Configurer un serveur AAA externe pour le VPN

À propos des serveurs AAA externes

Cet ASA peut être configuré pour utiliser un serveur LDAP, RADIUS ou TACACS+ externe afin de prendre en charge l'authentification, l'autorisation et la comptabilité (AAA) pour l'ASA. Le serveur AAA externe applique les autorisations et les attributs configurés. Avant de configurer l'ASA pour utiliser un serveur externe, vous devez configurer le serveur AAA externe avec les attributs d'autorisation ASA appropriés et, à partir d'un sous-ensemble de ces attributs, attribuer des autorisations spécifiques aux utilisateurs individuels.

Comprendre l'application des politiques aux attributs d'autorisation

L'ASA prend en charge plusieurs méthodes d'application des attributs d'autorisation d'utilisateur, également appelés droits ou autorisations d'utilisateur, aux connexions VPN. Vous pouvez configurer l'ASA pour obtenir les attributs utilisateur de n'importe quelle combinaison de :

- une politique d'accès dynamique (DAP) sur l'ASA
- un serveur d'authentification et/ou d'autorisation RADIUS ou LDAP externe
- une stratégie de groupe sur l'ASA

Si l'ASA reçoit des attributs de toutes les sources, les attributs sont évalués, fusionnés et appliqués à la politique d'utilisateur. En cas de conflit entre les attributs, les attributs du DAP prévalent.

L'ASA applique les attributs dans l'ordre suivant :

1. Attributs DAP sur l'ASA : introduits dans la version 8.0(2), ces attributs prévalent sur tous les autres. Si vous définissez un signet ou une liste d'URL dans DAP, il remplace un signet ou une liste d'URL définis dans la stratégie de groupe.
2. Attributs de l'utilisateur sur le serveur AAA externe : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie. Ne les confondez pas avec les attributs définis

pour les utilisateurs individuels dans la base de données AAA locale sur l'ASA (comptes d'utilisateurs dans ASDM).

3. Stratégie de groupe configurée sur l'ASA : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU=*group-policy*) pour l'utilisateur, l'ASA place l'utilisateur dans la stratégie de groupe du même nom et applique les attributs de la stratégie de groupe qui ne sont pas renvoyés par le serveur.

   Pour les serveurs LDAP, n'importe quel nom d'attribut peut être utilisé pour définir la stratégie de groupe pour la session. La carte d'attributs LDAP que vous configurez sur l'ASA associe l'attribut LDAP à l'attribut Cisco IETF-Radius-Class.

4. Stratégie de groupe affectée par le profil de connexion (appelé tunnel-group dans le CLI) : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une stratégie de groupe par défaut appliquée à l'utilisateur avant l'authentification. Tous les utilisateurs se connectant à l'ASA appartiennent initialement à ce groupe, qui fournit tous les attributs manquants dans le DAP, les attributs utilisateur renvoyés par le serveur, ou la stratégie de groupe attribuée à l'utilisateur.

5. Stratégie de groupe par défaut (DfltGrpPolicy) : les attributs par défaut du système fournissent les valeurs manquantes dans le DAP, les attributs d'utilisateur, la stratégie de groupe, ou le profil de connexion.

Lignes directrices relatives à l'utilisation de serveurs AAA externes

Les ASA appliquent les attributs LDAP en fonction du nom de l'attribut, et non de l'ID numérique. Les attributs RADIUS sont appliqués par ID numérique, et non par nom.

Pour ASDM version 7.0, les attributs LDAP comprennent le préfixe cVPN3000. Pour les versions 7.1 et ultérieures d'ASDM, ce préfixe a été supprimé.

Les attributs LDAP sont un sous-ensemble des attributs Radius, qui sont répertoriés dans le chapitre Radius.

Configurer l'authentification de plusieurs certificats

Vous pouvez désormais valider plusieurs certificats par session au moyen des protocoles client Secure Client (services client sécurisés) SSL et IKEv2. Par exemple, vous pouvez vous assurer que le nom d'émetteur du certificat de machine correspond à une autorité de certification particulière et, par conséquent, que le périphérique est un périphérique émis par l'entreprise.

L'option de certificats multiples permet l'authentification de certificat de la machine et de l'utilisateur au moyen de certificats. Sans cette option, vous ne pourriez authentifier par certificat que la machine ou l'utilisateur, mais pas les deux.

Remarque Étant donné que l'authentification par certificats multiples nécessite un certificat d'ordinateur et un certificat utilisateur (ou deux certificats utilisateur), vous ne pouvez pas utiliser le démarrage Secure Client (services client sécurisés) avant la connexion (SBL) avec cette fonctionnalité.

L'option de préremplissage du nom d'utilisateur permet d'analyser un champ du deuxième certificat (utilisateur) et de l'utiliser pour l'authentification AAA subséquente dans une connexion authentifiée par AAA et certificat. Le nom d'utilisateur, pour le préremplissage principal comme secondaire, est toujours extrait du deuxième certificat (utilisateur) reçu du client.

À partir de la version 9.14(1), l'ASA vous permet de préciser de quel certificat doivent provenir les noms d'utilisateur principal et secondaire lors de la configuration de l'authentification à certificats multiples et de l'utilisation de l'option de préremplissage du nom d'utilisateur pour l'authentification ou l'autorisation. Pour plus de renseignements, consultez Configurer plusieurs noms d'utilisateur de certificat, à la page 3

Avec l'authentification par certificats multiples, deux certificats sont authentifiés : le deuxième certificat (utilisateur) reçu du client est celui à partir duquel sont analysés les noms d'utilisateur principal et secondaire de pre-fill et de username-from-certificate.

Vous pouvez également configurer l'authentification par certificats multiples avec SAML.

Les attributs d'authentification webvpn existants sont modifiés pour inclure une option d'authentification à certificats multiples :

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml]
 | saml [certificate | multiple-certificate]}
```

Avec l'authentification à certificats multiples, vous pouvez prendre des décisions de politique en fonction des champs d'un certificat utilisé pour authentifier cette tentative de connexion. Les certificats utilisateur et machine reçus du client lors de l'authentification à certificats multiples sont chargés dans DAP afin de permettre la configuration de politiques fondées sur les champs du certificat. Pour ajouter l'authentification par certificats multiples à l'aide des Dynamic Access Policies (DAP) afin de pouvoir définir des règles pour autoriser ou refuser les tentatives de connexion, consultez la section *Ajouter plusieurs certificats d'authentification à DAP* dans la version appropriée du Guide de configuration ASDM du VPN ASA.

Configurer plusieurs noms d'utilisateur de certificat

Une nouvelle commande a été introduite dans l'ASA 9.14(1) pour configurer le certificat que l'ASA doit utiliser comme nom d'utilisateur principal et secondaire pour l'authentification ou l'autorisation. Vous pouvez préciser s'il faut utiliser le certificat machine envoyé en SSL ou en IKE (premier certificat) ou le certificat utilisateur envoyé par le client (deuxième certificat) pour obtenir les paramètres d'authentification et d'autorisation. Cette option est disponible et peut être configurée pour tous les groupes de tunnels, quel que soit le type d'authentification (**aaa**, **certificat** ou **certificat multiple (multiple-certificate)**). Cependant, la configuration ne prend effet que pour l'authentification par certificats multiples (**multi-certificat (multiple-certificate)** ou **aaa authentification de certificats multiples (aaa multiple-certificate)**). Lorsque l'option n'est pas utilisée pour l'authentification de plusieurs certificats, le deuxième certificat est utilisé par défaut pour l'authentification ou l'autorisation.

Procédure

Étape 1 Précisez s'il faut utiliser le nom d'utilisateur principal du premier ou du deuxième certificat :

username-from-certificate-choice {first-certificate | second-certificate}

Étape 2 Précisez s'il faut utiliser le nom d'utilisateur secondaire du premier ou du deuxième certificat :

secondary-username-from-certificate-choice {first-certificate | second-certificate}

Exemple :

```
tunnel-group tg1 webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tg1 type remote-access
tunnel-group tg1 general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

Configurer l'autorisation avec LDAP pour le VPN

Lorsque l'authentification de l'utilisateur LDAP pour l'accès VPN a réussi, l'ASA interroge le serveur LDAP, qui renvoie les attributs LDAP. Ces attributs comprennent généralement des données d'autorisation qui s'appliquent à la session VPN.

Il peut arriver que vous ayez besoin de l'autorisation d'un serveur de répertoire LDAP distinct du mécanisme d'authentification. Par exemple, si vous utilisez un serveur SDI ou de certificat pour l'authentification, aucune information d'autorisation n'est renvoyée. Pour les autorisations d'utilisateur dans ce cas, vous pouvez interroger un répertoire LDAP après une authentification réussie, ce qui effectue l'authentification et l'autorisation en deux étapes.

Pour configurer l'autorisation d'utilisateur du VPN à l'aide de LDAP, procédez comme suit.

Procédure

Étape 1 Créez un groupe de serveurs AAA.

aaa-server *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}

Exemple :

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

Étape 2 Créez un groupe de tunnels d'accès à distance IPsec nommé remotegrp.

tunnel-group *groupname*

Exemple :

```
hostname(config)# tunnel-group remotegrp
```

Étape 3 Associez le groupe de serveurs et le groupe de tunnels.

tunnel-group *groupname* **general-attributes**

Exemple :

```
hostname(config)# tunnel-group remotegrp general-attributes
```

Étape 4 Affecte un nouveau groupe de tunnels à un groupe de serveurs AAA précédemment créé pour l'autorisation.

authorization-server-group *group-tag*

Exemple :

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

Exemple

L'exemple suivant montre les commandes pour activer l'autorisation utilisateur avec LDAP. L'exemple crée ensuite un groupe de tunnels d'accès à distance IPsec nommé RAVPN et affecte ce nouveau groupe de tunnels au groupe de serveurs AAA LDAP précédemment créé pour l'autorisation :

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

Après avoir terminé ce travail de configuration, vous pouvez configurer des paramètres d'autorisation LDAP supplémentaires tels que un mot de passe de répertoire, un point de départ pour la recherche dans un répertoire et la portée d'une recherche dans le répertoire en saisissant les commandes suivantes :

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

Définir la configuration LDAP ASA

Cette section décrit comment définir la syntaxe de l'attribut LDAP AV-pair et comprend les renseignements suivants :

- Attributs Cisco pris en charge pour l'autorisation LDAP, à la page 6
- Syntaxe des attributs AV Pair Cisco, à la page 17
- Exemples d'ACL à l'aide de paires Cisco-AV, à la page 18

Remarque L'ASA applique les attributs LDAP en fonction du nom de l'attribut, et non de l'ID numérique. Les attributs RADIUS, en revanche, sont appliqués selon l'ID numérique, et non selon le nom.

L'autorisation désigne le processus d'application d'autorisations ou d'attributs. Un serveur LDAP défini comme serveur d'authentification ou d'autorisation applique les autorisations ou les attributs s'ils sont configurés.

Pour ASA Version 7.0, les attributs LDAP comprennent le préfixe cVPN3000. Pour les versions logicielles 7.1 et ultérieures, ce préfixe a été supprimé.

Attributs Cisco pris en charge pour l'autorisation LDAP

Cette section fournit une liste complète des attributs (voir) pour les ASA 5500, les concentrateurs VPN 3000 et les PIX série 500. Le tableau comprend des renseignements sur la prise en charge d'attributs pour le concentrateur VPN 3000 et les PIX série 500 afin de vous aider à configurer les réseaux avec une combinaison de ces périphériques.

Tableau 1 : Attributs Cisco pris en charge par l'ASA pour l'autorisation LDAP

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
Heures d'accès	O	O	O	Chaîne	Unique	Nom de la plage temporelle (par exemple, heures de travail)
Autoriser le mode d'extension de réseau	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
Délai d'expiration de l'utilisateur authentifié	O	O	O	nombre entier	Unique	1 à 35 791 394 minutes
Authorization-Required	O			nombre entier	Unique	0 = Non 1 = Oui
Authorization-Type	O			nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP
Banner1	O	O	O	Chaîne	Unique	Chaîne de bannière pour les clients VPN SSL sans client, les clients VPN SSL et les clients IPsec.
Banner2	O	O	O	Chaîne	Unique	Chaîne de bannière pour les clients VPN SSL sans client, les clients VPN SSL et les clients IPsec.

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
Cisco-AV-Pair	O	O	O	Chaîne	Multi	Une chaîne d'octets au format suivant : *[Préfixe] [Action] [Protocole] [Source] [Masque générique de la source] [Destination] [Masque générique de la destination] [Établi] [Log] [Opérateur] [Port]* Pour en savoir plus, consultez la section Syntaxe des attributs de paires Cisco-AV.
Cisco-IP-Phone-Bypass	O	O	O	nombre entier	Unique	0 = Désactivé 1 = Activé
Cisco-LEAP-Bypass	O	O	O	nombre entier	Unique	0 = Désactivé 1 = Activé
Client-Intercept-DHCP-Configure-Msg	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
Client-Type-Version-Limiting	O	O	O	Chaîne	Unique	Chaîne du numéro de version du client VPN IPsec
Intervalle de confiance	O	O	O	nombre entier	Unique	10 - 300 secondes
DHCP-Network-Scope	O	O	O	Chaîne	Unique	Adresse IP
Champ DN	O	O	O	Chaîne	Unique	Valeurs possibles : UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER et use-entire-name.
Firewall-ACL-In		O	O	Chaîne	Unique	ID de la liste d'accès
Firewall-ACL-Out		O	O	Chaîne	Unique	ID de la liste d'accès
Politique de groupe		O	O	Chaîne	Unique	Définit la politique de groupe pour la session VPN d'accès à distance. Pour les versions 8.2 et ultérieures, utilisez cet attribut au lieu de IETF-Radius-Class. Vous pouvez utiliser l'un des formats suivants : • nom de la stratégie de groupe • OU = nom de la stratégie de groupe • OU = nom de la stratégie de groupe :

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
IE-Proxy-Bypass-Local				Booléen	Unique	0 = Désactivé 1 = Activé
IE-Proxy-Exception-List				Chaîne	Unique	Une liste des domaines DNS. Les entrées doivent être séparées par la séquence de nouvelle ligne (\n).
IE-Proxy-Method	O	O	O	nombre entier	Unique	1 = Ne pas modifier les paramètres du proxy 2 = Ne pas utiliser de proxy 3 = Détecter automatiquement 4 = Utiliser le paramètre de l'ASA
IE-Proxy-Server	O	O	O	nombre entier	Unique	Adresse IP
IETF-Radius-Class	O	O	O		Unique	Définit la politique de groupe pour la session VPN d'accès à distance. Pour les versions 8.2 et ultérieures, utilisez l'attribut Group-Policy au lieu de IETF-Radius-Class. Vous pouvez utiliser l'un des formats suivants : • nom de la stratégie de groupe • OU = nom de la stratégie de groupe • OU = nom de la stratégie de groupe :
IETF-Radius-Filter-Id	O	O	O	Chaîne	Unique	Nom de la liste d'accès défini sur l'ASA. Le paramètre s'applique aux clients d'accès à distance VPN IPsec et SSL VPN.
IETF-Radius-Framed-IP-Address	O	O	O	Chaîne	Unique	Une adresse IP. Le paramètre s'applique aux clients d'accès à distance VPN IPsec et SSL VPN.
IETF-Radius-Framed-IP-Netmask	O	O	O	Chaîne	Unique	Un masque d'adresse IP. Le paramètre s'applique aux clients d'accès à distance VPN IPsec et SSL VPN.
IETF-Radius-Idle-Timeout	O	O	O	nombre entier	Unique	Secondes

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
IETF-Radius-Service-Type	O	O	O	nombre entier	Unique	1 = Login 2 = Framed 5 = Remote access 6 = Administrative 7 = Invite de commande NAS
IETF-Radius-Session-Timeout	O	O	O	nombre entier	Unique	Secondes
IKE-Keep-Alives	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Allow-Passwd-Store	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Authentication	O	O	O	nombre entier	Unique	0 = None 1 = RADIUS 2 = LDAP (autorisation uniquement) 3 = domaine NT 4 = SDI (RSA) 5 = Interne 6 = RADIUS avec expiration 7 = Kerberos ou Active Directory
IPsec-Auth-On-Rekey	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Backup-Server-List	O	O	O	Chaîne	Unique	Adresses de serveurs (délimitées par des espaces)
IPsec-Backup-Servers	O	O	O	Chaîne	Unique	1 = Utiliser la liste configurée sur le client 2 = Désactivé et effacer la liste des clients 3 = Utiliser la liste des serveurs de sauvegarde
IPsec-Client-Firewall-Filter-Name	O			Chaîne	Unique	Spécifie le nom du filtre à envoyer au client en tant que politique de pare-feu.
IPsec-Client-Firewall-Filter-Optional	O	O	O	nombre entier	Unique	0 = Obligatoire 1 = Facultatif

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
IPsec-Default-Domain	O	O	O	Chaîne	Unique	Spécifie le nom de domaine par défaut unique à envoyer au client (1 à 255 caractères).
IPsec-Extended-Auth-On-Rekey		O	O	Chaîne	Unique	Chaîne
IPsec-IKE-Peer-ID-Check	O	O	O	nombre entier	Unique	1 = Obligatoire 2 = Si pris en charge par le certificat de l'homologue 3 = Ne pas vérifier
IPsec-IP-Compression	O	O	O	nombre entier	Unique	0 = Désactivé 1 = Activé
IPsec-Mode-Config	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP-Port	O	O	O	nombre entier	Unique	4001 à 49 151 ; la valeur par défaut est 10 000.
IPsec-Required-Client-Firewall-Capability	O	O	O	nombre entier	Unique	0 = Aucun 1 = Politique définie par le pare-feu distant « Are-You-There » (AYT) 2 = Politique CPP poussée vers le client 4 = Politique du serveur
IPsec-Sec-association	O			Chaîne	Unique	Nom de l'association de sécurité
IPsec-Split-DNS-Names	O	O	O	Chaîne	Unique	Spécifie la liste des noms de domaine secondaires à envoyer au client (1 à 255 caractères).
IPsec-Split-Tunneling-Policy	O	O	O	nombre entier	Unique	0 = Tunneliser tout le trafic 1 = Tunnelisation fractionnée 2 = Réseau local autorisé
IPsec-Split-Tunnel-List	O	O	O	Chaîne	Unique	Spécifie le nom du réseau ou de la liste de contrôle d'accès qui décrit la liste d'inclusion du tunnel fractionné.

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
IPsec-Tunnel-Type	O	O	O	nombre entier	Unique	1 = Site à site 2 = Accès à distance
L2TP-Encryption	O			nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateless-Req
L2TP-MPPC-Compression	O			nombre entier	Unique	0 = Désactivé 1 = Activé
MS-Client-Subnet-Mask	O	O	O	Chaîne	Unique	Une adresse IP
PFS-Required	O	O	O	Booléen	Unique	0 = Non 1 = Oui
Port-Forwarding-Name	O	O		Chaîne	Unique	Nom de chaîne de caractères (par exemple, « Corporate-Apps »)
PPTP-Encryption	O			Integer	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 128 bits 8 = Stateless-Req Exemple : 15 = 40/128-Encr/Stateless-Req
PPTP-MPPC-Compression	O			nombre entier	Unique	0 = Désactivé 1 = Activé
Primary-DNS	O	O	O	Chaîne	Unique	Une adresse IP
Primary-WINS	O	O	O	Chaîne	Unique	Une adresse IP
Privilege-Level				nombre entier	Unique	Pour les noms d'utilisateur, 0 à 15

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
Required-Client-Firewall-Vendor-Code	O	O	O	nombre entier	Unique	1 = Cisco Systems (avec le client intégré Cisco) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (avec Cisco Intrusion Prevention Security Agent)
Required-Client-Firewall-Description	O	O	O	Chaîne	Unique	—
Required-Client-Firewall-Product-Code	O	O	O	nombre entier	Unique	Produits Cisco Systems : 1 = Cisco Intrusion Prevention Security Agent ou Cisco Integrated Client (CIC) Produits de Zone Labs : 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity Produit NetworkICE : 1 = BlackIce Defender/Agent Produits Sygate : 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Require-HW-Client-Auth	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
Require-Individual-User-Auth	O	O	O	nombre entier	Unique	0 = Désactivé 1 = Activé
Secondary-DNS	O	O	O	Chaîne	Unique	Une adresse IP
Secondary-WINS	O	O	O	Chaîne	Unique	Une adresse IP
SEP-Card-Attribution				nombre entier	Unique	Non utilisé
Connexions simultanées	O	O	O	nombre entier	Unique	De 0 à 2 147 483 647

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
Strip-Realm	O	O	O	Booléen	Unique	0 = Désactivé 1 = Activé
TACACS-Authtype	O	O	O	nombre entier	Unique	—
TACACS-Privilege-Level	O	O	O	nombre entier	Unique	—
Tunnel-Group-Lock		O	O	Chaîne	Unique	Nom du groupe de tunnels ou « none » (aucun)
Tunneling-Protocoles	O	O	O	nombre entier	Unique	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 et 4 sont mutuellement exclusifs (0 à 11, 16 à 27, 32 à 43, 48 à 59 sont des valeurs autorisées).
Use-Client-Address	O			Booléen	Unique	0 = Désactivé 1 = Activé
User-Auth-Server-Name	O			Chaîne	Unique	Adresse IP ou nom d'hôte
Port du serveur d'authentification de l'utilisateur	O	O	O	nombre entier	Unique	Numéro de port pour le protocole de serveur
User-Auth-Server-Secret	O			Chaîne	Unique	Mot de passe du serveur
WebVPN-ACL-Filters		O		Chaîne	Unique	Nom de liste d'accès de type Web
WebVPN-Apply-ACL-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé Avec la version 8.0 et les versions ultérieures, cet attribut n'est pas requis.

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
WebVPN-Citrix-Support-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé Avec la version 8.0 et les versions ultérieures, cet attribut n'est pas requis.
WebVPN-Enable-functions				nombre entier	Unique	Non utilisé — obsolète
WebVPN-Exchange-Server-Address				Chaîne	Unique	Non utilisé — obsolète
WebVPN-Exchange-Server-NETBIOS-Name				Chaîne	Unique	Non utilisé — obsolète
WebVPN-File-Access-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Browsing-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Entry-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Forwarded-Ports		O		Chaîne	Unique	Nom de la liste de transfert de port
WebVPN-Homepage	O	O		Chaîne	Unique	Une URL telle que http://www.exemple.com
WebVPN-Macro-Substitution-Value1	O	O		Chaîne	Unique	Consultez le guide de déploiement du VPN SSL pour obtenir des exemples à l'URL suivante : http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution-Value2	O	O		Chaîne	Unique	Consultez le guide de déploiement du VPN SSL pour obtenir des exemples à l'URL suivante : http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Auto-Download-Enable	O	O		Booléen	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
WebVPN-Port-Forwarding-Enable	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Single-Sign-On-Server-Name	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-Client-DPD	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-Compression	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-Enable	O	O		Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-Gateway-DPD	O	O		nombre entier	Unique	0 = Désactivé n = Valeur de détection d'homologue mort en secondes (30 à 3 600)
WebVPN-SVC-keepalive	O	O		nombre entier	Unique	0 = Désactivé n = Valeur de keepalive en secondes (15 - 600)
WebVPN-SVC-Keep-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-Rekey-Method	O	O		nombre entier	Unique	0 = Aucun 1 = SSL 2 = Nouveau tunnel 3 = Any (défini sur SSL)
WebVPN-SVC-Rekey-Period	O	O		nombre entier	Unique	0 = Désactivé n = période de nouvelle tentative en minutes (4 - 10080)

Nom de l'attribut	VPN 3000	ASA	PIX	Syntaxe/Type	Valeur unique ou valeurs multiples	Valeurs possibles
WebVPN-SVC-Required-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-URL-Entry-Enable	O	O		nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-URL-List		O		Chaîne	Unique	Nom de la liste d'URL

Types d'URL pris en charge dans les listes de contrôle d'accès

L'URL peut être une URL partielle, contenir des caractères génériques pour le serveur ou inclure un port.

Les types d'URL suivants sont pris en charge.

toutes les URL	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

Lignes directrices relatives à l'utilisation des paires Cisco-AV

- Utilisez les entrées de paire Cisco-AV avec le préfixe ip:inacl# pour appliquer les listes d'accès pour les tunnels distants IPsec et SSL VPN Client (SVC).
- Utilisez les entrées de paire Cisco-AV avec le préfixe webvpn:inacl# pour appliquer les listes d'accès aux tunnels sans client du VPN SSL (en mode navigateur).
- Pour les listes de contrôle d'accès de type Web, vous ne spécifiez pas la source, car l'ASA est la source.

