# Cisco IOS IPSでのルータ、SDM、およびCisco IOS CLIの設定

# 内容

 概要

 前提条件

 要件

 使用するコンポーネント

 表記法

 設定

 工場出荷時のデフォルトの SDF を使ったCisco IOS IPS の有効化

 デフォルトの SDF を有効にした後の追加シグネチャの追加

 シグネチャの選択とシグネチャカテゴリの操作

 デフォルト SDF ファイルのシグネチャの更新

 関連情報

# 概要

Cisco Router and Security Device Manager(SDM)2.2では、Cisco IOS<sup>®</sup> IPS設定がSDMアプリケーションに統合されています。Cisco IOS IPS を設定するために、別のウィンドウを起動する必要はありません。

Cisco SDM 2.2 では、新しい IPS コンフィギュレーション ウィザードにより、ルータ上で Cisco IOS IPS をイネーブルにするために必要な手順が指示されます。また、Cisco SDM 2.2 で Cisco IOS IPS のイネーブル化、ディセーブル化、調整を行うための高度な設定も使用できます。

あらかじめ調整されたシグネチャ定義ファイル(SDF)を使って、Cisco IOS IPS を実行するこ とを推奨します。attack-drop.sdf、128MB.sdf、256MB.sdf)。これらのファイルは、メモリ量が 異なるルータに対して作成されます。ファイルは Cisco SDM にバンドルされています。ルータで Cisco IOS IPS 初めてイネーブルにする場合は SDF が推奨されます。これらのファイルは、 <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u>(登録ユーザ専用)からダウンロード<u>するこ</u> <u>と</u>もできます。

デフォルトの SDF をイネーブルにするプロセスは、「工場出荷時のデフォルトの SDF を使った Cisco IOS IPS の有効化」で詳細に説明します。デフォルトの SDF が十分でないか、新しいシグ ネチャを追加する場合、「<u>Append Additional Signatures after Enabling Default SDF</u>」に記載され ている手順を使用できます。

# <u>前提条件</u>

#### <u>要件</u>

Cisco SDM 2.2を使用するには、Java Runtime Environment(JRE)バージョン1.4.2以降が必要です 。シスコが推奨する調整されたシグニチャファイル(DRAMに基づく)が、Cisco SDM(Cisco SDMのルータのフラッシュメモリにロードされる)にバンドルされています。

#### <u>使用するコンポーネント</u>

このドキュメントの情報は、Cisco ルータおよび Security Device Manager(SDM)2.2 に基づく ものです。

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ました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

#### <u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

### 設定

#### 工場出荷時のデフォルトの SDF を使ったCisco IOS IPS の有効化

#### CLI の手順

CLI を使って、ルータのフラッシュ上に 128 MB.sdf をロードするように Cisco IOS IPS を搭載した Cisco 1800 シリーズ ルータを構成するには、次の手順を実行します。

- 1. Security Device Event Exchange (SDEE) イベント通知をイネーブルにするようにルータを 設定します。 yourname#conf t
- 終了するには、コンフィギュレーション コマンド(1行に1つずつ)を入力して、Cntl キー を押した状態で Z キーを押します。 yourname(config)#ip ips notify sdee
- 3. インターフェイスの関連付けに使用される IPS ルール名を作成します。 yourname(config)#**ip ips name myips**
- 4. Cisco IOS IPS システムがシグネチャを読み取るファイルを指定する IPS location コマンド を設定します。この例では、フラッシュ上の次のファイルを使用します。128MB.sdf.このコ マンドのロケーション URL の部分は、ファイルをポイントする、フラッシュ、ディスク、 または FTP、HTTP、HTTPS、RTP、SCP、TFTP を介したプロトコルを使用する有効な URL になることがあります。

yourname(config)#ip ips sdf location flash:128MB.sdf

注:Telnetセッションを介してルータを設定する場合は、terminal monitorコマンドを有効に する必要があります。有効にしないと、シグニチャエンジンの構築時にSDEEメッセージが 表示されません。 5. トラフィックをスキャンするため Cisco IOS IPS を有効にするインターフェイスで IPS を有 効にします。このケースでは、インターフェイス fastEthernet 0 の双方向で有効にしました

```
yourname(config)#interface fastEthernet 0
yourname(config-if)#ip ips myips in
*Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS:
        SDF loaded successfully from opacl
*Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS:
        SDF loaded successfully from flash:128MB.sdf
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
       OTHER - 4 signatures - 1 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_READY:
       OTHER - 0 ms - packets for this engines will be scanned
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
       MULTI-STRING - 0 signatures - 2 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED:
       MULTI-STRING - there are no new signature definitions for this engine
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
       STRING.ICMP - 1 signatures - 3 of 15 engines
*Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
        STRING.ICMP - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING:
        STRING.UDP - 17 signatures - 4 of15 engines
*Oct 26 00:32:31.393: %IPS-6-ENGINE_READY:
       STRING.UDP - 448 ms - packets for this engine will be scanned
*Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING:
       STRING.TCP - 58 signatures - 5 of 15 engines
*Oct 26 00:32:33.641: %IPS-6-ENGINE_READY:
       STRING.TCP - 2248 ms - packets for this engine will be scanned
*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING:
       SERVICE.FTP - 3 signatures - 6 of 15 engines
*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY:
       SERVICE.FTP - 16 ms - packets for this engine will be scanned
*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING:
        SERVICE.SMTP - 2 signatures - 7 of 15 engines
*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY:
        SERVICE.SMTP - 28 ms - packets for this engine will be scanned
*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
       SERVICE.RPC - 29 signatures - 8 f 15 engines
*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
       SERVICE.RPC - 92 ms - packets for this engine will be scanned
*Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING:
       SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 00:32:33.801: %IPS-6-ENGINE_READY:
       SERVICE.DNS - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING:
       SERVICE.HTTP - 132 signatures - 10 of 15 engines
*Oct 26 00:32:44.505: %IPS-6-ENGINE_READY:
        SERVICE.HTTP - 10704 ms - packets for this engine will be scanned
*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING:
        ATOMIC.TCP - 11 signatures - 11 of 15 engines
*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY:
       ATOMIC.TCP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING:
       ATOMIC.UDP - 9 signatures - 12 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
       ATOMIC.UDP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
       ATOMIC.ICMP - 0 signatures - 13 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED:
       ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines
```

IPS ルールが初めてインターフェイスに適用されると、Cisco IOS IPS は SDF location コマ ンドで指定されたファイルからシグネチャを構築します。SDEE メッセージが コンソール に記録され、syslog サーバが設定されている場合は、syslog サーバに送信されます。 <number> of <number> engines が付いた SDEE メッセージは、シグネチャ エンジンの構築 プロセスを示しています。最後に、2 つの番号が同じである場合、すべてのエンジンが構築 されます。注:IP仮想リアセンブリは、オンにすると、そのインターフェイスを通じてルー タに着信するフラグメント化パケットを自動的に再構成するインターフェイス機能です。ト ラフィックがルータに着信するすべてのインターフェイスで、IP 仮想アセンブリを有効にす ることを推奨します。上記の例では、インターフェイス fastEthernet 0 で「IP 仮想アセンブ リ」をオンにするだけでなく、内部インターフェイス VLAN 1 でも同様にオンに設定します。

yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly

#### SDM 2.2 の手順

Cisco SDM 2.2 を使って Cisco IOS IPS を搭載した Cisco 1800 シリーズ ルータを設定するには、次の手順を実行します。

1. SDM アプリケーションで [Configure] をクリックし、次に [Intrusion Prevention] をクリック

Tasks [3]	intrusion Prevention System (IPS)	
Presidence and	eate IPS Edit IPS The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).	
Prevail and PCL	Use Case Scenario Network based Intrusion Prevention IPS rules applied to interface	
20 20 20 20 20 20 20 20 20 20 20 20 20 2	UN UN UN	
Intrusion Prevention	Launch IPS Rule Witand.	
Sec.		

2. [Create IPS] タブをクリックし、次に [Launch IPS Rule Wizard] をクリックします。Cisco SDM では、Cisco IOS IP 機能を設定するため、SDEE を介した IPS イベント通知が必要で す。デフォルトでは、この機能は無効になっています。Cisco SDM では、次の図に示すように、SDEE を介して IPSイベント通知を有効にするように指示されます。



3. [OK] をクリックします。[IPS Policies Wizard] ダイアログボックスの [Welcome to the IPS Policies Wizard] ウィンドウが表示されます。



4. [next] をクリックします。[Select Interfaces] ウィンドウが表示されます。

IPS Wizard       Select Interfaces         Select Interfaces to which the IPS rule should be applied. Also choose whether the rul should be applied to inbound or outbound.         Interface Name       Inbound         Outbound       Outbound         BRI0       C         FastEthernet0       V	PS Policies Wizard			<u>د</u>
Select the interfaces to which the IPS rule should be applied. Also choose whether the rule should be applied to inbound or outbound.          Interface Name       Inbound       Outbound         BRI0       □       □         FastEthernet0       Image: Comparison of the initial should be applied. Also choose whether the rule should be applied to inbound or outbound.	IPS Wizard	Select Interfaces		
Interface Name       Inbound       Outbound         BRI0            FastEthernet0		Select the interfaces to which the IPS rule s should be applied to inbound or outbound.	should be applied. Also cho	ose whether the rule
BRI0       □       □         FastEthernet0       I       I		Interface Name	Inbound	Outbound
FastEthernet0       Image: Comparison of the set		BRIO		
	likhak mu 17 stil	FastEthernet0	₹	. <del>ب</del>
Bart Market Barret M	And a second sec			

- 5. IPS を有効にするインターフェイスを選択し、[Inbound] または [Outbound] チェックボック スのいずれかをオンにして、そのインターフェイスの方向を示します。注:インターフェイ スでIPSを有効にする場合は、インバウンド方向とアウトバウンド方向の両方を有効にする ことを推奨します。
- 6. [next] をクリックします。[SDF Locations] ウィンドウが表示されます。
- 7. SDF の場所を設定するには、[Add] をクリックします。[Add a Signature Location] ダイアロ グボックスが表示されます。

DS Wizard	SDF Locations		
o mizaru	Specify the locations from w Cisco IOS IPS. If Cisco IOS I locations in order until it suc	hich the SDF (signature definition file IPS fails to load the SDF from the first cessfully loads the SDF file.	) should be loaded by the location, it tries the
120	SDF Locations		
1715			Add
			Delete
110	Concernation of the second		Move Up
17.25	Add a Signature Locat	ion	Move Down
	<ul> <li>Specify SDF onflash:</li> </ul>		
69	File Name onflash:	256MB.sdf	
	Specify SDF using U	RL:	cation it can
			control, is cont
	1 Uniteral		
AL	Exemple		
	(* [autosave]		
Renord	OK	Cancel Help	
			-

- 8. [Specify SDF on flash] ラジオ ボタンをクリックして、[File Name on flash] ドロップダウン リストから 256MB.sdf を選択します。
- 9. [Autosave] チェックボックスをオンにして、[OK] をクリックします。注: [Autosave] オプ ションにより、シグネチャが変更された場合、シグネチャファイルが自動的に保存されます 。[SDF Locations] ウィンドウに新しい SDF の場所が表示されます。



クアップを指定するために、追加の署名場所を追加できます。

- 10. [Use Built-In Signatures (as backup)] チェックボックスをオンにします。**注:1つ**以上の場所を指定していない限り、組み込みの署名オプションを使用しないことを推奨します。
- 11. 継続するには [Next] をクリックします。[Summary] ウィンドウが表示されます。



12. [Finish] をクリックします。[Commands Delivery Status] ダイアログボックスに、IPS エンジンがすべてのシグネチャをコンパイルしたときのステータスが表示されます。



13. プロセスが完了したら、[OK] をクリックします。[Signature Compilation Status] ダイアロ グボックスに、シグネチャコンパイル情報が表示されます。

Signal	ture Compilation St	atus		
IPS si	ignature engines are l	built and are n	eady to scan packets.	
No.	Engine	Status	No of Signatures	-
2	MULTI-STRING	Skipped	No New Signatures	
3	STRING.ICMP	✓ Loaded	1	
4	STRING.UDP	✓ Loaded	17	
5	STRING.TCP	✓ Loaded	58	
6	SERVICE.FTP	✓ Loaded	3	
7	SERVICE.SMTP	Loaded	2	
8	SERVICE.RPC	✓ Loaded	29	
9	SERVICE.DNS	Loaded	31	
10	SERVICE.HTTP	✓ Loaded	132	
11	ATOMIC.TCP	Loaded	11	
12	ATOMIC.UDP	✓ Loaded	9	
13	ATOMIC.ICMP	Skipped	No New Signatures	
14	ATOMIC.IPOPTIONS	Loaded	1	
15	ATOMIC.L3.IP	🖌 Loaded	.5	•
4				•
		Close	1	
			]	

ンジンと、そのエンジン内のシグネチャ数が表示されます。スタータス列に [Skipped] と 表示されたエンジンの場合、そのエンジン用にロードされたシグネチャはありません。

14. [Close] をクリックして、[Signature Compilation Status] ダイアログボックスを閉じます。

- 15. どのシグネチャがルータに現在ロードされているか検証するには、[Configure] をクリック し、次に [Intrusion Prevention] をクリックします。
- 16. [Edit IPS] タブをクリックし、次に [Signatures] をクリックします。[Signatures] ウィンド ウに IPS シグネチャリストが表示されます。

home 🖞	Configure 🔯 Monitor	@ Retresh		Save	Q. Search	P Help		CIS	
Tasks	🐱 Intrusion Prevention Sys	tem (IPS)							
	Create IPS Edit IPS								
tertine and	IPS Policies		d =	Select to	w. Al So	natures + Oriteria:NIA	•	Te	tal[303
tormectors	🚯 Global Settings	Selec	t Al	& Add	· Fai Edt	1 Delete C Enable O Dis	able	6	Detail
34	G SDEE Messages	Ecohind		Sel	la esa n	Name	Action	County	Eer
wall and RCL	Signatures	P. Criscieu		3157	Statisty L/	FTP PASV Port Spool	alarm	high	SERVE
S.	EP-Categories			11002	0	Grutella Server Reply	alarm	kow	STRIN
UPH	B- Attack	0	-	5088	0	vWWV Akopia MiniVend access	alarm	low	SERV
50	B- L2/L3/L4 Protocol	0		3153	0	FTP Improper Address	olarm	medium	SERV
ourity Audit	🖶 🛄 Releases	0		3129	0	Mmail Virus C Variant File Attac	alarm drop reset	medium	SERV
Nouting		0		5084	1	vWWV Albaba attack 2	alarm	low	SERV
1.		0		5084	0	vWWV Albaba effack 2	alarm	low	SERV
1		0		11212	0	Yahoo Messenger Through HT	olarm	informational	SERV
10H1		0		5080	0	vWWW IEM WebSphere access	alarm	low	SERV
<b>Q</b>		0		3218	0	vWWW SGI wrap bug	alarm	medium	SERV
n Prevention		0		5052	0	vWWV VTI Open attempt	olarm	medium	SERV
۰.		0		9535	0	Back Door TansScout	olarm	high	STRIN
of Service		0		6062	1	<b>CNS Authors Request</b>	alarm	low	SERVI
0.		1000			a superior		panapana		

### <u>デフォルトの SDF を有効にした後の追加シグネチャの追加</u>

#### CLI の手順

シグネチャの作成、または配布済み IOS-Sxxx.zip ファイルのシグネチャ情報の読み取りに使用で きる CLI コマンドはありません。SDM または IPS センサー 用 Management Center のいずれか を使って、Cisco IOS IPS システムのシグネチャを管理することを推奨します。

すでにシグネチャファイルを準備していて、このファイルを Cisco IOS IPS システムで実行して いる SDF とマージする場合は、次のコマンドを使用できます。

yourname#**show running-config | include ip ips sdf** ip ips sdf location flash:128MB.sdf yourname#

