目次

侵入防御システム（IPS）イベント 集約がであり、もの原因が IPS シグニチャ イベントに 0.0.0.0:0 として出て来る IP アドレスのためであるものこの資料に説明されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IPS シグニチャは設定を警告 します
- IPS イベント 集約 設定

注 イベント 集約 設定例については IPS 集約 設定例を参照して下さい。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 適応性があるセキュリティ アプライアンス モデル（ASA） 5500 または 5500x IPS モジュール
- IPS 4200、4300、か 4500 シリーズ IPS アプライアンス
- 高められるネットワークモジュール（NME） - IPS モジュール
- IPS 7.x ソフトウェア

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

IPS イベント 集約は単一 アラートに複数のイベントを集約するのに使用される方式です。 これはセンサーによって処理され、発信されるアラートの音量のリダクションという結果に終ります。

問題

IPS で生成されるイベントは 0.0.0.0:0 として攻撃者/対象の IP アドレスを示します。

解決策

IPS はシグニチャ アラートを生成するとき、シグニチャ ID のような情報を、タイムスタンプ、攻撃者/対象の IP アドレス、等提供します。 特定の条件下で、生成されるイベントは 0.0.0.0:0 として表示する 攻撃者/対象の IP アドレスを示します。 0.0.0.0:0 として表示する IP アドレスの後ろの原因は集約です。 集約を新しいカスタム シグニチャを追加しか、または現在のシグニチャを編集し、**アラート周波数を**選択するために設定するため、**> サマリ モード**。

利用可能 な 集約 オプションは次のとおりです:

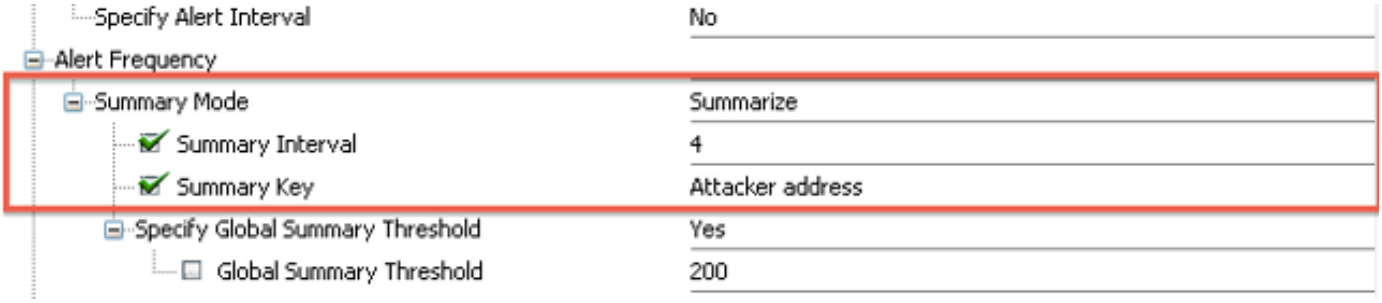
- 適用すべて-シグニチャが引き起こされる度にアラートを始動させます。
- -設定 される アドレスのためのアラートを始動させます適用。
- 要約して下さい-シグニチャが引き起こされる時最初にアラートを始動させます。 そのシグニチャのための追加アラートはサマリ間隔時間の間要約されます。
- グローバル集約-各サマリ間隔のためのアラートを始動させます。

概略キーおよびグローバル なサマリしきい値間の違いとは何か。

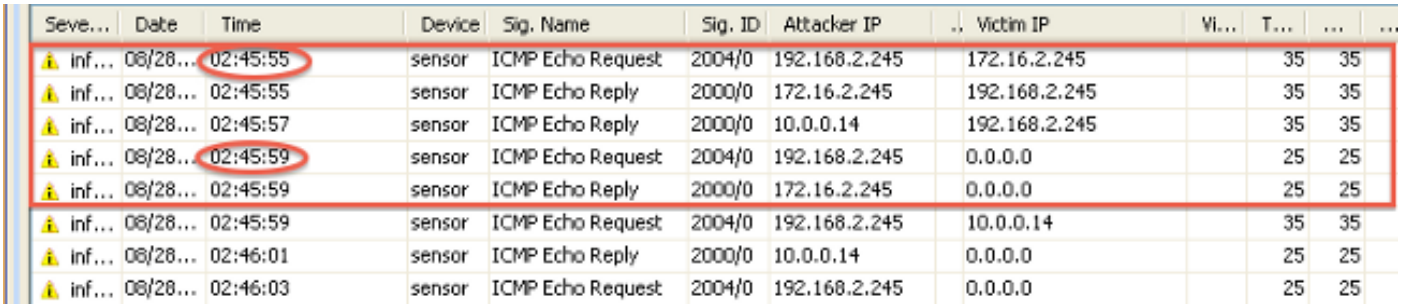
概略キーは完了するために IPS によって使用されるキー サマリ イベントを作成する方法をです。 デフォルトで、シグニチャを引き起こす 1 人の攻撃者が、1 正規事象あり、1 概略が作成されれば場合ことを意味するこれは攻撃者 アドレスです。 2 つの攻撃者がある場合、2 つの規則的な、2 つのサマリ イベントは設定されたサマリ間隔のために生成されます。 対象アドレスにサマリ キーを設定 し、1 つの対象を目標とする 2 つの攻撃者があれば、2 つの攻撃者は 1 規則的な、1 サマリ イベントだけ記録します。

