Konfigurationsbeispiel für Router- und Sicherheitsgeräte-Manager im Cisco IOS Intrusion Prevention System

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Verwendung von Cisco Router und Security Device Manager (SDM) Version 2.5 zum Konfigurieren von Cisco IOS[®] Intrusion Prevention System (IPS) in Version 12.4(15)T3 und höheren Versionen.

Die Verbesserungen in SDM 2.5 für IOS IPS sind:

- Gesamtzahl der kompilierten Signaturnummern, die in der GUI der Signaturliste angezeigt werden
- SDM-Signaturdateien (ZIP-Dateiformat) z. B. sigv5-SDM-S307.zip) und CLI-Signaturpakete (pkg-Dateiformat; z. B. IOS-S313-CLI.pkg) zusammen in einem Vorgang heruntergeladen werden können.
- Heruntergeladene Signaturpakete können optional automatisch an den Router gesendet werden.

Im Rahmen des ersten Bereitstellungsprozesses müssen folgende Aufgaben durchgeführt werden:

- 1. SDM 2.5 herunterladen und installieren
- 2. Verwenden Sie SDM Auto Update, um das IOS IPS-Signaturpaket auf einen lokalen PC herunterzuladen.
- 3. Starten Sie den IPS-Richtlinienassistenten, um IOS IPS zu konfigurieren.

4. Überprüfen des ordnungsgemäßen Ladens der IOS IPS-Konfiguration und -Signaturen Cisco SDM ist ein webbasiertes Konfigurationstool, das die Router- und Sicherheitskonfiguration mithilfe intelligenter Assistenten vereinfacht. Mit diesen Assistenten können Kunden einen Cisco Router schnell und einfach bereitstellen, konfigurieren und überwachen, ohne dass Kenntnisse über die Kommandozeile erforderlich sind. SDM Version 2.5 kann von Cisco.com unter <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm</u> heruntergeladen werden (nur <u>registrierte</u> Kunden). Die Versionshinweise finden Sie unter <u>http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/soft</u> <u>ware/release/notes/SDMr.25.html</u>

Hinweis: Cisco SDM erfordert eine Bildschirmauflösung von mindestens 1024 x 768.

Hinweis: Für Cisco SDM muss die Größe des Java-Arbeitsspeichers mindestens 256 MB betragen, um IOS IPS zu konfigurieren. Um die Heapgröße des Java-Speichers zu ändern, öffnen Sie das Java-Bedienfeld, klicken Sie auf die Registerkarte **Java**, klicken Sie auf **Ansicht** unter den Java-Applet-Laufzeiteinstellungen, und geben Sie **-Xmx256m** in die Spalte Java-Laufzeitparameter ein.

| 🍰 Java Runtime Sel | ttings | | × |
|-----------------------|----------|------------------------|---------------------|
| Java Runtime Versions | 5 | | |
| Product Name | Version | Location | Java Runtime Parame |
| JRE | 1.6.0_03 | C:\Program Files\Java\ | -Xmx256m |
| | | | |
| | | | |
| | | | |
| r | | | |
| | | | OK Cancel |
| | | | |

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS IPS ab Version 12.4(15)T3
- Cisco Router and Security Device Manager (SDM) Version 2.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Hinweis: Öffnen Sie eine Konsolen- oder Telnet-Sitzung mit dem Router (wobei "term monitor" aktiviert ist), um Nachrichten zu überwachen, wenn Sie mit SDM IOS IPS bereitstellen.

- 1. Laden Sie SDM 2.5 von Cisco.com unter <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm</u> herunter (nur <u>registrierte</u> Kunden), und installieren Sie es auf einem lokalen PC.
- 2. Führen Sie SDM 2.5 vom lokalen PC aus.
- 3. Wenn das Dialogfeld IOS IPS Login (IOS IPS-Anmeldung) angezeigt wird, geben Sie den Benutzernamen und das Kennwort ein, die Sie für die SDM-Authentifizierung des Routers

| | IOS IPS Login | 2 | < |
|------------|---------------|------------------------------|---|
| | Enter User na | ame and password for IOS IPS | |
| | Username: | admin | |
| | Password: | ***** | |
| | | OK Cancel | |
| verwenden. | | | |

- 4. Klicken Sie in der SDM-Benutzeroberfläche auf **Konfigurieren** und dann auf **Intrusion Prevention**.
- 5. Klicken Sie auf die Registerkarte Edit IPS (IPS bearbeiten).
- Wenn die SDEE-Benachrichtigung auf dem Router nicht aktiviert ist, klicken Sie auf OK, um die SDEE-Benachrichtigung zu

| Information | | × |
|-------------|---|---|
| į | SDEE notification is not enabled. IPS will enable SDEE notification so it can receive SDEE messages. | |
| | OK | |

- 7. Klicken Sie im Bereich Download Signaturdatei von Cisco.com auf der Registerkarte Edit IPS (IPS bearbeiten) auf das Optionsfeld Get the latest SDM file and CLI pkg (Aktuelle SDM-Datei und CLI pkg abrufen), und klicken Sie dann auf Browse (Durchsuchen), um ein Verzeichnis auf Ihrem Iokalen PC auszuwählen, in dem die heruntergeladenen Dateien gespeichert werden sollen.Sie können das Stammverzeichnis des TFTP- oder FTP-Servers auswählen, das später verwendet wird, wenn Sie das Signaturpaket für den Router bereitstellen.
- 8. Klicken Sie auf **Download** (Herunterladen).



9. Wenn das Dialogfeld "CCO-Anmeldung" angezeigt wird, verwenden Sie Ihren CCO-Benutzernamen und Ihr

| CCO Login | |
|---------------|---------------------|
| Enter CCO Use | ername and Password |
| Usemame: | user |
| Password: | **** |
| ОК | Cancel Help |
| | |

SDM stellt eine

Verbindung zu Cisco.com her und lädt sowohl die SDM-Datei (z. B. sigv5-SDM-S307.zip) als auch die CLI-Pkg-Datei (z. B. IOS-S313-CLI.pkg) in das in Schritt 7 ausgewählte Verzeichnis herunter.Nachdem beide Dateien heruntergeladen wurden, werden Sie von SDM aufgefordert, das heruntergeladene Signaturpaket auf den Router zu übertragen.



- 10. Klicken Sie auf Nein, da IOS IPS noch nicht auf dem Router konfiguriert wurde.
- 11. Nachdem SDM das neueste IOS CLI-Signaturpaket heruntergeladen hat, klicken Sie auf die Registerkarte **Create IPS (IPS erstellen**), um die erste IOS IPS-Konfiguration zu erstellen.
- 12. Wenn Sie aufgefordert werden, Änderungen auf den Router anzuwenden, klicken Sie auf Änderungen übernehmen.
- 13. Klicken Sie auf **IPS-Regelassistent starten**.Es wird ein Dialogfeld angezeigt, das Sie darüber informiert, dass SDM ein SDEE-Abonnement für den Router einrichten muss, um Warnungen



14. Klicken Sie auf OK.Das Dialogfeld "Authentifizierung erforderlich" wird

| Authenticatio | n Required | × |
|----------------|---|---|
| | | 1 |
| | | |
| | | |
| Enter legis de | balle ba accord lawel. I av view, accord on | |
| /172.25.90.3 | calls to access level_1 or view_access on 9: | |
| | | |
| User name: | Jadmin | |
| Password: | **** | 1 |
| | • | |
| Save this | password in your password list | |
| | | |
| | OK Cancel | 1 |
| | | 1 |
| Authorities | | |
| Authenticatio | h scheme: Integrated windows | |

angezeigt.

15. Geben Sie den Benutzernamen und das Kennwort ein, den Sie für die Authentifizierung von SDM am Router verwendet haben, und klicken Sie auf OK.Das Dialogfeld IPS Policies Wizard (IPS-Richtlinienassistent) wird angezeigt.

IPS Policies Wizard



Welcome to the IPS Policies Wizard

This wizard helps you to configure the IPS rules for an interface and to specify the location of the configuration and the signature file.

This wizard will assist you in configuring the following tasks:

* Select the interface to apply the IPS rule.

* Select the traffic flow direction that should be inspected by the IPS rules.

* Specify the signature file and public key to be used by the router.

* Specify the config location and select the category of signatures to be applied to the selected interfaces.

To continue, click Next.



16. Klicken Sie auf Weiter.

Help

| Inbound | Outbound |
|---------|----------|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

17. Wählen Sie im Fenster "Ausgewählte Schnittstellen" die Schnittstelle und die Richtung aus, auf die das IOS IPS angewendet wird, und klicken Sie dann auf **Weiter**, um fortzufahren.

| | Circulation File and Date | le Ker |
|-----------|--|--|
| PS Wizard | Signature File and Publ | iic Rey |
| | Signature File | |
| | Specify the signal | ture file you want to use with IOS IPS. |
| ~ | Signature File: | tftp://10.1.1.253/IOS-8313-CLI.pkg |
| - | C Get the latest sig | nature file from Cisco.com and save to PC. |
| 10 miles | Location: | Browse |
| AT | | Download |
| | | 000000 |
| | | |
| | Configure Public K | |
| C. | Configure Public K | (ey |
| R | Configure Public K Name: | (ey |
| | Configure Public K Name: Key: | Cey realm-cisco.pub FE3F0C87 89BCB7BB 994AE74C FA9E481D F65 50437722 FFBE85B9 5E4189FF CC189CB9 69C 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5535 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF F3020301 0001 |
| | Configure Public K Name: Key: | Cey realm-cisco.pub FE3F0C87 89BCB7BB 994AE74C FA9E481D F65 50437722 FFBE85B9 5E4189FF CC189CB9 69C 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5535 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF F3020301 0001 |
| | Configure Public K Name: Key: | Cey realm-cisco.pub FE3F0C87 89BCB7BB 994AE74C FA9E481D F65 50437722 FFBE85B9 5E4189FF CC189CB9 69C 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5533 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF F3020301 0001 |
| | Configure Public K Name: Key: | Gey realm-cisco.pub FE3F0C87 89BCB7BB 994AE74C FA9E481D F65 50437722 FFBE85B9 5E4189FF CC189CB9 69C 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5535 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF F3020301 0001 |

18. Klicken Sie im Bereich Signaturdatei des Fensters Signaturdatei und Öffentlicher Schlüssel auf das Optionsfeld Signaturdatei angeben, die Sie mit IOS IPS verwenden möchten, und klicken Sie dann auf die Schaltfläche Signaturdatei (..), um den Speicherort der Signaturpaket-Datei anzugeben, die dem in Schritt 7 angegebenen Verzeichnis

| Specify Signature File | × |
|--------------------------|------------------------------------|
| C Specify signature file | on flash |
| File Name on flash: | |
| Specify signature file | using URL |
| Protocol: | tftp 💌 |
| tftp:// | 10.1.1.253/IOS-S313-CLI.pkg |
| Example: | http://10.10.10.1/IOS-S259-CLI.pkg |
| C Specify signature file | on the PC |
| Location: | Browse |
| ок | Cancel Help |
| nt | |

19. Klicken Sie auf das Optionsfeld Signaturdatei mit URL angeben, und wählen Sie ein

Protokoll aus der Dropdown-Liste Protokoll aus. **Hinweis:** In diesem Beispiel wird TFTP verwendet, um das Signaturpaket auf den Router herunterzuladen.

- 20. Geben Sie den URL für die Signaturdatei ein, und klicken Sie auf OK.
- 21. Geben Sie im Fenster Signaturdatei und öffentlicher Schlüssel im Bereich Configure Public Key (Öffentlichen Schlüssel konfigurieren) realm-cisco.pub im Feld Name ein, und kopieren Sie diesen öffentlichen Schlüssel, und fügen Sie ihn in das Feld Schlüssel ein. 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93A8AF124AD6CC7A245097A975206BE3A206FBA13F6F12CB5B4E441F1617E630D5C02AC252912BE27F37FDD9C811FC7AF7DCDD81D943CDABC36007D128B199ABCBD34ED0F9085FADC1359C189EF30AF10AC0EFB6247E0764BF3E53053E5B2146A9D7A5EDE30298AF03DED7A5B89479039D20F306639AC64B93C0112A35FE3F0C8789BCB7BB994AE74CFA9E481DF65875D685EAF9746D9CC8E3F0B08B8550437722FFBE85B95E4189FFCC189CB969C46F9CA84DFBA57A0AF99EAD768C36006CF498079F88F8A3B3FB1F9FB7B3CB5539E1D19693CCBB551F78D2892356AE2F56D8268918EF3C80CA4F4D87BFCA3BBFF668E9689782A5CF31CB6EB4B094D3FJ30203010001FUEBCASEFAREAUFAREAUFAREAUFAREAU

Hinweis: Dieser öffentliche Schlüssel kann von Cisco.com unter folgender Adresse heruntergeladen werden: <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup</u> (nur <u>registrierte</u> Kunden).

22. Klicken Sie auf **Weiter**, um fortzufahren.

| PS Policies Wizard | |
|---------------------------------------|--|
| IPS Wizard | Config Location and Category |
| A A A A A A A A A A A A A A A A A A A | Config Location Specify the directory path of the IPS configuration files where IOS IPS sub-system stores the signature information and the user-defined modifications. If Cisco IOS IPS fails to contact the specified location, it will retry for a specific timeout period until it successfully contacts the specified location. |
| | Choose Category Signature categories are subsets of signatures created for routers with different amounts of available memory. The basic category is recommended for routers with less than 128 MB of memory. The advanced category is recommended for routers with 128 MB of memory, or more. Choose Category: |
| | Back Next > Finish Cancel Help |

23. Klicken Sie im Fenster Config Location (Speicherort und Kategorie) auf die Schaltfläche Config Location (Speicherort der Konfiguration) (..), um einen Speicherort für die Signaturdefinition und Konfigurationsdateien anzugeben.Das Dialogfeld "Konfigurationsstandort hinzufügen" wird

| Directory Name: | |
|------------------------------|------------------------|
| C Specify the config locatio | on using URL. |
| Protocol: | http |
| http:// | |
| Example: | http://10.10.10.1/ips5 |
| Number of Retries (1-5): | |
| Timeout (1-10): | (sec) |

24. Klicken Sie im Dialogfeld Speicherort für Konfiguration hinzufügen auf das Optionsfeld Konfigurationsspeicherort für diesen Router angeben, und klicken Sie dann auf die Schaltfläche Verzeichnisname (...), um die Konfigurationsdatei zu suchen.Das Dialogfeld Ordner auswählen wird angezeigt, in dem Sie ein vorhandenes Verzeichnis auswählen oder im Router-Flash ein neues Verzeichnis erstellen können, in dem die Signaturdefinitionsund Konfigurationsdateien gespeichert

| Choose Folder | × |
|---------------------|---|
| 🔄 New Folder | |
| ⊡-∰ flash: L ips | |
| | |
| OK Cancel Help | |

werden.

- 25. Klicken Sie oben im Dialogfeld auf **Neues Verzeichnis**, wenn Sie ein neues Verzeichnis erstellen möchten.
- 26. Wenn Sie das Verzeichnis ausgewählt haben, klicken Sie auf **OK**, um die Änderungen zu übernehmen, und klicken Sie dann auf **OK**, um das Dialogfeld Speicherort für Konfig. hinzufügen zu schließen.
- 27. Wählen Sie im Dialogfeld IPS Policies Wizard (IPS-Richtlinienassistent) die Signaturkategorie entsprechend der auf dem Router installierten Speicherkapazität aus. Sie können in SDM zwei Signaturkategorien auswählen: Einfach und Erweitert.Wenn auf dem Router 128 MB DRAM installiert sind, empfiehlt Cisco, die Kategorie "Basic" zu wählen, um Speicherzuweisungsfehler zu vermeiden. Wenn auf dem Router mindestens 256 MB DRAM installiert sind, können Sie eine der beiden Kategorien auswählen.
- 28. Wenn Sie eine zu verwendende Kategorie ausgewählt haben, klicken Sie auf Weiter, um zur Übersichtsseite fortzufahren. Die Übersichtsseite bietet eine kurze Beschreibung der Aufgaben, die bei der Erstkonfiguration von IOS IPS durchgeführt werden.



29. Klicken Sie auf der Übersichtsseite auf Fertig stellen, um die Konfigurationen und das Signaturpaket an den Router zu senden. Wenn die Option Preview-Befehle in den Einstellungen für Voreinstellungen in SDM aktiviert ist, zeigt SDM das Dialogfeld Deliver Configuration to Router (Konfiguration an Router bereitstellen) an, in dem eine Zusammenfassung der CLI-Befehle angezeigt wird, die vom SDM an den Router übermittelt werden.

| Preview commands that | at will be de | livered to the route | er's running configu | ration. | |
|--|---------------|----------------------|-----------------------|---------------------|--------------|
| ip ips notify SDEE | | | | | |
| ip ips name sdm_ips_ | rule | | | | |
| interface GigabitEthern | et0/1 | | | | |
| ip ips sdm_ips_rule in | 1 | | | | |
| exit | a hulin a l | | | | |
| ip ips comig location na | asnoipsi | | | | - |
| ip ips signature-catego cotonom all | iry | | | | |
| retired true | | | | | |
| exit | | | | | |
| 4 | | | | | F |
| The differences betwee outer is turned off. | n the runni | ng configuration a | nd the startup config | guration are lost v | whenever the |
| Save running config. | to router's | startup config. | | | |
| This operation can | take severa | al minutes | | | |
| rino operation can | | | | | |
| | | | | | |

30. Klicken Sie auf **Deliver**, um fortzufahren.Das Dialogfeld "Commands Delivery Status" (Status der Zustellung von Befehlen) wird angezeigt und zeigt den Status der Zustellung von Befehlen

| Commands Delivery Status | × |
|--|---|
| Command Delivery Status: | |
| Preparing commands for delivery Submitting 14 commands, please wait Configuration delivered to router. | * |
| <u>र</u> | |
| OK | |

31. Wenn die Befehle an den Router übermittelt werden, klicken Sie auf **OK**, um fortzufahren.Das Dialogfeld "IOS IPS-Konfigurationsstatus" zeigt an, dass die Signaturen



auf den Router geladen werden.

32. Beim Laden der Signaturen zeigt SDM die Registerkarte **Edit IPS (IPS bearbeiten**) mit der aktuellen Konfiguration an. Überprüfen Sie, welche Schnittstelle und in welche Richtung das IOS IPS aktiviert ist, um die Konfiguration zu überprüfen

| Cisco Router an | d Security Device Manager (SDM): 172. | 25.90.39 | | | | | |
|---|--|--|---|---|--|---|----------------|
| File Edit View | Tools Help | Rebech Save | Q Search | ? Heip | | | ahaha cisco |
| Tasks Interfaces and Interfaces and | Intrusion Prevention Syste Create IPS Edit IPS Security Das IPS Policies Global Settings Auto Update SEAP Configuration Target Value Rating Event Action Overrides Event Action Filters Signatures | Interfaces: All Interfaces: All Interface Name GraphEthernet0 GraphEthernet0 Vian1 Vian192 | ton Interfaces IP 172.25.90.39 10.1.1.8 no IP address 192.168.1.8 | Enable (Inbound Disabled Disabled Disabled | Edit O Desable Outbound Disabled Disabled Disabled Disabled | e E) Disable Al VFR status Cn Cn Cf Cn | Description |
| NIIT | PS Filter D ▲ PS rule traffic. | IPS Filter Details: IPS rule is en traffic. | ে Inbound Fi abled, but there | iter Coutto | and Filter figured for this rule. IPS will s | | n all inbound |

Die Router-Konsole zeigt, dass die Signaturen geladen wurden.

🖉 172.25.90.30 - TuTTY ied 13 16:41:08 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:41:08 PST Jan 13 2008 13 16:41:08 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13 engines 13 16:41:08 PST: %IPS-6-ENGINE_READY: multi-string - build time 8 ms - packets for thi *Jan Jan this engine will be scanned *Jan 13 16:41:00 PST: 4IPS-6-ENGINE DUILDING: service-http - 622 signatures - 2 of 13 engines *Jan 13 16:41:33 PST: 4IPS-6-ENGINE_READY: service-http - build time 24892 ms - packets for t this end ine will be scanned *Jan 13 16:41:133 PST: %IPS-6-ENGINE_BUILDING: string-top - 961 signatures - 3 of 13 engines *Jan 13 16:42:32 PST: %IPS-6-ENGINE_READY: string-top - build time 59424 ms - packets for this engin *Jan 13 16:42:32 PST: %IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines *Jan 13 16:42:33 PST: %IPS-6-ENGINE_READY: string-udp - build time 948 ms - packets for this engine will be scanned "Jan 13 16:42:33 PST: %IPS-6-ENGINE BUILDING: state - 28 signatures - 5 of 13 engines "Jan 13 16:42:33 PST: %IPS-6-ENGINE_READY: state - build time 104 ms - packets for this engine will be scanned "Jan 13 16:42:33 PST: %IPS-6-ENGINE_BUILDING: atomic-ip = 275 signatures = 6 of 13 engines "Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: atomic-ip = build time 532 ms = packets for this engine w *Jan 13 16:42:34 PST: 4IPS-6-ENGINE BUILDING: string-icmp = 3 signatures = 7 of 13 engines *Jan 13 16:42:34 PST: 4IPS-6-ENGINE_READY: string-icmp - build time 32 ms - packets for this engine will be scanned "Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines *Jan 13 16:42:34 PST: %IPS-6-ENGINE_PEADY: service-rpc - build time 200 ms - packets for this engine will be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-dns - 30 signatures - 10 of 13 engines *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BEADY: service-dns - build time 36 ms - packets for this engine will be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines *Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for this engine wi 11 be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures - 12 of 13 engine *Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms - packets for thi s engine will be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 26 signatures - 13 of 13 engines *Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 36 ms - packets for this engin be scanned Jan 13 16:42:34 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 86304 ms

33. Verwenden Sie den Befehl **show ip ips signature**, um zu überprüfen, ob die Signaturen ordnungsgemäß geladen wurden.

```
router#show ip ips signatures count
Cisco SDF release version S313.0
Trend SDF release version V0.0
|
snip
|
Total Signatures: 2158
Total Enabled Signatures: 829
Total Retired Signatures: 1572
Total Compiled Signatures: 580
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
```

Die erste Bereitstellung von IOS IPS mit SDM 2.5 ist abgeschlossen.

34. Überprüfen Sie die Signaturnummern mit SDM, wie in diesem Bild gezeigt.

| ile Edit View | Tools Help | | | | | | | |
|------------------|----------------------------------|--------------|--------------------------------------|--------------|--------------------------------|--------------|---------------|------------|
| 🚯 Home | Configure [Manitor | O Refrech | Save | Q. Search | ? Help | | • | cisco |
| Tasks | 😺 Intrusion Prevention Syste | em (IPS) | | | | | | |
| | Create IPS Edit IPS Security Dat | shboard II | PS Migration | 6 | | _ | | _ |
| 1 | PS Policies | Di Inpo | rt + View by | AJ Sign | oures + Criteria -NUA- | Total[2158] | Compiled[584 | 9 |
| Connections | Global Settings | dd - Dat E | Cal Edit C Englis O Disable O France | | | | | |
| 3 | Auto Update | Contract I | 1.000 | lo esta to | | | for such a | |
| rewall and RCL | 3 SEAP Configuration | Ened | 9423 | Subsigit | Back Door Psychward | produce-size | high | Proteiny P |
| <u></u> | Name Target Value Rating | i i | 9423 | 0 | Back Door Psychward | produce-aler | high | 100 |
| UPN | Event Action Overrides | | 5343 | 0 | Apache Host Header Cross Str | produce-aler | high | 100 |
| E ~ | Fivent Action Filters | i i | 3122 | 0 | SMTP EXPN root Recon | produce-aler | low | 85 |
| EN, | Signatures | 0 | 5099 | 0 | MSN Messenger Webcan Duffe | produce-aler | high | 60 |
| eouty Audi | 12-00 OS | | 5537 | 0 | ICQ Client DNS Request | produce-aler | informational | 100 |
| 000 | a Attack | 0 | 3316 | 0 | Project1 DOS | produce-aler | high | 75 |
| Routing | I Comer Services | 0 | 11003 | 0 | Gtelia File Request | produce-aler | low | 100 |
| 2 | B Reconnaissance | 0 | \$196 | 1 | Red Hat Stronghold Recon atta | produce-aler | low/ | 100 |
| NRT | B- Instant Messaging | 0 | 5196 | 0 | Red Hat Stronghold Recon atta | produce-aler | low | 100 |
| No. | Adware/Spyware | 0 | 5773 | 1 | Simple FHP Blog Unauthorized F | produce-aler | low | 70 |
| | 3 - ODoS | • | 5773 | 0 | Simple FHP Blog Unauthorized F | produce-alcr | low | 65 |
| sion Prevention | B- Network Services | 0 | 5411 | 0 | Linksys Http DoS | produce-aler | high | 85 |
| 1004 | B- P2P | • | 12019 | 0 | SideFind Activity | produce-aler | low | 65 |
| ality of Service | B-C Email | 0 | 5070 | 0 | WWW meades dl Access | produce-aler | nedun | 100 |
| 2 an | B- Releases | 0 | 3169 | 0 | FTP SITE EXEC for | produce-aler | high | 85 |
| NAC | | 0 | 5605 | 0 | Windows Account Locked | produce-aler | informational | 85 |
| - | | 4 | 1 | 1 | | | | 21 |
| Strong Tasks | | | | | Apply Changes Discard Ch | anges | | |
| - | | | | | | 10.504 | | |

Zugehörige Informationen

- <u>Cisco IOS IPS auf Cisco.com</u>
- <u>Cisco IOS IPS-Signalisierungspaket</u>
- Cisco IOS IPS-Signaturdateien für SDM
- Erste Schritte mit Cisco IOS IPS mit 5.x-Signaturformat
- Cisco IOS IPS Konfigurationsleitfaden
- Cisco IDS-Ereignisanzeige
- Technischer Support und Dokumentation für Cisco Systeme