

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:

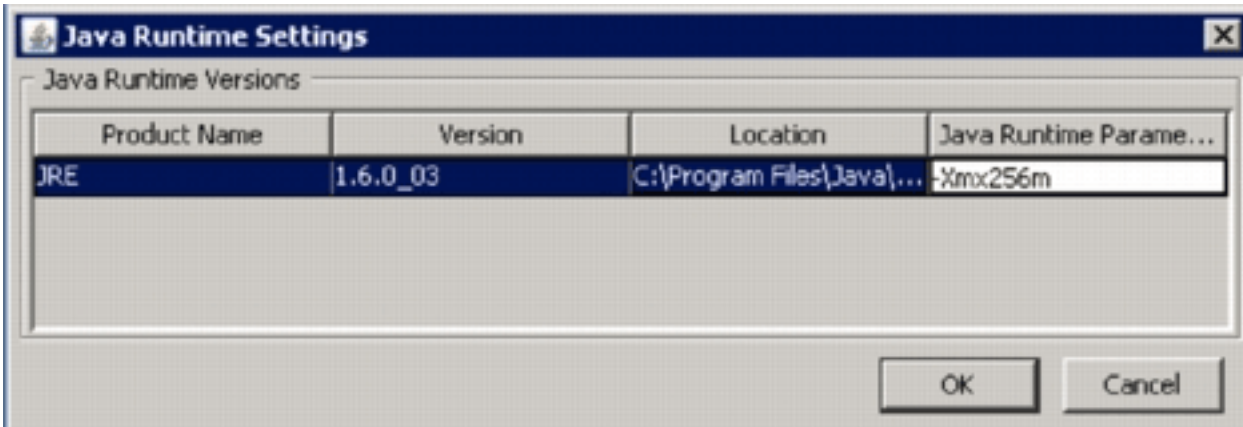
1. SDM 2.5 herunterladen und installieren
2. Verwenden Sie SDM Auto Update, um das IOS IPS-Signaturpaket auf einen lokalen PC herunterzuladen.
3. Starten Sie den IPS-Richtlinienassistenten, um IOS IPS zu konfigurieren.
4. Überprüfen des ordnungsgemäßen Ladens der IOS IPS-Konfiguration und -Signaturen

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 <http://www.cisco.com/cgi-bin/tablebuild.pl/sdm> heruntergeladen werden (nur [registrierte](#) Kunden). Die Versionshinweise finden Sie unter http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr.25.html

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.



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 [Cisco Technical Tips Conventions](#) (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 <http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm> herunter (nur [registrierte](#) 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

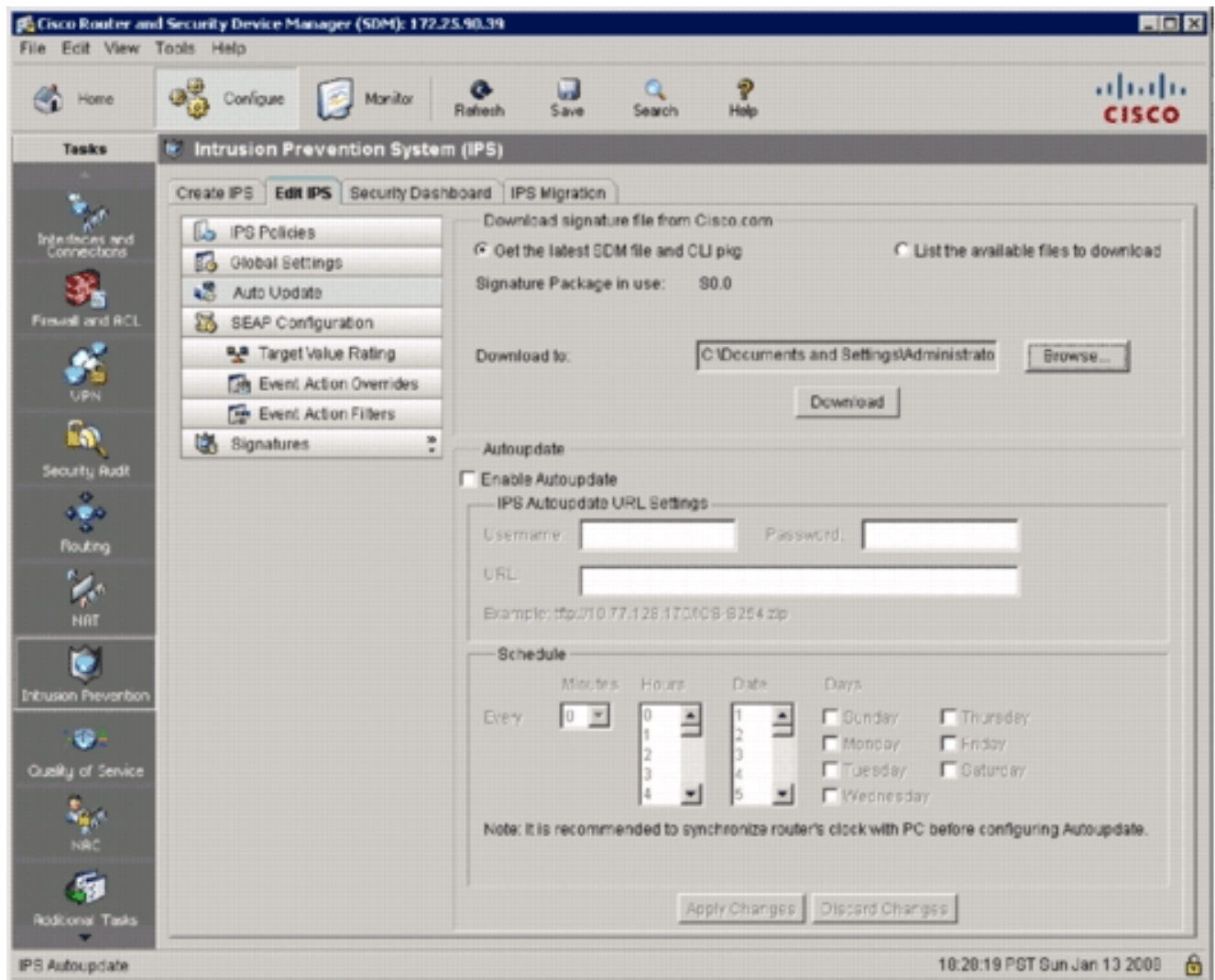


verwenden.

