Contenu

Introduction

Ce document explique ce qu'est la récapitulation d'événement de Système de prévention d'intrusion (IPS) et ce que sont les raisons pour les adresses IP qui apparaissent en tant que 0.0.0.0:0 dans des événements de signature IPS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La signature de Cisco IPS alerte la configuration
- Configuration de récapitulation d'événement IPS

> Remarque: Voir les exemples de configuration de récapitulation IPS pour des exemples de configuration de récapitulation d'événement.

Composants utilisés

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

- Appliance de sécurité adaptable (ASA) 5500 ou modules 5500x IPS
- IPS 4200, 4300, ou appliances IPS de gamme 4500
- Module réseau amélioré (NME) - Module IPS
- IPS de logiciel 7.x

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.

Informations générales

La récapitulation d'événement IPS est une méthode utilisée pour agréger de plusieurs événements dans une alerte simple. Ceci a comme conséquence une réduction du volume d'alertes traité et envoyé par le capteur.

Problème

Les événements générés sur l'IPS affichent l'adresse IP de l'attaquant/de victime en tant que 0.0.0.0:0.

Solution

Quand l'IPS génère des alertes de signature, il fournit des informations telles que l'ID de signature, horodateur, adresse IP de l'attaquant/de victime, et ainsi de suite. Dans certaines conditions, les événements générés affichent l'adresse IP de l'attaquant/de victime affichés en tant que 0.0.0.0:0. La raison derrière les adresses IP affichées en tant que 0.0.0.0:0 est récapitulation. Afin de configurer la récapitulation, pour ajouter une nouvelle signature faite sur commande ou pour éditer une signature en cours et pour sélectionner la **fréquence vigilante > mode récapitulatif**.

Les options disponibles de récapitulation sont :

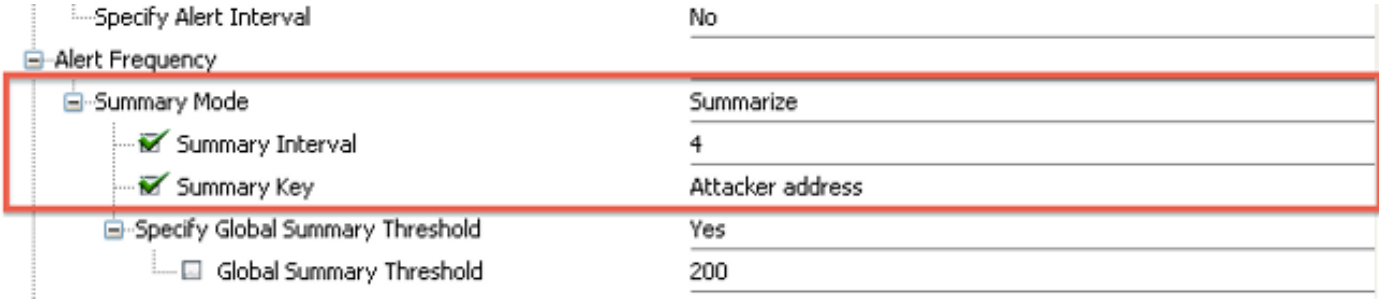
- Feu-tout - se déclenche une alerte chaque fois qu'une signature est déclenchée.
- Feu-une fois - se déclenche une alerte pour un positionnement d'adresse.
- Récapitulez - se déclenche une alerte la première fois qu'une signature est déclenchée. Des alertes supplémentaires pour cette signature sont récapitulées pour la durée de l'intervalle récapitulatif.
- Global-récapitulation - se déclenche une alerte pour chaque intervalle récapitulatif.

Quelle est la différence entre la clé récapitulative et le seuil récapitulatif global ?

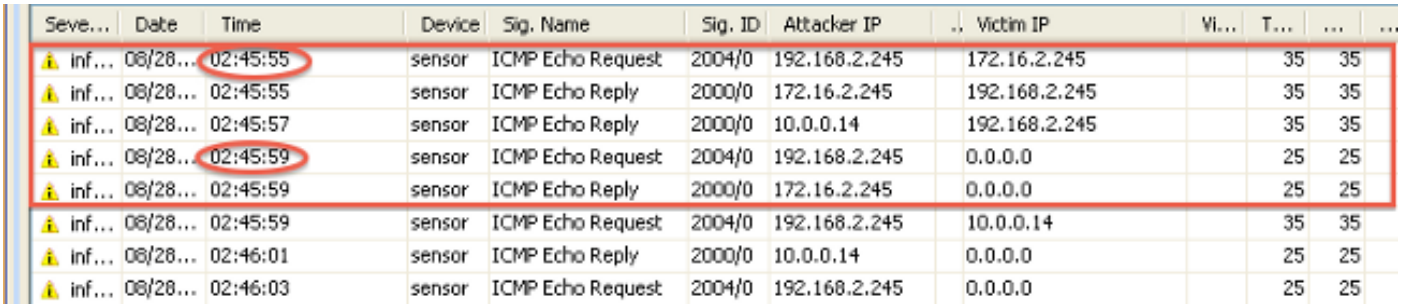
La clé récapitulative est une clé utilisée par l'IPS afin de conclure comment créer un événement récapitulatif. Par défaut, c'est une adresse d'attaquant qui signifie cela si vous avez un attaquant qui déclenche n'importe quelle signature, un événement régulier et un résumé est généré. Si vous avez deux attaquants, deux événements réguliers et deux récapitulatifs sont générés pour l'intervalle récapitulatif configuré. Si vous placez la clé récapitulative à l'adresse de victime et vous avez deux attaquants qui visent une victime, alors deux attaquants enregistreront seulement un militaire de carrière et un événement récapitulatif.

Le mode récapitulatif a deux options ; Clé récapitulative d'intervalle et de résumé. L'intervalle récapitulatif est représenté en quelques secondes et il se déclenche pour chaque intervalle récapitulatif. La clé récapitulative est un critère par lequel l'IPS décide de la façon créer l'événement récapitulatif. Par défaut, c'est l'adresse d'attaquant. Les options principales récapitulatives disponibles incluent :

- Adresse d'attaquant (par défaut)
- Adresse d'attaquant et port de victime
- Adresses d'attaquant et de victime
- Attaquant et adresses et ports de victime
- Adresse de victime



L'exemple précédent affiche une signature récapitulé avec un intervalle récapitulatif de 4 et la clé récapitulative comme adresse d'attaquant. Dans ce scénario, la signature se déclenche un événement normal la première fois après quoi dirige la signature est récapitulée pour un intervalle de 4 secondes.



Seve...	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Vi...	T...	...	...
inf...	08/28...	02:45:55	sensor	ICMP Echo Request	2004/0	192.168.2.245	172.16.2.245		35	35	
inf...	08/28...	02:45:55	sensor	ICMP Echo Reply	2000/0	172.16.2.245	192.168.2.245		35	35	
inf...	08/28...	02:45:57	sensor	ICMP Echo Reply	2000/0	10.0.0.14	192.168.2.245		35	35	
inf...	08/28...	02:45:59	sensor	ICMP Echo Request	2004/0	192.168.2.245	0.0.0.0		25	25	
inf...	08/28...	02:45:59	sensor	ICMP Echo Reply	2000/0	172.16.2.245	0.0.0.0		25	25	
inf...	08/28...	02:45:59	sensor	ICMP Echo Request	2004/0	192.168.2.245	10.0.0.14		35	35	
inf...	08/28...	02:46:01	sensor	ICMP Echo Reply	2000/0	10.0.0.14	0.0.0.0		25	25	
inf...	08/28...	02:46:03	sensor	ICMP Echo Request	2004/0	192.168.2.245	0.0.0.0		25	25	

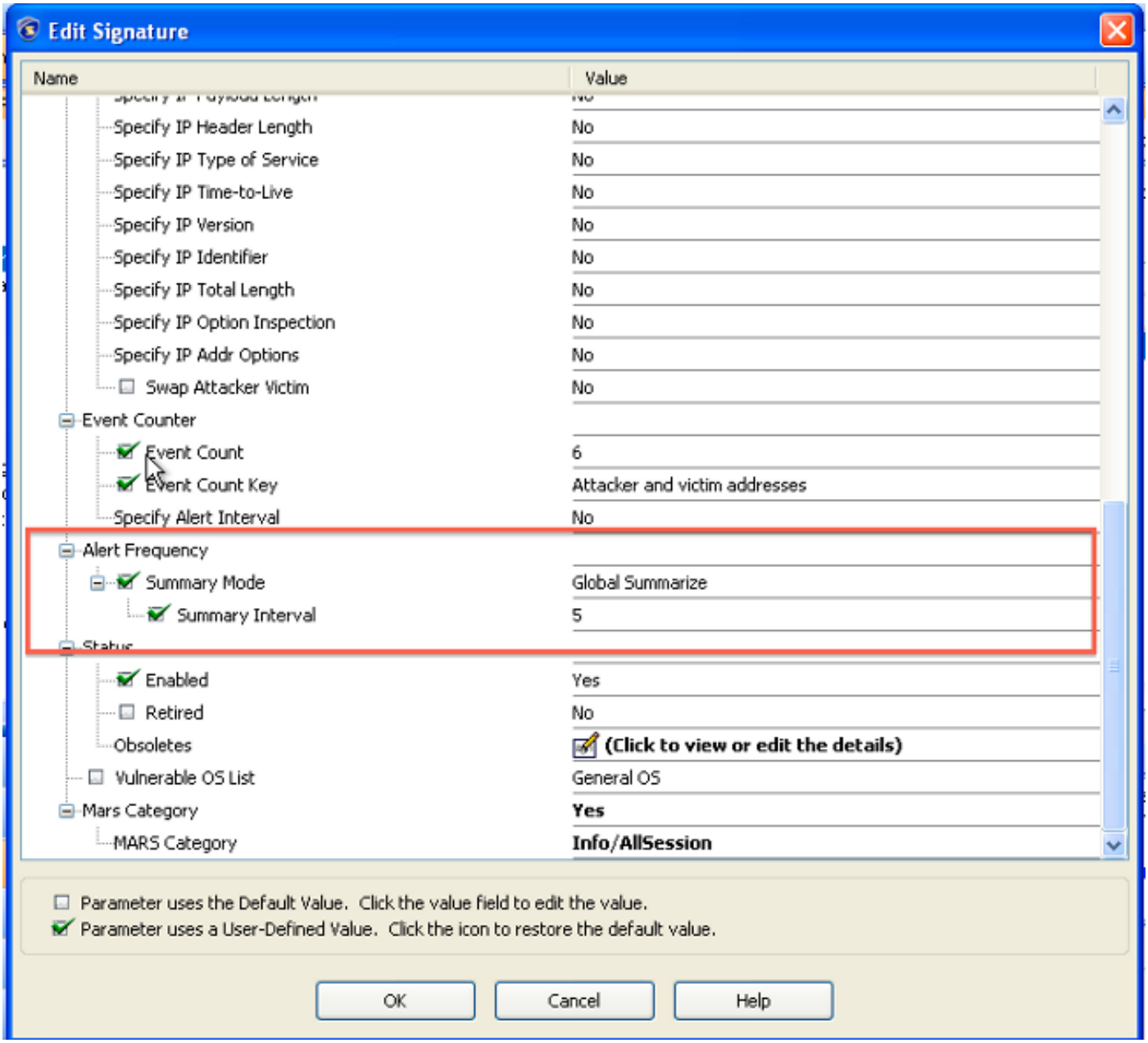
Seuil récapitulatif global - si le résumé global n'est pas spécifié et s'il y a deux adresses IP d'attaquant vues, l'IPS enregistre deux événements normaux. Après une période d'intervalle récapitulatif, deux événements récapitulés supplémentaires sont générés, un pour chaque adresse IP d'attaquant. Au total, vous feriez enregistrer 4 événements dans l'intervalle spécifié.

