Cisco Networking Academy
Mind Wide Open

Chapitre 5 :

Mise en œuvre de prévention des intrusions

CCNA Security v2.0

Samir DIABI

Sommaire

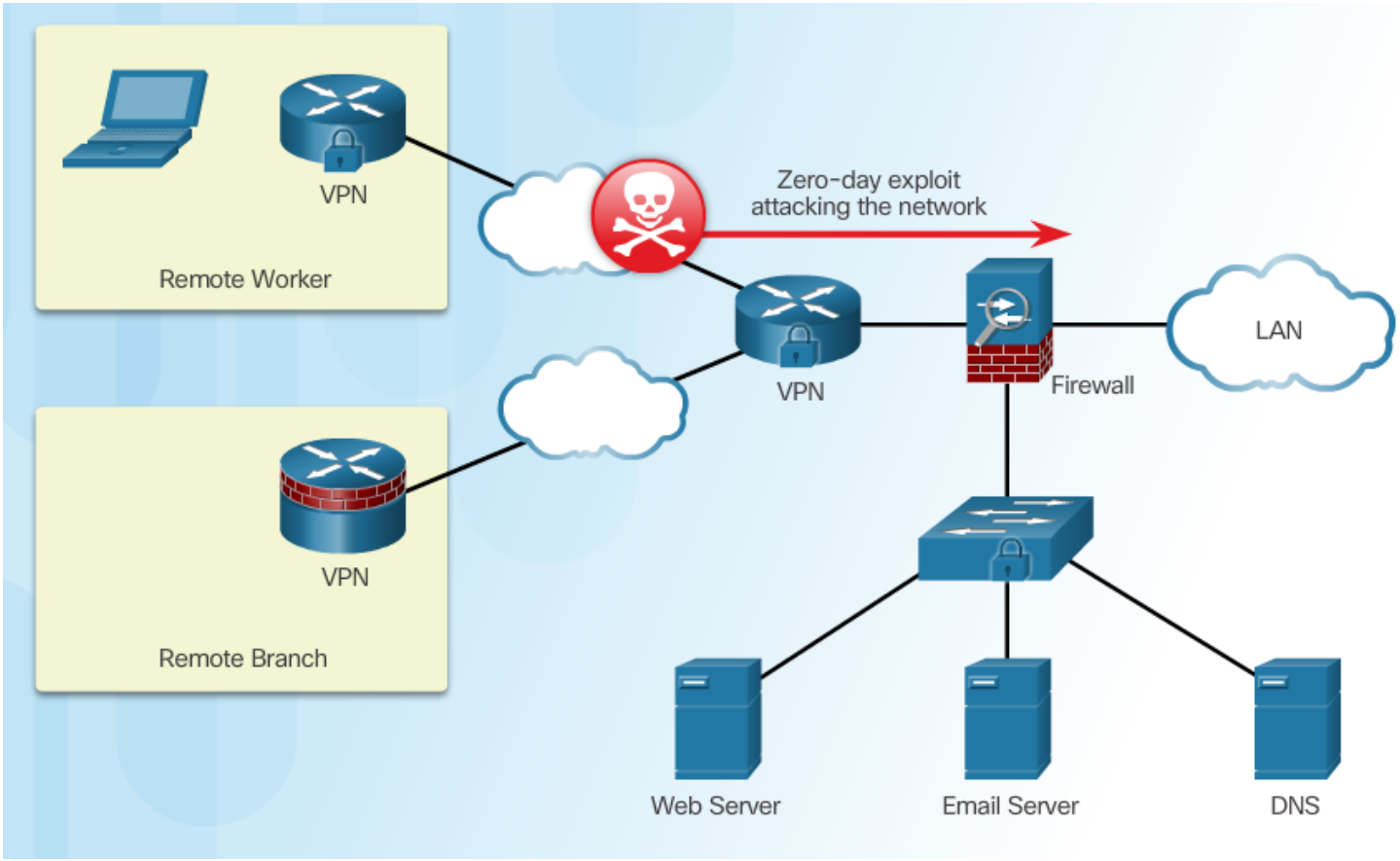
Section 5.1: Technologies IPS

À la fin de cette section, vous devriez être en mesure de :

- expliquer les attaques zero-day.
- Comprendre comment surveiller,
- détecter et arrêter les attaques.
- Décrire les avantages et les inconvénients de l'IDS et IPS.

Sujet 5.1.1:
Les caractéristiques de IDS et IPS

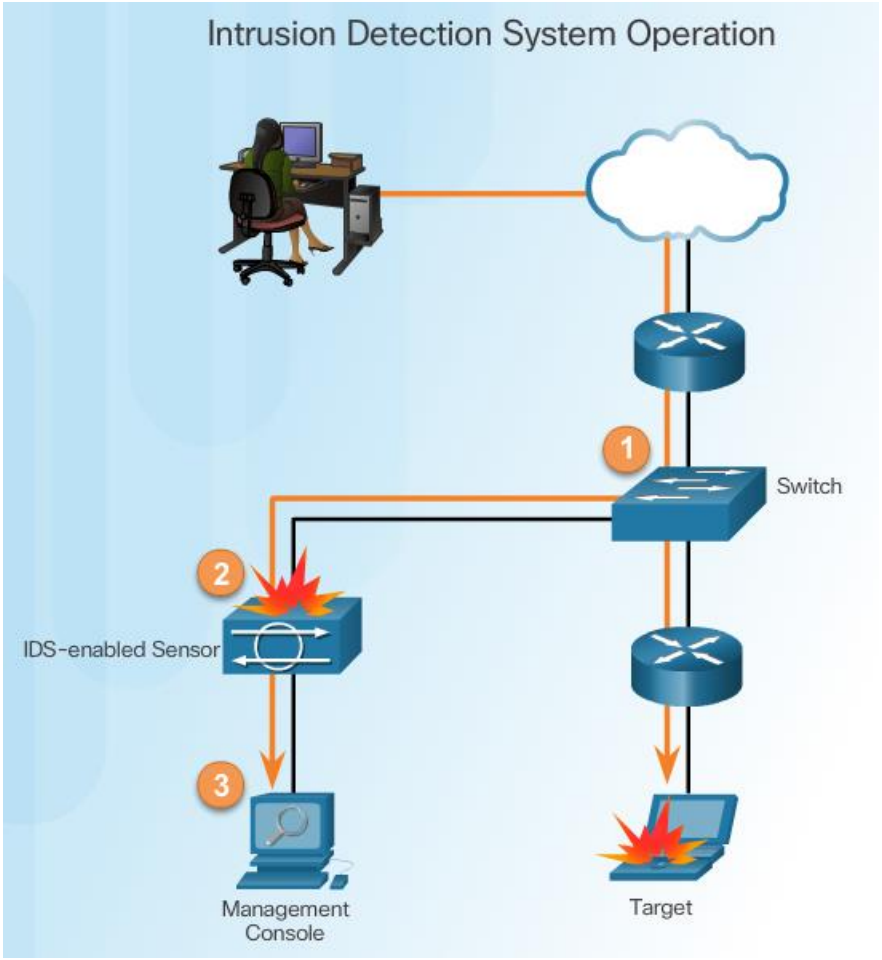
Les attaques Zero-Day



Surveiller les attaques

Avantages d'un IDS:

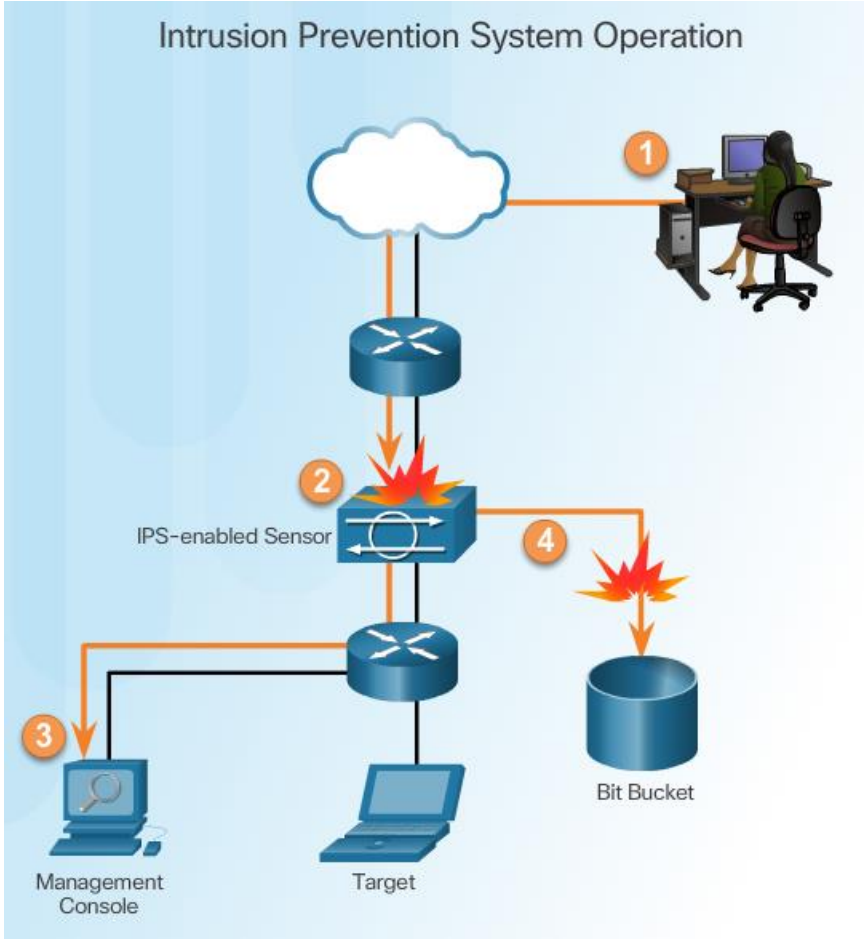
- Fonctionne passivement
- Nécessite que le trafic soit reflété afin de l'atteindre
- Le trafic réseau ne passe pas par l'IDS à moins qu'il ne soit reflété



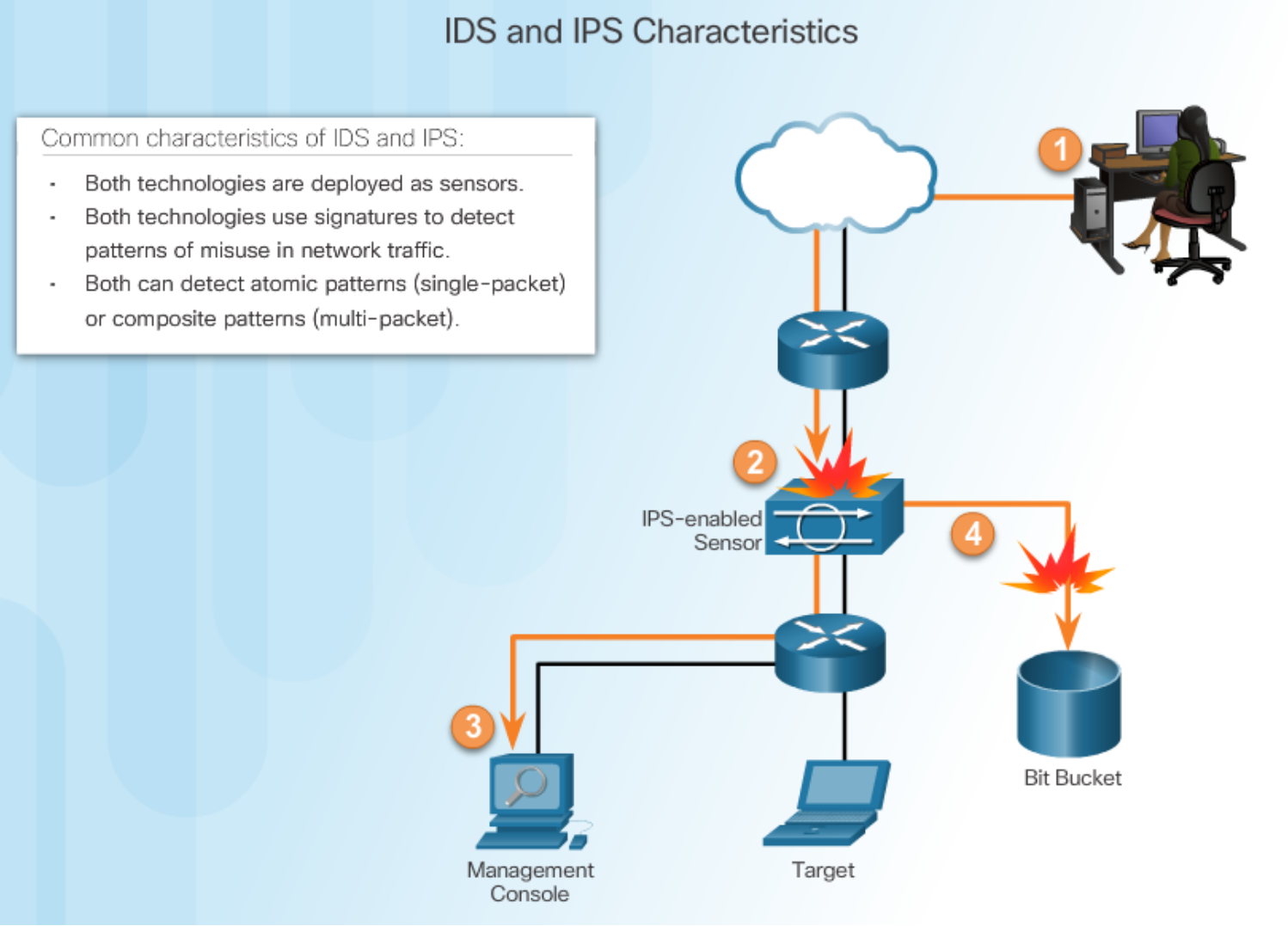
Détecter et arrêter les attaques

IPS:

- Mise en œuvre en mode inline
- Surveille le trafic de couche 3 et de couche 4
- Peut arrêter les attaques par paquets individuels d'atteindre la cible
- Répond immédiatement, ne permettant pas de transmettre un trafic malveillant



Les similitudes entre IDS et IPS



Avantages et inconvénients de l'IDS et de l'IPS

Avantages IDS:

- Pas d'impact sur le réseau
- Pas d'impact sur le réseau en cas de panne du capteur
- Aucun impact sur le réseau s'il existe une surcharge de capteur

Avantages IPS:

- Arrête les paquets de déclenchement
- Peut utiliser les techniques de normalisation des flux

Inconvénients IDS:

- L'action de réponse ne peut pas arrêter le déclencheur
- Syntonisation correcte requise pour les actions de réponse
- Plus vulnérables aux techniques d'évasion de sécurité du réseau

Inconvénients IPS:

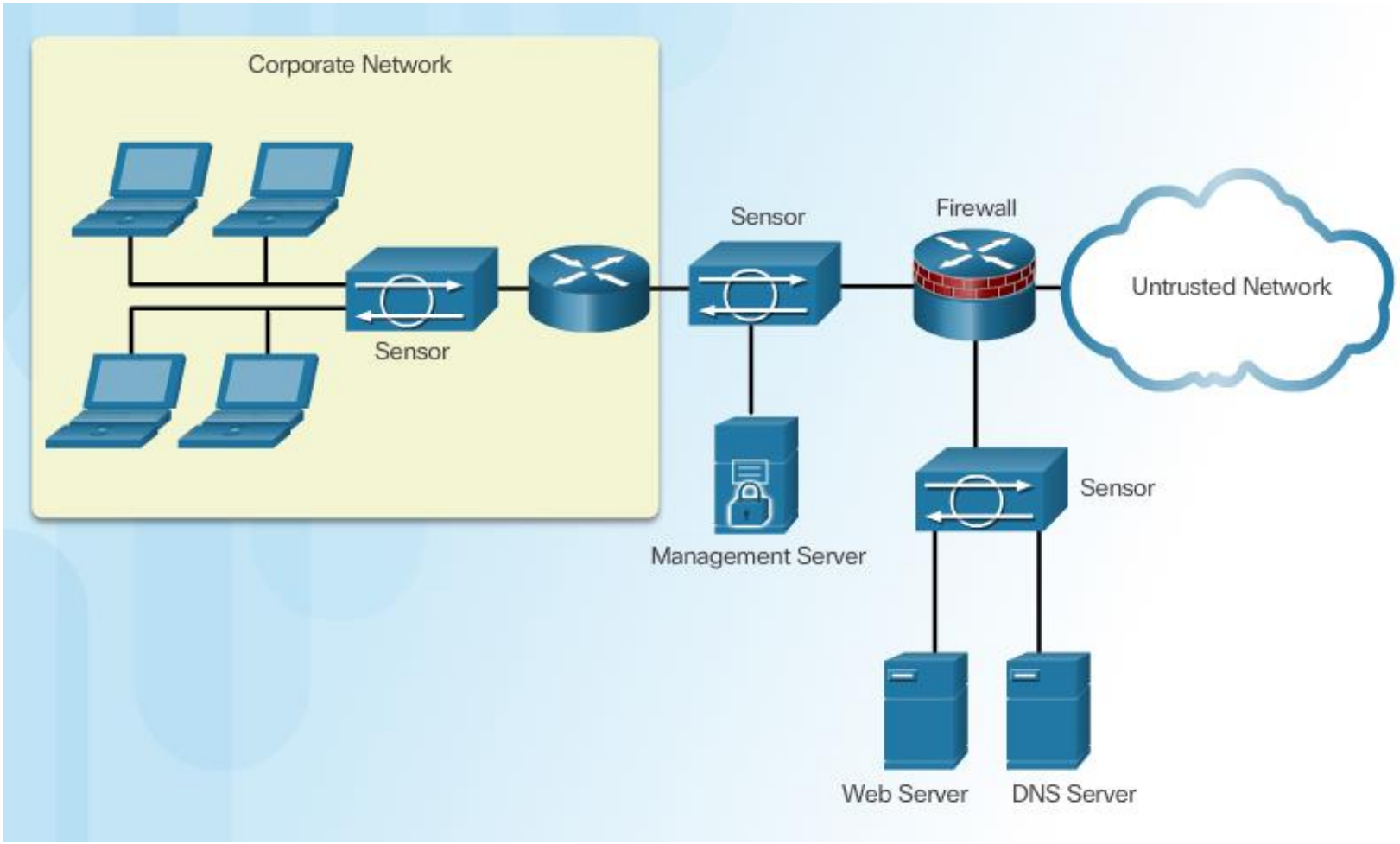
- Les problèmes de capteurs peuvent affecter le trafic réseau
- La surcharge des capteurs affecte le réseau
- Quelques répercussions sur le réseau