シグネチャ ロケーション コマンドで定義したシグネチャ ファイルは、ルータのリロード時、またはルータ IOS IPS の再設定時に、ルータがシグネチャ ファイルをロードするファイルです。マージ プロセスを正常に完了するには、シグネチャ ファイル ロケーション コマンドで定義されたファイルも更新する必要があります。

1. 現在設定されているシグネチャの場所を確認するには、show コマンドを使用します。出力 には設定されたシグネチャの位置が表示されます。このコマンドは、現在実行されているシ グネチャがどこからロードされたかを表示します。 yourname#show ip ips signatures

Builtin signatures are configured

Signatures were last loaded from flash:128MB.sdfCisco SDF release version S128.0Trend

SDF release version V0.0

# シグネチャ ファイルをマージするには、copy <url> ips-sdf コマンドを、前の手順で取得した情報と併せて使用します。

yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf Loading mysignatures.xml from 10.10.10.5 (via Vlan1): ! [OK - 1612 bytes] \*Oct 26 02:43:34.904: %IPS-6-SDF\_LOAD\_SUCCESS: SDF loaded successfully from opacl No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport 4715 \*Oct 26 02:43:34.920: %IPS-6-SDF\_LOAD\_SUCCESS: SDF loaded successfully from tftp://10.10.10.5/mysignatures.xml \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILDING: OTHER - 4 signatures - 1 of 15 engines \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILD\_SKIPPED: OTHER - there are no new signature definitions for this engine \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILDING: MULTI-STRING - 0 signatures -2 of 15 engines \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILD\_SKIPPED: MULTI-STRING - there are no new signature definitions for this engine \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILDING: STRING.ICMP - 1 signatures -3 of 15 engines \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILD\_SKIPPED: STRING.ICMP - there are no new signature definitions for this engine \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILDING: STRING.UDP - 17 signatures -4 of 15 engines \*Oct 26 02:43:34.920: %IPS-6-ENGINE\_BUILD\_SKIPPED: STRING.UDP - there are no new signature definitions for this engine \*Oct 26 02:43:34.924: %IPS-6-ENGINE\_BUILDING: STRING.TCP - 59 signatures -5 of 15 engines \*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED PARAM: STRING.TCP 9434:0 CapturePacket=False -This parameter is not supported \*Oct 26 02:43:37.264: %IPS-6-ENGINE\_READY: STRING.TCP - 2340 ms - packets for this engine will be scanned \*Oct 26 02:43:37.288: %IPS-6-ENGINE\_BUILDING: SERVICE.FTP - 3 signatures -6 of 15 engines \*Oct 26 02:43:37.288: %IPS-6-ENGINE\_BUILD\_SKIPPED: SERVICE.FTP - there are no new signature definitions for this engine \*Oct 26 02:43:37.288: %IPS-6-ENGINE\_BUILDING: SERVICE.SMTP - 2 signatures -7 of 15 engines \*Oct 26 02:43:37.288: %IPS-6-ENGINE\_BUILD\_SKIPPED: SERVICE.SMTP - there are no new signature definitions for this engine \*Oct 26 02:43:37.288: %IPS-6-ENGINE\_BUILDING: SERVICE.RPC - 29 signatures -8 of 15 engines \*Oct 26 02:43:37.288: %IPS-6-ENGINE\_BUILD\_SKIPPED: SERVICE.RPC - there are no new signature definitions for this engine \*Oct 26 02:43:37.292: %IPS-6-ENGINE\_BUILDING: SERVICE.DNS - 31 signatures -9 of 15 engines \*Oct 26 02:43:37.292: %IPS-6-ENGINE\_BUILD\_SKIPPED: SERVICE.DNS - there are no new signature definitions for this engine \*Oct 26 02:43:37.296: %IPS-6-ENGINE\_BUILDING: SERVICE.HTTP - 132 signatures -10 of 15 engines \*Oct 26 02:43:37.296: %IPS-6-ENGINE\_BUILD\_SKIPPED: SERVICE.HTTP - there are no new signature definitions for this engine \*Oct 26 02:43:37.316: %IPS-6-ENGINE\_BUILDING: ATOMIC.TCP - 11 signatures -11 of 15 engines \*Oct 26 02:43:37.316: %IPS-6-ENGINE\_BUILD\_SKIPPED: ATOMIC.TCP - there are no new signature definitions for this engine \*Oct 26 02:43:37.316: %IPS-6-ENGINE\_BUILDING: ATOMIC.UDP - 9 signatures -12 of 15 engines \*Oct 26 02:43:37.316: %IPS-6-ENGINE\_BUILD\_SKIPPED: ATOMIC.UDP - there are no new signature definitions for this engine \*Oct 26 02:43:37.320: %IPS-6-ENGINE\_BUILDING: ATOMIC.ICMP - 0 signatures -13 of 15 engines \*Oct 26 02:43:37.320: %IPS-6-ENGINE\_BUILD\_SKIPPED: ATOMIC.ICMP - there are

