L'utilisation ASA de l'attribut de LDAP trace l'exemple de configuration

Contenu

Introduction

Ce document décrit comment employer des cartes d'attribut de Protocole LDAP (Lightweight Directory Access Protocol) afin de configurer des stratégies dynamiques granulaires d'Accesss sur une appliance de sécurité adaptable (ASA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Secure Sockets Layer VPN (VPN SSL) sur le Cisco IOS®
- Authentification LDAP sur le Cisco IOS
- Services d'annuaire

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CISCO881-SEC-K9
- Logiciel de Cisco IOS, logiciel C880 (C880DATA-UNIVERSALK9-M), version 15.1(4)M, LOGICIEL de VERSION (fc1)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le LDAP est un protocole de l'application ouvert, constructeur-neutre, industriellement compatible pour accéder à et mettre à jour des services d'informations distribués de répertoire au-dessus d'un réseau IP. Les services d'annuaire jouent un important rôle dans le développement de l'intranet et des applications Web parce qu'ils permettent des informations sur des utilisateurs, des systèmes, des réseaux, des services, et des applications à partager dans tout le réseau.

Fréquemment, les administrateurs veulent fournir à des utilisateurs VPN différentes autorisations d'accès ou de contenu WebVPN. Ceci peut être fait si vous configurez différentes règles VPN sur le serveur VPN et assignez ces stratégie-positionnements à chaque utilisateur basé sur leurs qualifications. Tandis que ceci peut être fait manuellement, il est plus efficace d'automatiser le processus avec des services d'annuaire. Afin d'employer le LDAP pour assigner une stratégie de groupe à un utilisateur, vous devez configurer une carte qui trace un attribut de LDAP, tel que le **memberOf d'**attribut de Répertoire actif (AD), à l'attribut d'IETF-Rayon-**classe** qui est compris par le headend VPN.

Sur le Cisco IOS, la même chose peut être réalisée si vous configurez différents policy group sous le contexte de webvpn et employez des cartes d'attribut de LDAP afin de déterminer quel policy group l'utilisateur sera assigné comme décrit dans le document. Voir l'affectation de policy group

pour les clients d'AnyConnect qui utilisent le LDAP sur l'exemple de configuration de Headends de Cisco IOS.

Sur l'ASA, ceci est régulièrement réalisé par l'attribution de différentes stratégies de groupe à différents utilisateurs. Quand l'authentification LDAP est en service, ceci peut être réalisé automatiquement avec une carte d'attribut LDAP. Afin d'employer le LDAP pour assigner une stratégie de groupe à un utilisateur, vous devez tracer un attribut de LDAP, tel que le **memberOf d'**attribut d'AD à l'attribut de **stratégie de groupe** qui est compris par l'ASA. Une fois le mappage d'attribut est établi, vous doit tracer la valeur d'attribut configurée sur le serveur LDAP au nom d'une stratégie de groupe sur l'ASA.

> Remarque: L'attribut de **memberOf** correspond au groupe que l'utilisateur est une partie de dans le Répertoire actif. Il est possible que un utilisateur soit un membre de plus d'un groupe dans le Répertoire actif. Ceci cause de plusieurs attributs de **memberOf** d'être envoyés par le serveur, mais l'ASA peut seulement apparier un attribut à une stratégie de groupe.

FORUM AUX QUESTIONS

Q. Y a-t-il une limite de configuration sur le nombre de LDAP-attribut-MAPS pour l'ASA ?

R. Non, là ne sont aucune limite. des LDAP-attribut-MAPS sont dynamiquement allouées pendant la session d'Accès à distance VPN qui utilise l'authentification LDAP/autorisation.

Q. Y a-t-il une limite sur les nombres d'attributs qui peuvent être tracés par LDAP-attribut-MAP ?

R. Aucune limites de configuration.

Q. Y a-t-il une restriction sur combien de LDAP-serveurs auxquels une LDAP-attribut-MAP spécifique peut être appliquée ?

R. Aucune restriction. Le code de LDAP vérifie seulement que le nom de LDAP-attribut-MAP est valide.

Q. Y a-t-il des limites avec des LDAP-attribut-MAPS et les attributs muti-évalués comme le memberOf d'AD ?

R. Oui. Ici, seulement l'AD est expliqué, mais il applique à n'importe quel serveur LDAP qui utilise des attributs de multi-valeur pour des décisions politiques. La ldap-attribut-MAP a une limite avec des attributs à valeurs multiples comme le memberOf d'AD. Si un utilisateur est un memberOf de plusieurs groupes d'AD (qui est commun) et la LDAP-attribut-MAP s'assortit plus d'une d'entre eux, la valeur tracée sera choisie a basé sur l'alphabétisation des entrées appariées. Puisque ce comportement n'est pas évident ou intuitif, il est important d'avoir la connaissance claire au sujet

de la façon dont cela fonctionne.

Résumé : Si le mappage de LDAP a comme conséquence de plusieurs valeurs pour un attribut, la valeur d'attribut finale sera choisie comme suit :

- D'abord, sélectionnez les valeurs avec le plus petit nombre de caractères.
- Si ceci a comme conséquence plus d'une valeur, choisissez la valeur qui est la plus basse dans l'ordre alphabétique.

Exemples de cas d'utilisation

Le Répertoire-LDAP actif renvoie ces exemples de quatre memberOf pour une authentification de l'utilisateur ou une demande d'autorisation :

```
memberOf: value = CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Cisco-Eng,CN=Users,DC=stbu,OU=cisco,DC=com
memberOf: value = CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com
```

LDAP-MAP #1 : Supposez que cette LDAP-attribut-MAP est configurée pour tracer différentes stratégies de groupe ASA basées sur la configuration de memberOf :

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup4
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

Dans ce cas, les correspondances se produiront sur chacune des quatre valeurs de stratégie de groupe (ASAGroup1 - ASAGroup4). Cependant, la connexion sera assignée à la stratégie de groupe ASAGroup1 parce qu'elle se produit d'abord dans l'ordre alphabétique.

LDAP-MAP #2 : Cette LDAP-attribut-MAP est identique, à moins que le premier memberOf n'ait pas une MAP-valeur explicite assignée (aucun ASAGroup4). Notez que quand il n'y a aucune MAP-valeur explicite définie, le texte d'attribut reçu du LDAP est utilisé.

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

Comme dans le cas précédent, les correspondances se produisent sur chacune des quatre entrées. Dans ce cas, puisqu'aucune valeur tracée n'est donnée pour l'entrée APP-SSL-VPN, la valeur tracée se transférera sur des gestionnaires CN=APP-SSL-VPN, CN=Users, OU=stbu, DC=cisco, DC=com. Puisque CN=APP-SSL-VPN apparaît d'abord dans la commande aphabetical, APP-SSL-VPN sera sélectionné comme valeur de stratégie.

Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCub64284. Référez-vous à PIX/ASA 8.0 : Employez l'authentification LDAP pour assigner une stratégie de groupe à la procédure de connexion, qui affiche un cas simple de LDAP avec le memberOf qui pourrait fonctionner dans votre déploiement particulier.

Options de contournement/pratique recommandée

1. Stratégie d'accès dynamique d'utilisation (DAP) - DAP n'a pas cette limite d'analyser des attributs à valeurs multiples (comme le memberOf) ; mais DAP actuellement ne peut pas placer une stratégie de groupe de lui-même. Ceci signifie que la session devrait être correctement segmentée par l'intermédiaire des méthodes d'association de groupe de tunnels/stratégie de groupe. À l'avenir, DAP aura la capacité pour placer n'importe quel attribut d'authorizaiton, y compris la stratégie de groupe, (ID de bogue Cisco CSCsi54718), ainsi le besoin de LDAP-attribut-MAP à cet effet ne sera pas par la suite exigé.

2. En tant qu'une alternative et si le scénario de déploiement la permet, toutes les fois que vous devez employer une LDAP-attribut-MAP pour placer l'attribut de classe, vous possibles pourrait également utiliser un attribut simple-évalué (comme le service) que représente votre différentiation de groupe sur l'AD.

   Remarque: Dans un DN de memberOf tel que « CN=Engineering, OU=Office1, DC=cisco, DC=com », vous pouvez seulement prendre la décision sur le premier DN, qu'est CN=Engineering, pas l'unité organisationnelle (OU). Il y a une amélioration à pouvoir capable filtrer sur n'importe quel gisement de DN.

