Pratique recommandée pour implémenter PIE (Policy Import Export) dans Cisco NAC

Contenu

Introduction

Le but de ce document est de mettre en valeur les instructions de pratique recommandée pour assurer une implémentation réussie de la caractéristique de Policy Import Export (SECTEUR) dans le Cisco NAC.

Conditions préalables

Conditions requises

La connaissance est exigée de l'interface web de gestionnaire de Cisco NAC (Clean Access Manager) et des stratégies qui sont typiquement configurées. Référez-vous aux notes en version pour la version 4.5 de Cisco NAC pour ce qui est et n'est pas pris en charge avec le SECTEUR.

Composants utilisés

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

- Logiciel 4.5.0 de Cisco NAC

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Recommandations de pratique recommandée de SECTEUR

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Suivez les recommandations répertoriées ci-dessous pour assurer une implémentation réussie de caractéristique de Policy Import Export de CAM (SECTEUR).

1. Cisco recommande que vous configuriez les mêmes configurations automatiques de mise à jour sur le maître et le récepteur NACMs (sous la **Gestion de périphériques > le Clean Access > met à jour > mise à jour**) pour s'assurer que tout le NACMs ont les mêmes mises à jour de Cisco avant que vous exécutiez un sync de stratégie. C'est parce que les contrôles en cours sur le dépassement principal en vérifie le récepteur si vous exécutez des mises à jour de Cisco sur un récepteur NACM avec différentes configurations automatiques de mise à jour et puis exécutez un sync de stratégie.
2. Si vous avez un OOB NACM et n'importe quel legs NACM avec un permis réservé IB, assurez-vous que vous utilisez l'OOB NACM comme maître NACM et legs NACM comme récepteurs.
3. Une fois que le SECTEUR est activé pour un composant particulier entre le maître et le récepteur, les tables de récepteur/informations sont complètement remplacées par les informations qui sont poussées du maître. Il n'est pas cumulatif du côté de récepteur. Par exemple, si le récepteur a une règle de la circulation qui permet l'accès à mcafee.com et le maître a les règles de la circulation qui permettent l'accès à cisco.com et à abc.com, mais aucune règle pour mcafee.com, le récepteur et le maître n'auront des règles identiques une fois que le sync est exécuté : cisco.com et abc.com. Notez que la règle de la circulation pour mcafee.com n'existe pas sur le récepteur après le sync puisque le maître n'a pas eu cette règle. La pratique recommandée est de configurer le maître NACM comme désirée mais de ne pas modifier les paramètres de la stratégie sur les récepteurs.
4. Le nombre maximal de récepteurs pris en charge a 10. ans. Bien qu'il n'y ait aucune limite technique au nombre de récepteurs, la recommandation de pratique recommandée est de garder ceci au nombre pris en charge (moins de ou égal à 10).**Note**: Pour des Ha-paires NACM, les configurations de sync de stratégie sont désactivées pour le standby NACM.
5. Le maître et les récepteurs doivent exécuter la même version de la release de Cisco NAC (4.5 ou plus élevé).
6. Assurez-vous que les deux gestionnaires NAC font faire confiance les Certificats signés d'Autorité de certification (CA) et maître et récepteur aux Certificats de l'un l'autre. Les Certificats sont principaux pour sécuriser la synchronisation entre le maître et le récepteur. Le maître doit faire confiance au certificat présenté par le récepteur et vice-versa. Pour ceci,

il est nécessaire de s'assurer que chacun d'eux a la racine CA de leur certificat de pair (pleine chaîne si l'intermédiaire est impliqué) dans la liste de confiance CA. Dans des déploiements de production, la pratique recommandée est de remplacer les Certificats auto-signés sur le gestionnaire NAC par les Certificats signés CA. En bref, assurez-vous que les pratiques recommandées de certificat ssl de gestionnaire NAC sont rencontrées avant que vous implémentiez le SECTEUR.

7. Assurez-vous que vous êtes ouvert une session comme un utilisateur d'admin de plein contrôle au gestionnaire du maître NAC afin d'exécuter le sync automatique ou manuel de stratégie.
8. Le sync automatique te permet pour programmer un sync automatique de stratégie une fois que chaque nombre *X de* jours (le minimum est de 1 jour). Si vous désirez utiliser le sync automatique pour le SECTEUR, Cisco recommande vivement que vous d'exécuter un sync manuel et de le vérifier que le sync fonctionne avec succès avant que vous activiez le sync automatique entre vos gestionnaires NAC.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems