Contrôle de l'utilisateur avec le VPN d'accès à distance

Les rubriques suivantes traitent de la façon d'effectuer la sensibilisation et le contrôle des utilisateurs avec le VPN d'accès à distance :

La source d'identité du VPN d'accès à distance

Secure Client est le seul client pris en charge sur les périphériques de point terminal pour la connectivité VPN à distance vers les périphériques défense contre les menaces .

Lorsque vous configurez une passerelle VPN sécurisée comme indiqué dans la Créer une nouvelle politique VPN d'accès à distance, vous pouvez configurer une politique d'identité pour ces utilisateurs et associer la politique d'identité à une politique de contrôle d'accès, à condition que vos utilisateurs se trouvent dans un référentiel Active Directory.

Remarque Si vous utilisez le VPN d'accès à distance avec l'identité de l'utilisateur et RADIUS comme source d'identité, vous devez configurer le domaine (**Objets > Gestion des objets > Serveur AAA > Groupe de serveur RADIUS).**

Les informations de connexion fournies par un utilisateur distant sont validées par un domaine LDAP ou AD ou un groupe de serveurs RADIUS. Ces entités sont intégrées à la passerelle sécurisée Cisco Secure Firewall Threat Defense.

Remarque Si les utilisateurs s'authentifient auprès du VPN d'accès à distance en utilisant Active Directory comme source d'authentification, ils doivent se connecter avec leur nom d'utilisateur; le format `domaine\nom_utilisateur` ou `nom_utilisateur@domaine` échoue. (Active Directory fait référence à ce nom d'utilisateur sous le nom de *nom de connexion* ou parfois sous le nom de `sAMAccountName`.) Pour en savoir plus, consultez Attributs de dénomination des utilisateurs sur MSDN.

Si vous utilisez RADIUS pour l'authentification, les utilisateurs peuvent se connecter dans l'un des formats mentionnés ci-dessus.

Une fois authentifié au moyen d'une connexion VPN, l'utilisateur distant prend une *identité VPN*. Cette identité VPN est utilisée par *les politiques d'identité* sur la passerelle sécurisée Cisco Secure Firewall Threat Defense pour reconnaître et filtrer le trafic réseau appartenant à cet utilisateur distant.

Les politiques d'identité sont associées aux politiques de contrôle d'accès, qui déterminent qui a accès aux ressources réseau. C'est de cette façon que l'utilisateur distant a bloqué ou autorisé l'accès à vos ressources réseau.

Sujets connexes

Présentation du VPN
Aperçu du VPN d'accès à distance Cisco Secure Firewall Threat Defense
Principes de base du VPN
Fonctionnalités du VPN d'accès à distance
Lignes directrices et limites pour le VPN d'accès à distance
Créer une nouvelle politique VPN d'accès à distance

Configurer un VPN d'accès à distance pour le contrôle utilisateur

Avant de commencer

- Créez un domaine comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- Pour utiliser l'authentification, l'autorisation et l'audit (AAA), configurez un groupe de serveurs RADIUS comme indiqué dans Ajouter un groupe de serveurs RADIUS.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Devices (périphériques)** > **VPN** > **Remote Access** (accès distant).

Étape 3 Consultez Créer une nouvelle politique VPN d'accès à distance.

Prochaine étape

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans Créer une politique d'identité.
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans Association d'autres politiques au contrôle d'accès.
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration.
- Surveillez le trafic des utilisateurs VPN .

Dépanner la source d'identité du VPN d'accès à distance

- Pour d'autres renseignements de dépannage, voir Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs et Dépannage du contrôle d'utilisateur .
- Si vous rencontrez des difficultés avec le VPN d'accès à distance, vérifiez la connexion entre votre centre de gestion et un périphérique géré. Si la connexion échoue, toutes les connexions VPN d'accès à distance signalées par le périphérique ne peuvent pas être identifiées pendant le temps d'arrêt, sauf si les utilisateurs ont déjà été vus et téléchargés sur centre de gestion.

  Les utilisateurs non identifiés sont connectés en tant qu'utilisateurs inconnus sur centre de gestion. Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.
- Le nom d'hôte du périphérique géré doit comporter moins de 15 caractères pour que l'authentification Kerberos réussisse.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.

