méthode d'accès. (Figure 36 de référence.)Cliquez sur OK, et puis **appliquez**.Des sous-traitants seront identifiés par des attributs d'AAA DAP seulement. En conséquence, type d'attributs de point final : (Stratégie) ne sera pas configuré dans l'étape 4. Cette approche est seulement censée pour afficher la souplesse dans DAP.

4. Ajoutez un troisième accès dynamique **Guest_Access** nommé par stratégie et avec ce qui suit :Description : **Invité Access sans client**.Ajoutez (situé à la droite de la case d'attribut de point final) un type d'attribut de point final (stratégie) suivant les indications de la figure 37 ci-dessus. Cliquez sur OK si complet.De la liste déroulante au-dessus de la section d'aaa attribute, l'**utilisateur** choisi **a toutes les valeurs d'attributs suivantes d'AAA…**Ajoutez (situé à la droite de la case d'aaa attribute) un type d'aaa attribute (LDAP) suivant les indications de la figure 41 et de 42. Cliquez sur OK si complet.**Figure 41. Aaa attribute DAP — L'adhésion à des associations d'AAA sera utilisée comme critère DAP pour identifier un sous-traitant.**

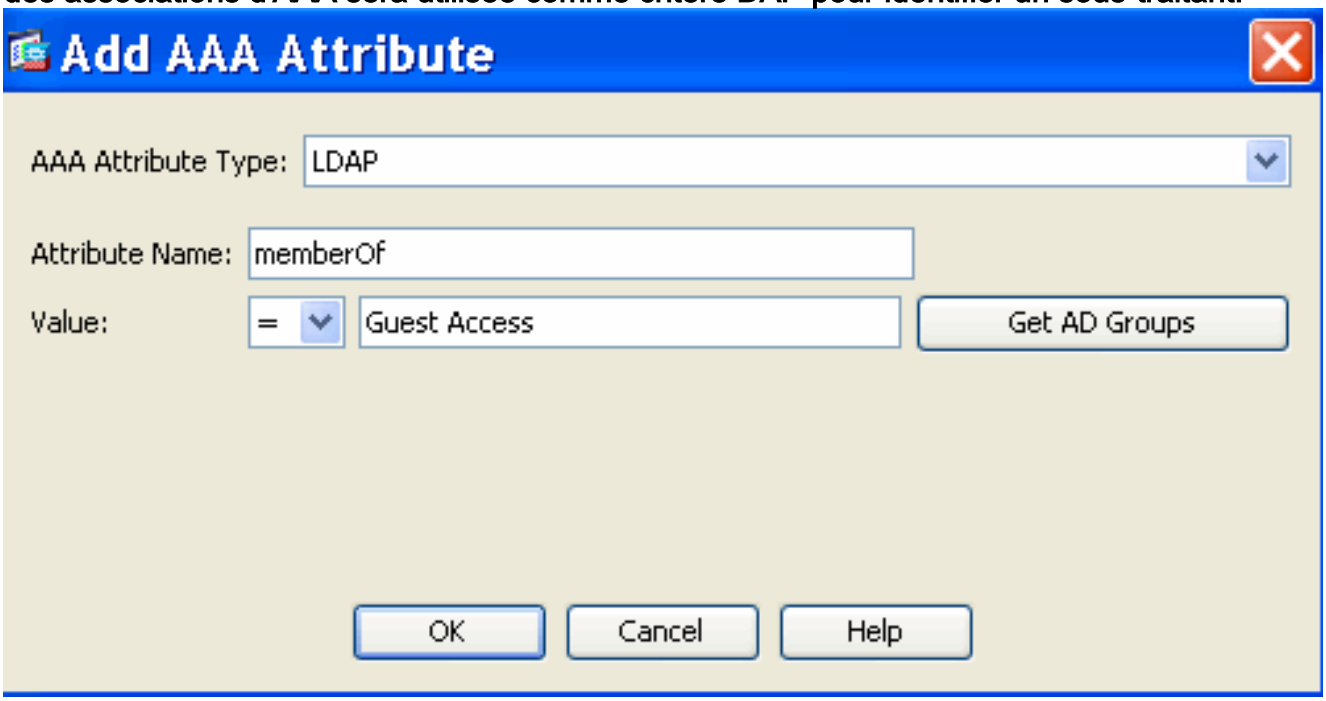


Figure 42. Aaa attribute DAP — L'adhésion à des associations d'AAA sera utilisée comme critère DAP pour permettre des capacités d'Accès à distance.

Sous l'onglet d'action, vérifiez que l'action est placée **de continuer**. (Figure 35 de référence.)Sous les signets tabulez, sélectionnez les **sous-traitants de** nom de liste du déroulant et puis cliquez sur Add. En outre, vérifiez que les **signets d'enable** est vérifiés. (Figure 40 de référence.)Sous l'onglet de méthode d'accès, sélectionnez le **portail web de** méthode d'accès. (Figure 36 de référence.)Cliquez sur OK, et puis **appliquez**.

Critères de sélection DAP — Basé sur celle des procédures ci-dessus de configuration DAP, vos critères de sélection pour les 4 stratégies DAP définies, devraient être compatibles aux figures 43, à 44, à 45 et à 46.

Figure 43. Points finaux gérés — Si les critères de cet enregistrement DAP sont satisfaits, les employés auront accès aux ressources de l'entreprise par l'intermédiaire d'un client/de connexion de réseau (client d'AnyConnect).

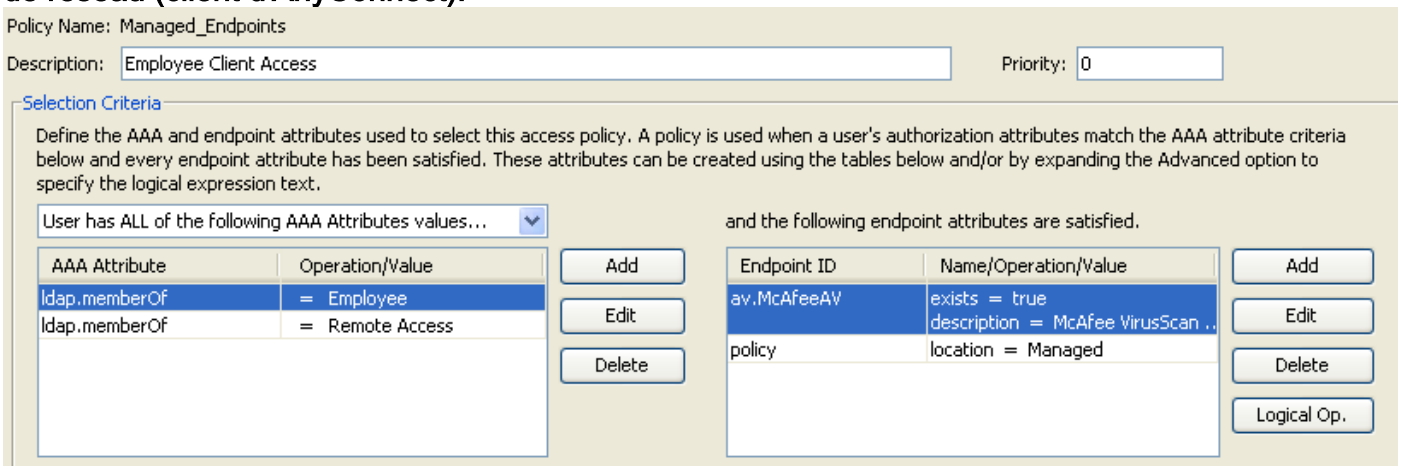


Figure 44. Points finaux de non pris en charge — Si les critères de cet enregistrement DAP est satisfaits, les employés auront accès aux ressources de l'entreprise par l'intermédiaire d'une connexion (portaile) sans client. Une liste URL pour des employés est également appliquée à cette stratégie.

