Politique de service

Les politiques de service offrent un moyen cohérent et flexible de configurer les fonctionnalités de l'ASA. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Une politique de service comprend plusieurs actions ou règles appliquées à une interface ou appliquées globalement.

À propos des politiques de service

Les rubriques suivantes décrivent le fonctionnement des politiques de service.

Les composants d'une politique de service

Les politiques de service permettent d'appliquer des services avancés au trafic que vous autorisez. Tout trafic autorisé par les règles d'accès peut faire l'objet de politiques de service et donc recevoir un traitement spécial, comme être redirigé vers un module de service ou faire l'objet d'une inspection d'application.

Vous pouvez avoir les types de politiques de service suivants :

- Une politique globale qui s'applique à toutes les interfaces.
- Une politique de service appliquée par interface. La politique peut être un ensemble de cartes pour le trafic passant par le périphérique et le trafic de gestion dirigé vers l'interface de l'ASA plutôt que de passer par elle.

Chaque politique de service est composée des éléments suivants :

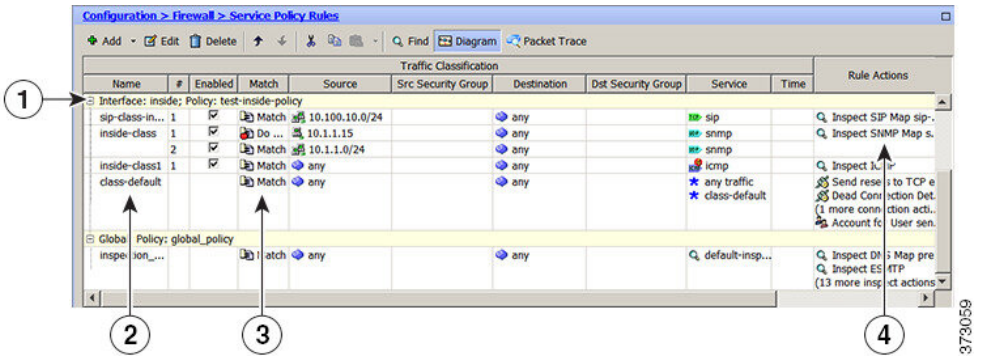
1. La liste des politiques de service, qui est l'ensemble ordonné de règles, et est nommée dans la commande **service-policy**. Dans ASDM, la liste des politiques est représentée sous forme de dossier sur la page des règles de politique de service.

2. Des règles, chaque règle étant une commande **class** dans la liste des politiques de service et les commandes associées à la commande **class**. Dans ASDM, chaque règle est affichée sur une ligne distincte, et le nom de la règle est le nom de la carte.

   La commande **class** définit les critères de correspondance de trafic pour la règle.

   Les commandes associées à la carte, telles que **inspect**, **set connection timeout**, etc., définissent les services et les contraintes à appliquer au trafic correspondant. Notez que les commandes d'inspection peuvent pointer vers des listes des politiques d'inspection, qui définissent les actions à appliquer au trafic inspecté. Gardez à l'esprit que les listes des politiques d'inspection ne sont pas la même chose que les listes des politiques de service.

L'exemple suivant compare la façon dont les politiques de service s'affichent dans l'interface de ligne de commande avec la façon dont elles s'affichent dans ASDM. Notez qu'il n'y a pas de mappage un à un entre les appels de figure et les lignes dans l'interface de ligne de commande.



L'interface de ligne de commande suivante est générée par les règles affichées dans la figure ci-dessus.

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
```

```
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

Fonctionnalités configurées avec les politiques de service

Le tableau suivant répertorie les fonctionnalités que vous configurez à l'aide des politiques de service.

Tableau 1 : Fonctionnalités configurées avec les politiques de service

Fonctionnalités	Pour le trafic de transit?	Pour le trafic de gestion?	Voir :
inspection des applications (plusieurs types)	**Tous** sauf la comptabilité RADIUS	**Comptabilité RADIUS** uniquement	• Premiers pas avec l'inspection du protocole de la couche application. • Inspection des protocoles Internet de base. • Inspection des protocoles vocaux et vidéo. • Inspection des réseaux mobiles.
Filtrage de journalisation des événements sécurisés NetFlow	**Oui**	**Oui**	Consultez le guide de mise en œuvre de NetFlow.
Régulation d'entrée et de sortie QoS	**Oui**	Non	Qualité de service.
File d'attente prioritaire standard QoS	**Oui**	Non	Qualité de service.

Fonctionnalités	Pour le trafic de transit?	Pour le trafic de gestion?	Voir :
Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP	**Oui**	**Oui**	Paramètres de connexion.
normalisationTCP	**Oui**	Non	Paramètres de connexion.
contournement de l'état du TCP	**Oui**	Non	Paramètres de connexion.
Statistiques d'utilisateurs pour le pare-feu d'identité	**Oui**	**Oui**	Consultez la commande **user-statistics** dans la référence de commande.

Sens d'application de la fonctionnalité

Les actions sont appliquées au trafic de manière bidirectionnelle ou unidirectionnelle, selon la fonctionnalité. Pour les fonctionnalités appliquées de manière bidirectionnelle, tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la liste des politiques est affecté si le trafic correspond à la carte de trafic dans les deux sens.

Remarque Lorsque vous utilisez une politique globale, toutes les fonctionnalités sont unidirectionnelles; les fonctionnalités qui sont normalement bidirectionnelles lorsqu'elles sont appliquées à une seule interface ne s'appliquent qu'au trafic entrant de chaque interface lorsqu'elles sont appliquées globalement. Comme la politique est appliquée à toutes les interfaces, la politique sera appliquée dans les deux sens, de sorte que la bidirectionnalité dans ce cas est redondante.

Pour les fonctionnalités appliquées de manière unidirectionnelle, par exemple la file d'attente de priorité QoS, seul le trafic qui entre (ou quitte, selon la fonctionnalité) l'interface à laquelle vous appliquez la liste des politiques est affecté. Consultez le tableau suivant pour connaître le sens d'application de chaque fonctionnalité.

Tableau 2 : Sens d'application sur une interface unique

Fonctionnalités	Sens d'application sur une interface unique	Sens d'application global
Inspection des applications (plusieurs types)	Bidirectionnel	Entrée
Filtrage NetFlow Secure Event Logging	S. O.	Entrée
Régulation du trafic entrant QoS	Entrée	Entrée
Régulation du trafic sortant QoS	Sortie	Sortie
File d'attente prioritaire standard QoS	Sortie	Sortie
Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP	Bidirectionnel	Entrée

Fonctionnalités	Sens d'application sur une interface unique	Sens d'application global
normalisationTCP	Bidirectionnel	Entrée
contournement de l'état du TCP	Bidirectionnel	Entrée
Statistiques d'utilisateurs pour le pare-feu d'identité	Bidirectionnel	Entrée

Correspondance des fonctionnalités dans une politique de service

Un paquet correspond aux règles de classe de trafic d'une politique de service pour pour une interface donnée selon les règles suivantes :

1. Un paquet ne peut correspondre qu'à une seule règle de classe de trafic pour chaque type de fonctionnalité.
2. Lorsque le paquet correspond à une règle de trafic pour un type de fonctionnalité, l'ASA ne tente pas de le mettre en correspondance avec les règles de trafic ultérieures pour ce type de fonctionnalité.
3. Si le paquet correspond à une règle de trafic ultérieure pour un type de fonctionnalité différent, l'ASA applique également les actions pour la règle de trafic ultérieure, si elle est prise en charge. Consultez Incompatibilité de certaines actions de fonctionnalité, à la page 6 pour obtenir plus d'informations sur les combinaisons non prises en charge.

Remarque L'inspection d'application comprend plusieurs types d'inspection, et la plupart s'excluent mutuellement. Pour les inspections qui peuvent être combinées, chaque inspection est considérée comme une fonctionnalité distincte.

Exemples de mise en correspondance de paquets

Par exemple :

- Si un paquet correspond à une règle de trafic pour les limites de connexion, ainsi qu'à une règle de trafic pour une inspection d'application, les deux actions sont appliquées.
- Si un paquet correspond à une règle de trafic pour l'inspection HTTP, mais correspond également à une autre règle de trafic qui inclut l'inspection HTTP, les actions de la deuxième règle de trafic ne sont pas appliquées.
- Si un paquet correspond à une règle de trafic pour l'inspection HTTP, mais correspond également à une autre règle de trafic qui comprend l'inspection FTP, les actions de la deuxième règle de trafic ne sont pas appliquées, car les inspections HTTP et FTP ne peuvent pas être combinées.
- Si un paquet correspond à une règle de trafic pour l'inspection HTTP, mais correspond également à une autre règle de trafic qui inclut l'inspection IPv6, les deux actions sont appliquées, car l'inspection IPv6 peut être combinée avec tout autre type d'inspection.

Ordre dans lequel plusieurs actions de fonctionnalité sont appliquées

L'ordre dans lequel les différents types d'actions d'une politique de service sont exécutés est indépendant de l'ordre dans lequel ils apparaissent dans le tableau de la politique.

Les actions sont effectuées dans l'ordre suivant :

1. régulation d'entrée QoS
2. Normalisation TCP, limites et délais d'expiration de connexion TCP et UDP, randomisation du numéro de séquence TCP et contournement de l'état TCP.

Remarque Lorsque l'ASA effectue un service de proxy (comme AAA) ou qu'il modifie la charge utile TCP (comme l'inspection FTP), le normaliseur TCP agit en mode double, où il est appliqué avant et après le service de modification du proxy ou de la charge utile.

3. Inspections d'application qui peuvent être combinées avec d'autres inspections :
    1. IPv6
    2. Options IP
    3. WAAS
4. Inspections d'application qui ne peuvent pas être combinées avec d'autres inspections. Consultez Incompatibilité de certaines actions de fonctionnalité, à la page 6 pour de plus amples renseignements.
5. Régulation de sortie QoS
6. File d'attente prioritaire standard QoS

Remarque Le filtrage de la journalisation des événements sécurisés NetFlow et les statistiques d'utilisateur pour le pare-feu d'identité sont indépendants de l'ordre.

Incompatibilité de certaines actions de fonctionnalité

Certaines fonctionnalités ne sont pas compatibles entre elles pour le même trafic. La liste suivante peut ne pas inclure toutes les incompatibilités ; pour en savoir plus sur la compatibilité de chaque fonctionnalité, consultez le chapitre ou la section correspondant à la fonctionnalité :

- Vous ne pouvez pas configurer la mise en file d'attente prioritaire QoS et la régulation QoS pour le même ensemble de trafic.
- La plupart des inspections ne doivent pas être combinées avec une autre inspection, donc l'ASA n'applique qu'une seule inspection si vous configurez plusieurs inspections pour le même trafic. Les exceptions sont répertoriées dans Ordre dans lequel plusieurs actions de fonctionnalité sont appliquées, à la page 6.

Remarque La classe de trafic d'inspection par défaut, qui est utilisée dans la politique globale par défaut, est un raccourci d'interface de ligne de commande spécial pour faire correspondre les ports par défaut pour toutes les inspections. Lorsqu'elle est utilisée dans une liste des politiques, cette carte de trafic garantit que l'inspection correcte est appliquée à chaque paquet, en fonction du port de destination du trafic. Par exemple, lorsque le trafic UDP pour le port 69 atteint l'ASA, l'ASA applique l'inspection TFTP; lorsque le trafic TCP pour le port 21 arrive, l'ASA applique l'inspection FTP. Ainsi, dans ce cas uniquement, vous pouvez configurer plusieurs inspections pour la même carte de trafic. Normalement, l'ASA n'utilise pas le numéro de port pour déterminer quelle inspection appliquer, ce qui vous donne ainsi la possibilité d'appliquer des inspections à des ports non standard, par exemple.

Mise en correspondance des fonctionnalités pour plusieurs politiques de service

Pour le trafic TCP et UDP (et ICMP lorsque vous activez l'inspection ICMP dynamique), les politiques de service fonctionnent sur les flux de trafic, et pas seulement sur les paquets individuels. Si le trafic fait partie d'une connexion existante qui correspond à une fonctionnalité dans une politique sur une interface, ce flux de trafic ne peut pas également correspondre à la même fonctionnalité dans une politique sur une autre interface; seule la première politique est utilisée.

Par exemple, si le trafic HTTP correspond à une politique sur l'interface interne pour inspecter le trafic HTTP, et que vous disposez d'une politique distincte sur l'interface externe pour l'inspection HTTP, ce trafic n'est pas également inspecté à la sortie de l'interface externe. De même, le trafic de retour pour cette connexion ne sera pas inspecté par la politique d'entrée de l'interface externe ni par la politique de sortie de l'interface interne.

Pour le trafic qui n'est pas traité comme un flux, par exemple ICMP lorsque vous n'activez pas l'inspection ICMP avec état, le trafic de retour peut correspondre à une liste des politiques différente sur l'interface de retour.

Lignes directrices pour les politiques de service

Lignes directrices relatives à l'inspection

Il existe une rubrique distincte qui fournit des lignes directrices détaillées sur les politiques de service d'inspection des applications. Consultez Lignes directrices relatives à l'inspection des applications.

Directives IPv6

Prend en charge IPv6 pour les fonctionnalités suivantes :

- Inspection d'application pour plusieurs protocoles, mais pas tous. Pour de plus amples renseignements, consultez la section Lignes directrices relatives à l'inspection des applications.
- Filtrage NetFlow Secure Event Logging
- Contournement de l'état du SCTP

- Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP
- normalisationTCP
- contournement de l'état du TCP
- Statistiques d'utilisateurs pour le pare-feu d'identité

Lignes directrices relatives aux cartes de trafic (classes de trafic)

Le nombre maximal de cartes de trafic (classes de trafic) de tous les types est de 255 en mode unique ou par contexte en mode multiple. Les cartes de trafic comprennent les types suivants :

- Classes de trafic de couche 3/4 (pour le trafic de transit et le trafic de gestion).
- Cartes de trafic d'inspection
- Cartes de trafic d'expressions régulières
- Commandes **match** utilisées directement sous une liste des politiques d'inspection

Cette limite inclut également les cartes de trafics par défaut de tous les types, ce qui limite les cartes de trafics configurées par l'utilisateur à environ 235.

Lignes directrices relatives aux politiques de service

- Les politiques de service d'interface sur les interfaces d'entrée prévalent sur la politique de service globale pour une fonctionnalité donnée. Par exemple, si vous avez une politique globale avec inspection FTP et une politique d'interface avec normalisation TCP, l'inspection FTP et la normalisation TCP sont appliquées à l'interface. Toutefois, si vous avez une politique globale avec inspection FTP et une politique d'interface d'entrée avec inspection FTP, seule l'inspection FTP de la politique d'interface d'entrée est appliquée à cette interface. Si aucune politique d'entrée ou globale ne met en œuvre une fonctionnalité, une politique de service d'interface sur l'interface de sortie qui spécifie la fonctionnalité est appliquée.
- Vous ne pouvez appliquer qu'une seule politique globale. Par exemple, vous ne pouvez pas créer une politique globale qui inclut l'ensemble de fonctionnalités 1 et une politique globale distincte qui inclut l'ensemble de fonctionnalités 2. Toutes les fonctionnalités doivent être incluses dans une seule politique.
- Lorsque vous apportez des modifications à la configuration de la politique de service, toutes les *nouvelles* connexions utilisent la nouvelle politique de service. Les connexions existantes continuent d'utiliser la politique qui était configurée au moment de l'établissement de la connexion. La sortie pour la commande **show** n'inclura pas de données sur les anciennes connexions.

  Par exemple, si vous supprimez une politique de service QoS d'une interface, puis ajoutez une version modifiée, alors la commande **show service-policy** n'affiche que les compteurs QoS associés aux nouvelles connexions qui correspondent à la nouvelle politique de service; les connexions existantes sur l'ancienne politique ne s'affichent plus dans la sortie de la commande.

  Pour vous assurer que toutes les connexions utilisent la nouvelle politique, vous devez déconnecter les connexions actuelles afin qu'elles puissent se reconnecter à l'aide de la nouvelle politique. Utilisez les commandes **clear conn** ou **clear local-host**.

Par défaut pour les politiques de service

Les rubriques suivantes décrivent les paramètres par défaut des politiques de service et le cadre de politique modulaire.

Configuration de la politique de service par défaut

Par défaut, la configuration comprend une politique qui correspond à tout le trafic d'inspection d'application par défaut et applique certaines inspections au trafic sur toutes les interfaces (politique globale). Toutes les inspections ne sont pas activées par défaut. Vous ne pouvez appliquer qu'une seule politique globale, donc si vous souhaitez modifier la politique globale, vous devez soit modifier la politique par défaut, soit la désactiver et en appliquer une nouvelle. (Une politique d'interface remplace la politique globale pour une fonctionnalité particulière.)

La politique par défaut inclut les inspections d'application suivantes :

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- SIP
- NetBios
- TFTP
- Options d'adresse IP

Cartes de trafics par défaut (classes de trafic)

La configuration comprend une carte de trafic de couche 3/4 par défaut (classe de trafic) que l'ASA utilise dans la politique globale par défaut appelée Default Inspection Traffic; il correspond au trafic d'inspection par défaut. Cette carte, qui est utilisée dans la politique globale par défaut, est un raccourci spécial pour faire correspondre les ports par défaut pour toutes les inspections.

Lorsqu'elle est utilisée dans une politique, cette carte garantit que l'inspection correcte est appliquée à chaque paquet, en fonction du port de destination du trafic. Par exemple, lorsque le trafic UDP pour le port 69 atteint l'ASA, l'ASA applique l'inspection TFTP; lorsque le trafic TCP pour le port 21 arrive, l'ASA applique

l'inspection FTP. Ainsi, dans ce cas uniquement, vous pouvez configurer plusieurs inspections pour la même carte de trafic. Normalement, l'ASA n'utilise pas le numéro de port pour déterminer quelle inspection appliquer, vous donnant ainsi la flexibilité d'appliquer des inspections à des ports non standard, par exemple.

Une autre carte de trafic qui existe dans la configuration par défaut est appelée class-default, et elle correspond à tout le trafic. Cette carte de trafic apparaît à la fin de toutes les listes des politiques de couche 3/4 et indique essentiellement à l'ASA de n'effectuer aucune action sur tout autre trafic. Si vous utilisez la classe par défaut (la classe Tout trafic dans ASDM), utilisez-la à des fins plus larges comme l'activation de l'aléatoire des séquences TCP, du décrément des TTL ou toute autre modification d'attribut facultatif. Ne l'utilisez pas pour l'inspection, car cela pourrait perturber le trafic. Certaines fonctionnalités sont uniquement disponibles pour class-default.

Configurer les politiques de service

La configuration d'une politique de service consiste à ajouter une ou plusieurs règles de politique de service par interface ou pour la politique globale. ASDM utilise un assistant pour vous guider dans le processus de création d'une politique de service. Pour chaque règle, vous identifiez les éléments suivants :

1. L'interface à laquelle vous souhaitez appliquer la règle ou la politique globale.
2. Le trafic auquel vous souhaitez appliquer les actions. Vous pouvez identifier le trafic des couches 3 et 4.
3. Les actions à appliquer à la classe de trafic. Vous pouvez appliquer plusieurs actions non incompatibles pour chaque classede trafic.

Après avoir créé une politique, vous pouvez ajouter des règles et déplacer, modifier ou supprimer des règles ou des politiques. Les rubriques suivantes expliquent comment configurer les politiques de service.

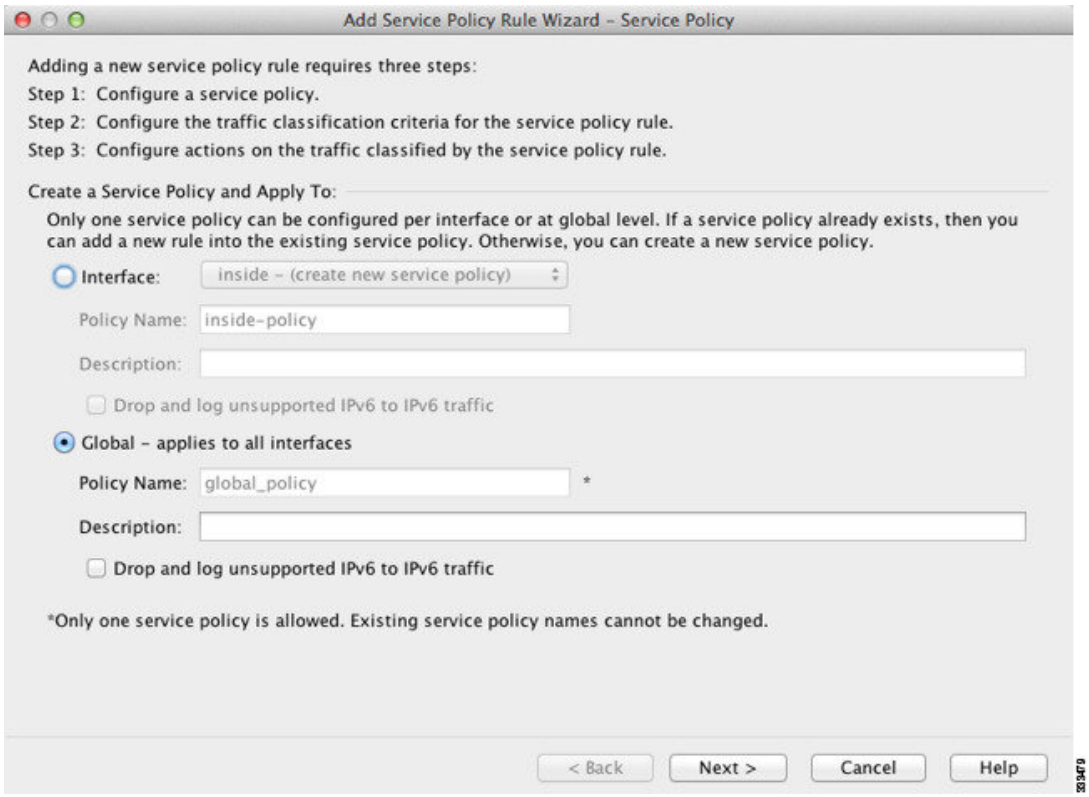
Ajouter une règle de politique de service pour le trafic de transit