Sujet 5.1.2:
Implémentations IPS basées sur le réseau

IPS basée sur l'hôte et sur le réseau

	Advantages	Disadvantages
Host-Based IPS	• Provides protection specific to a host operating system • Provides operating system and application level protection • Protects the host after the message is decrypted	• Operating system dependent • Must be installed on all hosts
Network-Based IPS	• Cost effective • Operating system independent	• Cannot examine encrypted traffic • Must stop malicious traffic prior to arriving at host

Capteurs IPS basés sur le réseau



Solutions IPS modulaires et à base d'appliance de Cisco

Cisco IPS AIM et le module réseau améliorés (IPS NME

Cisco ASA AIP-SSM

Capteurs Cisco IPS 4300 Series

Cisco Catalyst 6500 Series IDSM-2

Choisissez une solution IPS

Facteurs affectant la sélection et le déploiement du capteur IPS:

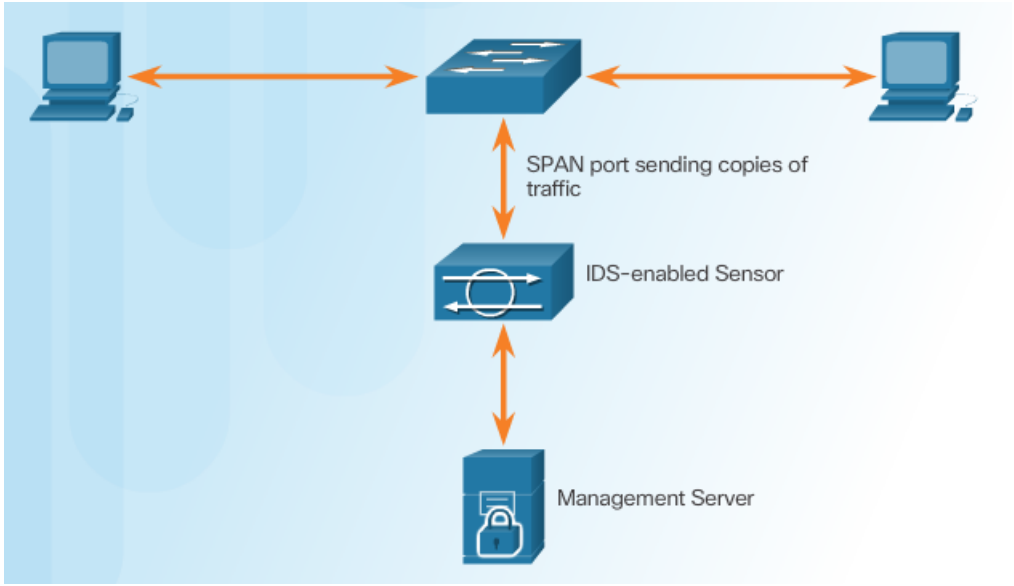
- Quantité de trafic réseau
- Topologie de réseau
- Budget de sécurité
- Personnel de sécurité disponible pour gérer IPS

IPS Avantages et inconvénients

	Advantages	Disadvantages
Network IPS	• Is cost-effective • Not visible on the network • Operating system independent • Lower level network events seen	• Cannot examine encrypted traffic • Cannot determine whether an attack was successful

Modes de déploiement

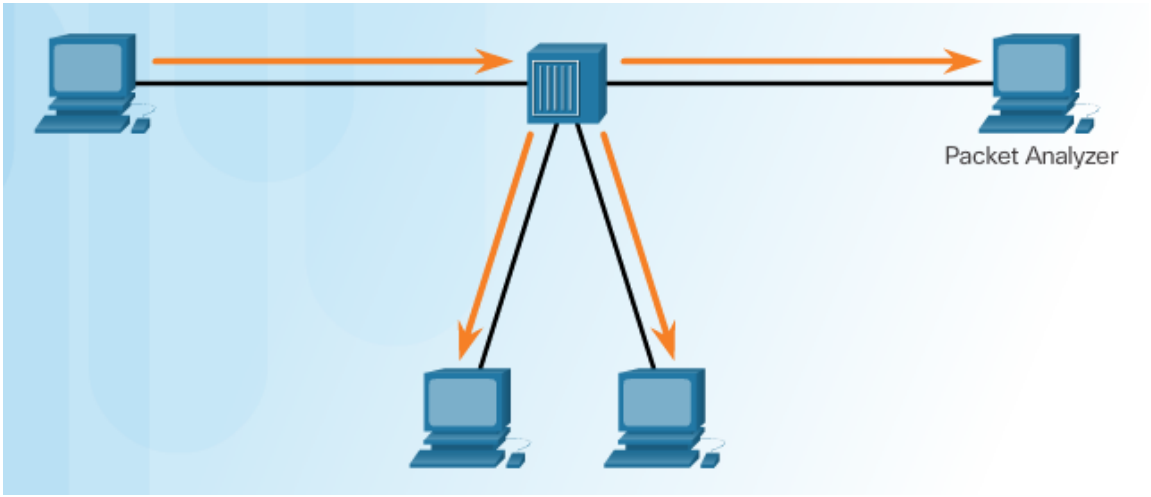
Mode promiscuous



Mode en ligne

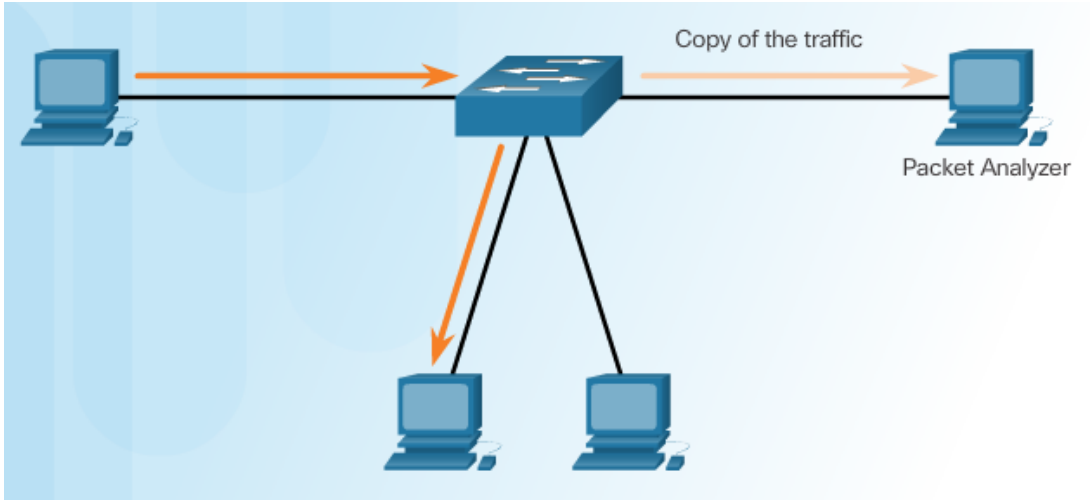
Sujet 5.1.3:
Analyseur de port commuté Cisco

Port Mirroring

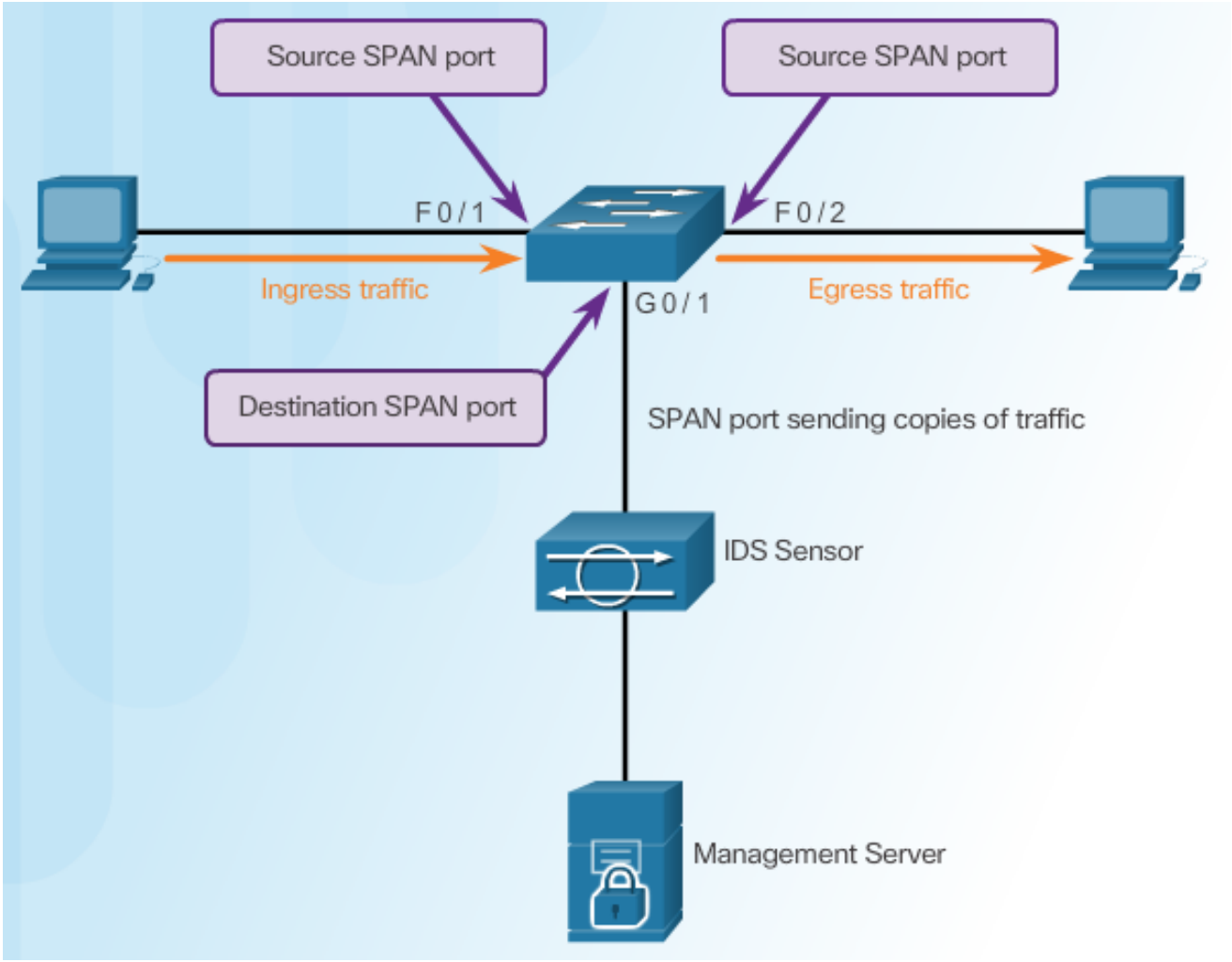


Traffic Sniffing en utilisant un concentrateur

Traffic Sniffing en utilisant un commutateur



Cisco SPAN



Configuration de Cisco SPAN à l'aide de la détection d'intrusion

Commandes Cisco SPAN :

- La commande Monitor session – utilisé pour associer un port source et un port de destination à une session SPAN.

Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```

- La commande Show monitor –Utilisé pour vérifier la session SPAN.

Section 5.2: Signatures IPS

Une fois la section terminée, vous devriez pouvoir:

- Comprendre les caractéristiques de signature IPS
- Expliquer les alarmes de signature IPS
- Gérer et surveiller IPS
- Comprendre la corrélation globale des périphériques Cisco IPS

Sujet 5.2.1:
IPS Signature Caractéristiques

Attributs de signature

Une signature est un ensemble de règles qu'un IDS et un IPS utilisent pour détecter une activité d'intrusion typique.

- Les signatures ont trois attributs distincts:
- Type
- Déclenchement (alarme)
- action

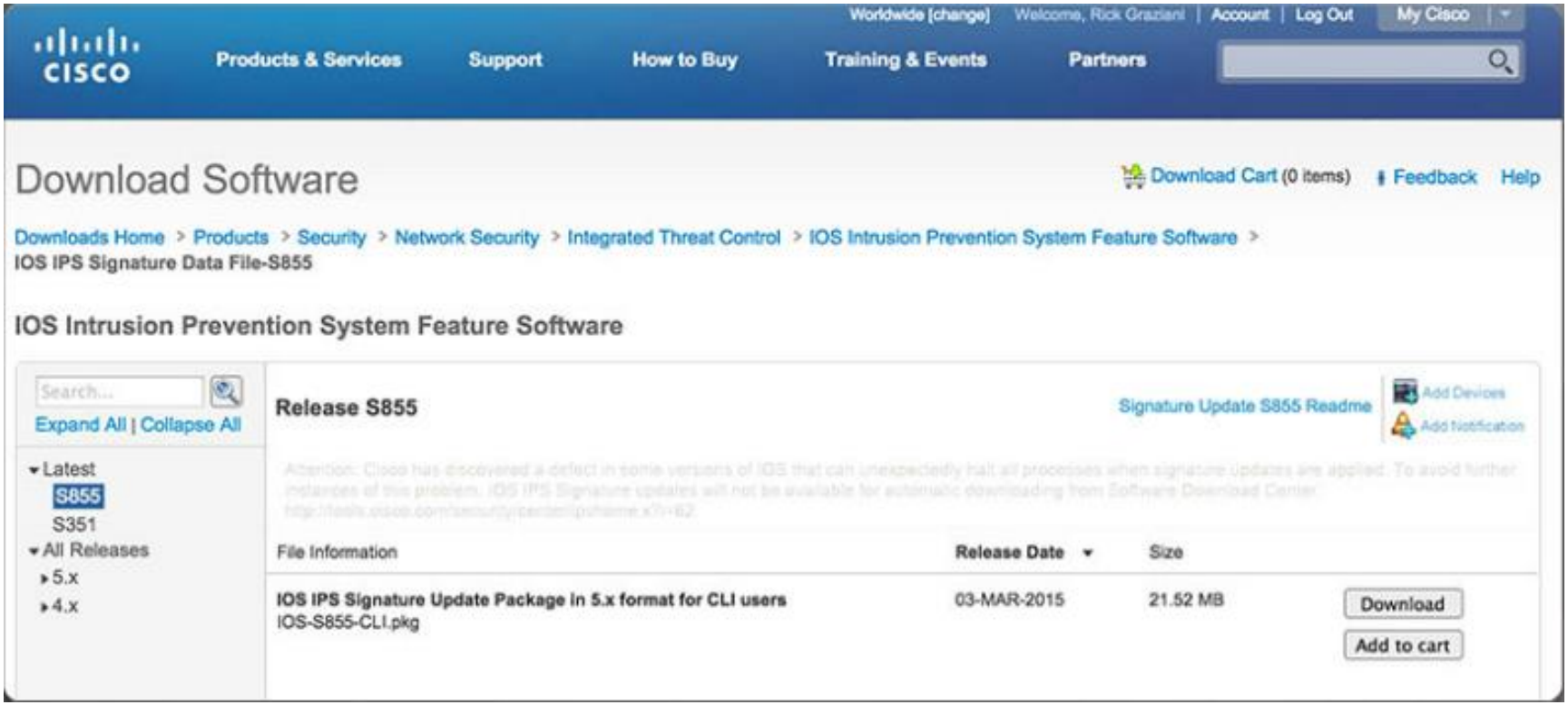
Types de Signature

Les signatures sont classées comme étant:

- Atomic - ce type de signature le plus simple consiste en un seul paquet, une activité ou un événement qui est examiné pour déterminer s'il correspond à une signature configurée. Si oui, une alarme est déclenchée et une action de signature est effectuée.
- Composite - ce type de signature identifie une séquence d'opérations réparties entre plusieurs hôtes sur une période arbitraire.

Fichier Signature

- À mesure que de nouvelles menaces sont identifiées, de nouvelles signatures doivent être créées et téléchargées sur un IPS.
- Un fichier de signature contient un paquet de signatures de réseau.

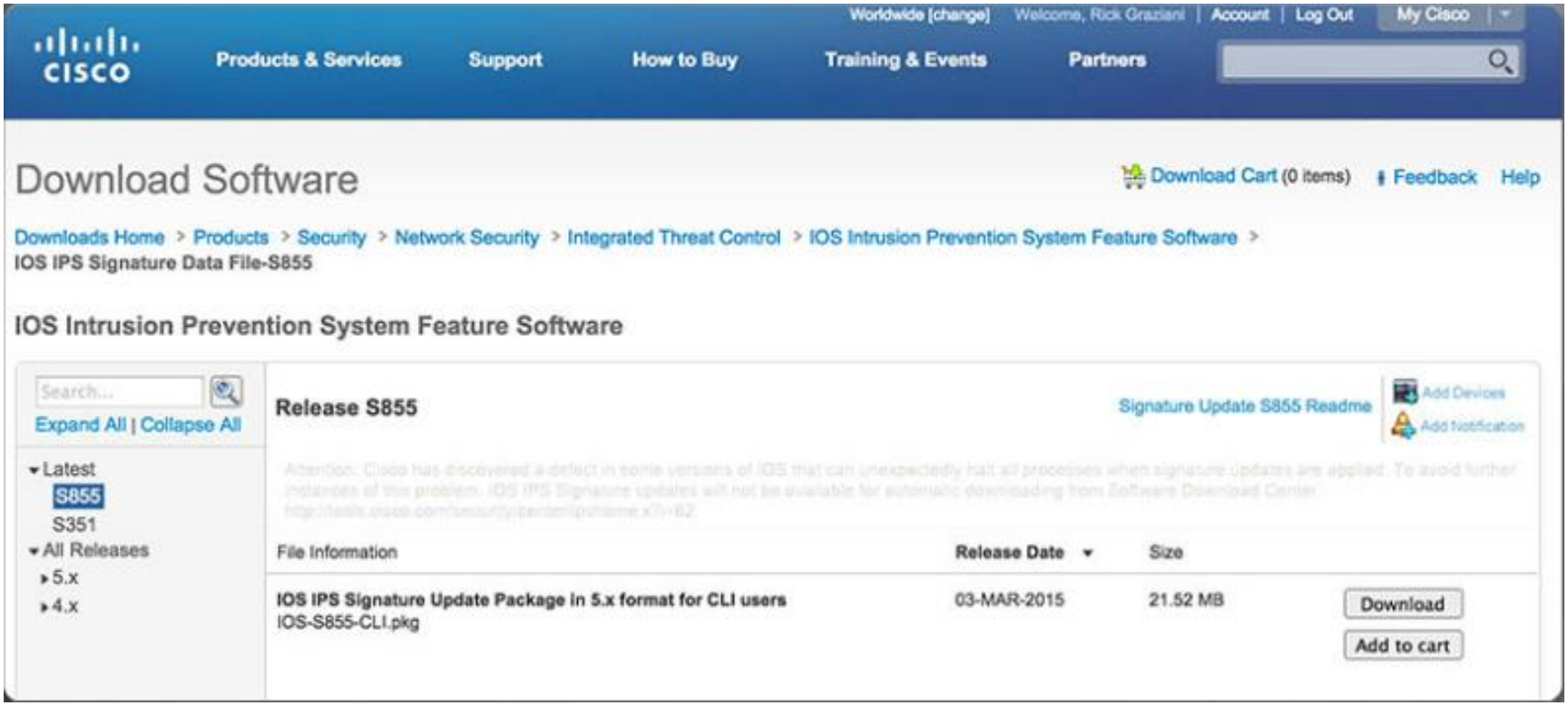


Signature Micro-Engines

Cisco IOS définit cinq micro-moteurs:

- Atomic - Signatures qui examinent des paquets simples.
- Service - Signatures qui examinent les nombreux services attaqués.
- Chaîne - Signatures qui utilisent des modèles basés sur l'expression régulière pour détecter les intrusions.
- Multi-string - Prise en charge de l'appariement flexible des modèles et des signatures Trend Labs.
- Autre - Moteur interne qui gère les différentes signatures.

