Synchronisation ESA externe vers SMA cloud

Table des matières

Introduction

Q. Quelles connexions sont autorisées des ESA externes vers SMA de cloud et des ESA de cloud vers SMA externe ?

R. Pour des raisons de sécurité, seuls les ports 25 et 587 sont autorisés à entrer dans les appliances CES des data centers. Les connexions sortantes à partir des data centers ne sont pas aussi restreintes et par conséquent tous les ports de service pertinents sont autorisés.

Remarque : externe fait référence à toutes les appliances qui ne sont hébergées dans aucun data center Cisco.

Un SMA se synchronise avec un ESA en établissant une connexion via le port SSH 22. Cela signifie que la connexion est initialisée à partir du SMA, par conséquent un SMA de cloud serait capable de se synchroniser avec un ESA en dehors des data centers CES.

Les services centralisés gérés entre un SMA et un ESA sont les suivants :

1. Reporting (récupéré par le SMA sur la connexion établie du port 22)

2. Suivi des messages (récupéré par le SMA sur la connexion établie du port 22)

3. Mise en quarantaine du spam (envoyé du ESA au SMA via le port 6025)

4. Quarantaine des stratégies, des virus et des attaques (envoyée du ESA au SMA via le port 7025)

Lorsque la connexion au port SSH 22 est initialisée à partir du SMA dans les data centers, les services de signalement et de suivi des messages fonctionnent lorsque le trafic de retour d'Internet est autorisé à revenir dans les data centers.

Les connexions de quarantaine du spam et de quarantaine des politiques, des virus et des attaques sont initialisées depuis l'ESA vers le SMA et sur des ports qui ne sont pas ouverts d'Internet vers les data centers. Par conséquent, ces deux services centralisés ne seront pas fonctionnels.

En résumé, un ESA externe ou des ESA peuvent être synchronisés avec un SMA de cloud avec uniquement les services Reporting and Message Tracking pris en charge.

L'inverse n'est absolument pas supporté. Il s'agirait d'ESA cloud se synchronisant avec un SMA externe. Rappelez-vous que la synchronisation est initialisée à partir du SMA sur le port 22 pour établir la connexion et que le port 22 n'est pas autorisé à partir d'Internet dans les centres de données que la connexion ne sera jamais réussie. Tous les ports sortants sont ouverts, de sorte que le trafic du service de quarantaine du spam sur le port 6025 et du service de quarantaine des stratégies, des attaques et des virus sur le port 7025 peut être envoyé des ESA du cloud vers le SMA externe, mais la connexion SSH initiale ne serait jamais établie, de sorte qu'elle empêcherait le reste de la fonctionnalité.

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.