no new signature definitions for this engine

- \*Oct 26 02:43:37.320: %IPS-6-ENGINE\_BUILDING: ATOMIC.IPOPTIONS 1 signatures 14 of 15 engines
- \*Oct 26 02:43:37.320: %IPS-6-ENGINE\_BUILD\_SKIPPED: ATOMIC.IPOPTIONS there are no new signature definitions for this engine
- \*Oct 26 02:43:37.320: %IPS-6-ENGINE\_BUILDING: ATOMIC.L3.IP 5 signatures 15 of 15 engines
- \*Oct 26 02:43:37.320: %IPS-6-ENGINE\_BUILD\_SKIPPED: ATOMIC.L3.IP there are no new signature definitions for this engine

yourname#

copy コマンドを実行すると、ルータはシグネチャ ファイルをメモリにロードし、シグネチャ エンジンを構築します。コンソール SDEE メッセージの出力では、各シグネチャ エンジンの構築状態が表示されます。%IPS-6-ENGINE\_BUILD\_SKIPPED は、このエンジンには新規シグネチャがないことを示しています。%IPS-6-ENGINE\_READY は、新規シグネチャがあり、エンジンが準備できていることを示しています。前述のとおり、「15 of 15 engines」というメッセージは、すべてのエンジンが構築済みであることを示しています。 IPS-7-UNSUPPORTED\_PARAM は、Cisco IOS IPS が特定のパラメータをサポートしていないことを示しています。たとえば CapturePacket と ResetAfterIdle です。注: これらのメッセージは情報専用で、Cisco IOS IPS のシグネチャ機能やパフォーマンスへの影響はありません。これらのログメッセージは、ロギングレベルをデバッグ(レベル7)より上に設定することでオフにできます。

シグネチャ ロケーション コマンドで定義されている SDF を更新し、ルータのリロード時に、更新されたシグネチャと一緒にマージされたシグネチャ セットが設定されるようにします。この例では、マージされたシグネチャを 128MB.sdf フラッシュ ファイルに保存した後のファイル サイズの差異を示しています。

yourname#**show flash:** 

-#- --length-- ----date/time----- path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- ---- date/time----- path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf

警告:新しい128MB.sdfには、お客様がマージしたシグニチャが含まれています。内容は、シスコのデフォルトの 128MB.sdf ファイルとは異なります混乱を避けるために、このファイルを別の名前に変更することを推奨します。名前を変更した場合、シグネチャロケーション コマンドも変更する必要があります。

#### SDM 2.2 の手順

Cisco IOS IPS を有効にすると、Cisco SDM インポート機能を使って、シグネチャ セットを実行 しているルータに新しいシグネチャを追加できます。新しいシグネチャをインポートするには、 次の手順を実行します。

- 1. 追加のシグネチャをインポートするには、デフォルト SDF または IOS-Sxxx.zip 更新ファイ ルを選択します。
- 2. [Configure] をクリックし、次に [Intrusion Prevention] をクリックします。
- 3. [Edit IPS] タブをクリックし、次に [Import] をクリックします。

5 IPS Policies	Import •	Select k	y: All Sig	natures - Criteria:N(A,	•	To	tal(303)
🖏 Global Settings	From PC		d • 🗃 Edit	1 Delete 🔘 Enable 🔾 Dis	able	6	Details
G SDEE Messages	From rout	er flash	04000	Ninna	Antino	Caucada	- E
🛃 Signatures	P LINEAUN T	21.67	Subsigit	FTD DASU Ded Second	Action	Seventy	CEPA
All Categories		3137	•	FIP PASY Port spoor	ausem	riigen	SERVI
D OS	•	11002	0	Gnutella Server Reply	alarm	low	STRIN
E- Attack	0	5088	0	vWWW Akopia Min/Vend access	alarm	low	SERVI
E L2/L3/L4 Protocol	0	3153	0	FTP Improper Address	alarm	medium	SERVI
È- <mark>`</mark> Releases	0	3129	0	Mimail Virus C Variant File Attac	alarm drop reset	medium	SERVI
	0	5084	1	vWWV Alibaba attack 2	alarm	low	SERVI
	0	5084	0	vWWV Alibaba attack 2	alarm	low	SERVI
	0	11212	0	Yahoo Messenger Through HT	alarm	informational	SERVI
	0	5080	0	vWWV IBM WebSphere access	alarm	low	SERVI
	0	3218	0	vWWV SGI wrap bug	alarm	medium	SERVI
	0	5052	0	vWWV VTI Open attempt	alarm	medium	SERVI
	0	9535	0	Back Door TansScout	alarm	high	STRIN
	0	6062	1	DNS Authors Request	alarm	low	SERVI
	1 T		1 . 1			· · · ·	

- 4. [Import] ドロップダウン リストから [From PC] を選択します。
- 5. シグネチャのインポート元のファイルを選択します。

Import	2 🛛
Look jn: 😂 CCOSigs	- 🖶 🖆 📰 -
105-5208.zip         105-5214.zip           105-5209.zip         105-5215.zip           105-5210.zip         105-5216.zip           105-5211.zip         105-5217.zip           105-5212.zip         105-5213.zip	
Ela name IIOC C217 in	> >
Files of type: All Files (".")	Cancel

この例では、Cisco.com からダウンロー

- ドした最新のアップデートを、ローカルの PC ハード ディスクに保存します。
- 6. [Open] をクリックします。警告:メモリの制約により、既に展開されているシグネチャの 上に追加できる新しいシグネチャの数は限られています。選択したシグネチャの数が多すぎ る場合、メモリ不足のため、ルータは新しいシグネチャをすべてロードできない場合があり ます。シグネチャ ファイルのロードが完了すると、[IPS Import] ダイアログボックスが表示