Télécharger le fichier Signature



Sujet 5.2.2:
IPS Signature Alarms

Signature Alarm

Detection Type	Advantages
Pattern-based Detection	• Easy configuration • Fewer false positives • Good signature design
Anomaly-based Detection	• Simple and reliable • Customized policies
Policy-based Detection	• Easy configuration • Can detect unknown attacks
Honey pot-based Detection	• Window to view attacks • Distract and confuse attackers • Slow down and avert attacks • Collect information about attack

Detection Type	Disadvantages
Pattern-based Detection	• No detection of unknown signatures • Initially a lot of false positives • Signatures must be created, updated, and tuned
Anomaly-based Detection	• Generic output • Policy must be created
Policy-based Detection	• Difficult to profile typical activity in large networks • Traffic profile must be constant
Honey pot-based Detection	• Dedicated honey pot server • Hot pot server must not be trusted

Détection par motif

	Signature Type	
	Atomic Signature	Composite Signature
Pattern-based Detection	No state required to examine pattern to determine if signature action should be applied.	Must contain state or examine multiple items to determine if signature action should be applied.
Example	Detecting an Address Resolution Protocol (ARP) request that has a source Ethernet address of FF:FF:FF:FF:FF:FF.	Searching for the string "confidential" across multiple packets in a TCP session.

Détection basée sur l'anomalie

	Signature Type	
	Atomic Signature	Composite Signature
Anomaly-based Detection	No state required to identify activity that deviates from normal profile.	State required to identify activity that deviates from normal profile.
Example	Detecting traffic that is going to a destination port that is not in the normal profile.	Verifying protocol compliance for HTTP traffic.

Détection basée sur les politiques et le miel à base de pot

	Signature Type	
	Atomic Signature	Composite Signature
Policy-based Detection	No state required to identify undesirable behavior.	Previous activity (state) required to identify undesirable behavior.
Example	Detecting abnormally large fragmented packets by examining only the last fragment.	A Sun Unix host sending RPC requests to remote hosts without initially consulting the Sun PortMapper program.

Avantages de la solution Cisco IOS IPS

Avantages:

- Il utilise une infrastructure de routage sous-jacente pour fournir une couche supplémentaire de sécurité.
- Il est intégré et est pris en charge sur une large gamme de plates-formes de routage.
- Il offre une protection contre les menaces à tous les points d'entrée du réseau lorsqu'il est utilisé en combinaison avec les solutions Cisco IDS, Cisco IOS Firewall, VPN et NAC
- La taille de la base de données de signature utilisée par les périphériques peut être adaptée à la quantité de mémoire disponible dans le routeur.

Mécanismes de déclenchement d'alarme

Comprendre les types d'alarme :

Alarm Type	Network Activity	IPS Activity	Outcome
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting

Sujet 5.2.3:
IPS Signature Actions

Signature Actions

Résumé des catégories d'action :

Category	Specific Alert
Generating an alert	Produce alert
	Produce verbose alert
Logging the activity	Log attacker packets
	Log pair packets
	Log victim packets
Dropping or preventing the activity	Deny attacker inline
	Deny connection inline
	Deny packet inline
Resetting a TCP connection	Reset TCP connection
Blocking future activity	Request block connection
	Request block host
	Request SNMP trap
Allow the activity	This action will permit the traffic to appear as normal based on configured exceptions. An example would be allowing alerts from an approved IT scanning host.

Gérer les alertes générées

Générer une alerte :

Specific Alert	Description
Produce alert	This action writes the event to the Event Store as an alert.
Produce verbose alert	This action includes an encoded dump of the offending packet in the alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected. *

Activités de journal pour une analyse ultérieure

Enregistrement de l'activité:

Specific Alert	Description
Log attacker packets	This action starts IP logging on packets that contain the attacker address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log pair packets	This action starts IP logging on packets that contain the attacker and victim address pair. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log victim packets	This action starts IP logging on packets that contain the victim address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

Refuser l'activité

Suppression ou prévention de l'activité :

Specific Alert	Description
Deny attacker inline	• This action terminates the current packet and future packets from this attacker address for a specified period of time. • The sensor maintains a list of the attackers currently being denied by the system. • Entries may be removed from the list manually or automatically based on a timer. • The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset and attacker A remains on the denied attacker list until the timer expires. • If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
Deny connection inline	This action terminates the current packet and future packets on this TCP flow.
Deny packet inline	This action terminates the packet.

Réinitialiser, bloquer et autoriser le trafic

Réinitialisation de la connexion et blocage de l'activité:

Specific Alert	Description
Reset TCP connection	This action sends TCP resets to hijack and terminate the TCP flow.
Request block connection	This action sends a request to a blocking device to block this connection.
Request block host	This action sends a request to a blocking device to block this attacker host.
Request SNMP trap	This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

