Comment vérifier des alertes d'inspection et de signature du trafic IPS

Contenu

Introduction

Ce document fournit les étapes pour l'utiliser afin de vérifier l'exécution des options d'un capteur de Système de prévention d'intrusion (IPS) et de test de signature dans un environnement de production.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Release 6.2(x)E4 de système de prévention des intrusions
- Release 7.0(x)E4 de système de prévention des intrusions
- Release 7.1(x)E4 de système de prévention des intrusions

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.

Communications de la direction internes, externes et

Employez ces étapes afin de vérifier l'accès et la préparation de Gestion IPS :

- Accédez à la console dans l'IPS. Si c'est une question de module, alors entrez :**session 1 des** gammes 5500 et 5585 de l'appliance de sécurité adaptable (ASA),**session IPS d'un** 5500x,**la session d'emplacement/port de service-module ids-sensor** sur un module réseau a amélioré le module (NME),**sessionslot_number** dans CatOS, et**processeur 1 de module_number de session slot** dans l'IOS pour le système de détection d'intrusion (IDSM) et les modules IDSM-2 (de la seconde génération).
- Ouvrez une session avec le nom d'utilisateur et mot de passe qui a été configuré dans la première installation. Le nom d'utilisateur et mot de passe par défaut est « Cisco ». Référez-vous au guide d'installation pour la release appropriée pour plus de détails.
- Si l'installation est déjà complète, alors poursuivez à la connectivité IP de test à la Gestion IPS.
- Écrivez la commande d'**hôte de statistiques d'exposition**, et l'essai de cingler et obtenir l'accès de Protocole Secure Shell (SSH) à l'adresse IP de Gestion IPS. Si ceci fonctionne, alors continuez à l'étape suivante. Sinon, dépannez alors les problèmes de Connectivité avec le guide de configuration pour la release appropriée.
- Sélectionnez la commande de **show version**. Vérifiez la version de logiciel est en cours, cela un permis est installé, la version de signature est la plus tardive, toutes les engines sont opérationnelles, et ce le certificat d'hôte est valide.
- Si toutes les étapes précédentes sont validées, alors accédez à l'adresse de gestion de l'IPS par l'intermédiaire de HTTPS et lancez IDM. Javas 6 doivent être installées. Si Java 6 n'est pas disponible, alors installez le Manager Express IPS (IME) de la page Web IPS.**Remarque:** Java 7 n'est pas prise en charge pour lancer le gestionnaire de périphériques IPS (IDM) ou pour accéder à des options IPS dans Adaptive Security Device Manager (ASDM) à ce moment.
- Si la Connectivité est réussie, alors dans l'IDM, allez à la **Gestion de configuration** > de **capteur > autorisation et update license de Cisco.com**. Même si un permis valide existe, ceci confirme la Connectivité à l'Internet.
- Si réussi, alors allez à la **configuration** > aux **stratégies > corrélation > inspection/réputation globales** et cliquez sur en fonction la **corrélation globale de test** pour s'assurer les travaux de DN. Afin de vérifier ceci, aller à la **surveillance > événements** et sélectionner seulement l'**avertissement, l'erreur et mortel** et les confirmer si les mises à jour **globales de corrélation** échouent.**Remarque:** La corrélation globale n'est pas disponible sur le logiciel IPS plus tôt que la version 7.0 IPS.

Vérifiez l'inspection du trafic

Après que vous vérifiiez des transmissions par l'IPS, vous pouvez vérifier l'inspection du trafic avec ces étapes.

- Vérifiez que le capteur sentant l'état de lien d'interface est **haut** et reçoit le trafic. Ouvrez une session à l'interface de capteur et sélectionnez ces commandes :

sensor# **show interface** *!! In the output, find the applicable section for the sensing interface(s) in !! question and confirm that the Link Status value is "Up". If so, note the !! value shown for the Total Packets Received counter. After a few seconds, !! run the command again and compare the current value to the previous. !! If the value has increased, the sensing interface(s) in-question is Up !! and receiving traffic. Example:* sensor# **show interface** MAC statistics from interface GigabitEthernet0/0 Interface function = Sensing interface Link Status = Up Total Packets Received = 100 sensor# **show interface** MAC statistics from interface GigabitEthernet0/0 Interface function = Sensing interface Link Status = Up Total Packets Received = 150 *!! If a sensing interface's Link Status value is expected to be "Up", but is !! not, verify that it is properly and physically connected to a switchport or !! other network device. If so, verify that the switchport or other network !! device is configured properly and the remote interface (the switchport or !! NIC on the other network device) is not administratively-disabled !! ("shutdown"). If needed, try to swap cables with another that is known !! to be good. !! If a sensing interface's Total Packets Received counter does not increment, !! check the configuration of the switchport or other network device to which !! the sensing interface is connected. If the sensing interface is supposed to !! be the destination of a SPAN/monitor session, verify the SPAN/monitor !! configuration on the switch the sensing interface is connected.*