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



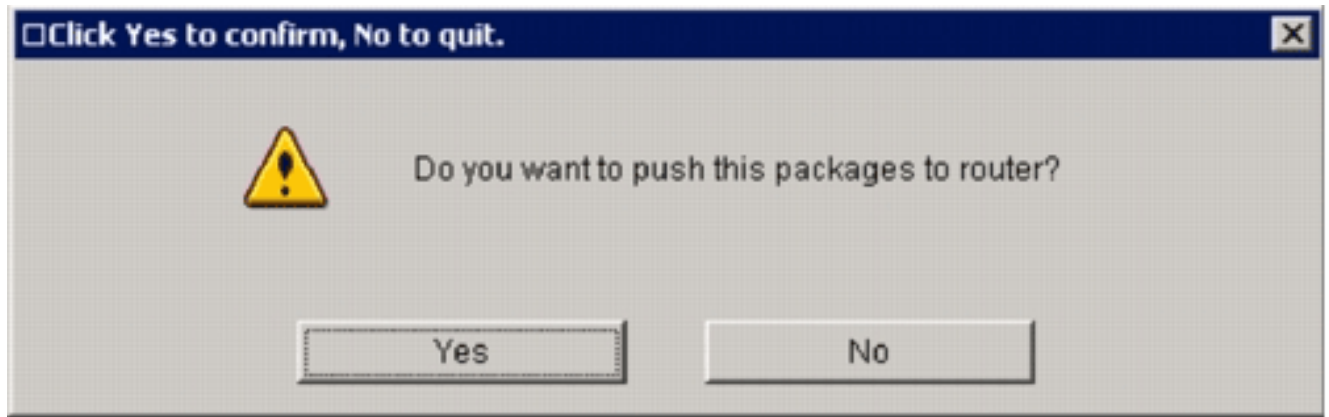
7. Klicken Sie im Bereich Download Signaturdatei von Cisco.com auf der Registerkarte Edit IPS (IPS bearbeiten) auf das Optionsfeld **Get the latest SDM file and CLI pkg (Aktuelle SDM-Datei und CLI pkg abrufen)**, und klicken Sie dann auf **Browse (Durchsuchen)**, um ein Verzeichnis auf Ihrem lokalen 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)**.



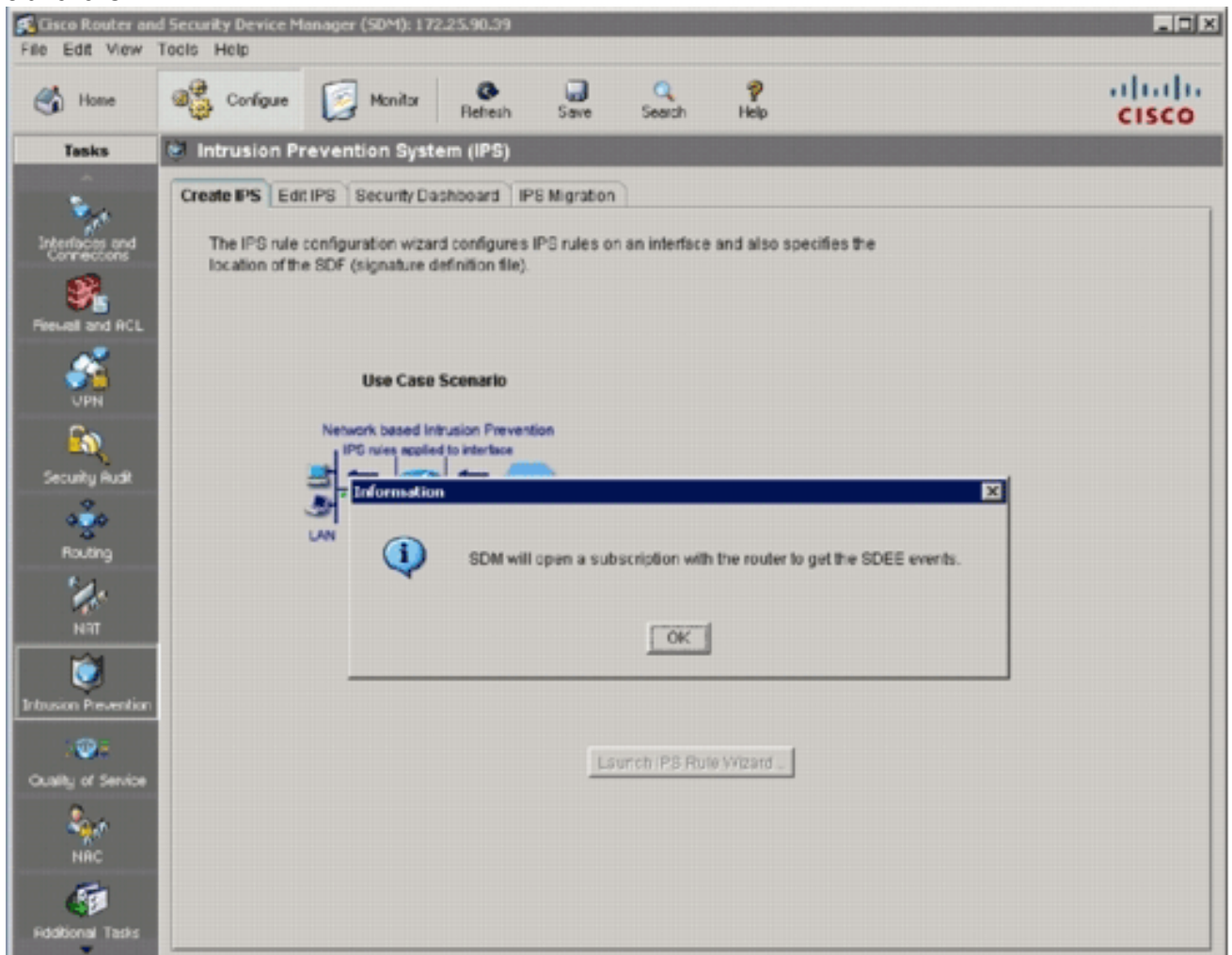
9. Wenn das Dialogfeld "CCO-Anmeldung" angezeigt wird, verwenden Sie Ihren CCO-Benutzernamen und Ihr



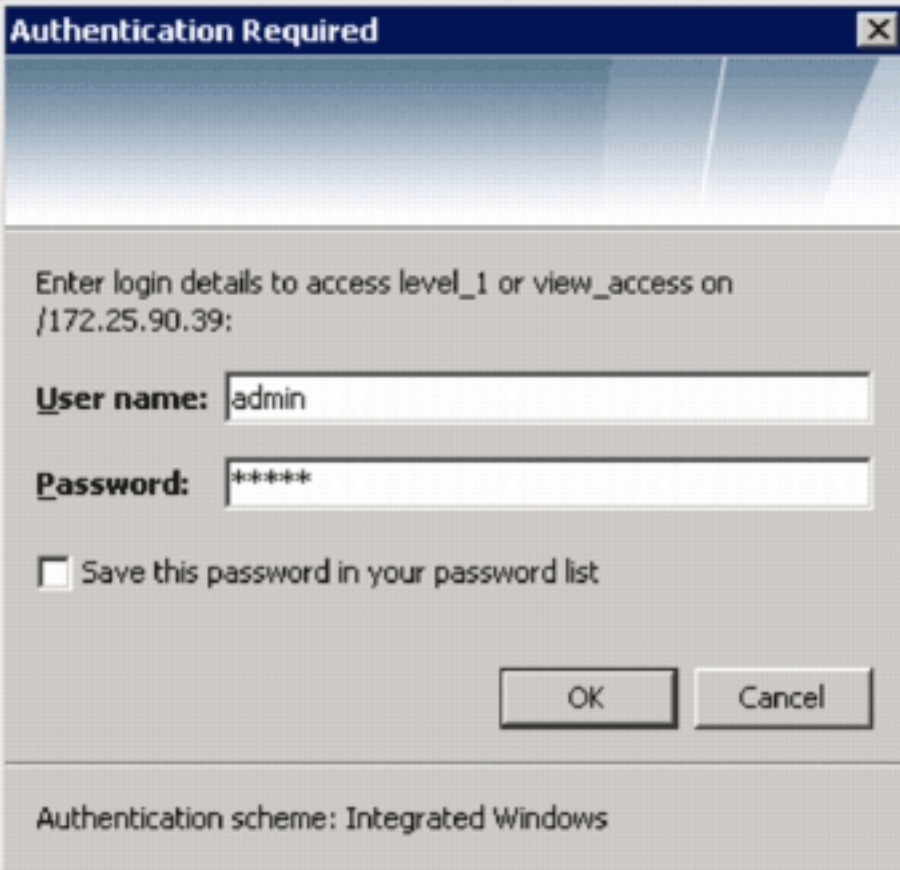
Kennwort. SDM stellt eine Verbindung zu Cisco.com her und lädt sowohl die SDM-Datei (z. B. sigv5-SDM-S307.zip) als auch die CLI-Pkg-Datei (z. B. IOS-S313-CLI.pkg) in das in Schritt 7 ausgewählte Verzeichnis herunter. Nachdem beide Dateien heruntergeladen wurden, werden Sie von SDM aufgefordert, das heruntergeladene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