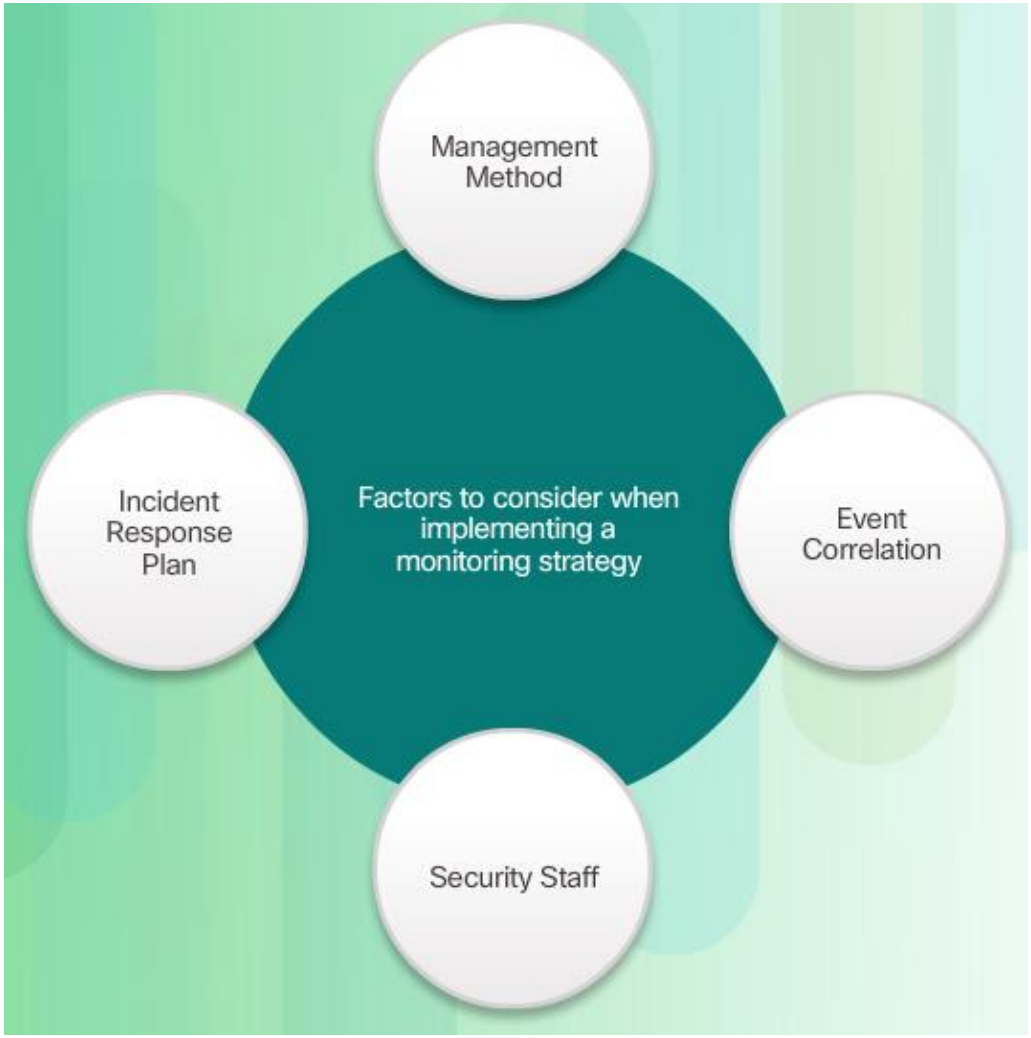
Sujet 5.2.4:
Gérer et surveiller IPS

Surveiller l'activité

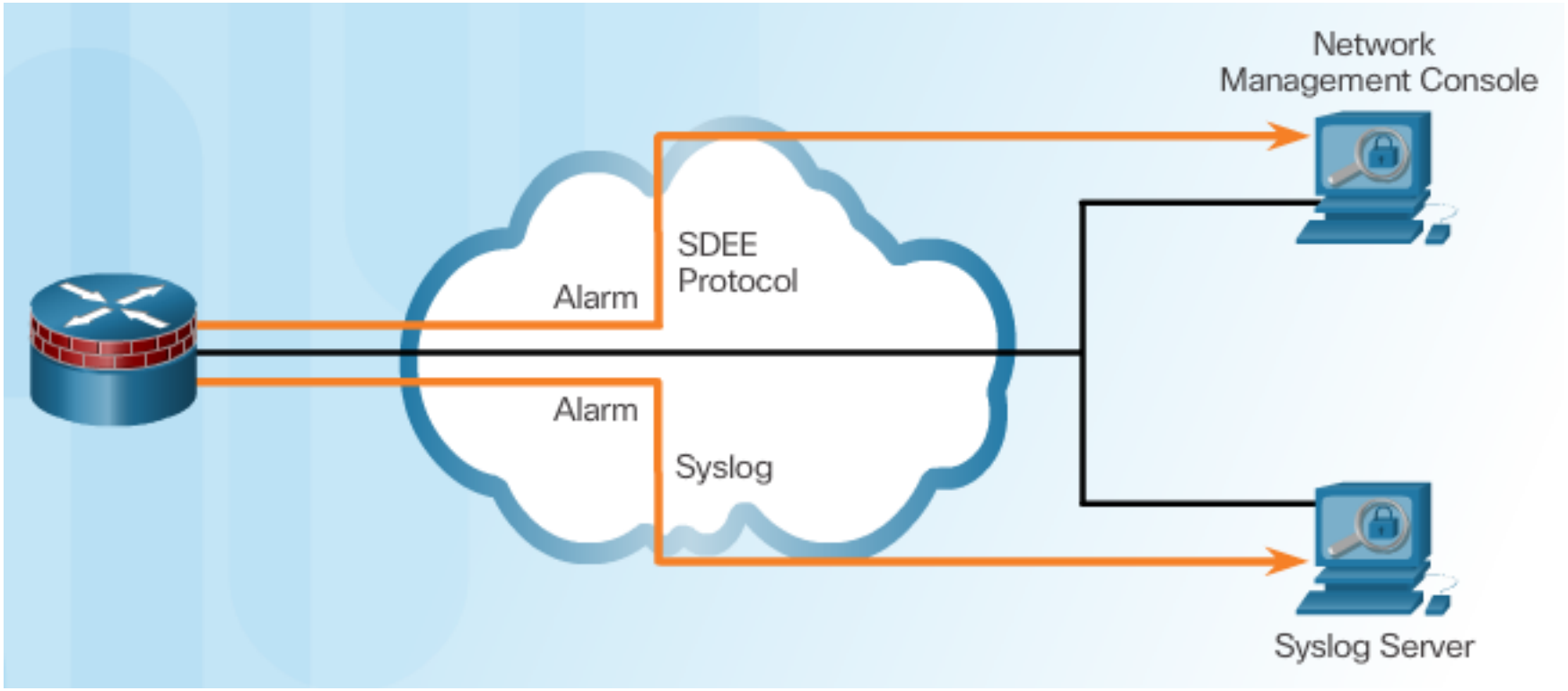
Considérations relatives à la planification et à la surveillance IPS:

- Méthode de gestion
- Corrélation d'événement
- Personnel de sécurité
- Plan d'intervention d'incident