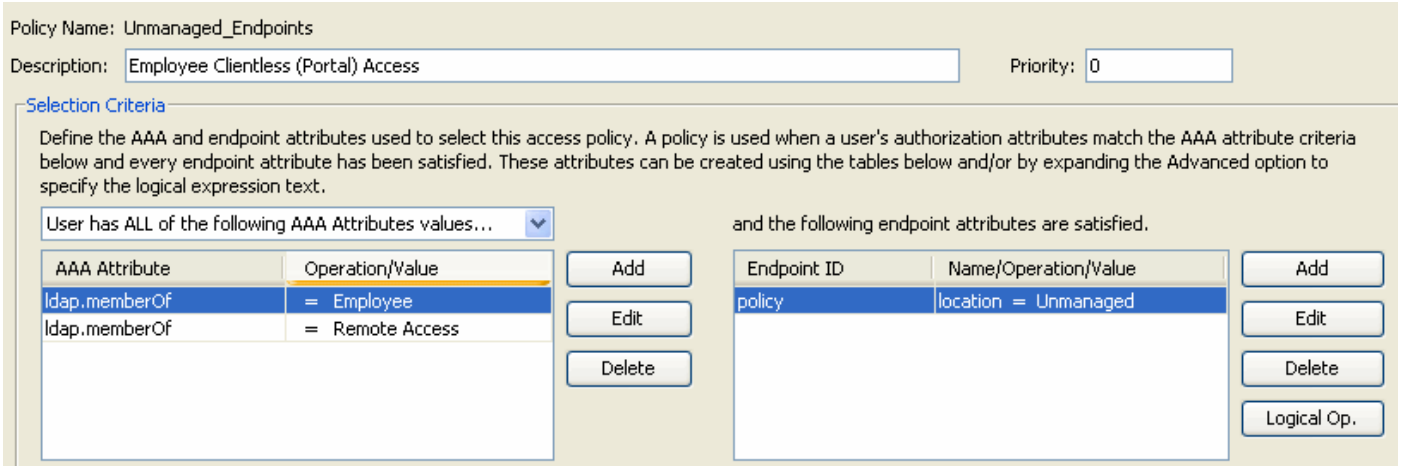


Figure 45. Accès invité — Si les critères de cet enregistrement DAP sont satisfaits, les sous-traitants auront accès aux ressources de l'entreprise par l'intermédiaire d'une connexion (portaile) sans client. Une liste URL pour des sous-traitants est également appliquée à cette stratégie.

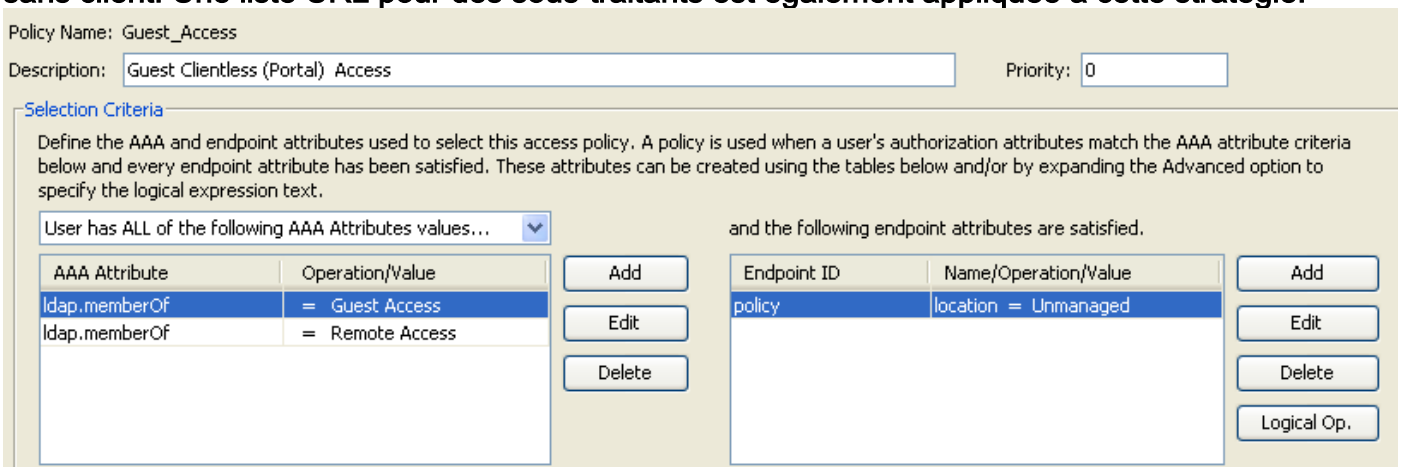
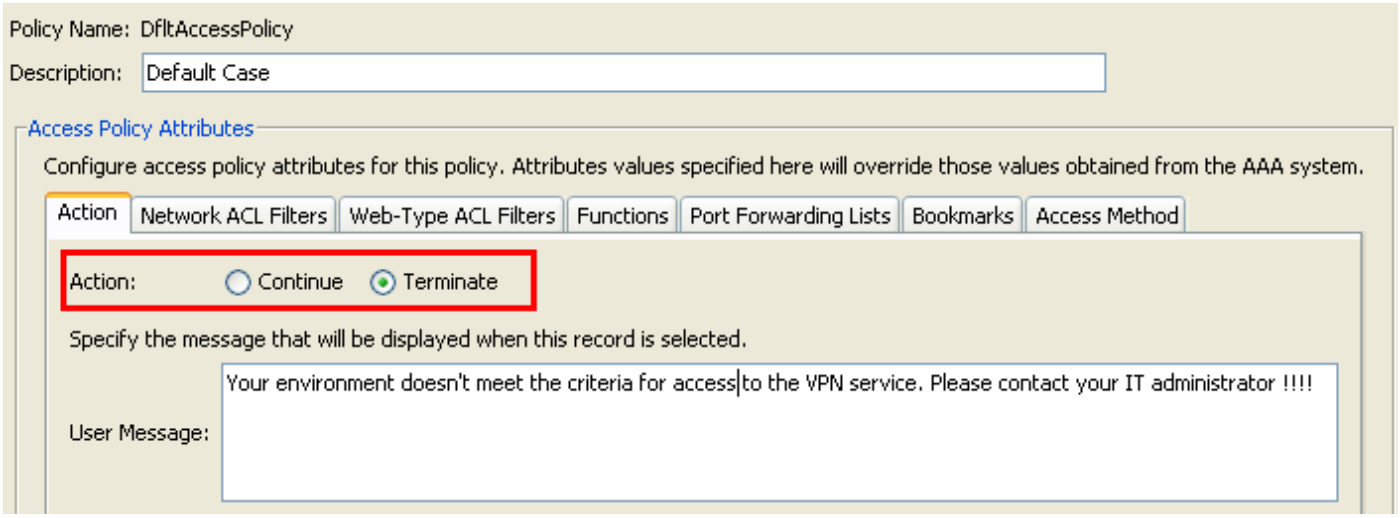


Figure 46. Stratégie par défaut DAP — Si les critères pour tous les enregistrements DAP ci-dessus ne sont pas satisfaits, des employés et les sous-traitants, par défaut, seront refusés l'accès.



Conclusion

Basé sur les conditions requises de VPN SSL de l'Accès à distance du client remarquables dans cet exemple, cette solution répondra à leurs exigences de l'Accès à distance VPN.

Avec évoluer et les environnements dynamiques VPN sur la fusion, Dynamic Access Policies peut

s'adapter et mesurer pour fréquenter des modifications de configuration d'Internet, de divers rôles que chaque utilisateur peut habiter dans une organisation, et des procédures de connexion des sites géré et de non pris en charge d'Accès à distance avec différents configurations et niveaux de sécurité.

Dynamic Access Policies sont complétés par des Technologies existantes nouvelles et prouvées comprenant, estimation de point final, balayage d'hôte, Secure Desktop, AAA et des stratégies avancés d'accès local. En conséquence, les organismes peuvent avec confiance fournir l'accès VPN sécurisé à n'importe quelle ressource de réseau de n'importe quel emplacement.

Informations connexes

- Support et documentation techniques - Cisco Systems