Pour ajouter une règle de politique de service pour le trafic de transit, utilisez l'assistant Ajouter une règle de politique de service. Vous serez invité à choisir la portée de la politique, pour une interface spécifique ou globale :

- Les politiques de service d'interface prévalent sur la politique de service globale pour une fonctionnalité donnée. Par exemple, si vous avez une politique globale avec inspection FTP et une politique d'interface avec des limites de connexion TCP, l'inspection FTP et les limites de connexion TCP sont appliquées à l'interface. Toutefois, si vous avez une politique globale avec inspection FTP et une politique d'interface avec inspection FTP, seule l'inspection FTP de la politique d'interface est appliquée à cette interface.
- Les politiques de service globales fournissent des services par défaut à toutes les interfaces. Sauf s'ils sont remplacés par une politique spécifique à l'interface, les services globaux sont appliqués. Par défaut, il existe une politique globale qui comprend une règle de politique de service pour l'inspection d'application par défaut. Vous pouvez ajouter une règle à la politique globale à l'aide de l'assistant.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, puis cliquez sur **Add (Ajouter)** ou **Add** > **Add Service Policy Rule (Ajouter une règle de politique de service)**.



Étape 2 Dans la zone Créer une politique de service et l'appliquer à :

a) Choisissez si la politique s'applique à une **interface** spécifique ou **globale** à toutes les interfaces.
b) Si vous sélectionnez Interface, choisissez le nom de l'interface. Si l'interface a déjà une politique, vous ajoutez une règle à la politique existante.
c) Si l'interface n'a pas encore de politique de service, saisissez le nom de la nouvelle politique.
d) (Facultatif) Saisissez une description pour la politique.
e) (Facultatif) Cochez l'option **Drop and log unsupported IPv6 to IPv6 traffic** (Abandonner et journaliser le trafic IPv6 à IPv6 non pris en charge) pour générer un journal système (767001) pour le trafic IPv6 abandonné par les inspections d'application qui ne prennent pas en charge le trafic IPv6. Par défaut, les journaux système ne sont pas générés.
f) Cliquez sur **Next** (suivant).

Étape 3 Sur la page Traffic Classification Criteria (Critères de classification du trafic), choisissez l'une des options suivantes pour préciser le trafic auquel appliquer les actions de politique et cliquez sur **Next** (Suivant).

- **Créez une nouvelle classe de trafic.** Saisissez un nom et une description facultative.

  Déterminez le trafic à l'aide de l'un des critères suivants :

  - **Trafic d'inspection par défaut** : la classe correspond aux ports TCP et UDP par défaut utilisés par toutes les applications que l'ASA peut inspecter. Lorsque vous cliquez sur **Next** (Suivant), les services et les ports définis par cette classe s'affichent.

    Cette option, qui est utilisée dans la politique globale par défaut, est un raccourci spécial qui, lorsqu'elle est utilisée dans une règle, garantit que l'inspection correcte est appliquée à chaque paquet, en fonction du port de destination du trafic. Pour en savoir plus, consultez Cartes de trafics par défaut (classes de trafic), à la page 9.

Consultez Inspections par défaut et limites de la NAT pour obtenir la liste des ports par défaut. L'ASA comprend une politique globale par défaut qui correspond au trafic d'inspection par défaut et applique les inspections courantes au trafic sur toutes les interfaces. Toutes les applications dont les ports sont inclus dans la classe Default Inspection Traffic (Trafic d'inspection par défaut) ne sont pas activées par défaut dans la liste des politiques.

Vous pouvez spécifier une classe Source and Destination IP Address (Adresse IP source et de destination) (qui utilise une ACL) avec la classe Default Inspection Traffic (Trafic d'inspection par défaut) pour restreindre le trafic correspondant. Comme la classe Default Inspection Traffic (Trafic d'inspection par défaut) spécifie les ports et les protocoles à mettre en correspondance, tous les ports et protocoles dans l'ACL sont ignorés.

- **Adresses IP source et de destination (utilise l'ACL)** : la classe correspond au trafic spécifié par une liste de contrôle d'accès étendue. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès et l'assistant crée l'ACL. Vous pouvez également sélectionner une liste de contrôle d'accès existante.

  Lors de la définition de l'ACE, l'option Match (Correspondance) crée une règle selon laquelle les actions sont appliquées au trafic qui correspond aux adresses. L'option Do Not Match (aucune correspondance) exempte le trafic de l'application des actions précisées. Par exemple, vous souhaitez mettre en correspondance tout le trafic dans 10.1.1.0/24 et y appliquer des limites de connexion, à l'exception de 10.1.1.25. Dans ce cas, créez deux règles, une pour 10.1.1.0/24 en utilisant l'option Match (Correspondance) et l'autre pour 10.1.1.25 à l'aide de l'option Do Not Match (aucune correspondance). Assurez-vous d'organiser les règles de sorte que la règle Do Not Match (aucune correspondance) soit au-dessus de la règle Match (Correspondance), sinon 10.1.1.25 correspondra d'abord à la règle Match (Correspondance).