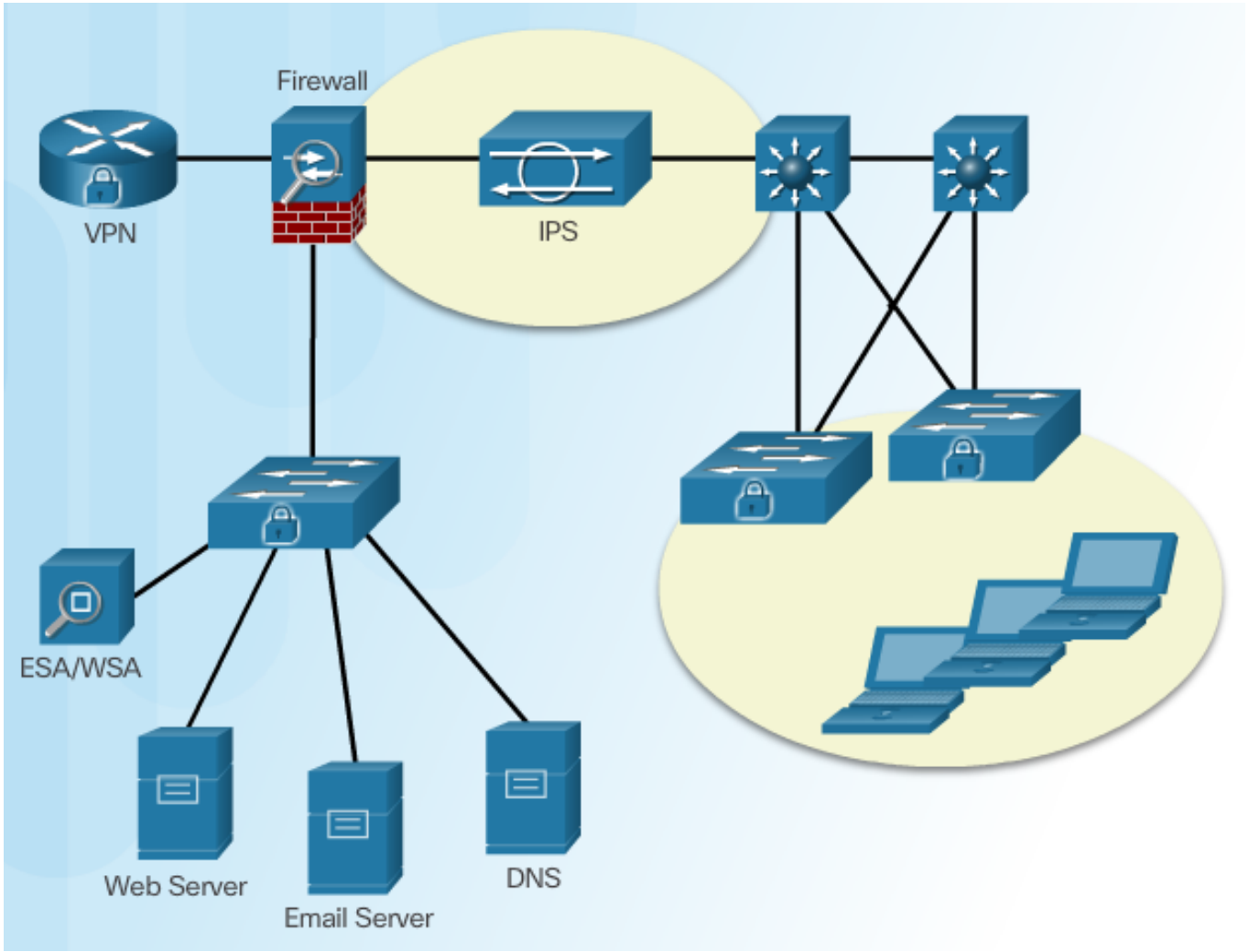
Considérations de surveillance



Échange d'événements de périphériques sécurisés



Pratiques exemplaires de configuration IPS



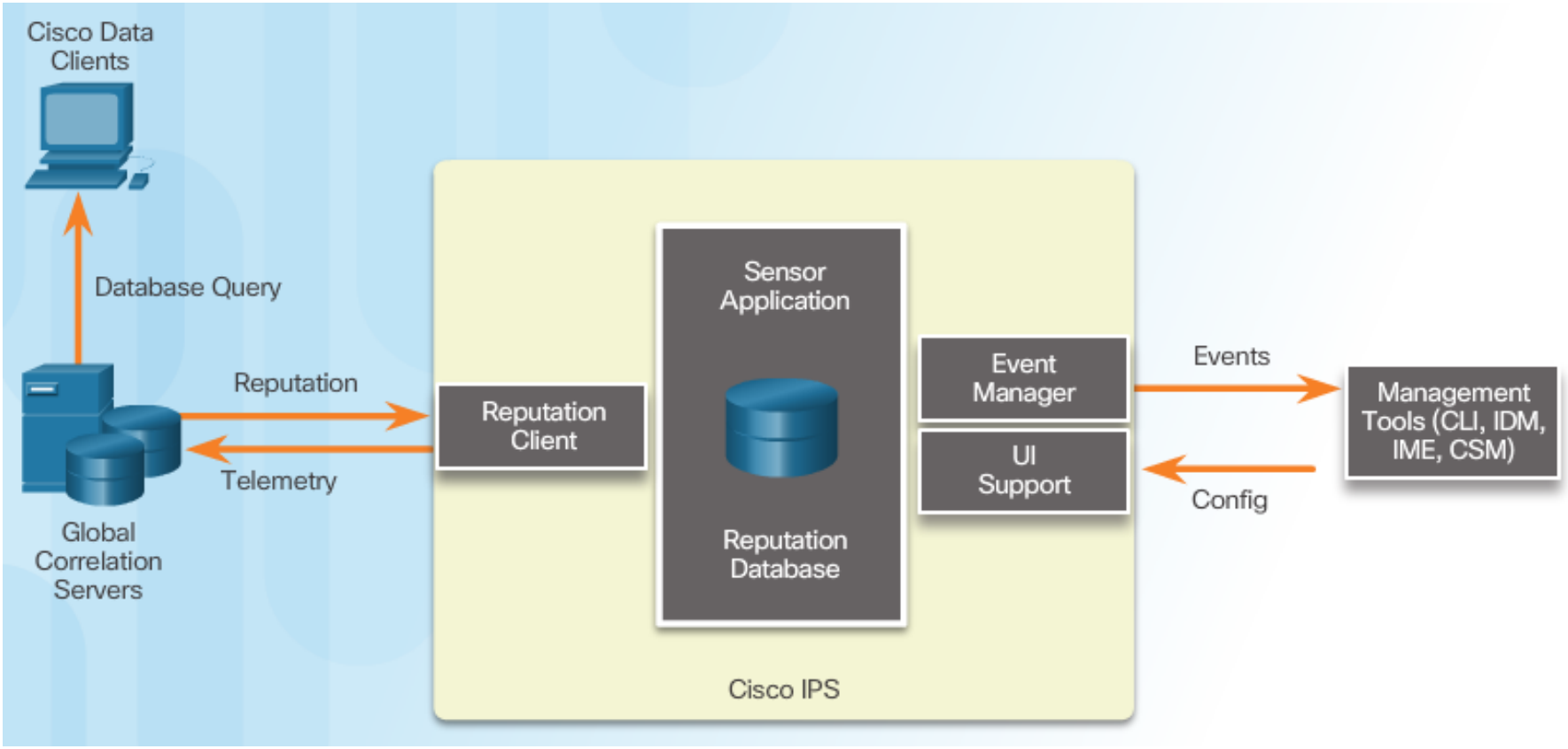
Sujet 5.2.5:
Corrélation mondiale IPS

Corrélation globale de Cisco

Objectifs de la corrélation globale:

- Faire face de manière intelligente aux alertes pour améliorer l'efficacité
- Améliorer la protection contre les sites malveillants connus
- Partage des données de télémétrie avec le réseau SensorBase pour améliorer la visibilité des alertes et des capteurs à l'échelle mondiale
- Simplification des paramètres de configuration
- Gestion automatique des téléchargements et téléchargements d'informations de sécurité

Cisco Réseau SensorBase



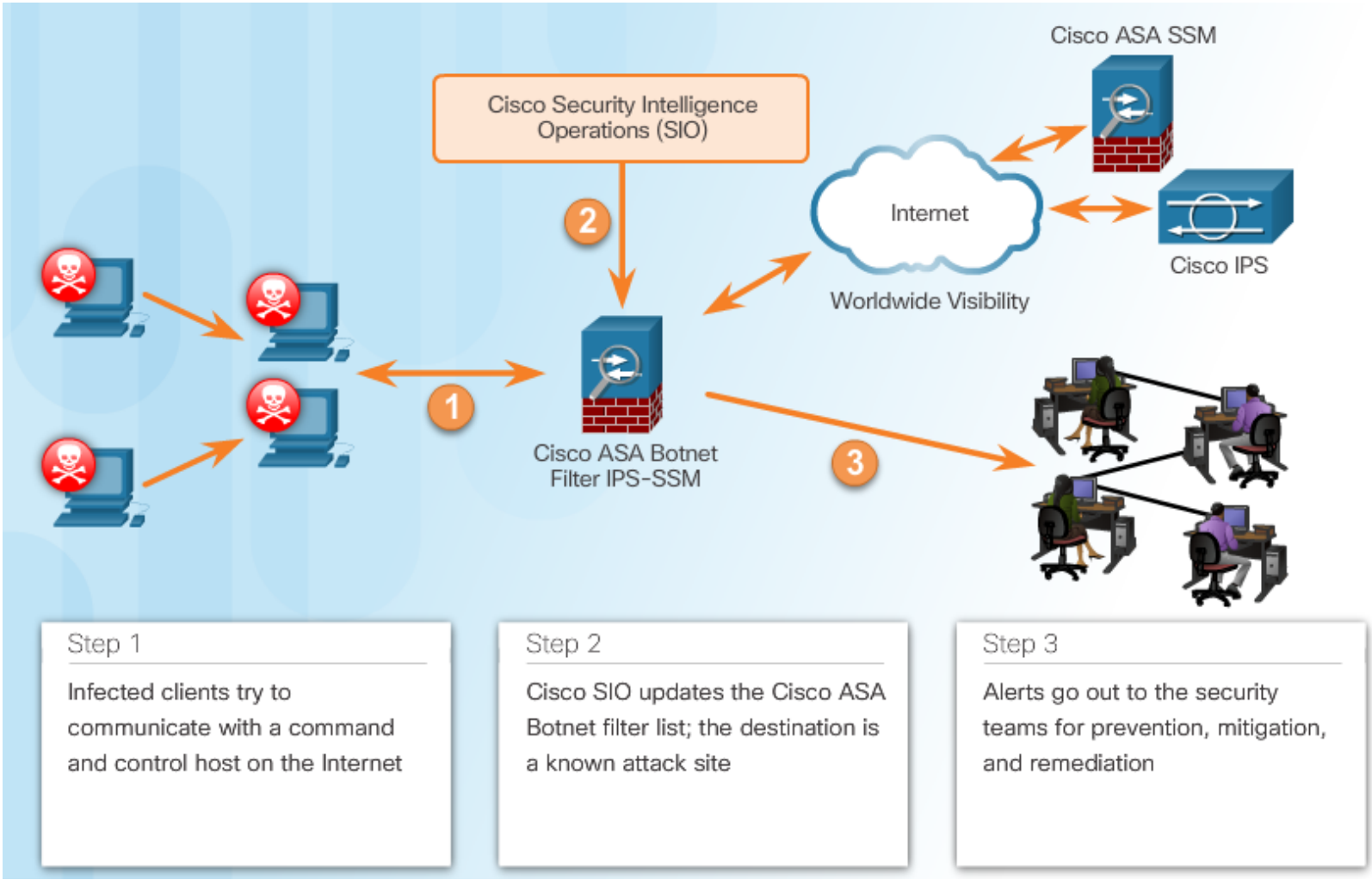
Fonctionnement de l'Intelligence de sécurité Cisco

La participation au réseau regroupe les données suivantes:

- ID de signature
- Adresse IP de l'attaquant
- Port attaquant
- Taille maximale du segment
- Adresse IP de la victime
- Port de victime
- Version de signature
- Chaîne d'options TCP
- Score de réputation
- Évaluation des risques

Réputations, listes noires et filtres de trafic

Réputations, listes noires et filtres de trafic



Section 5.3: Mettre en œuvre IPS

À la fin de cette section, vous devriez pouvoir:

- Comprendre comment configurer Cisco IOS IPS avec CLI
- Expliquer comment vérifier et surveiller IPS

Sujet 5.3.1:
Configurer Cisco IOS IPS avec CLI

Mettre en œuvre IOS IPS

Étape 1. Téléchargez les fichiers IOS IPS.

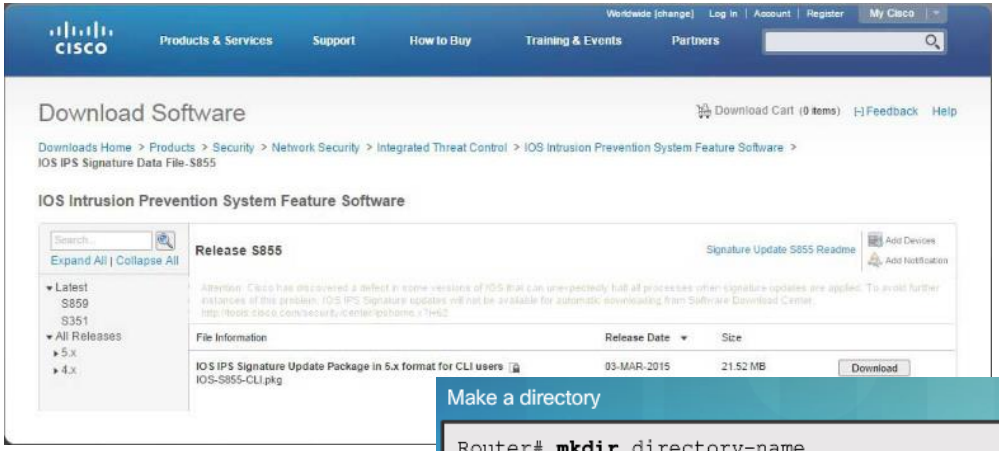
Étape 2. Créez un répertoire de configuration IOS IPS dans Flash.

Étape 3. Configurez une clé cryptographique IOS IPS.

Étape 4. Activer IOS IPS.

Étape 5. Chargez le paquet de signature IOS IPS sur le routeur.