B- Attack	Name	Deployed
E-Service	KaZaA v2 UDP Client Probe	Yes
General Service	KaZaA v2 UDP Client Probe	Yes
-DNS	KaZaA v2 UDP Client Probe	Yes
Finger	Gnutella Client Request	Yes
FTP	Gnutella Server Reply	Yes
Ident	Gtella File Request	No
IMAP	Bearshare File Request	No
NNTP	KaZaA Client Activity	Yes
-NETBIOS/SMB	Gnucleus File Request	Yes
NTP	Limewire File Request	No
POP	Morpheus File Request	No
RPC	Phex File Request	No
SMTP	Swapper File Request	No
SNMP	XoloX File Request	No
TELNET	GTK-Gnutella File Request	Yes
File Sharing	Mutelia File Request	No
SOCKS	Hotline Client Login	No
I I I I I I I I I I I I I I I I I I I	Hotline File Transfer	No

7. 左のツリー ビューに移動し、インポートするシグネチャの横の [Import] チェックボックスを オンにします。

8. [Merge] ラジオ ボタンをクリックし、次に [OK] をクリックします。**注:[**Replace]オプショ ンは、ルータで設定されている現在のシグニチャを、インポートする選択したシグニチャに 置き換えます。[OK] をクリックすると、Cisco SDM アプリケーションはルータにシグネチ

Signature Delive	ry Status	
Delivering SDF to	o router	
	-	

ャを配布します。

┛注:シグネ

**チャ**のコンパイルおよびロード中に高いCPU使用率が発生します。インターフェイスで Cisco IOS IPS を有効にすると、シグネチャ ファイルのロードが開始されます。ルータで SDF のロードが完了するまで約 5 分かかります。Cisco IOS ソフトウェア CLI から show process cpu コマンドを使って、CPU の使用率を表示できます。ただし、ルータが SDF を ロードしている間は、その他のコマンドや他の SDF のロードは実行しないでください。こ のような操作を実行すると、シグネチャ コンパイル プロセスが完了するまでの時間が長く なります(SDF のロード時に CPU 使用率が 100 パーセントに近くなるため)。シグネチ ャのリストを参照して、*enabled 状態でない場合、シグネチャを有効にする必要があります* 。シグニチャの総数は519に増加しました。この数には、ファイル共有サブカテゴリに属す るIOS-S193.zipファイルで使用可能なすべてのシグニチャが含まれます。

b IPS Policies		De Impo	nt =	Select t	y: Al Sig	natures 💌 Criteria: 🔤N/A	•	To	tal[305]
Global Settings		R Selec	t Al	Ad	d 🕶 💽 Edit	1 Delete 🔘 Enable 🔾 Dis	able	Q	, Details
SDEE Messages		Enabled	1	Sig D	SubSig ID	Name	Action	Severity	Eng
Signatures	÷			3157	0	FTP PASV Port Spoof	olarm	high	SERVI
D OS		0		11002	0	Gnutella Server Reply	alarm	low	STRIN
Attack     Candca		0		5088	0	VWW Akopia MiniVend access	alarm	low	SERVI
E Call L2/L3/L4 Protocol		0		3153	0	FTP Improper Address	alarm	medium	SERVI
🖻 🚰 Releases		•		3129	0	Mimail Virus C Variant File Attac	alarm drop reset	medium	SERVI
		0		5084	1	WWW Alibaba attack 2	alarm	low	SERVI
		0		5084	0	WWW Albaba attack 2	alarm	low	SERVI
		0		11212	0	Yahoo Messenger Through HT	alarm	informational	SERVI
		0		5080	0	WWW IBM WebSphere access	alarm	low	SERVI
		0		3218	0	vWWV SGI wrap bug	alarm	medium	SERV1
		0		5052	0	√WWV VTI Open attempt	alarm	medium	SERVI
		0		9535	0	Back Door TansScout	alarm	high	STRIN
		0		6062	1	DNS Authors Request	alarm	low	SERVI
		+ ["						· · /	

Cisco SDM を使って Cisco IOS IPS 機能を管理する方法についてのより高度なトピックについて は、次の URL の Cisco SDM ドキュメントを参照してください。

## シグネチャの選択とシグネチャ カテゴリの操作

ネットワーク用に正しいシグネチャを効果的に選択する方法を決定するには、保護対象のネット ワークに関していくつか知らなければならないことがあります。Cisco SDM 2.2 以降では、更新 されたシグネチャ カテゴリにより、ユーザはネットワークを保護する正しいシグネチャ セットを 選択できます。

カテゴリは、シグネチャをグループ化する方法です。これにより、シグネチャの選択を、相互に 関連するシグネチャのサブセットに狭めることができます。1 つのシグネチャは 1 カテゴリにだ け属することもあれば、複数のカテゴリに属することもあります。

上位5つのカテゴリを以下に示します。

- OS:運用システムベースのシグニチャ分類
- 攻撃 攻撃に基づくシグネチャの分類
- ・サービス サービスに基づくシグネチャの分類
- ・レイヤ2~4プロトコル:プロトコルレベルのシグニチャ分類
- ・リリース リリースに基づくシグネチャの分類