Configurez - Échantillonnez les cas d'utilisation

Remarque: Chaque exemple décrit dans cette section est une configuration autonome, mais peut être mélangé et apparié les uns avec les autres pour produire la stratégie désirée d'Access.

Conseil : Les noms et les valeurs d'attribut distinguent les majuscules et minuscules. Si le mappage ne se produit pas correctement, soyez certain que l'orthographe et la capitalisation correctes a été utilisée dans la carte d'attribut de LDAP pour des noms et les valeurs d'attribut de Cisco et de LDAP.

1. Application utilisateur Utilisateur de stratégie d'attributs

N'importe quel attribut standard de LDAP peut être tracé à un attribut spécifique de constructeur réputé d'appareils (le VSA). Un ou plusieurs attributs de LDAP peuvent être tracés à un ou plusieurs attributs de LDAP de Cisco. Pour une liste complète des VSAs de LDAP de Cisco, référez-vous les attributs pris en charge de Cisco pour l'autorisation de LDAP. Cet exemple affiche comment imposer une bannière pour le LDAP user1. User1 peut être n'importe quel type d'Accès à distance VPN : IPsec, SVC, ou webvpn sans client. Cet exemple emploie Properties/général/attribut/champ de bureau pour imposer le Banner1.

Remarque: Vous pourriez employer l'attribut/champ de service d'AD pour tracer au VSA d'IETF-Rayon-classe de Cisco afin d'imposer des stratégies d'une stratégie de groupe ASA/PIX. Il y a des exemples de ceci plus tard dans le document.

L'attribut-mappage de LDAP (pour l'AD et le Sun de Microsoft) est pris en charge en date de la version 7.1.x PIX/ASA. N'importe quel attribut Microsoft/AD peut être tracé à un attribut de

Cisco. Voici la procédure pour exécuter ceci :

1. Sur le serveur AD/LDAP :User1 choisi.Clic droit **> Properties**.Sélectionnez un onglet à utiliser afin de placer un attribut (exemple. Onglet Général).Sélectionnez un champ/attribut, par exemple le champ de « bureau », pour être utilisé afin d'imposer la time-range, et entrez dans le texte de la bannière (exemple, accueil au LDAP ! ! ! !). La configuration de « bureau » sur le GUI est enregistrée dans l'attribut « physicalDeliveryOfficeName » AD/LDAP.

2. Sur l'ASA, afin de créer une table de mappage d'attribut de LDAP, tracez l'attribut « physicalDeliveryOfficeName » AD/LDAP à l'attribut "Banner1" ASA :
```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Associez la carte d'attribut de LDAP à l'entrée d'AAA-serveur :
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Établissez la session d'Accès à distance et la vérifiez que la bannière le « accueil au LDAP ! ! ! ! » est présenté à l'utilisateur VPN.

2. Utilisateurs de LDAP d'endroit dans une stratégie de groupe spécifique - exemple générique

Cet exemple explique l'authentification d'user1 sur le serveur AD-LDAP et récupère la valeur de champ de service ainsi il peut être tracé à une stratégie de groupe ASA/PIX de laquelle des stratégies seront imposées.

1. Sur le serveur AD/LDAP :User1 choisi.Clic droit **> Properties**.Sélectionnez un onglet à utiliser afin de placer un attribut (exemple. Onglet d'organisation).Sélectionnez un champ/attribut, par exemple « service », pour être utilisé afin d'imposer une stratégie de groupe, et écrivez la valeur de la stratégie de groupe (Group-Policy1) sur l'ASA/PIX. La configuration de « service » sur le GUI est enregistrée dans l'attribut « service » AD/LDAP.

2. Définissez une table de LDAP-attribut-MAP.
```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

   Remarque: En raison de l'implémentation de l'ID de bogue Cisco CSCsv43552, un nouvel attribut de LDAP-attribut-MAP, stratégie de groupe, a été introduit afin de remplacer l'IETF-Rayon-classe. Le CLI sur la version 8.2 ASA prend en charge le mot clé d'IETF-Rayon-classe comme choix valide dans les commandes de map name et de MAP-valeur afin de lire

un fichier de 8.0 configs (scénario de mise à niveau de logiciel). Le code d'Adaptive Security Device Manager (ASDM) a été déjà mis à jour pour n'afficher plus l'IETF-Rayon-classe comme choix quand vous configurez une entrée de mappage d'attribut. Supplémentaire, l'ASDM écrira l'attribut d'IETF-Rayon-classe (si lu dedans d'un config 8.0) comme attribut de stratégie de groupe.

3. Définissez la stratégie de groupe Group_policy1 sur l'appliance et les attributs requis de stratégie.

4. Établissez le tunnel d'Accès à distance VPN et le vérifiez que la session hérite des attributs de Group-Policy1 (et de tous autres attributs applicables de la stratégie de groupe par défaut).

   Remarque: Ajoutez plus d'attributs à la carte au besoin. Cet exemple affiche que seulement le minimum contrôlait cette fonction spécifique (placez un utilisateur dans une stratégie de groupe de la particularité ASA/PIX 7.1.x). Le troisième exemple affiche ce type de carte.

Configurez une stratégie de groupe NOACCESS

Vous pouvez créer une stratégie de groupe NOACCESS afin de refuser la connexion VPN quand l'utilisateur n'est pas une partie de groupes l'uns des de LDAP. Cet extrait de configuration est affiché pour votre référence :

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

Vous devez appliquer cette stratégie de groupe comme stratégie de groupe par défaut au groupe de tunnels. Ceci permet les utilisateurs qui obtiennent un mappage de la carte d'attribut de LDAP, par exemple ceux qui appartiennent à un groupe désiré de LDAP, pour obtenir leurs stratégies de groupe désirées et les utilisateurs qui n'obtiennent aucun mappage, par exemple ceux qui n'appartiennent pas aux groupes désirés l'uns des de LDAP, pour obtenir la stratégie de groupe NOACCESS du groupe de tunnels, qui bloque l'accès pour eux.

Conseil : Puisque l'attribut de VPN-simultané-procédures de connexion est placé à 0 ici, il doit explicitement être aussi bien défini dans toutes les autres stratégies de groupe ; autrement, il sera hérité de la stratégie de groupe par défaut pour ce groupe de tunnel, qui est dans ce cas la stratégie NOACCESS.

3. Application basée sur groupe de stratégie d'attributs - Exemple

Remarque: L'implémentation/difficulté de l'ID de bogue Cisco CSCse08736 est exigée, ainsi l'ASA devrait exécuter au moins la version 7.2.2.

1. Sur le serveur AD-LDAP, les utilisateurs et les ordinateurs de Répertoire actif, installent un article utilisateur (VPNUserGroup) qui représente un groupe où les attributs VPN sont configurés.

2. Sur le serveur AD-LDAP, les utilisateurs et les ordinateurs de Répertoire actif, définissent chaque champ du service de l'article utilisateur pour indiquer le groupe-enregistrement (VPNUserGroup) dans l'étape 1. Le nom d'utilisateur dans cet exemple est **web1**.

   Remarque: L'attribut d'AD de service a été utilisé seulement parce que logiquement le « service » se rapporte à la stratégie de groupe. En réalité, n'importe quel champ a pu être utilisé. La condition requise est que ce champ doit tracer à la stratégie de groupe d'attribut de Cisco VPN suivant les indications de cet exemple.

3. Définissez une table de LDAP-attribut-MAP :

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

   La description et le bureau de deux attributs AD-LDAP (représentés par description et PhysicalDeliveryOfficeName de noms d'AD) sont les attributs d'enregistrement de groupe (pour VPNUSerGroup) que les cartes à Cisco VPN attribue Banner1 et IETF-Rayon-Session-délai d'attente.

   L'attribut de service est pour que l'article utilisateur trace au nom de la stratégie de groupe externe sur l'ASA (VPNUSer), qui trace alors de nouveau à l'enregistrement de VPNuserGroup sur le serveur AD-LDAP, où des attributs sont définis.

   Remarque: Cisco attribuent (stratégie de groupe) doit être défini dans la LDAP-attribut-MAP. Son AD-attribut tracé peut être n'importe quel attribut settable d'AD. Cet exemple utilise le service parce que c'est le nom le plus logique qui se rapporte à la stratégie de groupe.

4. Configurez l'AAA-serveur avec le nom de LDAP-attribut-MAP à utiliser pour des exécutions d'authentification LDAP, d'autorisation, et de comptabilité (AAA) :

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 90.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. Définissez un groupe de tunnels avec avec l'authentification LDAP ou l'autorisation de LDAP.

   Exemple avec l'authentification LDAP. Exécute l'authentification + application de stratégie d'attribut (d'autorisation) si des attributs sont définis.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
```

```
accounting-server-group RadiusACS28
5520-1(config)#
```
Exemple avec l'autorisation de LDAP. Configuration utilisée pour l'usage des Certificats numériques.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. Définissez une stratégie de groupe externe. Le nom de la stratégie de groupe est la valeur de l'article utilisateur AD-LDAP qui représente le groupe (VPNUserGroup).

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. Établissez le tunnel et le vérifiez que des attributs sont imposés. Dans ce cas, la bannière et la session-timeout est imposée de l'enregistrement de VPNuserGroup sur l'AD.

4. L'application de Répertoire actif de « assignent une adresse IP statique » pour IPsec et tunnels de SVC

L'attribut d'AD est des msRADIUSFramedIPAddress. L'attribut est configuré dans l'utilisateur Properties d'AD, onglet Numérotation, « assignent une adresse IP statique ».

Voici les étapes :

1. Sur le serveur d'AD, sous l'utilisateur Properties, l'onglet Numérotation, « assignent une adresse IP statique », écrivent la valeur de l'adresse IP afin d'assigner à la session IPsec/SVC (10.20.30.6).

2. Sur l'ASA créez une LDAP-attribut-MAP avec ce mappage :

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFrameIPAdddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. Sur l'ASA, vérifiez la VPN-adresse-assigment est configuré pour inclure le « VPN-adr-assigner-AAA » :

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

4. Établissez les sessions distantes d'autorité IPsec/SVC (RA) et vérifiez avec « le distant de

VPN-sessiondb d'exposition|svc » qui « champ d'adresse IP attribuée le » est correct (10.20.30.6).

5. L'application de Répertoire actif « de l'accès distant d'autorisation d'Accès à distance, permettent/refusent Access »

Prend en charge toutes les sessions distantes VPN Acccess : IPSec, webvpn, et SVC. Permettez Access a une valeur de VRAI. Refusez Acccess a une valeur de FAUX. Le nom d'attribut d'AD est msNPAllowDialin.

Cet exemple explique la création d'une LDAP-attribut-MAP qui emploie les Tunnellisation-protocoles de Cisco pour créer permettent Access (VRAI) et refuse des conditions (FAUSSES). Par exemple, si vous tracez le tunnel-protocol=L2TPover IPsec (8), vous pouvez créer un état FAUX si vous essayez d'imposer l'accès pour le webvpn et l'IPsec. La logique inverse s'applique aussi.

Voici les étapes :

1. Sur le serveur user1 Properties d'AD, l'accès distant, sélectionnent l'approprié permettent Access ou refusent l'accès pour chaque utilisateur.

   Remarque: Si vous sélectionnez la troisième option « accès de contrôle par la stratégie d'accès à distance, » aucune valeur n'est retournée du serveur d'AD, ainsi les autorisations qui sont imposées sont basées sur la configuration interne de la stratégie de groupe ASA/PIX.

2. Sur l'ASA, créez une LDAP-attribut-MAP avec ce mappage :

   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```

   Remarque: Ajoutez plus d'attributs à la carte au besoin. Cet exemple affiche que seulement le minimum contrôlait cette fonction spécifique (permettez ou refusez accès basé sur sur la configuration d'accès distant).

   Queest-ce que la LDAP-attribut-MAP signifie ou impose ?

   msNPAllowDialin 8 FAUX de MAP-valeur

   Refusez Access pour un user1. L'état FAUX de valeur trace à tunnel-Protocol L2TPoverIPsec, (valeur 8).

   Permettez Access pour user2. L'état de valeur vrai trace à tunnel-Protocol le webvpn + l'IPsec, (valeur 20).

   Un webvpn/utilisateur d'IPsec, authenticaticated comme user1 sur l'AD, échouerait en raison de la non-concordance de tunnel-Protocol.

Un L2TPoverIPsec, authenticaticated comme user1 sur l'AD, échouerait en raison de la règle de refuser.

Un webvpn/utilisateur d'IPsec, authenticaticated comme user2 sur l'AD, réussirait (permettez la règle + protocole apparié de tunnel).

Un L2TPoverIPsec, authenticaticated comme user2 sur l'AD, échouerait en raison de la non-concordance de tunnel-Protocol.
Soutien de tunnel Protocol, comme défini dans RFC 2867 et 2868.

6. Application de Répertoire actif de « membre » de l'adhésion /Group pour permettre ou refuser Access

Ce cas est étroitement rapporté pour affaire 5, prévoit un écoulement plus logique, et est la méthode recommandée, puisqu'il établit le contrôle d'adhésion à des associations comme condition.

1. Configurez l'utilisateur d'AD pour être « membre » d'un groupe spécifique. Utilisez un nom qui le place en haut de la groupe-hiérarchie (ASA-VPN-consultants). Dans AD-LDAP, l'adhésion à des associations est définie par l'attribut « memberOf » d'AD.

   Il est important que le groupe soit en haut de la liste, puisque vous pouvez actuellement seulement s'appliquer les règles à la première chaîne de « memberOf » de groupe. Dans la version 7.3, vous pourrez exécuter le filtrage et l'application de multiple-groupe.
2. Sur l'ASA, créez une LDAP-attribut-MAP avec le le mappage minimum :