Téléchargez les fichiers IOS IPS



Make a directory

```
Router# mkdir directory-name
```

Rename a directory

```
Router# rename current-name new-name
```

Display a directory

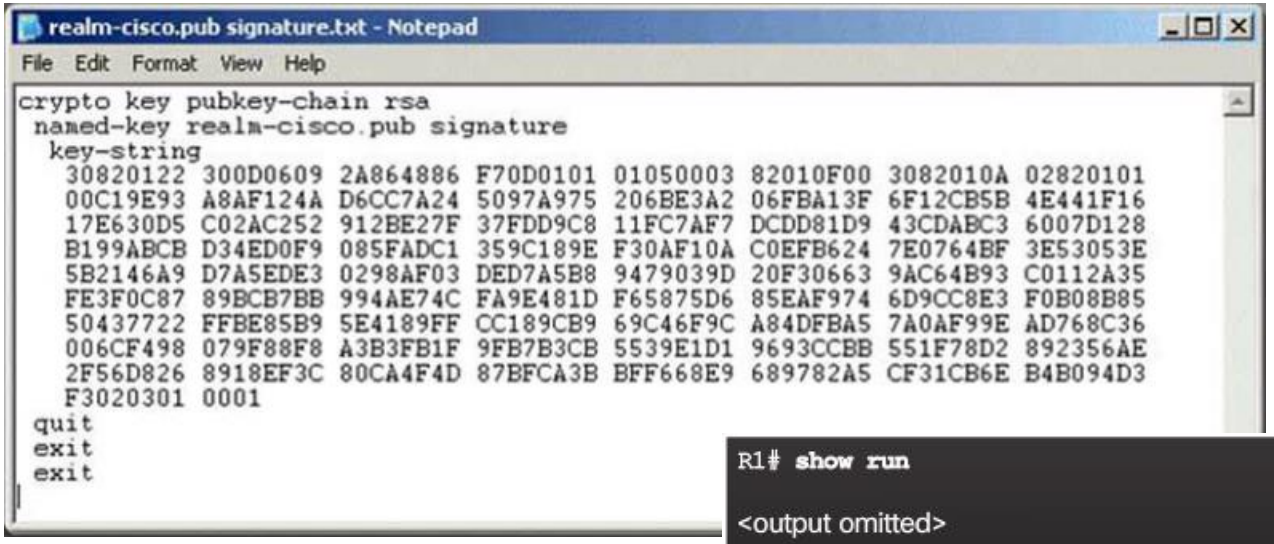
```
Router# dir [/all] [filesystem: ]
```

```
R1# mkdir IPSDIR
Create directory filename [IPSDIR]?
Created dir flash0:/IPSDIR
R1# dir flash:
Directory of flash0:/

   14  -rw-        1381  Feb 18 2015 20:37:14 +00:00  R2backup.cfg
   15  drw-           0  Feb 28 2015 01:14:12 +00:00  IPSDIR

256487424 bytes total (175632384 bytes free)
R1#
```

IPS Crypto Key




```
R1# show run

<output omitted>

crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
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

<output omitted>
```

Activer IOS IPS

Create a rule name

```
Router(config)# ip ips name [rule-name]
```

Configure IPS signature storage location

```
Router(config)# ip ips config location flash:<directory-name>
```

```
R1(config)# ip ips name IOSIPS
R1(config)# ip ips name IOSIPS list ?
  <1-199>  Numbered access list
  WORD     Named access list

R1(config)#
R1(config)# ip ips config location flash:IPS
R1(config)#
```

Specify the method of event notification

```
Router(config)# ip ips notify [ sdee | log ]
```

Parameter	Description
sdee	Sends messages in SDEE format.
log	Sends messages in syslog format.Note: If an option is not specified, alert messages are sent in syslog format.

```
R1(config)# ip http server
R1(config)# ip ips notify ?
  SDEE  Send events to SDEE
  log   Send events as syslog messages

R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
R1(config)#
```

Activer IOS IPS

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips ?
  advanced  Advanced
  basic     Basic
  <cr>

R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# end
Do you want to accept these changes? [confirm]
R1#
*Dec 9 04:29:39.119: Applying Category configuration to
signatures ...
R1#
```

Apply an IPS rule to an interface

```
Router(config)# ip ips ips-name { in | out }
```

Parameter	Description
in	Applies IPS to inbound traffic.
out	Applies IPS to outbound traffic.

```
R1(config)# interface g0/0
R1(config-if)# ip ips IOSIPS in
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ip ips IOSIPS in
R1(config-if)# ip ips IOSIPS out
R1(config-if)# end
```

Chargez le paquet de signature IPS dans la RAM

```
R1# copy tftp://192.168.1.3/IOS-S416-CLI.pkg idconf
Loading IOS-S416-CLI.pkg from 192.168.1.3 (via GigabitEthernet0/1): !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9553609 bytes]

Feb 27 18:17:42.507: %IPS-6-ENGINE_BUILDS_STARTED:  18:17:42 UTC Feb 27 2015
Feb 27 18:17:42.515: %IPS-6-ENGINE_BUILDING: atomic-ip - 342 signatures - 1 of 13 engines
Feb 27 18:17:45.975: %IPS-6-ENGINE_READY: atomic-ip - build time 3460 ms - packets for this
engine will be scanned
Feb 27 18:17:45.975: %IPS-6-ENGINE_BUILDING: normalizer - 10 signatures - 2 of 13 engines
Feb 27 18:17:45.979: %IPS-6-ENGINE_READY: normalizer - build time 4 ms - packets for this
engine will be scanned

<output omitted>


Feb 27 18:17:51.391: %IPS-6-ENGINE_BUILDING: service-dns - 39 signatures - 10 of 13 engines
Feb 27 18:17:51.427: %IPS-6-ENGINE_READY: service-dns - buil
R1#d time 36 ms - packets for this engine will be scanned
Feb 27 18:17:51.427: %IPS-6-ENGINE_BUILDING: string-udp - 78 signatures - 11 of 13 engines
Feb 27 18:17:51.483: %IPS-6-ENGINE_READY: string-udp - build time 56 ms - packets for this
engine will be scanned
Feb 27 18:17:51.483: %IPS-6-ENGINE_BUILDING: multi-string - 17 signatures - 12 of 13
engines
Feb 27 18:17:51.519: %IPS-6-ENGINE_READY: multi-string - build time 36 ms - packets for
this engine will be scanned
Feb 27 18:17:51.519: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 13 of 13 engines
R1#
```

Chargez le paquet de signature IPS dans la RAM

Copy the downloaded signature package from the FTP server to the router:

```
Router# copy ftp://ftp_user: password @ Server_IP_address/signature_package idconf
```

The `idconf` parameter instructs the router that an IDConf configuration file is being copied.

```
R1# show ip ips signature count

Cisco SDF release version S416.0
Trend SDF release version V0.0

Signature Micro-Engine: atomic-ip: Total Signatures 342
      atomic-ip enabled signatures: 90
      atomic-ip retired signatures: 321
      atomic-ip compiled signatures: 21
      atomic-ip obsoleted signatures: 3

<output omitted>

Total Signatures: 3027
   Total Enabled Signatures: 1048
   Total Retired Signatures: 2726
   Total Compiled Signatures: 301
   Total Obsoleted Signatures: 9

R1#
```

Démonstration et retrait des signatures

Réception d'une signature individuelle:

```
R1# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

Rétablir une catégorie de signature:

```
R1# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

Sujet 5.3.2:
Modification des signatures Cisco IOS IPS

Modifier les actions de signature

Change router actions for a signature or signature category

```
Router(config-sigdef-sig)# event-action action
```

Parameter	Description
deny-attacker-inline	Terminates the current packet and future packets from this attacker address for a specified period of time.
deny-connection-inline	Terminates the current packet and future packets on this TCP flow.
deny-packet-inline	Terminates the packet.
produce-alert	Writes the event to the Event Store as an alert.
reset-tcp-connection	Sends TCP resets to hijack and terminate the TCP flow. Only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

Sujet 5.3.3:
Vérifier et surveiller IPS

Verify IOS IPS

Les commandes **Show** pour vérifier la configuration IOS IPS :

- show ip ips
- show ip ips all
- show ip ips configuration
- show ip ips interfaces
- show ip ips signatures
- show ip ips statistics

Les commandes **Clear** pour désactiver IPS:

- clear ip ips configuration
- clear ip ips statistics

Signaler les alertes IPS

```
R1# config t
R1(config)# logging 192.168.10.100
R1(config)# ip ips notify log
R1(config)# logging on
R1(config)#
```

Activer SDEE

```
R1# config t
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip ips notify sdee
R1(config)# ip sdee events 500
R1(config)#
```

Clear the SDEE events or buffer:

```
Router# clear ip ips sdee {events| subscription}
```

Modify the SDEE buffer size:

```
Router(config)# ip sdee events events
```

Section 5.4: Résumé

Objectifs du chapitre:

- Décrivez les technologies IPS et leur mise en œuvre.
- Expliquer les signatures IPS.
- Décrivez le processus de mise en œuvre d'IPS.

Merci .

cisco Cisco Networking Academy

Mind Wide Open

Ressources de l'instructeur

- **Rappelez-vous**, il existe des tutoriels utiles et des guides d'utilisation disponibles via votre page d'accueil NetSpace. (Https://www.netacad.com)
- Ces ressources couvrent une variété de sujets, y compris la navigation, les évaluations et les affectations.
- Une capture d'écran a été fournie ici en soulignant les tutoriels liés à l'activation des examens, à la gestion des évaluations et à la création de quiz.