上記の各カテゴリは、さらにサブカテゴリに分類されます。

たとえば、インターネットと VPN 経由で企業ネットワークへのブロードバンド接続が確立して いるホーム ネットワークを考えてみましょう。ブロードバンド ルータでは、すべての接続で、イ ンターネットから発信されたトラフィックが接続されているホーム ネットワークへ送信されない ように、インターネットへのオープン(非 VPN)接続で Cisco IOS Firewall が有効にされていま す。ホーム ネットワークからインターネットへのすべてのトラフィックは許可されます。 Windows ベースの PC と、HTTP(Web ブラウジング)や電子メールなどのアプリケーションを 使用するとします。

ユーザが必要とするアプリケーションだけがルータを介して通過できるように、ファイアウォー ルを設定します。これにより、ネットワーク全体に広がる、不要なトラフィックや潜在的に悪意 のあるトラフィックのフローが制御されます。ホーム ユーザが特定のサービスを必要としなかっ たり、使用しない場合を考えてみましょう。そのサービスがファイアウォールを通過することが 許可されている場合、攻撃に使用されて脅威がネットワーク全体に及ぶおそれのある穴が潜在す ることになります。ベスト プラクティスは、必要なサービスのみを許可することです。ここでは 、有効にするシグネチャを選択する方がより簡単です。ファイアウォールを通過することを許可 するサービスに対するシグネチャだけを有効にするだけですみます。この例では、サービスには 電子メールと HTTP が含まれます。Cisco SDM はこの設定を簡略化します。

カテゴリを使って必要なシグネチャを選択するには、[Service] > [HTTP] の順に選択して、すべて のシグネチャを有効にします。この選択プロセスは、すべての HTTP シグネチャを選択し、その シグネチャをルータにインポートできる、シグネチャのインポート ダイアログでも動作します。

選択する必要がある追加カテゴリには、DNS、NETBIOS/SMB、HTTPS および SMTP が含まれ ます。

#### <u>デフォルト SDF ファイルのシグネチャの更新</u>

構築された3つのSDF(attack-drop.dsf、128MB.sdf、および256MB.sdf)は、現在 http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup(登録ユーザ専用)のCisco.comで公開され ています。 これらのファイルの新バージョンは、使用可能になるとすぐに公開されます。これら のデフォルトの SDF で Cisco IOS IPS を実行するルータを更新するには、Web サイトにアクセ スして、これらのファイルの最新バージョンをダウンロードしてください。

#### CLI の手順

- ダウンロードしたファイルを、これらのファイルのダウンロード元としてルータで設定されている場所にコピーします。ルータで現在設定されている場所を確認するには、show running-config | in ip ips sdfコマンド
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   この例では、ルータは、フラッシュ上の 256MB.sdf を使用します。このファイルは、新しくダウンロードした 256MB.sdf をルータのフラッシュにコピーすると更新されます。
- Cisco IOS IPS サブシステムをリロードして、新しいファイルを実行します。Cisco IOS IPS をリロードするには次の2つの方法があります。ルータをリロードするか、IOS IPS サブシ ステムを再設定して、シグネチャをリロードするようトリガーすることです。Cisco IOS IPS を再設定するには、設定済みのインターフェイスからすべての IPS ルールを削除し、イ ンターフェイスに IPS ルールを適用し直すことです。これにより、Cisco IOS IPS システム のリロードがトリガーされます。

#### SDM 2.2 の手順

ルータ上のデフォルト SDF を更新するには、次の手順を実行します。

1. [Configure] をクリックし、次に [Intrusion Prevention] をクリックします。

2. [Edit IPS] タブをクリックし	次に [Global Settings]	タブをクリックします。
------------------------	----------------------	-------------

ate IPS Edit IPS			
IPS Policies			ම
3 Global Settings		Item Name	item Value
SDEE Messages		Syslog	Enabled
X Signatures		SDEE SDEE Alasta	Enabled
a ciginalares	-	SDEE Alerts SDEE Macesaac	200
		SDEE Subscription	1
		Engine Options	
		Fail Closed	Disabled
		Use Built-in Signatures (as backup)	Enabled
		Deny Action on IPS interface	Disabled
		Shun Event	
		Timeout	30
		Configured SDF Locations: 4 Add 3	Edit 🏦 Delete 🚖 Move Up 🐺 Move Down 🔊 Reload
		Configured SDF Locations: 4 Add a f	Edit 🏦 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload
		Configured SDF Locations: Add a final file for the file of the fil	Edit 🏦 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload
		Configured SDF Locations: Add at 1 Add at 1 flash:0128MB.sdf (autosave)	Edit 🏦 Delete 🚖 Move Up 🤑 Move Down 🔊 Reload
		Configured SDF Locations: Add a finash:0128MB.sdf (autosave)	Edit 🏦 Delete 🏦 Maye Up 🤑 Move Down 🔊 Reload
		Configured SDF Locations:	Edit 👚 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload
		Configured SDF Locations:	Edit 🏦 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload
		Configured SDF Locations:	Edit 🏦 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload
		Configured SDF Locations:	Edit 🏦 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload
		Configured SDF Locations:	Edit 🏦 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload
		Configured SDF Locations:	Edit 🏦 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload
		Configured SDF Locations:  Add  Add	Edit 🏦 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload

UIの上部にグローバル設定が表示されます。UIの下半分は、現在設定されている SDF の位置を示します。この場合、フラッシュ メモリから読み込まれた 256MB.sdf ファイルが設定 されています。