  Remarque
  Lorsque vous créez une nouvelle classe de trafic de ce type, vous ne pouvez spécifier qu'une seule entrée de contrôle d'accès (ACE) au départ. Une fois que vous avez terminé d'ajouter la règle, vous pouvez ajouter des ACE supplémentaires en ajoutant une nouvelle règle à la même interface ou à la politique globale, puis en spécifiant **Add rule to existing traffic class (Ajouter une règle à la classe de trafic** existante) (voir ci-dessous).

- **Groupe de tunnels** : la classe correspond au trafic d'un groupe de tunnels (profil de connexion) auquel vous souhaitez appliquer la QoS. Vous pouvez également spécifier une autre option de correspondance de trafic pour affiner la correspondance de trafic, à l'exclusion de Any Traffic (Tout trafic), Source and Destination IP Address (Adresse IP source et de destination) (utilise une ACL) ou Default Inspection Traffic (Trafic d'inspection par défaut).

  Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à sélectionner le groupe de tunnels (vous pouvez en créer un nouveau si nécessaire). Pour contrôler chaque flux, cochez **Match flow destination IP address** (Faire correspondre l'adresse IP de destination du flux). Tout le trafic acheminé vers une adresse de destination IP unique est considéré comme un flux.

- **TCP or UDP or SCTP Destination Port** (Port de destination TCP, UDP ou SCTP) : la classe correspond à un port unique ou à une plage contiguë de ports. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à choisir le protocole et à saisir le numéro de port; cliquez sur **...** pour en choisir un déjà défini dans ASDM.

  Astuces
  Pour les applications qui utilisent plusieurs ports non contigus, utilisez Source and Destination IP Address (Adresse IP source et de destination) (utilise une ACL) pour faire correspondre chaque port.

- **Plage RTP** : la carte de trafic correspond au trafic RTP. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir une plage de ports RTP comprise entre 2 000 et 65 534. Le nombre maximal de ports dans la plage est de 16 383.
- **IP DiffServ CodePoints (DSCP)** : la carte correspond à jusqu'à huit valeurs DSCP dans l'en-tête IP. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à sélectionner ou à saisir les valeurs souhaitées (déplacez-les dans la liste Correspondance sur DSCP).
- **Précédence IP** : la carte de trafic correspond à jusqu'à quatre valeurs de priorité, représentées par l'octet TOS dans l'en-tête IP. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les valeurs.
- **Tout trafic** : correspond à tout le trafic.

- **Ajouter une règle à la carte de trafic existante**. Si vous avez déjà une règle de politique de service sur la même interface ou si vous en ajoutez à la politique de service globale, cette option vous permet d'ajouter une ACE à une ACL existante. Vous pouvez ajouter une ACE à n'importe quelle liste de contrôle d'accès que vous avez créée précédemment lorsque vous avez choisi l'option d'adresse IP source et de destination (utilise l'ACL) pour une règle de politique de service sur cette interface. Pour cette classe de trafic, vous ne pouvez avoir qu'un seul ensemble d'actions de règles, même si vous ajoutez plusieurs ACE. Vous pouvez ajouter plusieurs ACE à la même classe de trafic en répérant l'ensemble de cette procédure. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès.
- **Utilisez une classe de trafic existante.** Si vous avez créé une classe de trafic utilisée par une règle sur une interface différente, vous pouvez réutiliser la définition de classe de trafic pour cette règle. Notez que si vous modifiez la classe de trafic pour une règle, la modification est transmise par toutes les règles qui utilisent cette classe de trafic. Si votre configuration comprend des commandes **class-map** que vous avez saisies au niveau de l'interface de ligne de commande, ces noms de carte de trafic sont également disponibles (bien que pour afficher la définition de la carte de trafic, vous devez créer la règle).
- **Utilisez la classe class-default, comme classe de trafic**. Cette option utilise la classe class-default, qui correspond à tout le trafic. La carte class-default est créée automatiquement par l'ASA et placée à la fin de la politique. Si vous ne lui appliquez aucune action, elle est toujours créée par l'ASA, mais pour des besoins internes uniquement. Vous pouvez appliquer des actions à cette carte, si vous le souhaitez, ce qui peut être plus pratique que de créer une nouvelle carte de trafic qui correspond à tout le trafic. Vous ne pouvez créer qu'une seule règle pour cette politique de service en utilisant la carte class-default, car chaque carte de trafic ne peut être associée qu'à une seule règle par politique de service.

Étape 4 Si vous avez sélectionné un critère de correspondance de trafic qui nécessite une configuration supplémentaire, saisissez les paramètres souhaités et cliquez sur **Next** (Suivant).

Étape 5 Sur la page Actions de règle, configurez une ou plusieurs actions de règle. Consultez Fonctionnalités configurées avec les politiques de service, à la page 3 pour obtenir une liste des fonctionnalités et des actions que vous pouvez appliquer, avec des pointeurs vers des détails supplémentaires.

Étape 6 Cliquez sur **Terminer**.