- Alternativement dans IDM, vérifiez toutes les interfaces de surveillance affichent une valeur de lien d'**état** traversant **haut de maison >** d'**interface**.
- Vérifiez que le capteur du capteur a au moins une interface de détection assignée et examinez le trafic. Ouvrez une session au capteur et sélectionnez cette commande. sensor# **show stat virtual** *!! In the output, find the List of interfaces monitored by this virtual !! sensor line and confirm that at least one (1) sensing interface(s) is !! listed. Additionally, find the Total packets processed since reset !! line/counter and confirm its value is greater-than (>) zero (0). !! Example:* sensor# **show stat virtual** Statistics for Virtual Sensor vs0 List of interfaces monitored by this virtual sensor = GigabitEthernet0/0 General Statistics for this Virtual Sensor Total packets processed since reset = 200 *!! If there are no sensing interface(s) listed (or, if additional sensing !! interfaces need to be assigned), login to the sensor using an !! administrative account and issue the following commands !! (**NOTE**: In the example provided, the GigabitEthernet0/0 sensing interface !! is assigned to virtual-sensor vs0. Replace that particular configuration !! line accordingly with the actual sensing interface you wish to assign to !! the virtual-sensor. If you need to assign multiple sensing interfaces, !! repeat that line (one per sensing interface)):* sensor# **conf t** sensor(config) # **service analysis-engine** sensor(config-ana) # **virtual-sensor vs0** sensor(config-ana-vir)# **physical-interface GigabitEthernet0/0** sensor(config-ana-vir)# **exit** sensor(config-ana)# **exit** Apply Changes?[yes]: yes *!! NOTE: The above example assigns a Promiscuous sensing interface to the vs0 !! virtual-sensor. Inline sensing interfaces must first be "paired" together !! and then the logical pair assigned to a virtual-sensor. Details can be !! found in the official product configuration guide's Configuring !! Interfaces section.*
- Alternativement, vérifiez que des interfaces sont assignées à **vs0** dans IDM dans le cadre de **configuration >** de **stratégies >** de **stratégies IPS**.
- Entrez dans le SSH à l'IPS et sélectionnez la commande d'**emplacement/port d'interface d'affichage de paquet** et vérifiez le trafic est vu sur l'interface.**Remarque:** Le mot clé d'***expression*** permet à l'utilisation des expressions de **tcpdump** afin d'afficher seulement le trafic qui apparie l'expression utilisée.sensor# **packet display gigabitEthernet0/1 expression ip host 198.51.100.1** Warning: This command will cause significant performance degradation tcpdump: WARNING: ge0_1: no IPv4 address assigned tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes 18:32:24.247864 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172 18:32:24.247868 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172 18:32:24.257249 IP 198.51.100.1.2000 > 192.0.2.1.16384: UDP, length 172 *!! Alternatively, in the case of VLAN tagging:* sensor# **packet display gigabitEthernet0/1 expression vlan 20 and ip host 192.51.100.1**

Vérifiez les feux de signature

- Des événements de signature peuvent être visualisés dans la section de surveillance.
- Des signatures peuvent être modifiées sous la **configuration > toutes les signatures**.
- Signatures 2000/0 et 2004/0 d'enable (réponse d'écho de Protocole ICMP (Internet Control Message Protocol) et requête d'écho d'ICMP) ; initiez un ping par le capteur, et vérifiez le journal d'événements à l'onglet de surveillance.Si l'ICMP est bloqué :Pour 1107/0, référez-vous à RFC1918 - *Adressez vu.*Afin de déclencher cette signature, le positionnement **se retirent à faux** et **activent pour rectifier** sur cette signature et pour observer l'IPS dans les plages RFC 1918 déclencher les signatures.Ces adresses sont 10.0.0.0/8, 172.16.0.0-172.31.255.255, 192.168.0.0/16.Ceci ne peut pas être vu sur un SSC-5 parce qu'on l'exige pour que la signature unretired.Pour 3409/0, telnet au port 80.Avec l'installation de web server, le port 80 est ouvert et le telnet est réussi. Quand le telnet est réussi, l'événement se déclenche sur l'IPS.Une prise de contact à trois voies de TCP est exigée pour que le capteur dépiste la connexion TCP valide. Dans le cas du routage asymétrique ou d'une rediffusion d'une capture partielle de paquet, le trafic n'entraîne pas un feu de la signature.

Après le test est complet, restaurez les par défaut sur toutes les signatures modifiées :

Informations connexes

- Scénarios de configuration de Gestion IPS sur un module 5500x IPS
- Guide de configuration CLI de capteur de Système de protection contre les intrusions Cisco IPS 7.0
- Guide de configuration CLI de capteur de Système de protection contre les intrusions Cisco IPS 7.1
- Manager Express IPS
- Secure Shell (SSH)
- Support et documentation techniques - Cisco Systems