3. [File] メニューから [File Management] を選択します。[File Management] ダイアログボック スが表示されます。

Name	Size(bytes)	Time Modified
128MB.sdf	504630	08/25/05 01:37:02
256MB.sdf	725688	01/28/06 10:40:00
backup.cfg	5,564	10/07/05 10:10:32
c180x-advipservicesk9-mz.124-6.T	17,795,940	03/11/06 14:08:26
common.tar	1,007,616	10/24/05 00:32:16
home.shtml	1,038	10/24/05 00:32:16
home.tar	113152	10/24/05 00:32:16
sdm.tar	4,049,920	10/24/05 00:32:18
sdmconfig-18x.cfg	1,820	03/04/06 22:15:56
 sdmips.sdf	527028	03/13/06 03:14:42
securedesktop-ios-3.1.1.27-k9.pkg	1,684,577	03/04/06 22:17:02
sigcategories.xml	321559	11/11/05 10:49:46
ssiclient-win-1.0.2.127.pkg	319662	03/04/06 22:17:18
<u>a</u> aaa	128MB.sdf 256MB.sdf backup.cfg c180x-advipservicesk9-mz.124-6.T common.tar home.shtml home.tar sdm.tar sdmconfig-18xx.cfg sdmips.sdf securedesktop-ios-3.1.1.27-k9.pkg sigcategories.xml sslclient-win-1.0.2.127.pkg	128MB.sdf         504630           256MB.sdf         725688           backup.cfg         5,564           c180x-advipservicesk9-mz.124-6.T         17,795,940           common.tar         1,007,616           home.shtml         1,038           home.tar         113152           sdm.tar         4,049,920           sdmconfig-18xx.cfg         1,820           sdmips.sdf         527028           securedesktop-ios-3.1.1.27-k9.pkg         1,684,577           sigcategories.xml         321559           ssiclient-win-1.0.2.127.pkg         319662

4. [Load file from PC] をクリックします。[Save File] ダイアログボックスが表示されます。

Save File			2 🔀
Look jn: 🔯	SDF	• • 🗈 🖒	* 🗊 •
128MB.sdf			
256MB.sdf			
attack-drop	.sor		
F1	Correction of the		
File pame:	256MB.sdf		Upen
Files of type:	All Files (".")	•	Cancel

す

5. 更新が必要な SDF を選び、[Open] をクリックします。SDM 警告メッセージが表示されま

~		
	This directory already contains	a file named 256MB.sdf. Do you want to
_	overwrite?	

6. 既存のファイルを置き換えるには、[Yes] をクリックします。ダイアログ ボックスが表示され、アップロードの進捗状況が示されます。



7. アップロード プロセスが完了したら、SDF ロケーション ツールバーの上にある [Reload Signatures] をクリックします。この操作により、Cisco IOS IPS がリロードされます。

			ार्थ E
Global Sattings	Item Name	Item Value	
Olopai Settings	Desian	Enabled	_
SDEE Messages	SPEE	Enabled	
Signatures	* SDEE Alerts	200	
	SDEE Messages	200	
	SDEE Subscription	1	
	Engine Options		
	Fail Closed	Disabled	
	Use Built-in Signatures (as backup)	Enabled	
	Deny Action on IPS interface	Disabled	
	Shun Event		
	Shun Event Timeout Configured SDF Locations: & Add @ Ed	30 t 🏦 Delete 🏦 Move Up 🌷 Move Down 🔊 R	eload Signatu
	Shun Event Timeout Configured SDF Locations: Or Add C Ed flash://sdmips.sdf flash://128MB.sdf (autosave)	30 t 🏦 Delete 🎓 Move Up 🐥 Move Down 🔊 R	eloəd Signatu
	Shun Event Timeout Configured SDF Locations:	30 t 합 Delete 🎓 Move Up 🐥 Move Down 🔊 R	eloəd Signatu
	Shun Event Timeout Configured SDF Locations:  Add  E Ed flash://sdmips.sdf flash://128MB.sdf (autosave)	30 t 👕 Delete 🎓 Move Up 🐥 Move Down 🔊 R	eload Signatu
	Shun Event Timeout Configured SDF Locations: Add C Ed flash://isdmips.sof flash://i28MB.sdf (autosave)	30 t 👚 Delete 🎓 Move Up 🐥 Move Down 🔊 R	eload Signatu
	Shun Event Timeout Configured SDF Locations: Add C Ed flash://isdmips.sdf flash://i28MB.sdf (autosave)	30 t 🏦 Delete 🏦 Move Up 🖊 Move Down 🔊 R	eload Signatu
	Shun Event Timeout Configured SDF Locations: Add C Ed flash://isdmips.sdf flash://i28MB.sdf (autosave)	30 t 👚 Delete 🏦 Move Up 🖊 Move Down 🔊 R	eload Signatu
	Shun Event Timeout Configured SDF Locations: Add C Ed flash://isdmips.sdf flash://i28MB.sdf (autosave)	30 t 👚 Delete 🏦 Move Up 🖊 Move Down 🔊 R	eload Signatu

注:IOS-Sxxx.zipパッケージには、Cisco IOS IPSがサポートするすべてのシグニチャが含ま れています。このシグネチャ パッケージのアップグレードは、使用可能になり次第、 Cisco.com で公開されます。このパッケージに含まれている署名を更新するには、ステップ 2を参<u>照してください</u>。



- <u>Cisco Intrusion Prevention System</u>
- <u>セキュリティ製品に関する Field Notices (CiscoSecure Intrusion Detection を含む)</u>
- ・<u>テクニカルサポート Cisco Systems</u>