N'observe pas les paramètres corrects pour les statistiques VPN

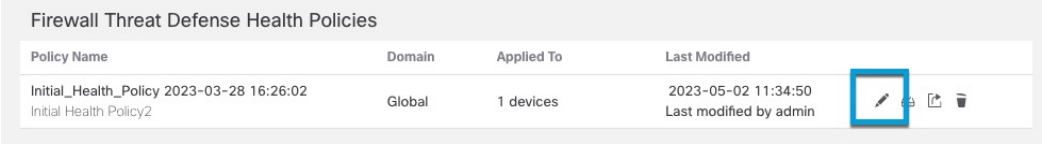
Cette tâche décrit les étapes à suivre après avoir activé ou désactivé le paramètre **Statistiques VPN** dans une politique d'intégrité. Si cette tâche n'est pas effectuée, les périphériques gérés ont une politique d'intégrité avec des paramètres incorrects.

Procédure

Étape 1 Connectez-vous au Cisco Secure Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **System** (⚙) > **Politique** > **d'intégrité**.

Étape 3 Sous Politiques d'intégrité de Firewall Threat Defense, cliquez sur **Edit** (✎) à côté de la politique à modifier.



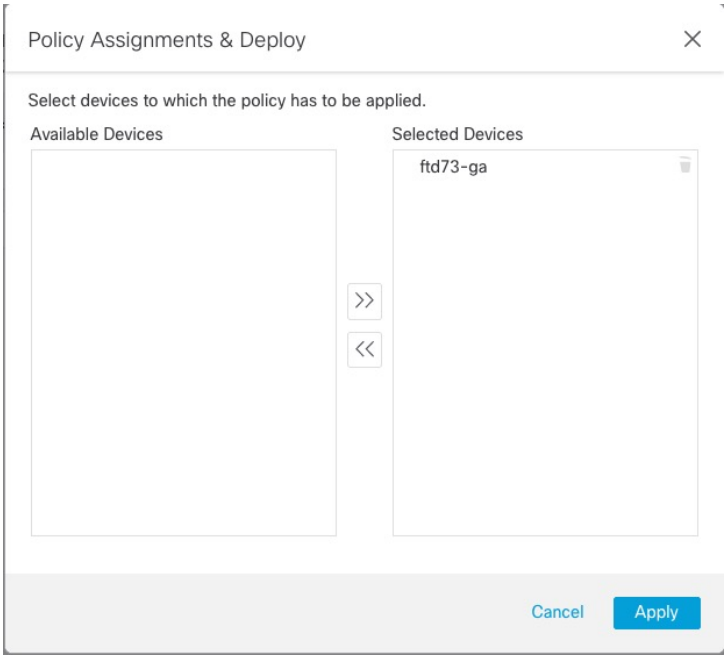
Étape 4 Dans la page à l'onglet **Health Modules** (Modules d'intégrité), faites défiler la liste vers le bas pour trouver **Statistiques VPN**.

Étape 5 Vérifiez que le paramètre des statistiques VPN est correct ou modifiez-le si nécessaire.

Étape 6 Si vous avez modifié le paramètre, cliquez sur **Enregistrer**, puis sur **Annuler** pour revenir à la politique d'intégrité.

Étape 7 Sous Politiques d'intégrité de Firewall Threat Defense,liquer sur **Déployer la politique d'intégrité** () pour appliquer la politique.

Étape 8 Dans la boîte de dialogue **Policy Assignments & Deploy** (affectation et déploiement des politiques), déplacez les périphériques sur lesquels déployer la politique d'intégrité vers le champ **Selected Devices** (périphériques sélectionnés).



Étape 9 Cliquez sur **Apply**.
Un message s'affiche lorsque la politique d'intégrité est déployée.

Étape 10 Une fois le déploiement de la politique d'intégrité terminé, cliquez sur **Politiques** > **Contrôle d'accès** pour modifier une politique de contrôle d'accès.

Étape 11 Cliquez sur **Edit** () à côté de la politique que vous souhaitez modifier.

Étape 12 Apportez une modification mineure à la politique, par exemple en modifiant son nom.

Étape 13 Enregistrez la politique de contrôle d'accès.

Étape 14 Déployer les changements de configuration..

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.