サマリ モードに 2 つのオプションがあります; サマリ間隔および概略キー。 サマリ間隔は秒に表され、各サマリ間隔のために起動 します。 概略キーはサマリ イベントを作成する IPS が方法で決定する基準です。 デフォルトで、これは攻撃者 アドレスです。 利用可能 な概略キー オプションは下記のものを含んでいます:

- 攻撃者 アドレス (デフォルト)
- 攻撃者 アドレスおよび対象ポート
- 攻撃者および対象アドレス
- 攻撃者および対象アドレスおよびポート
- 対象アドレス



4 のサマリ間隔および攻撃者 アドレスとして概略キーと要約される前例はシグニチャを示します。 このシナリオでは、シグニチャは 4 秒の間隔のために正常なイベントを最初に始動させましたりそのあとでシグニチャを要約されます指します。



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	

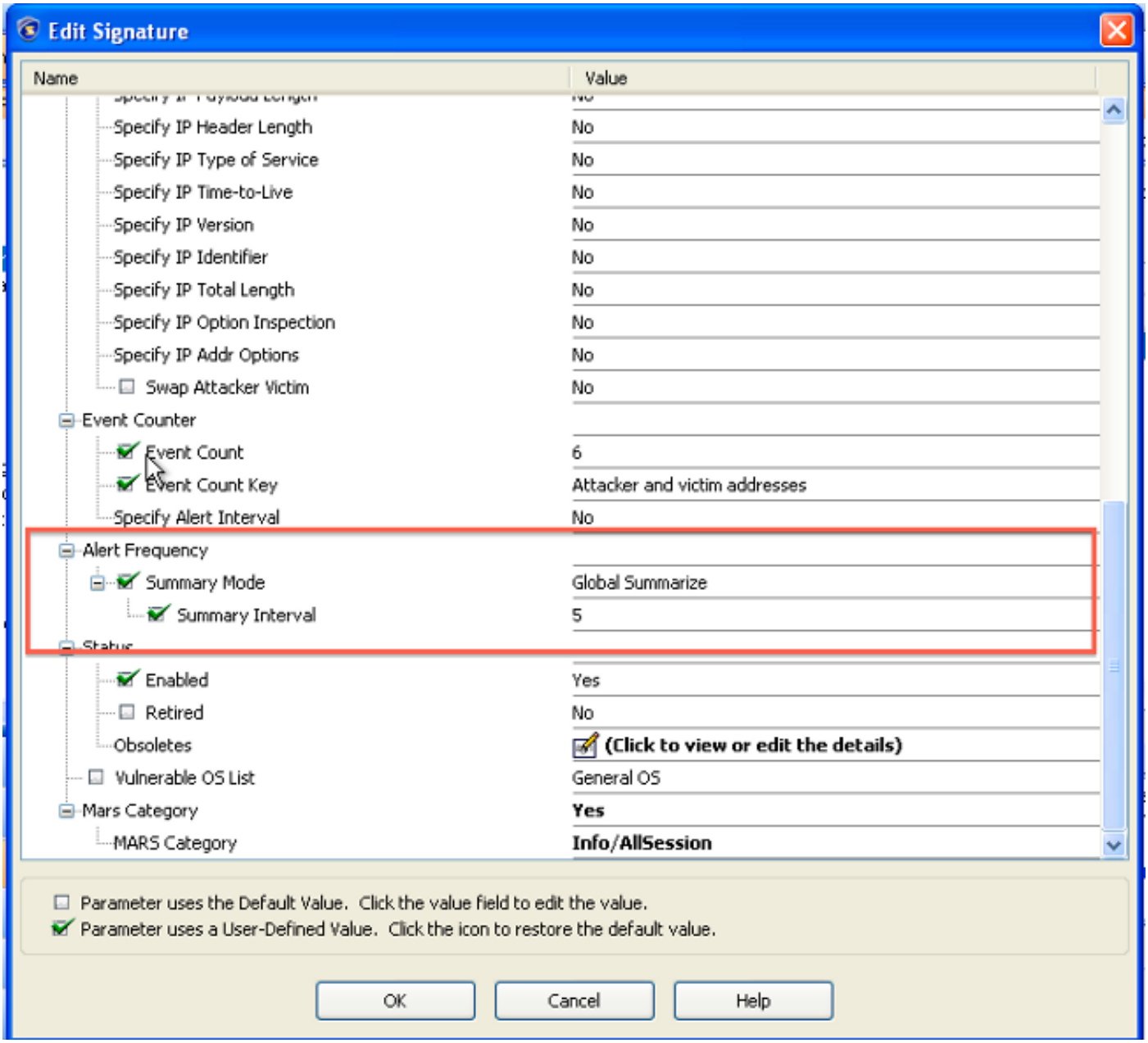
グローバル なサマリしきい値-グローバル な概略が規定 されなければ、そして参照される 2 攻撃者 IP アドレスがあれば IPS は 2 つの正常なイベントを記録します。 サマリ間隔の期間以降に、2 つの追加要約されたイベントは、各攻撃者 IP アドレスのための 1 つ生成されます。 合計では、4 つのイベントを規定の間隔の内に記録してもらいます。

グローバル なサマリしきい値によっての有効に されて グローバル な 集約が、2 および前例を繰り返したら、IPS 記録します 3 つのイベントを言って下さい: 各攻撃者 アドレスの最初のヒット用の 2 つおよび 1 つは規定の間隔内のすべての攻撃者 (2 この場合) のためのイベントを要約しました。 この場合攻撃者およびヒットの数を拡大したらグローバル な 集約が多くのイベント/ログをおよびこうしてプロセッササイクル保存することが、わかります。

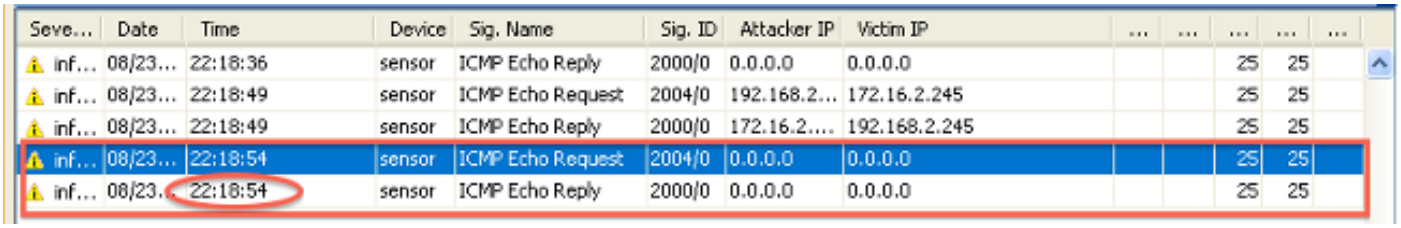
グローバル な 集約に秒に設定される「サマリ間隔」である 1 つのサブ オプションだけあります。 シグニチャはグローバルsummarizarion に設定 されるとき、各サマリ間隔のために起動 します。 すなわち、サマリ間隔が '5' に設定 されれば シグニチャが引き起こされ時、その後 5 秒の各サマリ間隔のために起動 する最初に、アラートを始動させます。

シグニチャを編集するために、**> アクティブなシグニチャ** Configuration > Policies の順に選択 し、次に関連したシグニチャを捜して下さい。

たとえば、「ICMP 要求」のための SIG ID は 2004 年です。 シグニチャを右クリックし、ここに示されているダイアログボックスに到達するために『Edit』 を選択 して下さい:



以前のコンフィギュレーション 断片では、サマリ モードは 5 秒のサマリ間隔と「グローバルに要約します」設定 されました。



要約され、'0.0.0.0' としてそれ故に攻撃者/対象 IP アドレスを表示するアラートのサンプルはシグニチャの ICMPエコー要求」および「ICMPエコー応答を」示します。

「シグニチャ 1102.0 イベント (不可能な IPパケット) 」とグローバル な 集約 イベントを間違えないで下さい。 ハッカーは要約されたイベントのように見えるかもしれないこのシグニチャを引き起こす可能性があるソース/宛先 IP アドレスおよびポートのためのすべてのゼロの使用の IPS を避けることを試みるかもしれません。

関連情報

- Cisco 侵入防御システム シグニチャ FAQ
- Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.1
- IPS 集約の設定例
- テクニカルサポートとドキュメント - Cisco Systems