Meilleures pratiques de planification des mises à jour de contenu Secure Firewall

Problème

Les entreprises qui gèrent des périphériques Firewall Threat Defense (FTD) avec Firewall Management Center (FMC) ont besoin de conseils sur les meilleures pratiques d'application des mises à jour de sécurité et de contenu. Plus précisément, il existe une incertitude quant à la fréquence à laquelle différents types de mises à jour doivent être appliqués, quant à savoir si les mises à jour peuvent être planifiées plutôt qu'appliquées immédiatement, et quant à l'impact opérationnel de ces mises à jour. La question se pose parce que Cisco publie des mises à jour de contenu fréquemment, parfois hebdomadaires, et que les administrateurs doivent comprendre si ces mises à jour doivent être appliquées immédiatement après la publication ou si elles peuvent être planifiées en fonction des fenêtres de maintenance de l'entreprise et des politiques de gestion des modifications.

Environnement

- Cisco Secure Firewall Firepower, toutes versions
- Firepower Management Center, toutes versions

Résolution

Ce tableau indique l'objectif de chaque type de mise à jour dans Firepower.

Type de mise à jour	Objectif	Remarques
SRU/LSP	Mises à jour des règles d'intrusion (Snort 2 et Snort 3 respectivement)	Conserve les règles de détection/prévention des intrusions

GeoDB	Données de géolocalisation pour les adresses IP	Utilisé pour le filtrage du trafic basé sur la géolocalisation
VDB	Informations de vulnérabilité et empreintes des hôtes	Utilisé pour l'évaluation des vulnérabilités et l'analyse des risques

Les mises à jour de contenu Cisco Secure Firewall sont classées en trois types distincts, chacun avec des fréquences de diffusion et des pratiques de planification recommandées différentes. Ce tableau présente les recommandations de planification des meilleures pratiques pour chaque type de mise à jour :

Type de mise à jour	Fréquence De Libération	Calendrier suggéré	Planification FMC par défaut	Chemin de navigation (à modifier)
SRU/LSP	Fréquent	Quotidien	Quotidien	Système > Mises à jour du contenu > Mises à jour des règles
GeoDB	~Hebdomadaire	Hebdo	Hebdo	Système > Mises à jour du contenu > Mises à jour de géolocalisation
VDB	~Mensuel	Hebdo	Hebdo	Système > Outils : Planification > Téléchargement hebdomadaire de logiciels

Pour optimiser les configurations et la position de sécurité, la meilleure pratique consiste à appliquer l'une de ces mises à jour dès qu'elles sont publiées par Cisco. Certains de ces fichiers de mise à jour peuvent être assez volumineux et des allocations de bande passante doivent être prises en compte. Il est conseillé d'installer les mises à jour les plus importantes en dehors des heures de pointe, si vous utilisez le même réseau.

Mises à jour SRU/LSP (Intrusion Rules)

Les mises à jour SRU (Snort Rule Updates) et LSP (Lightweight Security Packages) contiennent des règles de détection et de prévention des intrusions. Ces mises à jour doivent être appliquées aussi fréquemment que possible sur le plan opérationnel pour assurer la protection contre les menaces émergentes.

Pour modifier la planification SRU/LSP : Accédez à System > Content Updates > Rule Updates dans l'interface FMC pour ajuster les paramètres d'heure, de date et de fréquence.

Les mises à jour SRU/LSP prennent en charge le déploiement automatisé et peuvent être planifiées pour un déploiement automatique après le téléchargement et l'installation.

Mises à jour de GeoDB (Geolocation Database)

Les mises à jour de la base de données de géolocalisation fournissent des données de localisation géographique actuelles pour les adresses IP et sont généralement publiées chaque semaine.

Pour modifier la planification GeoDB : Accédez à System > Content Updates > Geolocation Updates dans l'interface FMC pour ajuster les paramètres de planification.

Les mises à jour GeoDB peuvent être planifiées pour le téléchargement et l'installation, mais le déploiement sur des périphériques gérés nécessite une diffusion manuelle et ne peut pas être entièrement automatisé comme les mises à jour SRU/LSP.

Mises à jour VDB (Vulnerability Database)

Les mises à jour de la base de données de vulnérabilité sont publiées environ tous les mois et sont gérées comme des mises à jour logicielles plutôt que comme des mises à jour de contenu.

Pour modifier la planification VDB : Accédez à Système > Outils : Planification et modification de la tâche de téléchargement hebdomadaire de logiciels afin d'ajuster la fréquence et la durée du téléchargement.

Les mises à jour de VDB font partie des mises à jour logicielles et ne peuvent pas être déployées indépendamment. Ils sont inclus lors des déploiements manuels qui compilent toutes les modifications en attente.

Considérations de déploiement

Lors du déploiement des mises à jour, le FMC compile toutes les modifications de configuration en attente et peut inclure plusieurs types de mises à jour de contenu en une seule opération de déploiement. Certaines mises à jour peuvent entraîner de brefs redémarrages du service Snort pendant le déploiement, ce qui doit être pris en compte lors de la planification des mises à jour pendant les heures de production.

Les organisations doivent aligner les calendriers de mise à jour sur leurs politiques de gestion des changements et envisager de planifier les mises à jour pendant les fenêtres de maintenance si de

brèves interruptions de service constituent un problème pour leur environnement opérationnel.

Motif

Il s'agissait d'une demande de configuration et d'orientation opérationnelle plutôt que d'un dysfonctionnement technique. La nécessité d'apporter des clarifications découle de l'incertitude entourant les pratiques de planification des mises à jour, les capacités d'automatisation et l'impact opérationnel des différents types de mises à jour de contenu dans les environnements Cisco Secure Firewall.

Autres informations utiles

- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Mises à jour
- 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.