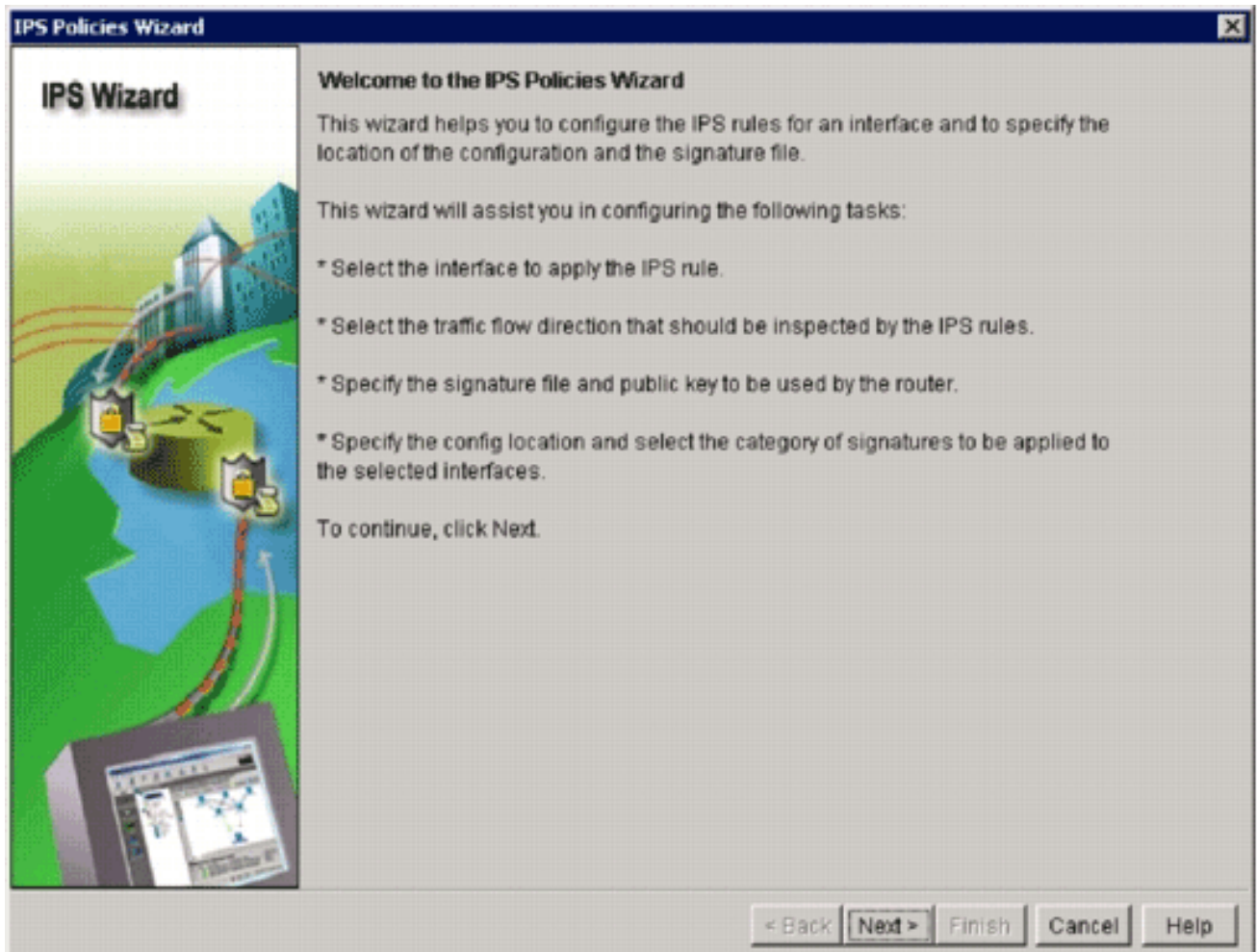
14. Klicken Sie auf **OK**. Das Dialogfeld "Authentifizierung erforderlich" wird



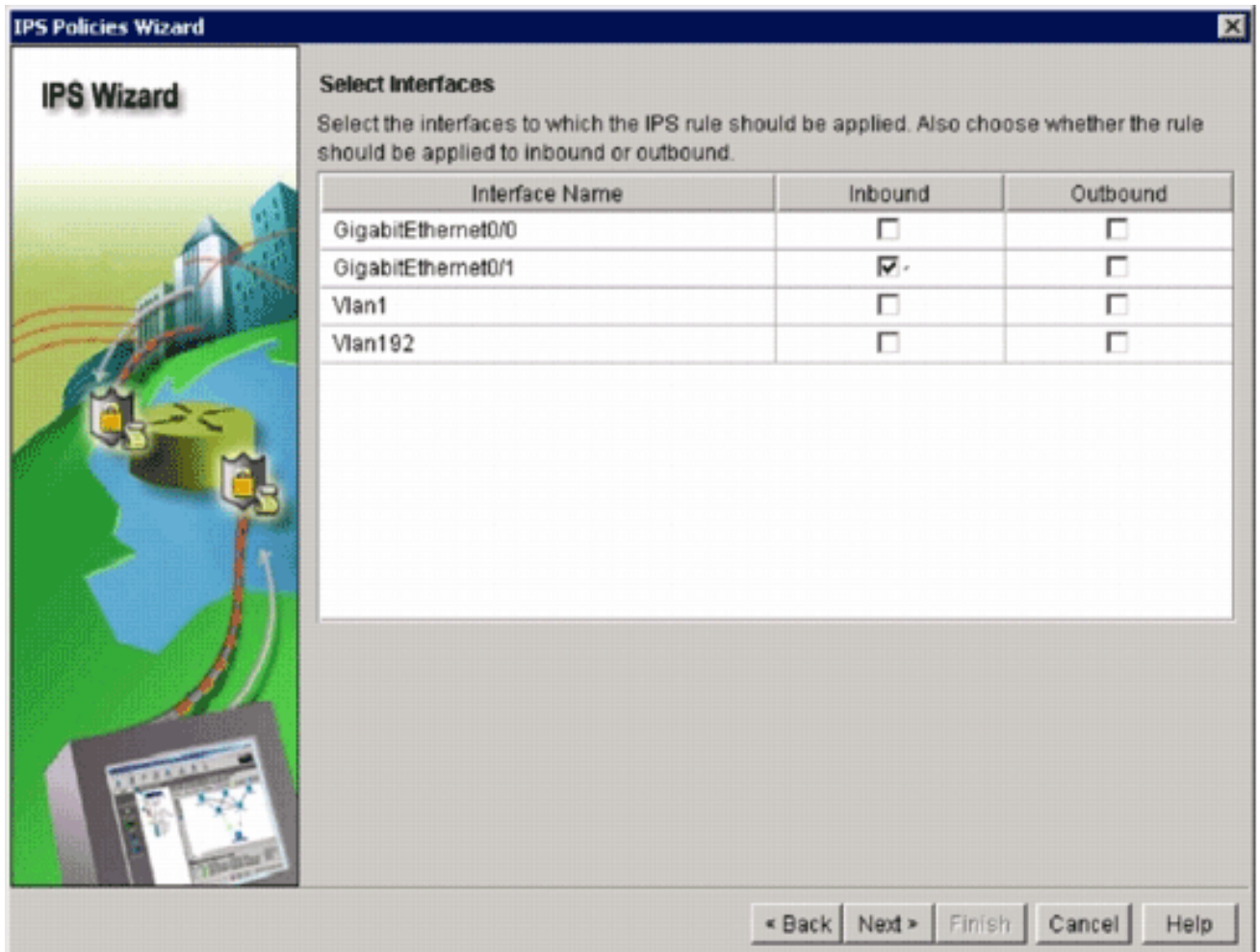
The image shows a Windows-style dialog box titled "Authentication Required". The dialog has a blue header bar with a close button (X) in the top right corner. Below the header, there is a light blue gradient background. The main content area is light gray and contains the following text: "Enter login details to access level_1 or view_access on /172.25.90.39:". Below this text are two input fields. The first is labeled "User name:" and contains the text "admin". The second is labeled "Password:" and contains six asterisks "*****". Below the password field is a checkbox with the label "Save this password in your password list", which is currently unchecked. At the bottom right of the dialog are two buttons: "OK" and "Cancel". At the very bottom of the dialog, there is a footer area with the text "Authentication scheme: Integrated Windows".

