Clarifier l'impact sur les performances et les meilleures pratiques pour le déchiffrement SSL/TLS sur FTD

Table des matières

Problème

Un utilisateur envisage d'activer le décodage SSL/TLS sur un périphérique Firewall Threat Defense (FTD) et doit comprendre l'impact potentiel sur les performances du périphérique avant la mise en oeuvre. Les principales préoccupations sont les suivantes :

- Impact sur le débit du pare-feu, la latence et les performances globales de traitement du trafic.
- L'utilisation prévue du processeur et de la mémoire augmente après l'activation du déchiffrement.
- Directives de dimensionnement et références de performances pour des modèles FTD spécifiques.
- Limites recommandées pour les sessions décryptées simultanées.
- Meilleures pratiques et conditions préalables pour le déploiement en production.

Environnement

- Firepower 4115. D'autres plates-formes matérielles peuvent également être affectées.
- FTD Version 7.4.2 (Build 172). D'autres versions logicielles peuvent également être affectées.
- Prise en compte de la fonctionnalité de décodage SSL/TLS.
- Planification du déploiement en environnement de production.

Résolution

Le décryptage SSL/TLS ajoute une surcharge de traitement au Firepower 4115, mais l'impact réel dépend fortement de la quantité de trafic décryptée et de l'inspection appliquée après le décryptage.

Analyse de l'impact des performances

Les impacts du déchiffrement SSL/TLS incluent :

- Débit effectif réduit.
- Latence plus élevée.
- Augmentation de l'utilisation du processeur Snort/inspection.
- Augmentation du CPU et de la mémoire qui ne peut pas être prédite avec précision en tant que pourcentage fixe sans analyse réelle du profil du trafic.

Tests de performances FPR 4115

Spécifications du banc d'essai Firepower 4115 publié par Cisco :

- Débit de déchiffrement matériel TLS : 6,5 Gbit/s.
- Débit FW + AVC : 33 Gbit/s.
- Nombre maximal de sessions simultanées avec AVC : 15 millions.
- Nombre maximal de nouvelles connexions par seconde avec AVC : 210 000.

Remarque importante sur le dimensionnement : Le banc d'essai de décryptage matériel TLS 6,5 Gbit/s est basé sur des conditions de test spécifiques. Le débit de production peut être plus faible si vous décryptez un pourcentage important du trafic, si vous inspectez le trafic décrypté à l'aide de politiques d'intrusion/de fichiers/de programmes malveillants ou si vous traitez de nombreuses

sessions TLS de courte durée.

Cisco ne publie pas de numéro distinct de « nombre maximal de sessions décryptées simultanées » pour Firepower 4115 sur FTD 7.4.2. En pratique, la capacité est validée à l'aide de la combinaison de trafic, des sessions simultanées, du débit de connexion, des suites de chiffrement et de la charge de la stratégie d'inspection.

Approche recommandée pour le déploiement en production

Étape 1: Commencez par un pilote limité

- N'activez pas initialement les règles générales de « décryptage total ».
- Commencez par les utilisateurs, les sous-réseaux ou les catégories de destination sélectionnés.
- Conservez une gestion par défaut prudente avec Ne pas décrypter pour le trafic qui ne nécessite pas d'inspection.

Étape 2: Exclure le trafic qui est généralement interrompu par le déchiffrement

- Sites bancaires/financiers.
- Portails de santé.
- Applications épinglées par certificat.
- Certains logiciels en tant que service (SaaS) et certaines applications cloud/de sécurité des terminaux.
- Applications sensibles critiques, sauf si elles ont été explicitement testées.

Étape 3: Gardez les règles SSL simples et ordonnées avec soin

- Placez les exclusions Ne pas déchiffrer spécifiques au-dessus des règles de déchiffrement plus générales.
- Évitez si possible les correspondances trop larges ou trop complexes.

- N'utilisez pas la version TLS ou les conditions de la suite de chiffrement pour les règles Decrypt-Resign/Known-Key, car les documents Cisco indiquent que cela peut entraîner un comportement imprévisible.

Étape 4: Valider le certificat de préparation

- Pour le déchiffrement-résignation sortant, le certificat de l'autorité de certification de signature doit être approuvé par les points de terminaison clients.
- Pour le déchiffrement de clé connue entrante, le pare-feu doit disposer du certificat de serveur/matériel de clé privée correct.

Étape 5: Surveillance pendant le déploiement

- Suivre l'utilisation globale du processeur et, plus important, l'utilisation du processeur Snort/inspection.
- Suivre les connexions simultanées et les nouvelles connexions par seconde.
- Examiner les erreurs d'état de flux SSL/de connexion dans les événements de connexion.
- Surveillez les indicateurs de sursouscription TLS et les défaillances spécifiques aux applications.

Pour plus d'informations sur la surveillance de la vérification du processeur :

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Pensez comme un ingénieur TAC : Un guide sur les principaux points noirs de Cisco Secure Firewall

Pour le suivi des connexions et des nouvelles connexions par seconde, vérifiez :

- Meilleures pratiques de journalisation

Pour le suivi des erreurs d'état de flux SSL/d'échange lors de la vérification des événements de connexion et des indicateurs de sursouscription TLS :

- Dépannage de la surinscription TLS/SSL

Étape 6: Revenez en arrière ou réduisez la portée si vous voyez :

- Inspection soutenue saturation du processeur.
- Augmentation de la latence visible par l'utilisateur.
- Échecs de connexion TLS.
- Les applications métier échouent après le déchiffrement.
- Sursouscription ou erreurs SSL excessives.

Étape 7: Considérer l'impact de TLS 1.3

L'adoption de TLS 1.3 peut affecter la visibilité et le comportement, car certaines caractéristiques de prise de contact et d'inspection diffèrent de TLS 1.2.

Motif

Le déchiffrement SSL/TLS nécessite des ressources de calcul supplémentaires pour déchiffrer, inspecter et rechiffrer les flux de trafic. L'impact sur les performances varie considérablement en fonction des modèles de trafic, des politiques d'inspection appliquées au trafic déchiffré et de la configuration de déploiement spécifique. Sans une planification appropriée et une mise en oeuvre progressive, les entreprises peuvent subir une dégradation inattendue des performances dans les environnements de production.

Autres informations utiles

- Guide de configuration des périphériques Cisco Secure Firewall Management Center - Règles de décodage
- Guide de politique de déchiffrement de Cisco Secure Firewall
- Meilleure pratique pour l'ordre des règles de stratégie de décodage
- Simplification du déchiffrement grâce au pare-feu sécurisé Cisco 7.7
- Meilleures pratiques des règles de décodage
- Fiche technique sur la gamme Cisco Firepower 4100
- 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.