```
ldap attribute-map LDAP-MAP
map-name memberOf Tunneling-Protocols
map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4

5540-1#
```

   Remarque: Ajoutez plus d'attributs à la carte au besoin. Ce les exemples affiche que seulement le minimum contrôlait cette fonction spécifique (permettez ou refusez accès basé sur sur l'adhésion à des associations).

   Queest-ce que la LDAP-attribut-MAP signifie ou impose ?

   On permettra User=joe_consultant, une partie d'AD, qui est membre de groupe « ASA-VPN-consultants » d'AD l'accès seulement si l'utilisateur utilise IPsec (tunnel-protocol=4=IPSec).

   User=joe_consultant, une partie d'AD, échouera accès VPN pendant n'importe quel autre client d'Accès à distance (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, et ainsi de suite).

   On ne permettra pas dedans User=bill_the_hacker puisque l'utilisateur n'a aucune adhésion d'AD.

7. L'application de Répertoire actif des « heures de connexion/heure ordonne »

Ce cas d'utilisation décrit comment installer et imposer les règles d'heure sur AD/LDAP.

Voici la procédure pour faire ceci :

1. Sur le serveur AD/LDAP :Sélectionnez l'utilisateur.Clic droit **> Properties**.Sélectionnez un onglet à utiliser afin de placer un attribut (exemple. Onglet Général).Sélectionnez un champ/attribut, par exemple le champ de « bureau », pour être utilisé afin d'imposer la time-range, et écrivez le nom de la time-range (par exemple, Boston). La configuration de « bureau » sur le GUI est enregistrée dans l'attribut « physicalDeliveryOfficeName » AD/LDAP.

2. Sur l'ASA

   Créez une table de mappage d'attribut de LDAP.Tracez l'attribut « physicalDeliveryOfficeName » AD/LDAP à l'attribut « Access-heures » ASA.

   Exemple :

   ```
   B200-54(config-time-range)# show run ldap
   ldap attribute-map TimeOfDay
   map-name physicalDeliveryOfficeName Access-Hours
   ```

3. Sur l'ASA, associez la carte d'attribut de LDAP à l'entrée d'AAA-serveur :

   ```
   B200-54(config-time-range)# show runn aaa-server microsoft
   aaa-server microsoft protocol ldap
   aaa-server microsoft host audi-qa.frdevtestad.local
   ldap-base-dn dc=frdevtestad,dc=local
   ldap-scope subtree
   ldap-naming-attribute sAMAccountName
   ldap-login-password hello
   ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
   ldap-attribute-map TimeOfDay
   ```

4. Sur l'ASA, créez un objet de time-range qui a la valeur de nom qui est assignée à l'utilisateur (valeur de bureau dans étape 1) :`B200-54(config-time-range)# show runn time-range`
   ```
   !
   time-range Boston
   periodic weekdays 8:00 to 17:00
   !
   ```

5. Établissez la session d'Accès à distance VPN :

   La session devrait réussir si dans la time-range.La session en cas de défaillance en dehors de la time-range.

8. Employez la configuration de LDAP-MAP pour tracer un utilisateur dans une stratégie de groupe spécifique et pour utiliser l'ordre d'autorisation-serveur-groupe, dans le cas de l'Authentification double

1. Dans ce scénario, l'Authentification double est utilisée. Le premier serveur d'authentification utilisé est RAYON et la deuxième authentification divisent utilisé est un serveur LDAP.

Configurez le serveur LDAP aussi bien que le serveur de RAYON. Voici un exemple :

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

Definine l'attribut-MAP de LDAP. Voici un exemple :

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

Définissez le groupe de tunnels et associez le RAYON et le serveur LDAP pour l'authentification. Voici un exemple :

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

Visualisez la stratégie de groupe qui est utilisée dans la configuration de groupe de tunnels :

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

Avec cette configuration, des utilisateurs d'AnyConnect qui ont été tracés correctement avec l'utilisation des attributs de LDAP n'ont pas été placés dans la stratégie de groupe, Test-stratégie-Safenet. Au lieu de cela, ils étaient encore placés dans la stratégie de groupe par défaut, dans ce cas NoAccess.

Voyez que l'extrait du met au point (mettez au point le LDAP 255) et des Syslog à informationnel de niveau :

```
---------------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

---------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is being set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

La panne d'exposition de ces Syslog en tant qu'utilisateur était donnée la stratégie de groupe de NoAccess qui a eu la simultané-procédure de connexion réglée à 0 quoique les Syslog indiquent qu'il a récupéré une stratégie de groupe de particularité d'utilisateur.

Afin d'avoir l'assigné à l'utilisateur dans la stratégie de groupe, basée sur la LDAP-MAP, vous devez avoir cette commande : **test-LDAP d'autorisation-serveur-groupe** (dans ce cas, le test-**LDAP** est le nom de serveur LDAP). Voici un exemple :

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Maintenant, si le premier serveur d'authentification (RAYON, dans cet exemple) envoyait les attributs d'utilisateur-particularité, par exemple l'attribut d'IEFT-classe, dans ce cas, l'utilisateur sera tracé à la stratégie de groupe envoyée par le RAYON. Ainsi quoique le serveur secondaire fasse configurer une carte de LDAP et les attributs du LDAP de

l'utilisateur tracent l'utilisateur à une stratégie de groupe différente, la stratégie de groupe envoyée par le premier serveur d'authentification sera imposée.

Afin d'avoir la place d'utilisateur dans une stratégie de groupe basée sur l'attribut de carte de LDAP, vous devez spécifier cette commande sous le groupe de tunnels : **test-LDAP d'autorisation-serveur-groupe**.

3. Si le premier serveur d'authentification est le SDI ou l'OTP, qui ne peuvent pas passer l'attribut d'utilisateur-particularité, alors l'utilisateur tomberait dans la stratégie de groupe par défaut du groupe de tunnels. Dans ce cas, NoAccess quoique le mappage de LDAP soit correct.

   Dans ce cas, vous également auriez besoin de la commande, test-**LDAP d'autorisation-serveur-groupe**, sous le groupe de tunnels pour que l'utilisateur soit placé dans la stratégie de groupe correcte.

4. Si chacun des deux serveurs sont le mêmes RAYON ou serveurs LDAP, alors vous n'avez pas besoin de l'ordre d'autorisation-serveur-**groupe** pour que le verrouillage de stratégie de groupe fonctionne.

Vérifiez

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                 Index        : 2
Assigned IP  : 10.34.63.1              Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES          Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                   Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet     Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN         : none
```

Dépannez

Utilisez cette section afin de dépanner votre configuration.

Débuggez la transaction de LDAP

Ceux-ci met au point peuvent être utilisés afin d'aider à isoler des questions avec la configuration DAP :

- **mettez au point le LDAP 255**
- **mettez au point le suivi de dap**

- debug aaa authentication

L'ASA ne peut pas authentifier des utilisateurs de serveur LDAP

Au cas où l'ASA ne pourrait pas authentifier les utilisateurs du LDAP servent, voici un certain échantillon met au point :

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

De ces derniers met au point, ou le format de DN de procédure de connexion de LDAP est incorrect ou le mot de passe est incorrect ainsi vérifiez chacun des deux afin de résoudre le problème.