angezeigt.

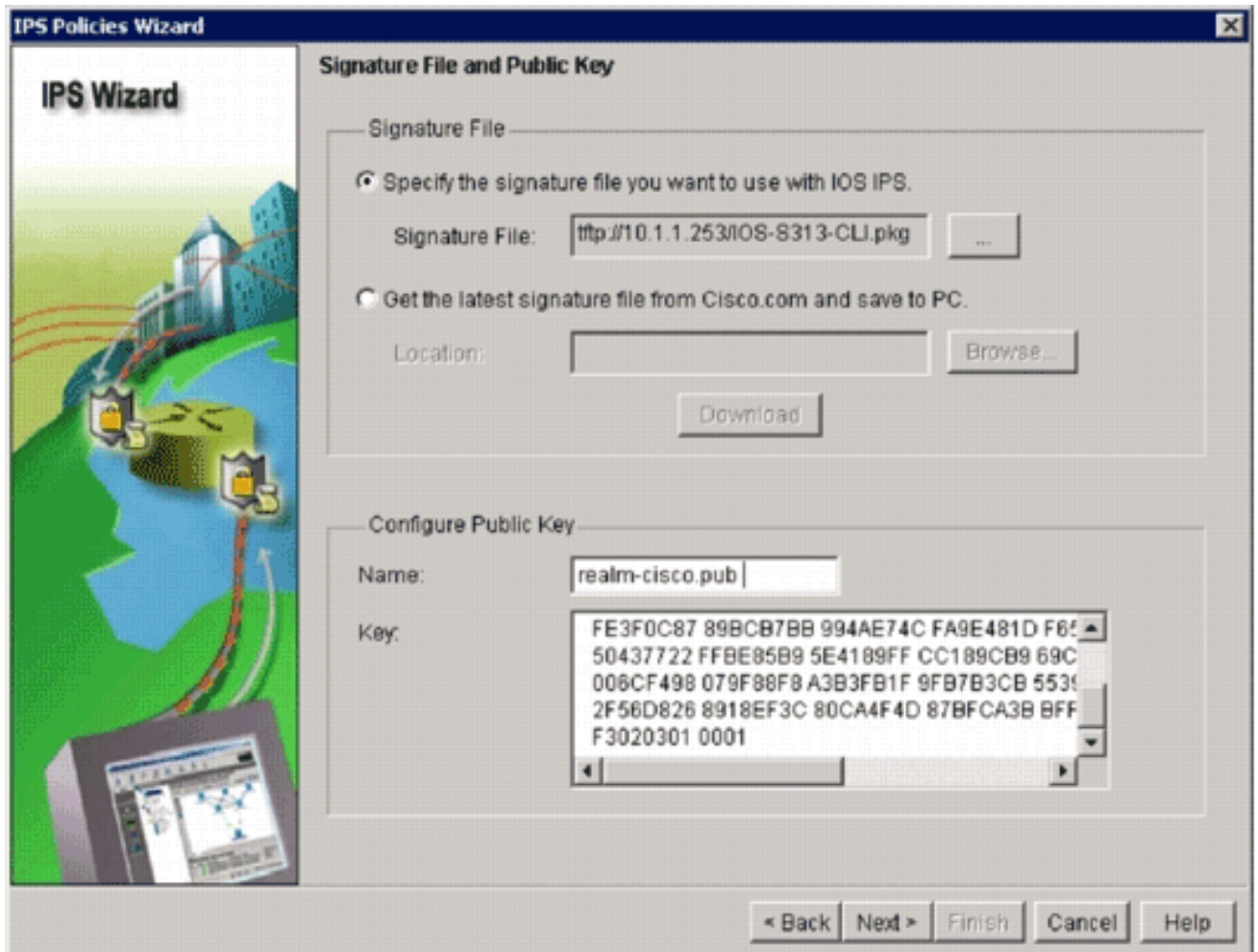
15. Geben Sie den Benutzernamen und das Kennwort ein, den Sie für die Authentifizierung von SDM am Router verwendet haben, und klicken Sie auf **OK**. Das Dialogfeld IPS Policies Wizard (IPS-Richtlinienassistent) wird angezeigt.



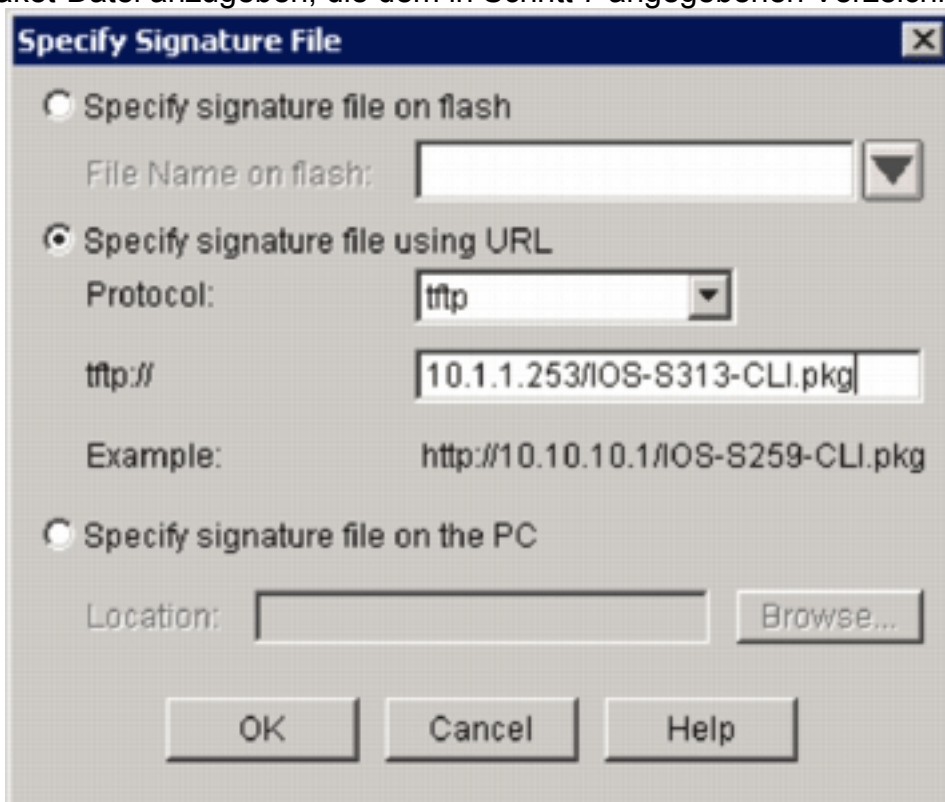
16. Klicken Sie auf
Weiter.



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.



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



entspricht.

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.

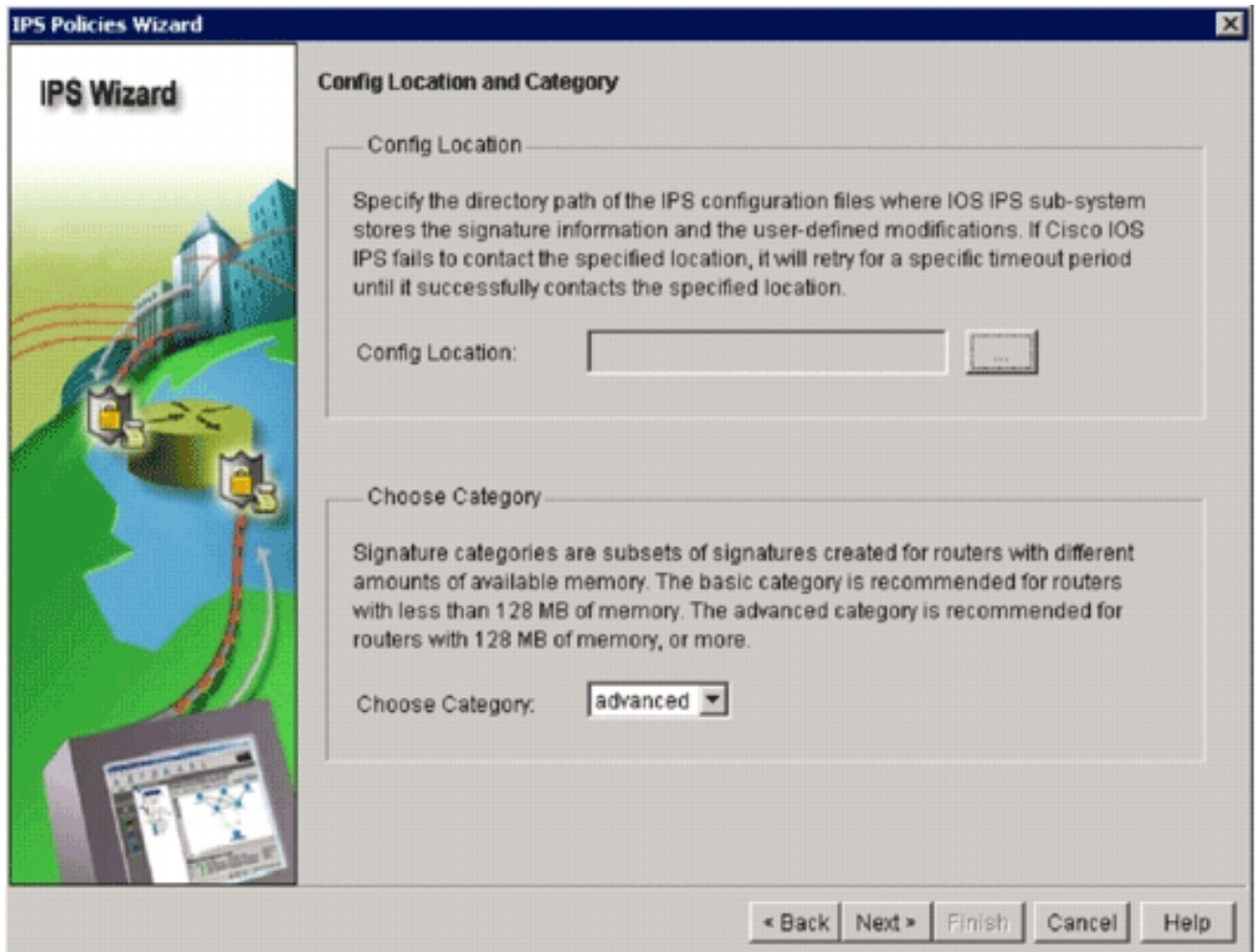
20. Geben Sie den URL für die Signaturdatei ein, und klicken Sie auf **OK**.

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.

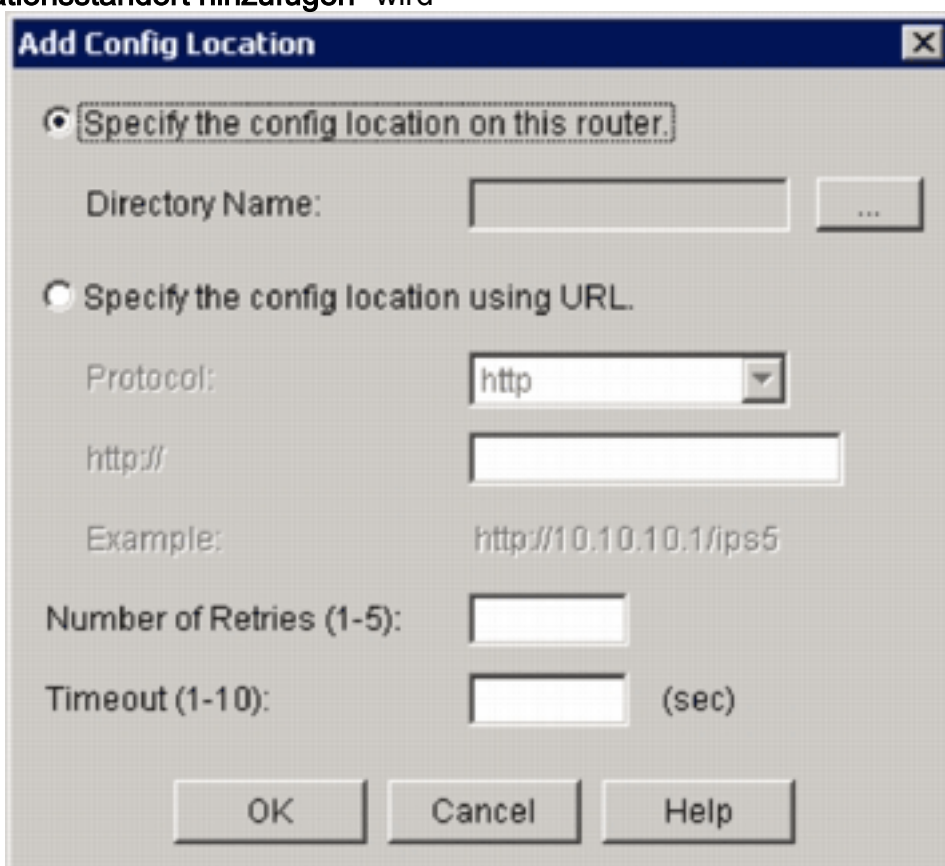
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101  
  