Ajouter une règle de politique de service pour le trafic de gestion

Pour ajouter une règle de politique de service pour le trafic dirigé vers l'ASA à des fins de gestion, utilisez l'assistant Add Service Policy Rule (Ajouter une règle de politique de service). Vous serez invité à choisir la portée de la politique, pour une interface spécifique ou globale :

- Les politiques de service d'interface prévalent sur la politique de service globale pour une fonctionnalité donnée. Par exemple, si vous avez une politique globale avec inspection de comptabilité RADIUS et une politique d'interface avec limites de connexion, la comptabilité RADIUS et les limites de connexion sont appliquées à l'interface. Toutefois, si vous avez une politique globale avec la comptabilité RADIUS et une politique d'interface avec la comptabilité RADIUS, seule la comptabilité RADIUS de la politique d'interface est appliquée à cette interface.
- Les politiques de service globales fournissent des services par défaut à toutes les interfaces. Sauf s'ils sont remplacés par une politique spécifique à l'interface, les services globaux sont appliqués. Par défaut, il existe une politique globale qui comprend une règle de politique de service pour l'inspection d'application par défaut. Vous pouvez ajouter une règle à la politique globale à l'aide de l'assistant.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, puis cliquez sur **Add (Ajouter)** ou **Add** > **Add Management Service Policy Rule (Ajouter une règle de politique de service de gestion)**.

Étape 2 Dans la zone Créer une politique de service et l'appliquer à :

a) Choisissez si la politique s'applique à une **interface** spécifique ou **globalement** à toutes les interfaces.
b) Si vous sélectionnez Interface, choisissez le nom de l'interface. Si l'interface a déjà une politique, vous ajoutez une règle à la politique existante.
c) Si l'interface n'a pas encore de politique de service, saisissez le nom de la nouvelle politique.
d) (Facultatif) Saisissez une description pour la politique.
e) Cliquez sur **Next** (suivant).

Étape 3 Sur la page Traffic Classification Criteria (Critères de classification du trafic), choisissez l'une des options suivantes pour préciser le trafic auquel appliquer les actions de politique et cliquez sur **Next** (Suivant).

- **Créez une nouvelle classe de trafic.** Saisissez un nom et une description facultative.

  Déterminez le trafic à l'aide de l'un des critères suivants :

  - **Adresses IP source et de destination (utilise l'ACL)** : la classe correspond au trafic spécifié par une liste de contrôle d'accès étendue. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès et l'assistant crée l'ACL. Vous pouvez également sélectionner une liste de contrôle d'accès existante.

    Lors de la définition de l'ACE, l'option Match (Correspondance) crée une règle selon laquelle les actions sont appliquées au trafic qui correspond aux adresses. L'option Do Not Match (aucune correspondance) exempte le trafic de l'application des actions précisées. Par exemple, vous souhaitez mettre en correspondance tout le trafic dans 10.1.1.0/24 et y appliquer des limites de connexion, à l'exception de 10.1.1.25. Dans ce cas, créez deux règles, une pour 10.1.1.0/24 en utilisant l'option Match (Correspondance) et l'autre pour 10.1.1.25 à l'aide de l'option Do Not Match (aucune correspondance). Assurez-vous d'organiser les règles de sorte que la règle Do Not Match (aucune

correspondance) soit au-dessus de la règle Match (Correspondance), sinon 10.1.1.25 correspondra d'abord à la règle Match (Correspondance).

- **TCP or UDP or SCTP Destination Port** (Port de destination TCP, UDP ou SCTP) : la classe correspond à un port unique ou à une plage contiguë de ports. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à choisir le protocole et à saisir le numéro de port; cliquez sur **...** pour en choisir un déjà défini dans ASDM.

  Astuces
  Pour les applications qui utilisent plusieurs ports non contigus, utilisez Source and Destination IP Address (Adresse IP source et de destination) (utilise une ACL) pour faire correspondre chaque port.

- **Ajoutez une règle à la classe de trafic existante**. Si vous avez déjà une règle de politique de service sur la même interface ou si vous en ajoutez à la politique de service globale, cette option vous permet d'ajouter une ACE à une ACL existante. Vous pouvez ajouter une ACE à n'importe quelle liste de contrôle d'accès que vous avez créée précédemment lorsque vous avez choisi l'option d'adresse IP source et de destination (utilise l'ACL) pour une règle de politique de service sur cette interface. Pour cette classe de trafic, vous ne pouvez avoir qu'un seul ensemble d'actions de règles, même si vous ajoutez plusieurs ACE. Vous pouvez ajouter plusieurs ACE à la même classe de trafic en répérant l'ensemble de cette procédure. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès.

- **Utilisez une classe de trafic existante.** Si vous avez créé une classe de trafic utilisée par une règle sur une interface différente, vous pouvez réutiliser la définition de classe de trafic pour cette règle. Notez que si vous modifiez la classe de trafic pour une règle, la modification est transmise par toutes les règles qui utilisent cette classe de trafic. Si votre configuration comprend des commandes **class-map** que vous avez saisies au niveau de l'interface de ligne de commande, ces noms de classe de trafic sont également disponibles (bien que pour afficher la définition de la classe de trafic, vous devez créer la règle).

Étape 4 Si vous avez sélectionné un critère de correspondance de trafic qui nécessite une configuration supplémentaire, saisissez les paramètres souhaités et cliquez sur **Next** (Suivant).

Étape 5 Sur la page Actions de règle, configurez une ou plusieurs actions de règle.

