

ني عم ثدح صخلم لي طعت/ني كمت - IPS 6.x ربع IDM

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [تمكين/تعطيل ملخص حدث معين باستخدام IDM](#)
- [تكوين IDM](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية تمكين/تعطيل ملخص حدث معين في الإصدار x.6 من برنامج نظام منع التسلل (IPS) باستخدام مدير أجهزة (IDM) IPS.

ملاحظة: يجب تكوين قوائم الوصول في أجهزة IPS للسماح بالوصول من المضيف أو الشبكة حيث يتم تثبيت برامج الإدارة مثل IDM و IEV (عارض أحداث IDS) وتعمل بشكل صحيح. راجع قسم [تغيير قائمة الوصول من تكوين مستشعر نظام منع التسلل من Cisco باستخدام واجهة سطر الأوامر 5.0](#) للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

يتم إنشاء هذا المستند بافتراض أن IPS 6.x مثبت ويعمل بشكل صحيح.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مستشعر Cisco 4200 Series IPS الذي يشغل إصدار البرنامج E1(2)6.0.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين مسموح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

تمكين/تعطيل ملخص حدث معين باستخدام IDM

للحصول على فهم واضح، يقدم هذا قسم مثال حيث أنت يمكن/أعجزت الملخص ل التوقيع id: 5748.

تكوين IDM

أكمل الخطوات التالية.

1. بدء تشغيل IDM.
2. طقطقت منزل in order to رأيت الصفحة الرئيسية من ال IDM. تعرض هذه الصفحة معلومات الجهاز.

The screenshot displays the Cisco IDM 6.0 web interface for a device with IP 10.77.241.142. The interface is divided into several sections:

- Device Information:** Host Name: sensor, IP Address: 10.77.241.142, IPS Version: 6.0(2)E1, Device Type: IDS-4235, IDM Version: 6.0.2, Total Memory: 881 MB, Bypass Mode: Auto_off, Total Data Storage: 174.7 MB, Missed Packets Percentage: 0, Total Sensing Interface: 1.
- Interface Status:** A table showing interface status for GigabitEthernet0/1 (Up) and GigabitEthernet0/0 (Down).
- System Resources Status:** CPU usage (0%) and Memory usage (747MB) are shown with graphs and a summary table (Used: 747, Free: 134, Total: 881).
- Alert Summary:** High (0), Med. (0), Low (0), Info. (0), Threat Rating > 80 (0).
- Alert Profile:** A graph showing alert counts over time, with a legend for High, Med., Low, Info., and Threat Rating > 80.

3. أخترت تشكيل < سياسات < تعريفات التوقيع < sig0 < تشكيل التوقيع < تحديد ب: معرف SIG in order to عرضت كل التوقعات المتاحة في المستشعر.

Cisco IDM 6.0 - 10.77.241.142

File Help

Home Configuration Monitoring Back Forward Refresh Help

Sensor Setup

- Network
- Allowed Hosts
- SSH
 - Authorized Keys
 - Known Host Key
 - Sensor Key
- Certificates
 - Trusted Hosts
 - Server Certificate
- Time
- Users
- Interface Configuration
 - Summary
 - Interfaces
 - Interface Pairs
 - VLAN Pairs
 - VLAN Groups
 - Bypass
 - Traffic Flow Notificati
- Analysis Engine
 - Virtual Sensors
 - Global Variables
- Policies
 - Signature Definitions
 - sig0
 - Event Action Rules
 - rules0
 - Anomaly Detections
 - ad0

Signature Configuration | Custom Signature Wizard | Signature Variables | Miscellaneous

Select By: Active Signatures

Sig ID	Subsig ID	Name	Enabled	Severity
1000	0	IP options-Bad Option List	Yes	Informational
1004	0	IP options-Loose Source Route	No	High
1006	0	IP options-Strict Source Route	Yes	High
1007	0	IPv6 over IPv4	No	Informational
1101	0	Unknown IP Protocol	Yes	Informational
1102	0	Impossible IP Packet	Yes	High
1104	0	IP Localhost Source Spoof	Yes	High
1107	0	RFC 1918 Addresses Seen	No	Informational
1108	0	IP Packet with Proto 11	Yes	High
1109	3	Cisco IOS Interface DoS	No	Medium
1109	2	Cisco IOS Interface DoS	No	Medium
1109	1	Cisco IOS Interface DoS	No	Medium
1109	0	Cisco IOS Interface DoS	No	Medium
1200	0	IP Fragmentation Buffer Full	Yes	Informational
1201	0	IP Fragment Overlap	No	Informational
1202	0	IP Fragment Overrun - Datagram T...	Yes	High
1203	0	IP Fragment Overwrite - Data is O...	Yes	High