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16  
  
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128  
  
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E  
  
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35  
  
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85  
  
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36  
  
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE  
  
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3  
  
F3020301 0001
```

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

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

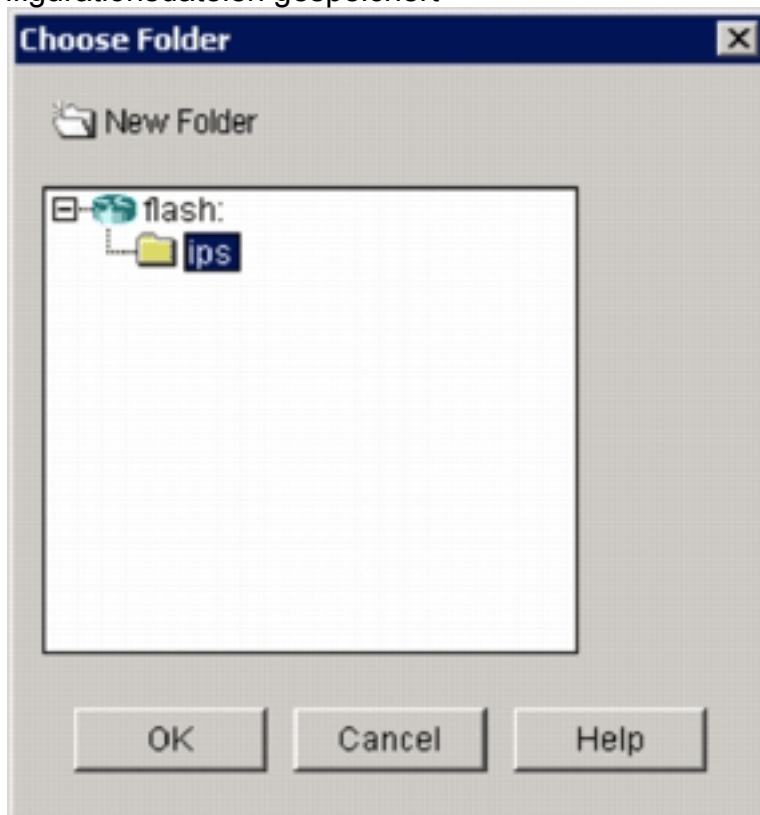


23. Klicken Sie im Fenster Config Location (Speicherort und Kategorie) auf die Schaltfläche **Config Location (Speicherort der Konfiguration) (..)**, um einen Speicherort für die Signaturdefinition und Konfigurationsdateien anzugeben. Das Dialogfeld "Konfigurationsstandort hinzufügen" wird



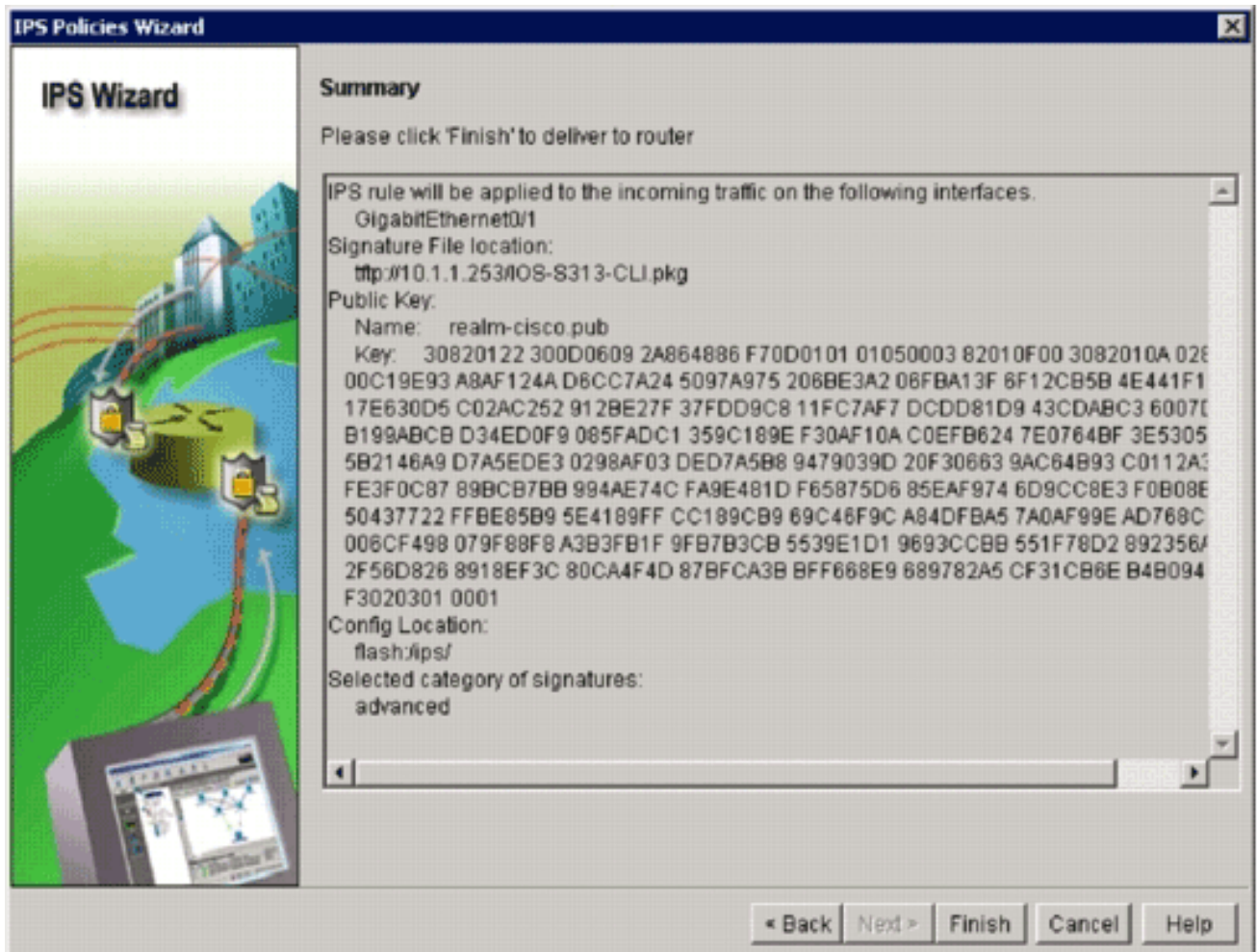
angezeigt.

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 Signaturdefinitions- und Konfigurationsdateien gespeichert

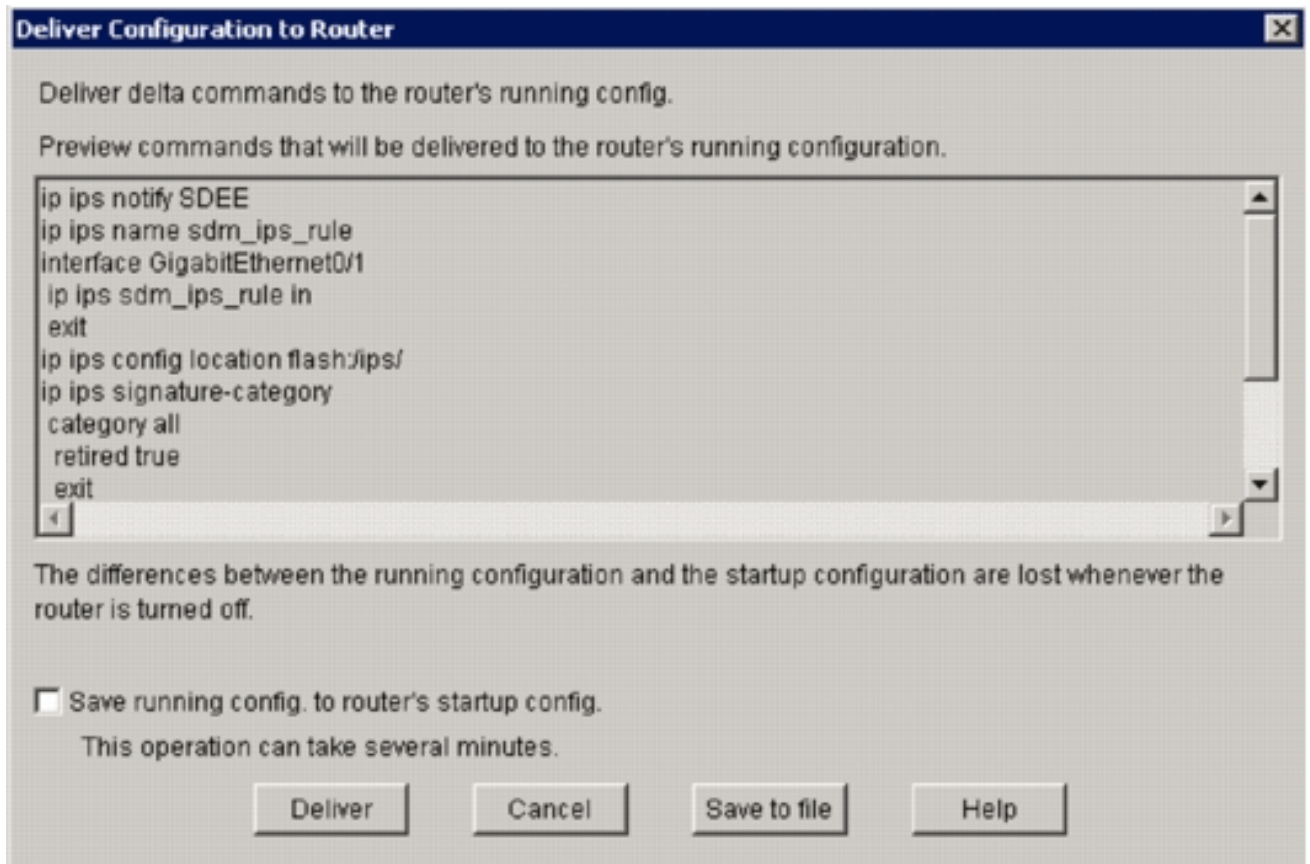


werden.

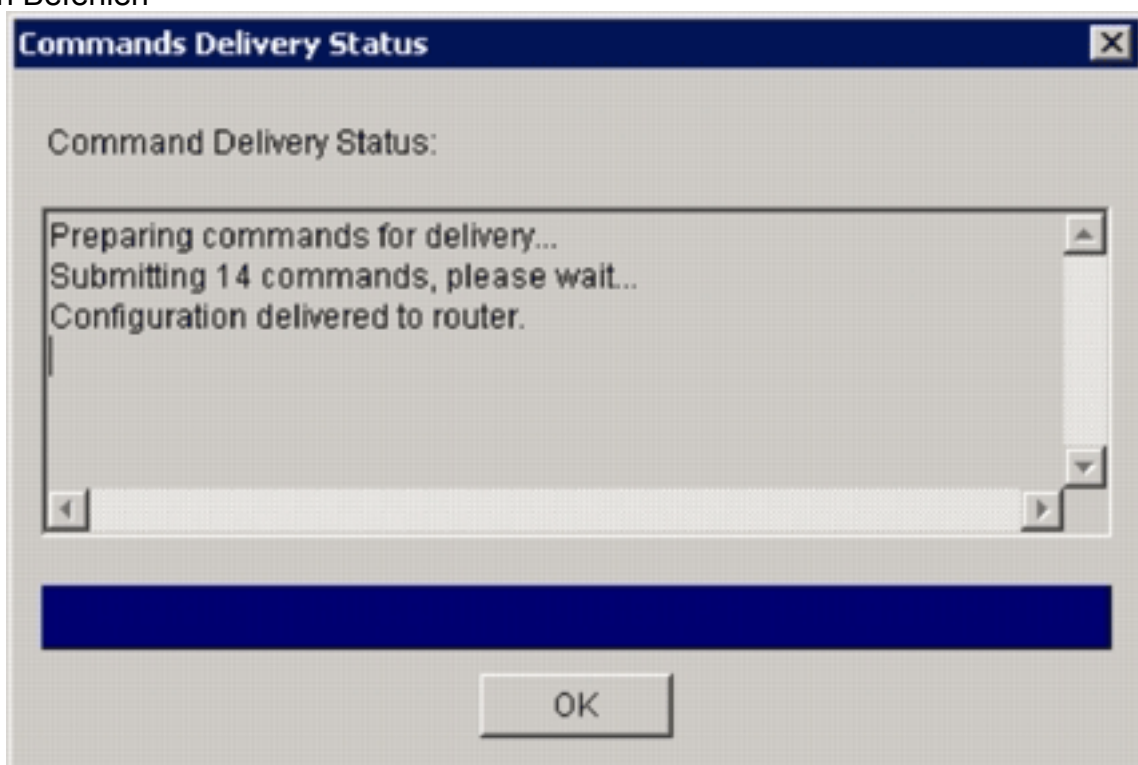
25. Klicken Sie oben im Dialogfeld auf **Neues Verzeichnis**, wenn Sie ein neues Verzeichnis erstellen möchten.
26. Wenn Sie das Verzeichnis ausgewählt haben, klicken Sie auf **OK**, um die Änderungen zu übernehmen, und klicken Sie dann auf **OK**, um das Dialogfeld Speicherort für Konfig. hinzufügen 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.



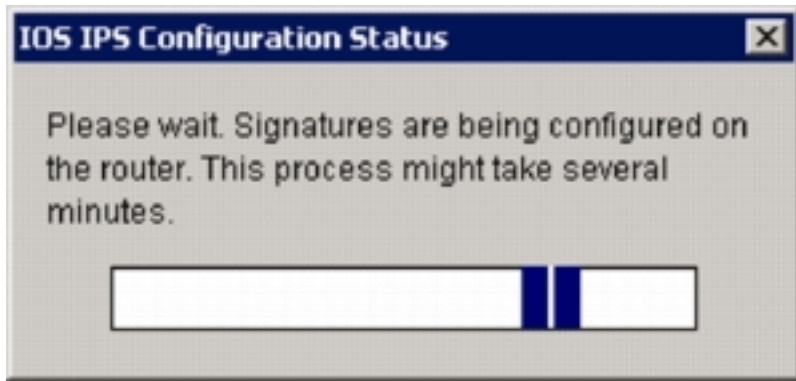
29. Klicken Sie auf der Übersichtsseite auf **Fertig stellen**, um die Konfigurationen und das Signaturpaket an den Router zu senden. Wenn die Option Preview-Befehle in den Einstellungen für Voreinstellungen in SDM aktiviert ist, zeigt SDM das Dialogfeld Deliver Configuration to Router (Konfiguration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



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

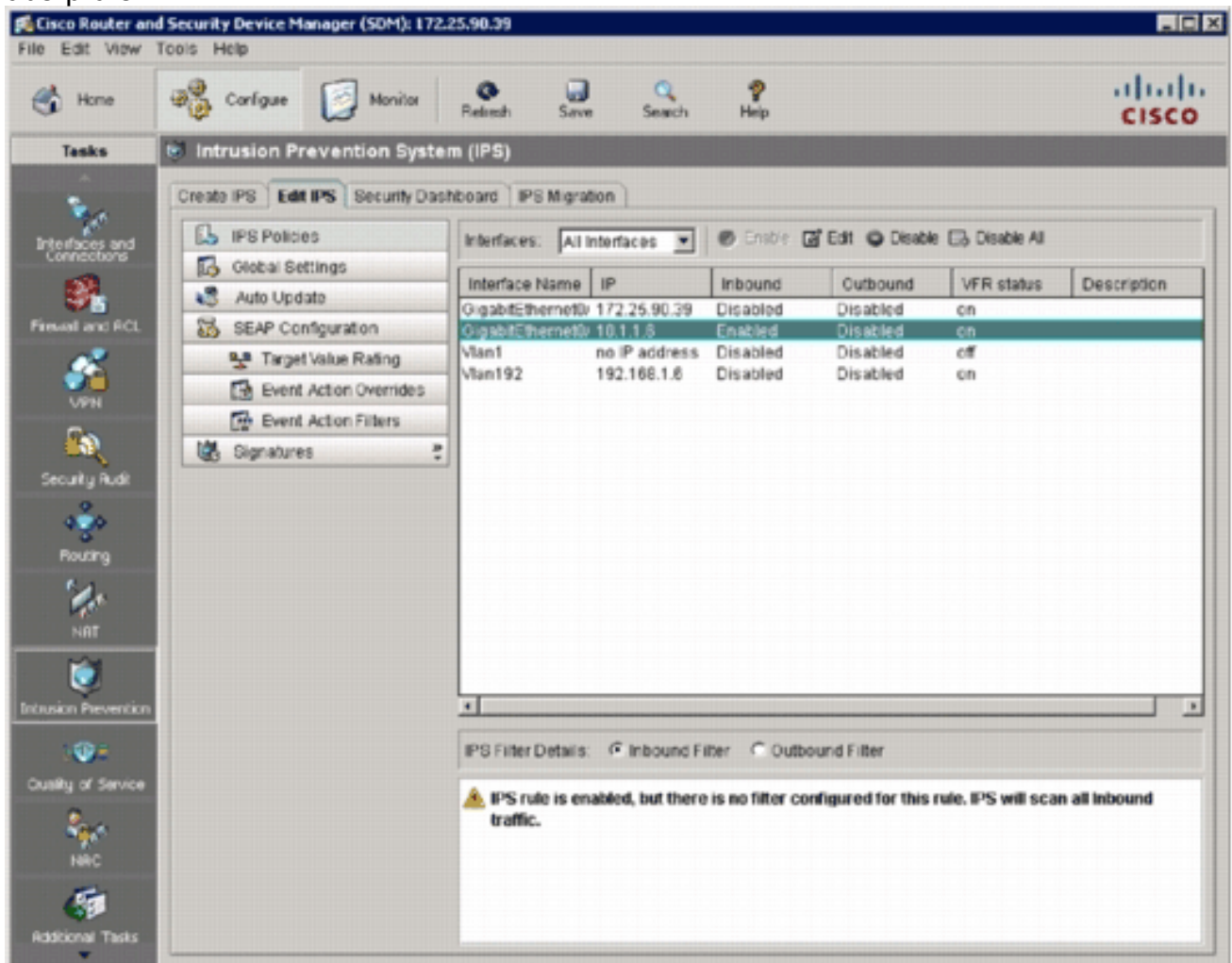


- an.
31. Wenn die Befehle an den Router übermittelt werden, klicken Sie auf **OK**, um fortzufahren. Das Dialogfeld "IOS IPS-Konfigurationsstatus" zeigt an, dass die Signaturen



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.



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

```
172.25.90.30 - TTY
ied
*Jan 13 16:41:08 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:41:08 PST Jan 13 2008
*Jan 13 16:41:08 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13 engines
*Jan 13 16:41:08 PST: %IPS-6-ENGINE_READY: multi-string - build time 8 ms - packets for this engine
will be scanned
*Jan 13 16:41:00 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures - 2 of 13 engines
*Jan 13 16:41:33 PST: %IPS-6-ENGINE_READY: service-http - build time 24892 ms - packets for this engine
will be scanned
*Jan 13 16:41:33 PST: %IPS-6-ENGINE_BUILDING: string-tcp - 961 signatures - 3 of 13 engines
*Jan 13 16:42:32 PST: %IPS-6-ENGINE_READY: string-tcp - build time 59424 ms - packets for this engine
will be scanned
*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 572 ms - packets for this engine w
ill be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
*Jan 13 16:42:34 PST: %IPS-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_READY: 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 - 38 signatures - 10 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: 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 w
ill be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures - 12 of 13 engine
s
*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 engine
e will 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.

Cisco Router and Security Device Manager (SDM): 172.25.90.39

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

CISCO

Tasks

Intrusion Prevention System (IPS)

Create IPS Edit IPS Security Dashboard IPS Migration

IPS Policies
Global Settings
Auto Update
SEAP Configuration
Target Value Rating
Event Action Overrides
Event Action Filters
Signatures

OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases

Import View by: All Signatures Criteria: --N/A-- **Total[2158] Configured[588]**

Select All Add Edit Enable Disable Pause Refresh

Enabled	I	Sig ID	SubSig ID	Name	Action	Severity	Fidelity %
+		9423	1	Back Door Psychward	produce-aler	high	85
+		9423	0	Back Door Psychward	produce-aler	high	100
+		5343	0	Apache Host Header Cross Site	produce-aler	high	100
+		3122	0	SMTP EXN root Recon	produce-aler	low	85
-		5099	0	MSN Messenger Webcam Buffer	produce-aler	high	80
+		5537	0	ICQ Client DNS Request	produce-aler	informational	100
+		3316	0	Project DOS	produce-aler	high	75
-		11003	0	Gtella File Request	produce-aler	low	100
+		5196	1	Red Hat Stronghold Recon at	produce-aler	low	100
+		5196	0	Red Hat Stronghold Recon at	produce-aler	low	100
+		5773	1	Simple PHP Blog Unauthorized F	produce-aler	low	70
+		5773	0	Simple PHP Blog Unauthorized F	produce-aler	low	85
+		5411	0	Linksys Hits DoS	produce-aler	high	85
+		12019	0	SideFind Activity	produce-aler	low	85
+		5070	0	VNAV remote di Access	produce-aler	medium	100
-		3169	0	FTP SITE EXEC tw	produce-aler	high	85
-		5605	0	Windows Account Locked	produce-aler	informational	85

Apply Changes Discard Changes

IPS Signatures

16:53:02 PST Sun Jan 13 2008

Zugehörige Informationen

- [Cisco IOS IPS auf Cisco.com](#)
- [Cisco IOS IPS-Signalisierungspaket](#)
- [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](#)