- Pour configurer l'inspection de comptabilité RADIUS, choisissez une liste d'inspection dans la liste déroulante RADIUS Accounting Map (Liste de comptabilité RADIUS) ou cliquez sur **Configure** (Configurer) pour ajouter une liste. Consultez Fonctionnalités configurées avec les politiques de service, à la page 3 pour de plus amples renseignements.
- Pour configurer les paramètres de connexion, consultez Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services).

Étape 6 Cliquez sur **Terminer**.

Gérer l'ordre des règles de politique de service

L'ordre des règles de politique de service sur une interface ou dans la politique globale affecte la façon dont les actions sont appliquées au trafic. Consultez les lignes directrices suivantes sur la façon dont un paquet correspond aux règles d'une politique de service :

- Un paquet ne peut correspondre qu'à une seule règle dans une politique de service pour chaque type de fonctionnalité.
- Lorsque le paquet correspond à une règle qui comprend des actions pour un type de fonctionnalité, l'ASA ne tente pas de le mettre en correspondance avec les règles ultérieures, y compris ce type de fonctionnalité.
- Si le paquet correspond à une règle ultérieure pour un type de fonctionnalité différent, l'ASA applique également les actions pour la règle ultérieure.

Par exemple, si un paquet correspond à une règle pour les limites de connexion et correspond également à une règle pour l'inspection des applications, les deux actions découlant d'une règle sont appliquées.

Si un paquet correspond à une règle d'inspection d'application, mais correspond également à une autre règle qui inclut l'inspection d'application, les actions de la deuxième règle ne sont pas appliquées.

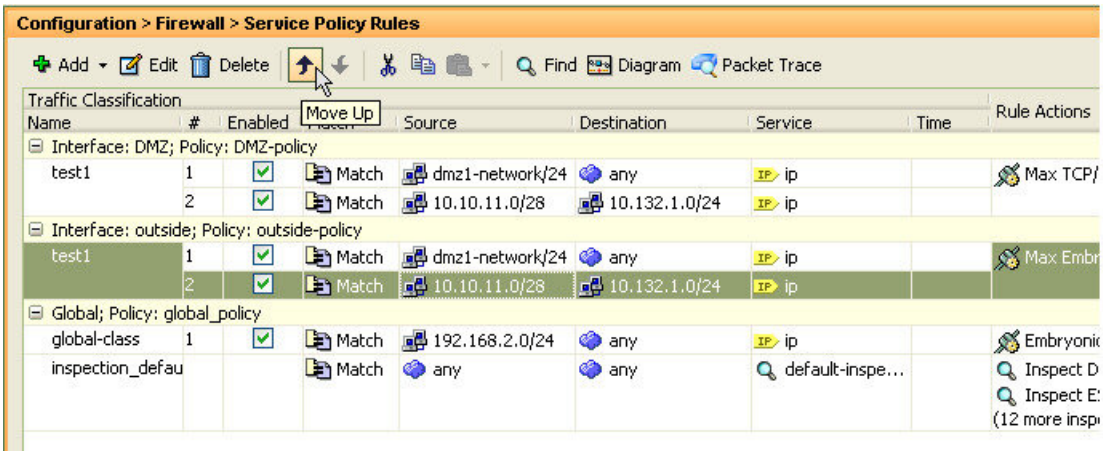
Si votre règle comprend une liste de contrôle d'accès avec plusieurs ACE, l'ordre des ACE affecte également le flux de paquets. L'ASA teste le paquet par rapport à chaque ACE dans l'ordre dans lequel les entrées sont répertoriées. Une fois qu'une correspondance est trouvée, aucune autre Ace n'est vérifiée. Par exemple, si vous créez une entrée ACE au début d'une liste de contrôle d'accès qui autorise explicitement tout le trafic, aucune autre instruction n'est jamais vérifiée.

Pour modifier l'ordre des règles ou des ACE dans une règle, procédez comme suit :

Procédure

Étape 1 Dans le volet **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, choisissez la règle ou l'ACE que vous souhaitez déplacer vers le haut ou vers le bas.

Étape 2 Cliquez sur le bouton **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas).



Remarque
Si vous réorganisez les ACE dans une liste de contrôle d'accès utilisée dans plusieurs politiques de service, la modification est transmise dans toutes les politiques de service.

Étape 3 Lorsque vous avez terminé de réorganiser vos règles ou vos règles ACE, cliquez sur **Apply** (Appliquer).

Historique des politiques de service

Nom de la caractéristique	Versions	Description
Cadre de politique modulaire	7.0(1)	Le cadre de politique modulaire a été lancé.
carte de trafic de gestion à utiliser avec le trafic de comptabilité RADIUS	7.2(1)	La carte de trafic de gestion a été introduite pour une utilisation avec le trafic de comptabilité RADIUS. Les commandes suivantes ont été introduites : **class-map type management**, et **inspect radius-accounting**.
listes des politiques d'inspection	7.2(1)	La liste des politiques d'inspection a été introduite. La commande suivante a été introduite : **class-map type inspect**.
Expressions régulières et listes des politiques	7.2(1)	Les expressions régulières et les listes des politiques ont été introduites pour être utilisées dans les listes des politiques d'inspection. Les commandes suivantes ont été introduites : **class-map type regex**, **regex**, **match regex**.
match any pour les listes des politiques d'inspection	8.0(2)	Le mot-clé **match any** a été introduit pour une utilisation avec des listes des politiques d'inspection : le trafic peut correspondre à un ou plusieurs critères pour correspondre à la carte de trafic. Auparavant, uniquement **match all** était disponible.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.