La récapitulation globale étant activé avec un seuil récapitulatif global de dites, deux, et si vous répétez l'exemple précédent, alors l'IPS enregistre TROIS événements : deux pour des hit initiaux pour chaque adresse d'attaquant et on ont récapitulé l'événement pour tous les attaquants (deux dans ce cas) dans l'intervalle spécifié. Maintenant si vous agrandissiez le nombre d'attaquants et de hit, vous verriez qu'une récapitulation globale enregistre beaucoup d'événements/logs et ainsi des cycles du processeur.

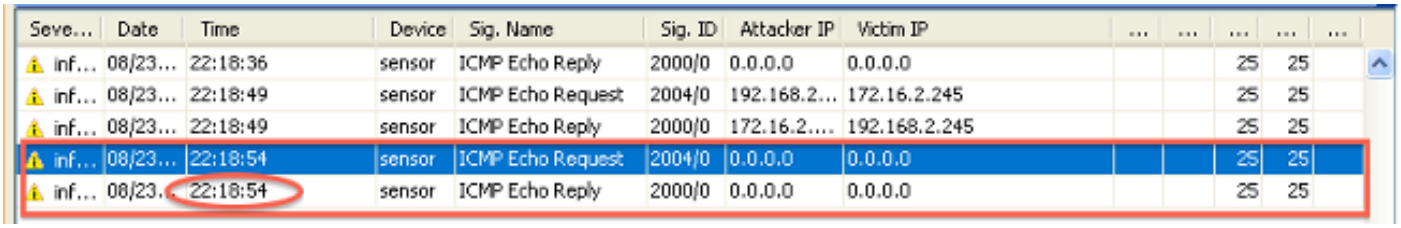
La récapitulation globale a seulement une sous-option qui est « l'intervalle récapitulatif » qui est configuré en quelques secondes. Quand la signature est placée à global-summarizarion, elle se déclenche pour chaque intervalle récapitulatif. C'est-à-dire, si l'intervalle récapitulatif est placé au '5', il se déclenche une alerte la première fois que la signature est déclenchée et ensuite elle se déclenche pour chaque intervalle récapitulatif de 5 secondes.

Afin d'éditer une signature, une **configuration** choisie **> des stratégies > signature active** et puis rechercher la signature appropriée.

Par exemple, l'ID de SIG pour la « demande d'ICMP » est 2004. Cliquez avec le bouton droit la signature et choisi **éditez** afin d'obtenir dans la boîte de dialogue affichée ici :



Dans l'extrait de configuration précédente, le mode récapitulatif a été placé à « global récapitulent » avec un intervalle récapitulatif de 5 secondes.



Seve...	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	...	...	...	...	...
inf...	08/23...	22:18:36	sensor	ICMP Echo Reply	2000/0	0.0.0.0	0.0.0.0			25	25	
inf...	08/23...	22:18:49	sensor	ICMP Echo Request	2004/0	192.168.2...	172.16.2.245			25	25	
inf...	08/23...	22:18:49	sensor	ICMP Echo Reply	2000/0	172.16.2....	192.168.2.245			25	25	
inf...	08/23...	22:18:54	sensor	ICMP Echo Request	2004/0	0.0.0.0	0.0.0.0			25	25	
inf...	08/23...	22:18:54	sensor	ICMP Echo Reply	2000/0	0.0.0.0	0.0.0.0			25	25	

L'échantillon d'alertes affichent les signatures « requête d'écho d'ICMP » et « réponse d'écho d'ICMP », qui ont été récapitulées et par conséquent affichent les adresses IP d'attaquant/victime comme '0.0.0.0'.

Ne confondez pas les événements globaux de récapitulation avec des « événements de la signature 1102.0 (paquet IP impossible) ». Les pirates informatiques pourraient essayer d'éluder un IPS avec l'utilisation de tous les zéros pour la source/adresses IP de destination et de mettre en communication qui pourraient déclencher cette signature, qui pourrait ressembler à un événement récapitulé.

Informations connexes

- Forums aux questions de signatures de Système de protection contre les intrusions Cisco
- Guide de configuration CLI de capteur de Système de protection contre les intrusions Cisco IPS 7.1
- Exemples de configuration de récapitulation IPS
- Support et documentation techniques - Cisco Systems