Tableau 2 : Jetons pris en charge par l'ASA

Jeton	Champ de syntaxe	Description
ip:inacl# *Num* =	S.O. (identifiant)	(Où *Num* est un entier unique.) Introduit toutes les listes de contrôle d'accès basées sur des paires AV. Applique les listes d'accès pour les tunnels distants IPsec et SSL VPN (SVC).
webvpn:inacl# *Num* =	S.O. (identifiant)	(Où *Num* est un entier unique.) Introduit toutes les listes de contrôle d'accès SSL sans client basées sur des paires AV. Applique les listes d'accès pour les tunnels sans client (mode navigateur).
deny (Refuser)	Action	Refuse l'action. (Par défaut)

Jeton	Champ de syntaxe	Description
permit (Autoriser)	Action	Autorise l'action.
ICMP	Protocole	Internet Control Message Protocol (ICMP)
1	Protocole	Internet Control Message Protocol (ICMP)
IP	Protocole	Protocole Internet (IP)
0	Protocole	Protocole Internet (IP)
TCP	Protocole	protocole TCP (Transmission Control Protocol)
6	Protocole	protocole TCP (Transmission Control Protocol)
UDP	Protocole	Protocole de datagrammes utilisateur (UDP)
17	Protocole	Protocole de datagrammes utilisateur (UDP)
Tous	Nom d'hôte	La règle s'applique à tout hôte.
hôte	Nom d'hôte	Toute chaîne alphanumérique qui dénote un nom d'hôte.
se connecter	Journal	Lorsque l'événement se produit, un message de journal de filtre s'affiche. (Identique à permit and log ou deny and log.)
lt	Opérateur	Valeur inférieure à
gt	Opérateur	Valeur supérieure à
eq	Opérateur	Égal à la valeur
neq	Opérateur	Non égal à la valeur
plage	Opérateur	Plage inclusive. Doit être suivi de deux valeurs.

Syntaxe des attributs AV Pair Cisco

La paire AV Cisco (Attribute Value) (numéro d'identifiant 26/9/1) peut être utilisée pour appliquer les listes d'accès d'un serveur RADIUS (comme Cisco ACS) ou d'un serveur LDAP par l'intermédiaire d'un mappage d'attributs LDAP.

La syntaxe de chaque règle Cisco-AV-Pair est la suivante :

[Préfixe] [Action] [Protocole] [Source] [Masque générique de la source] [Destination] [Masque générique de la destination] [Établi] [Log] [Opérateur] [Port]

Tableau 3 : Règles de syntaxe des attributs d'AV-Pair

Champ	Description
Action	Action à effectuer si la règle correspond à deny (refus) ou permit (permis).

Champ	Description
Destination	Réseau ou hôte qui reçoit le paquet. Précisez-le comme une adresse IP, un nom d'hôte ou le mot-clé **any**. Si vous utilisez une adresse IP, le masque de caractère générique source doit suivre.
Masque de caractère générique de destination	Le masque de caractère générique qui s'applique à l'adresse de destination.
Journal	Génère un message de journal FILTER. Vous devez utiliser ce mot-clé pour générer des événements de niveau de gravité 9.
Opérateur	Opérateurs logiques : supérieur à, inférieur à, égal à, différent de.
Port	Le nombre d'un port TCP ou UDP dans la plage de 0 à 65 535.
Préfixe	Un identifiant unique pour l'AV pair (par exemple : ip:inacl#1= pour les listes d'accès standard ou webvpn:inacl# = pour les listes d'accès VPN SSL sans client). Ce champ ne s'affiche que lorsque le filtre a été envoyé en tant que paire AV.
Protocole	Numéro ou nom d'un protocole IP. Il s'agit d'un entier dans la plage de 0 à 255 ou de l'un des mots-clés suivants : **icmp**, **igmp**, **ip**, **tcp**, **udp**.
Source	Réseau ou hôte qui envoie le paquet. Précisez-le comme une adresse IP, un nom d'hôte ou le mot-clé **any**. Si vous utilisez une adresse IP, le masque de caractère générique source doit suivre. Ce champ ne s'applique pas au VPN SSL sans client, car l'ASA a le rôle de la source ou du proxy.
Masque de caractère générique source	Le masque de caractère générique qui s'applique à l'adresse source. Ce champ ne s'applique pas au VPN SSL sans client, car l'ASA a le rôle de la source ou du proxy.

Exemples d'ACL à l'aide de paires Cisco-AV

Cette section présente des exemples de paires AV Cisco et décrit l'effet d'autorisation ou de refus qui en résulte.

Remarque Chaque numéro d'ACL dans inacl# doit être unique. Cependant, ils n'ont pas besoin d'être séquentiels (par exemple, 1, 2, 3, 4). Autrement dit, ils peuvent être 5, 45, 135.

Tableau 4 : Exemples de paires AV Cisco et de l'effet d'autorisation ou de refus correspondant

Exemple de paire AV Cisco	Effet d'autorisation ou de refus
`ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log`	Permet le trafic IP entre les deux hôtes à l'aide d'un client VPN IPsec ou SSL à tunnel complet.
`ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log`	Autorise le trafic TCP de tous les hôtes vers l'hôte spécifié sur le port 80 uniquement, au moyen d'un client VPN IPsec ou SSL à tunnel complet.

Exemple de paire AV Cisco	Effet d'autorisation ou de refus
`webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share`	Autorise le trafic VPN SSL sans client vers l'URL spécifiée, refuse le trafic SMTP vers un serveur précis et autorise l'accès au partage de fichiers (CIFS) sur le serveur spécifié.
`webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log`	Refuse l'accès Telnet et autorise l'accès SSH sur les ports non par défaut 2323 et 2222, respectivement, ou d'autres flux de trafic d'application utilisant ces ports pour le VPN SSL sans client.
`webvpn:inacl#1=permit url ssh://10.86.1.2webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 logwebvpn:inacl#48=deny url telnet://10.86.1.2webvpn:inacl#100=deny tcp 10.86.1.6 eq 23`	Autorise l'accès SSH du VPN SSL sans client au port par défaut 22 et refuse respectivement l'accès Telnet au port 23. Cet exemple suppose que vous utilisez des modules d'extension Telnet ou SSH Java appliqués par ces listes de contrôle d'accès.

Exemples d'autorisation d'accès à distance Active Directory/LDAP

Cette section présente des exemples de procédures pour configurer l'authentification et l'autorisation sur l'ASA à l'aide du serveur Microsoft Active Directory. Elle comprend les rubriques suivantes:

- Appliquer la politique aux attributs basés sur l'utilisateur, à la page 19
- Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client (services client sécurisés) , à la page 21
- Appliquer l'autorisation ou le refus d'accès entrant, à la page 23
- Appliquer les règles d'heures de connexion et d'heure du jour, à la page 25

D'autres exemples de configuration disponibles sur Cisco.com comprennent les notes techniques suivantes.

- ASA/PIX : exemple de mappage des clients VPN aux stratégies de groupe de VPN à l'aide de la configuration LDAP
- PIX/ASA 8.0 : utiliser l'authentification LDAP pour attribuer une stratégie de groupe à la connexion

Appliquer la politique aux attributs basés sur l'utilisateur

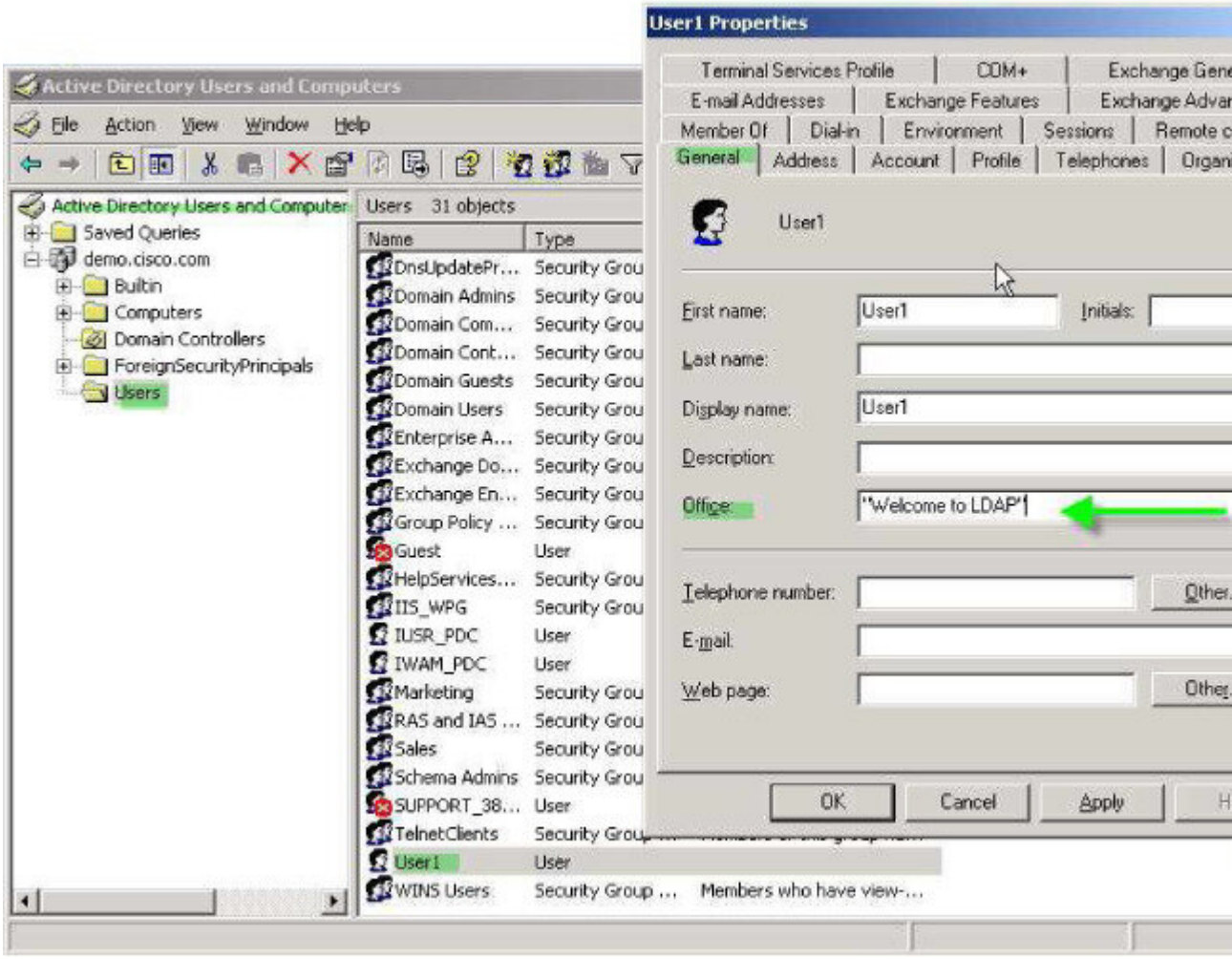
Cet exemple affiche une bannière simple à l'utilisateur, indiquant comment vous pouvez mapper n'importe quel attribut LDAP standard à un attribut spécifique au fournisseur (VSA) bien connu, et vous pouvez mapper un ou plusieurs attributs LDAP à un ou plusieurs attributs LDAP de Cisco. Il s'applique à tout type de connexion, y compris le client VPN IPsec et Secure Client (services client sécurisés).

Pour appliquer une bannière simple à un utilisateur configuré sur un serveur LDAP AD, utilisez le champ Office sous l'onglet General (Général) pour saisir le texte de la bannière. Ce champ utilise l'attribut nommé physicalDeliveryOfficeName. Sur l'ASA, créez une carte d'attributs qui associe physicalDeliveryOfficeName à l'attribut Cisco Banner1.

Lors de l'authentification, l'ASA récupère la valeur de physicalDeliveryOfficeName du serveur, associe la valeur à l'attribut Cisco Banner1 et affiche la bannière à l'utilisateur.

Procédure

Étape 1 Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue Propriétés puis l'onglet **General (Général)** et saisissez le texte de la bannière dans le champ Office (Bureau), qui utilise l'attribut AD/LDAP physicalDeliveryOfficeName.



Étape 2 Créez une correspondance d'attributs LDAP sur l'ASA.

Créez la carte Banner et faites correspondre l'attribut AD/LDAP physicalDeliveryOfficeName à l'attribut Cisco Banner1 :

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

Étape 3 Associez la carte d'attributs LDAP au serveur AAA.

Entrez en mode de configuration de l'hôte du serveur AAA pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS_LDAP et associez la carte d'attributs Banner que vous avez créée précédemment :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

Étape 4 Testez l'application de la bannière.

Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client (services client sécurisés)

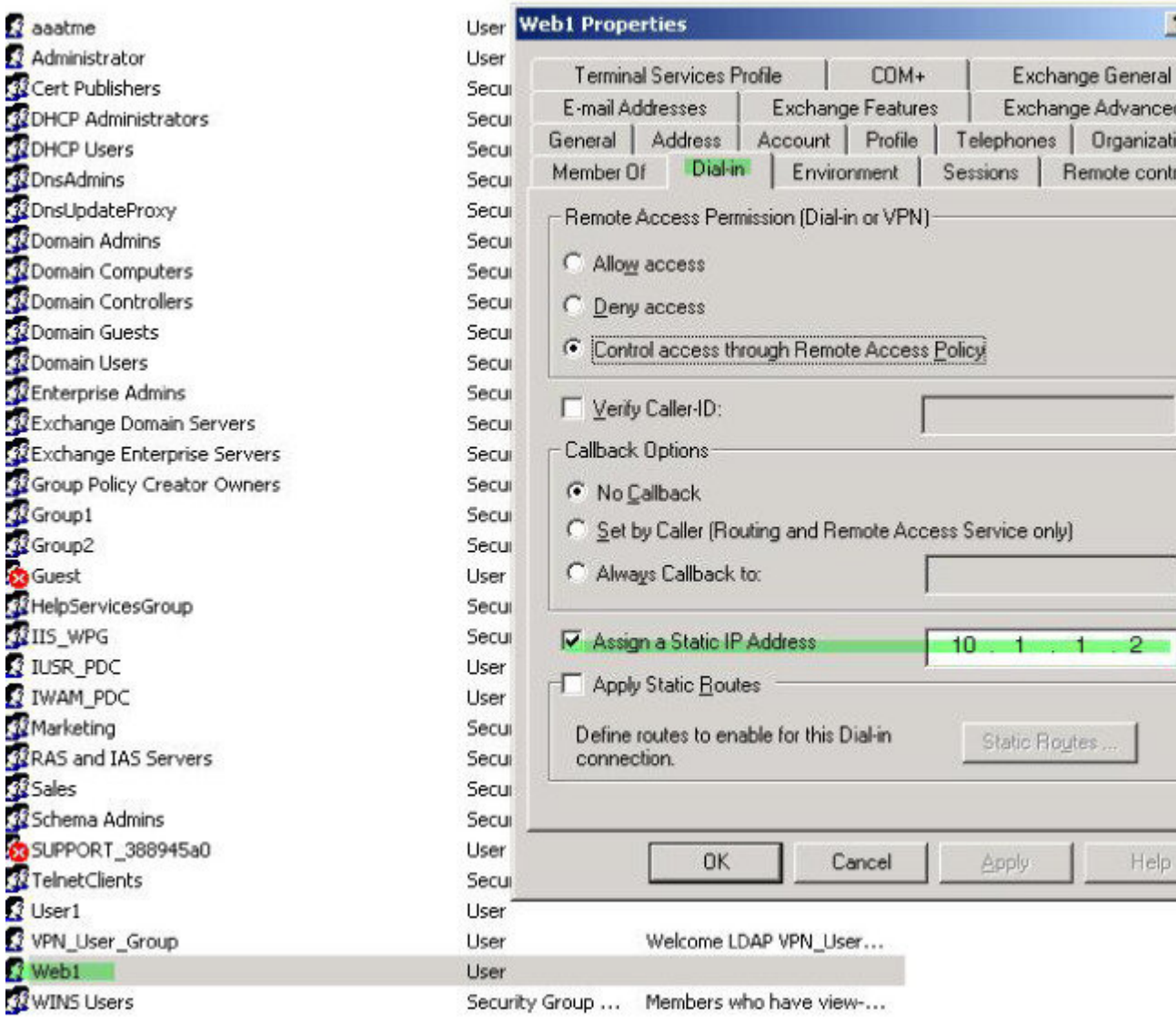
Cet exemple s'applique aux clients de tunnel complet, tels que le client IPsec et les clients VPN SSL.

Pour appliquer les affectations d'adresses IP statiques Secure Client (services client sécurisés), configurez l'utilisateur Web1 Secure Client (services client sécurisés) pour qu'il reçoive une adresse IP statique, saisissez l'adresse dans le champ Assign Static IP Address (Attribuer une adresse IP statique) de l'onglet Dial-in (Accès distant) sur le serveur LDAP AD (ce champ utilise l'attribut msRADIUSFramedIPAddress), puis créez une carte d'attributs qui mappe cet attribut à l'attribut Cisco IETF-Radius-Framed-IP-Address.

Lors de l'authentification, l'ASA récupère la valeur de msRADIUSFramedIPAddress du serveur, la mappe à l'attribut Cisco IETF-Radius-Framed-IP-Address et fournit l'adresse statique à Web1.

Procédure

Étape 1 Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue Properties (Propriétés), puis l'onglet **Dial-in (Accès distant)**, cochez la case **Assign Static IP Address (Attribuer une adresse IP statique)** et saisissez l'adresse IP 10.1.1.2.



Étape 2 Créez une mise en correspondance d'attributs pour la configuration LDAP affichée.

Mappez l'attribut AD msRADIUSFramedIPAddress utilisé par le champ d'adresse statique avec l'attribut Cisco IETF-Radius-Framed-IP-Address :

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

Étape 3 Associez la carte d'attributs LDAP au serveur AAA.

Entrez en mode de configuration d'hôte de serveur AAA pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS_LDAP, puis associez la carte d'attributs static_address que vous avez créée précédemment :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

```
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

Étape 4 Vérifiez que la commande **vpn-address-assignment** est configurée pour spécifier AAA en affichant cette partie de la configuration :

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

Étape 5 Établissez une connexion à l'ASA avec le Secure Client (services client sécurisés). Observez que l'utilisateur reçoit l'adresse IP configurée sur le serveur et mappée à l'ASA.

Étape 6 Utilisez la commande **show vpn-sessiondb svc** pour afficher les détails de la session et vérifier l'adresse attribuée :

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Appliquer l'autorisation ou le refus d'accès entrant

Cet exemple crée une mise en correspondance d'attributs LDAP qui précise les protocoles de tunnellisation autorisés par l'utilisateur. Vous associez les paramètres d'autorisation d'accès et de refus d'accès de l'onglet Dial-in à l'attribut Cisco Tunneling-Protocol, qui prend en charge les valeurs de bitmap suivantes :

Valeur	Protocole de tunnellisation
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	SSL sans client
32	Client SSL—Secure Client (services client sécurisés) ou client VPN SSL
64	IPsec (IKEv2)

[1] (1) IPsec et L2TP sur IPsec ne sont pas pris en charge simultanément. Par conséquent, les valeurs 4 et 8 s'excluent mutuellement.
[2] (2) Voir note 1.

Utilisez cet attribut pour créer une condition Allow Access (TRUE) ou Deny Access (FALSE) pour les protocoles et appliquer la méthode pour laquelle l'utilisateur est autorisé à accéder.

Consultez la note technique ASA/PIX : Mappage des clients VPN avec les stratégies de groupe VPN à l'aide de l'exemple de configuration LDAP pour obtenir un autre exemple d'application de l'autorisation d'accès par numérotation ou de refus d'accès.

Procédure

Étape 1 Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue des propriétés, puis l'onglet **Dial-in**, et cliquez sur le bouton radio Allow Access (autoriser l'accès).

Remarque
Si vous choisissez l'option Contrôle de l'accès par la stratégie d'accès à distance, aucune valeur n'est renvoyée par le serveur et les autorisations appliquées sont basées sur les paramètres de stratégie de groupe internes de l'ASA.

Étape 2 Créez une mise en correspondance d'attributs pour autoriser une connexion IPsec et Secure Client (services client sécurisés), mais refuser une connexion SSL sans client.

a) Créez la carte tunneling_protocols :

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Mappez l'attribut AD msNPAllowDialin utilisé par le paramètre Allow Access (autoriser l'accès) avec l'attribut Cisco Tunneling-Protocols (protocoles de tunnellisation) :

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) Ajoutez des valeurs de carte :

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

Étape 3 Associez la carte d'attributs au serveur AAA.

a) Passez en mode de configuration d'hôte de serveur aaa pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS_LDAP :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) Associez la carte d'attributs tunneling_protocols que vous avez créée :

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

Étape 4 Vérifiez que la carte d'attributs fonctionne comme configurée.

Essayez les connexions à l'aide du protocole SSL sans client, l'utilisateur doit être informé qu'un mécanisme de connexion non autorisée est la raison de l'échec de la connexion. Le client IPsec doit se connecter, car IPsec est un protocole de tunnellisation autorisé en fonction de la carte d'attributs.

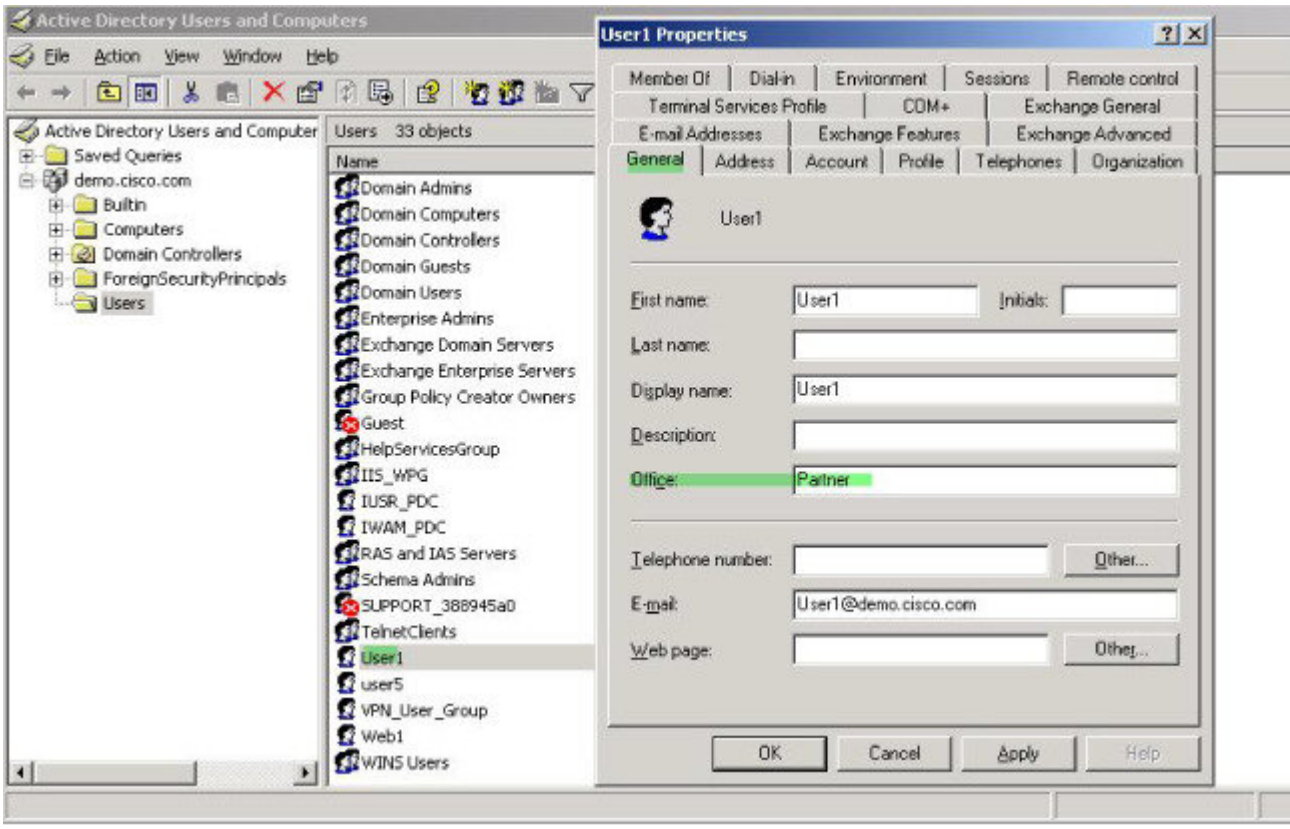
Appliquer les règles d'heures de connexion et d'heure du jour

L'exemple suivant montre comment configurer et appliquer les heures pendant lesquelles un utilisateur SSL sans client (comme un partenaire commercial) est autorisé à accéder au réseau.

Sur le serveur AD, utilisez le champ Office (Bureau) pour saisir le nom du partenaire, qui utilise l'attribut physicalDeliveryOfficeName. Nous créons ensuite une carte d'attributs sur l'ASA pour faire correspondre cet attribut à l'attribut Cisco Access-Hours. Lors de l'authentification, l'ASA récupère la valeur de physicalDeliveryOfficeName et l'associe à Access-Hours.

Procédure

Étape 1 Sélectionnez l'utilisateur, cliquez avec le bouton droit sur **Properties (Propriétés)** puis ouvrez l'onglet **General** (Général) :



Étape 2 Créez une carte d'attributs.

Créez la carte d'attributs access_hours et faites correspondre l'attribut AD physicalDeliveryOfficeName utilisé par le champ Office à l'attribut Cisco Access-Hours.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

Étape 3 Associez la carte d'attributs LDAP au serveur AAA.

Entrez dans le mode de configuration de l'hôte du serveur aaa pour l'hôte 10.1.1.2 du groupe de serveurs AAA MS_LDAP et associez la carte d'attributs access_hours que vous avez créée.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

Étape 4 Configurez les plages de temps pour chaque valeur autorisée sur le serveur.

Configurez les heures d'accès du partenaire de 9 h à 17 h du lundi au vendredi :

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.