Vérification du décodage IPS dans Cisco Secure Access

Table des matières

Problème

Lors de l'utilisation de Cisco Secure Access avec RAVPN (Remote Access VPN) via Secure Client, les entreprises doivent vérifier si le décryptage et l'inspection IPS (Intrusion Prevention System) sont effectués correctement pour le trafic vers des sites Web spécifiques. Le principal défi consiste à confirmer que les processus de décryptage et d'inspection TLS fonctionnent correctement par le biais de méthodes autres que les journaux d'interface utilisateur de gestion standard tels que la recherche d'activité. Les exigences de vérification spécifiques incluent l'identification des contrôles de certificat côté client ou des mécanismes de débogage/reporting qui peuvent prendre en charge la validation des tests et fournir une confirmation supplémentaire du fonctionnement du système de prévention des intrusions au-delà de l'interface de gestion.

Environnement

- Cisco Secure Access (CSA) avec fonctionnalité RAVPN
- Cisco Secure Client pour les connexions VPN d'accès à distance
- Fonctionnalités de déchiffrement et d'inspection IPS activées
- Trafic TLS/SSL nécessitant un déchiffrement pour l'inspection de sécurité
- Trafic Web des clients RAVPN vers des sites Web externes

Résolution

Il existe deux méthodes pour vérifier que le décryptage et l'inspection IPS fonctionnent correctement pour le trafic VPN d'accès à distance dans Cisco Secure Access :

Méthode 1 : Recherche d'activité de l'interface utilisateur de gestion (méthode principale)

La fonction de recherche d'activité de l'interface de gestion Cisco Secure Access fournit la méthode la plus fiable pour confirmer les opérations de déchiffrement et d'inspection IPS. Cette interface affiche des journaux détaillés et des analyses indiquant quand le trafic a été décrypté et inspecté par les services de sécurité.

Pour accéder à la recherche d'activité :

Accédez au tableau de bord de gestion Cisco Secure Access et localisez la fonctionnalité Recherche d'activité pour consulter les journaux d'inspection du trafic et l'état de déchiffrement pour des sessions utilisateur et des sites Web de destination spécifiques.

Pour activer les journaux de décodage, ce paramètre peut être activé sur les paramètres globaux :

Tableau de bord -> Sécurisé -> Stratégie d'accès -> Paramètres par défaut et paramètres globaux -> Paramètres globaux -> Journalisation du décodage.

Méthode 2 : Vérification du certificat côté client

Comme méthode de vérification supplémentaire, vous pouvez effectuer des contrôles de certificat côté client pour confirmer que le déchiffrement du trafic est en cours.

Lorsque Cisco Secure Access parvient à décrypter et à inspecter le trafic TLS, il présente son propre certificat au client au lieu du certificat d'origine du site Web.

Pour vérifier le déchiffrement via l'inspection de certificat :

1. Consultez le certificat du site Web
Ouvrez les détails du certificat dans le navigateur et vérifiez l'émetteur et la période de validité.

Si le certificat est émis par l'autorité de certification racine d'accès sécurisé Cisco avec une période de validité d'environ 10 jours, il indique le déchiffrement du système de prévention des intrusions au niveau du pare-feu.

Si la validité du certificat est d'environ 5 jours, elle indique un déchiffrement basé sur la passerelle Web sécurisée.

2. Validez l'émetteur du certificat (attribution de noms DC)

Cette méthode de vérification de certificat côté client sert de technique de confirmation supplémentaire avec la méthode de recherche d'activité principale, fournissant une assurance supplémentaire que les processus de déchiffrement IPS fonctionnent comme prévu.

Système de prévention des intrusions Ne pas déchiffrer :

Le déchiffrement pour le système de prévention des intrusions aura lieu si :

· Il est activé dans les paramètres globaux ET

· Le système de prévention des intrusions est activé pour au moins une des règles de stratégie d'accès (je pense que même si la règle est désactivée, cette condition s'applique toujours)

Souhaitent contourner un domaine du déchiffrement du système de prévention des intrusions

Utilisez la liste Ne pas déchiffrer fournie par le système et ajoutez le domaine dans la liste Ne pas déchiffrer fournie par le système.

ou

Utiliser le déchiffrement basé sur la source sous Paramètres globaux sur l'accès sécurisé Cisco -

REMARQUE : cela fonctionnera si AUCUNE NAT sortante n'est configurée sur la configuration du tunnel réseau sur Secure Access.

Motif

La nécessité de recourir à plusieurs méthodes de vérification découle de la nécessité de valider l'application des politiques de sécurité dans les environnements d'entreprise. Alors que les journaux de l'interface utilisateur de gestion offrent une visibilité complète, les méthodes de

vérification côté client offrent des points de confirmation supplémentaires qui peuvent être utiles pour les scénarios de test de conformité, de dépannage et de validation où l'accès direct aux interfaces de gestion peut être limité ou lorsque plusieurs points de vérification sont nécessaires pour des procédures de test complètes.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.