Select All

Actions

Edit

Restore Defaults

Enable

Disable

Add

Clone

Delete

4. أختار معرف SIG من القائمة المنسدلة تحديد حسب ثم أدخل معرف SIG 5748 للعثور على توقيع معين.

Cisco IDM 6.0 - 10.77.241.142

File Help

Home Configuration Monitoring Back Forward Refresh Help

Sensor Setup

- Network
- Allowed Hosts
- SSH
 - Authorized Keys
 - Known Host Key
 - Sensor Key
- Certificates
 - Trusted Hosts
 - Server Certificate
- Time
- Users
- Interface Configuration
 - Summary
 - Interfaces
 - Interface Pairs
 - VLAN Pairs
 - VLAN Groups
 - Bypass
 - Traffic Flow Notificati
- Analysis Engine
 - Virtual Sensors
 - Global Variables
- Policies
 - Signature Definitions
 - sig0
 - Event Action Rules
 - rules0
 - Anomaly Detections
 - ad0

Signature Configuration | Custom Signature Wizard | Signature Variables | Miscellaneous

Select By: Sig ID Enter Sig ID (eg. 1000-2000): 5748 Find

Sig ID	Subsig ID	Name	Enabled	Severity
5748	5	Non-SMTP Session Start	Yes	Informational
5748	4	Non-SMTP Session Start	Yes	Informational
5748	3	Non-SMTP Session Start	Yes	Informational
5748	2	Non-SMTP Session Start	Yes	Informational
5748	1	Non-SMTP Session Start	Yes	Informational
5748	0	Non-SMTP Session Start	Yes	Low

Select All

Actions

Edit

Restore Defaults

Enable

Disable

Add

Clone

Delete

5. طغقة يحرر in order to حررت التوقيع.

6. في نافذة تحرير التوقيع، اختر تعريف التوقيع < تردد التنبه > وضع الملخص، وقم بتغيير العملية من تلخيص إلى إطلاق الكل في القائمة المنسدلة وضع الملخص.

Name	Value
Regex String	^([*Nn][Nn][*Oo][Nn][Oo][*Oo][Nn][Oo][Oo][*Pp])
Service Ports	25
Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	Yes
Max Match Offset	4
Specify Min Match Offset	No
Swap Attacker Victim	No
Event Counter	
Event Count	1
Event Count Key	Attacker and victim addresses and ports
Specify Alert Interval	No
Alert Frequency	
Summary Mode	Summarize
Summary Interval	Fire All
Summary Key	Fire Once
Specify Global Summary Threshold	Global Summarize
Specify Global Summary Threshold	Summarize
Status	
Enabled	Yes
Retired	No
Obsoletes	
Vulnerable OS List	(Click to view or edit the details)
Vulnerable OS List	General OS
Mars Category	Yes
MARS Category	Info/Misc/Mail

7. تأكد من تعيين عتبة الملخص العام إلى لا.

Name	Value
Regex String	^[^Nn][Nn][^Oo][Oo][^Pp]
Service Ports	25
Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	Yes
Max Match Offset	4
Specify Min Match Offset	No
Swap Attacker Victim	No
Event Counter	
Event Count	1
Event Count Key	Attacker and victim addresses and ports
Specify Alert Interval	No
Alert Frequency	
Summary Mode	Summarize
Summary Interval	15
Summary Key	Attacker address
Specify Global Summary Threshold	No
Status	No
Enabled	Yes
Retired	No
Obsoletes	<input checked="" type="checkbox"/> (Click to view or edit the details)
Vulnerable OS List	General OS
Mars Category	Yes
MARS Category	Info/Misc/Mail

معلومات ذات صلة

- [صفحة دعم نظام منع الاقتحام من Cisco](#)
- [صفحة دعم مدير جهاز Cisco IPS](#)
- [يحصل يبدأ مع IOS IPS](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل