

Régles de déchiffrement et exemple de politique

Ce chapitre s'appuie sur les concepts abordés dans ce guide pour fournir un exemple spécifique de politique SSL avec des règles de déchiffrement qui respectent nos bonnes pratiques et nos recommandations. Vous devriez être en mesure d'appliquer cet exemple à votre situation et de l'adapter aux besoins de votre organisation.

En résumé :

- Pour le trafic de confiance (comme le transfert d'une sauvegarde de serveur compressée volumineuse), contournez complètement l'inspection en utilisant le préfiltre et le déchargement de flux.
- Mettez en *premier* tous les règles de déchiffrement qui peuvent être évalués rapidement, comme ceux qui s'appliquent à des adresses IP spécifiques.
- Mettez en *dernier* les règles de déchiffrement qui nécessitent un traitement, **déchiffrer-resigner** et les règles qui bloquent les versions de protocoles et les suites de chiffrement non sécurisés.
- Bonnes pratiques de Régles de déchiffrement, à la page 1
- Visite virtuelle de la Politique de déchiffrement, à la page 5

Bonnes pratiques de Régles de déchiffrement

Ce chapitre fournit un exemple de politique SSL avec des règles de déchiffrement qui illustre nos bonnes pratiques et recommandations. Nous traiterons d'abord des paramètres des politiques SSL et de contrôle d'accès, puis nous passerons en revue toutes les règles et les raisons pour lesquelles nous recommandons de les classer de manière particulière.

Voici la politique SSL dont nous parlerons dans ce chapitre.

SSL Policy Example

Rule	es Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings									
									+	Add Category	+ Add Rule	् Search F	Rules	
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
Adm	inistrator Rules													
This	s category is empty													
Stan	dard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	OD not decrypt	
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	1
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo	any	any	any	any	OD not decrypt	
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Pho	any	any	any	any	OD not decrypt	1
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign	1
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	1
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	1
Root	Rules													
This	s category is empty													
Defa	ault Action										[Do not decrypt		- F

Inspection de contournement avec préfiltre et déchargement de flux

Le préfiltre est la première phase du contrôle d'accès, avant que le système n'effectue des évaluations plus exigeantes en ressources. Le préfiltrage est simple, rapide et précoce. Le préfiltre utilise des critères d'en-tête externe limités pour gérer rapidement le trafic. Comparez cela à l'évaluation ultérieure, qui utilise des en-têtes internes et possède des capacités d'inspection plus robustes.

Configurez le préfiltre afin d' :

- Améliorer les performances : plus vous excluez tôt le trafic qui ne nécessite pas d'inspection, mieux c'est. Vous pouvez utiliser un fastpath ou bloquer certains types de tunnels relais en texte brut en fonction de leurs en-têtes d'encapsulation externes, sans inspecter leurs connexions encapsulées. Améliorer les performances : vous pouvez accélérer ou bloquer toutes les autres connexions qui bénéficient d'un traitement anticipé.
- Adapter l'inspection approfondie au trafic encapsulé : vous pouvez modifier le zonage de certains types de tunnels afin de pouvoir gérer ultérieurement leurs connexions encapsulées en utilisant les mêmes critères d'inspection. Un changement de zonage est nécessaire, car après le préfiltre, le contrôle d'accès utilise les en-têtes internes.

Si vous avez un Firepower 4100/9300 disponible, vous pouvez utiliser un flux de déchargement volumineux, une technique par laquelle le trafic de confiance peut contourner le moteur d'inspection pour obtenir de meilleures performances. Vous pouvez l'utiliser, par exemple, dans un centre de données pour transférer des sauvegardes de serveur.

Sujets connexes

Délestages de flux importants

Préfiltrage ou contrôle d'accès Bonnes pratiques de préfiltrage Fastpath

Bonnes pratiques Ne pas déchiffrer

Journaliser le trafic

Nous vous *déconseillons de* créer des règles **Ne pas déchiffrer** qui ne journalisent rien car ces règles prennent encore du temps de traitement sur l'appareil géré. Si vous configurez un type de règles de déchiffrement, *activez la journalisation* pour voir le trafic mis en correspondance.

Directives pour le trafic déchiffrable

Nous pouvons déterminer qu'une partie du trafic n'est pas déchiffrable, soit parce que le site Web lui-même n'est pas déchiffrable, soit parce que le site Web utilise l'épinglage SSL, qui empêche les utilisateurs d'accéder à un site déchiffré sans erreur dans leur navigateur.

Pour en savoir plus sur l'épinglage de certificats, consultez À propos de l'épinglage TLS/SSL.

Nous maintenons la liste de ces sites comme suit :

- Un groupe de nom distinctif (DN) nommé Cisco-Undecryptable-Sites
- Le filtre d'application certificat épinglé

Si vous déchiffrez du trafic et que vous ne souhaitez pas que les utilisateurs voient des erreurs dans leur navigateur lorsqu'ils consultent ces sites, nous vous recommandons de configurer une règle « **Ne pas déchiffrer** » vers le bas de votre règles de déchiffrement.

Vous trouverez ci-dessous un exemple de configuration d'un filtre d'application de certificat épinglé.



Déchiffrer - Resigner et Déchiffrer - Bonnes pratiques relatives aux clés connues

Cette rubrique traite des bonnes pratiques pour **Déchiffrer – Resigner** et **Déchiffrer - Clé connue** règle de déchiffrement.

Bonnes pratiques de déchiffrement et de resignature avec l'épinglage de certificats

Certaines applications ont recours à une technique appelée « *TLS/SSL épinglage* » ou « épinglage de *certificat* », qui intègre l'empreinte du certificat de serveur d'origine dans l'application elle-même. Par conséquent, si vous avez configuré un règle de déchiffrement avec une action **Déchiffrer - Resigner**, lorsque l'application reçoit un certificat résigné d'un périphérique géré, la validation échoue et la connexion est abandonnée.

Comme l'épinglage TLS/SSL est utilisé pour éviter les attaques de l'homme du milieu, il n'y a aucun moyen de l'éviter ou de le contourner. Vous avez les options suivantes :

- Créez une règle **Ne pas déchiffrer** pour les applications classées avant les règles **Déchiffrer Resigner**.
- Demander aux utilisateurs d'accéder aux applications à l'aide d'un navigateur Web.

Pour en savoir plus sur l'épinglage de certificats, consultez À propos de l'épinglage TLS/SSL.

Déchiffrement : bonnes pratiques relatives aux clés connues

Étant donné qu'une action de règle **Déchiffrer - Clé connue** est destinée à être utilisée pour le trafic dirigé vers un serveur interne, vous devez toujours ajouter un réseau de destination à ces règles (condition de règle**Networks**). De cette façon, le trafic va directement au réseau sur lequel se trouve le serveur, ce qui réduit le trafic sur le réseau.

Donner la priorité aux Régles de déchiffrement

Mettez en premier toutes les règles qui peuvent être mises en correspondance par la première partie du paquet; par exemple, une règle qui fait référence à des adresses IP (condition de règle **Networks** (Réseaux)).

Placer les Régles de déchiffrement en dernier

Les règles avec les conditions de règle suivantes doivent être les dernières, car ces règles exigent que le trafic soit examiné par le système pendant la plus longue période :

- Applications
- Catégorie
- Certificate (certificat)
- Nom distinctif (DN)
- État du certificat
- Suite de chiffrement
- Version

Visite virtuelle de la Politique de déchiffrement

Ce chapitre fournit une discussion étape par étape et une procédure pas à pas sur la façon de créer un politique de déchiffrement à l'aide des règles utilisant nos bonnes pratiques. Vous verrez un aperçu de la politique de déchiffrement, suivi d'un résumé des bonnes pratiques et, finalement, d'une discussion sur les règles de la politique.

Voici les politique de déchiffrement dont nous parlerons dans ce chapitre.

SSI Enter	- Policy Example												Save	Cancel
Rule	es Trusted CA Certificates	Undecryptab	le Actions	Advanced Set	tings									
									+ Ad	d Category	+ Add Rule	् Search F	Rules	×
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
Adm	inistrator Rules													
This	a category is empty													
Stan	dard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕑 Do not decrypt	1
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	/1
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not decrypt	1
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	⊘Do not decrypt	/1
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign	/1
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	1
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	1
Root	Rules													
This	s category is empty													
Defa	ult Action											Do not decrypt		•

Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Paramètres de politique et de règle recommandés, à la page 5

- Trafic vers le préfiltre, à la page 9
 - PremierRègle de déchiffrement : Ne pas déchiffrer le trafic spécifique, à la page 9
 - Régles de déchiffrement suivantes : déchiffrer un trafic de test spécifique, à la page 10
 - Créer une règle de déchiffrement nouvelle signature pour les catégories, à la page 13
 - Ne pas déchiffrer les catégories, les réputations ou les applications à faible risque, à la page 11
 - Dernières Régles de déchiffrement : bloquer ou surveiller les certificats et les versions de protocole, à la page 14

Paramètres de politique et de règle recommandés

Nous recommandons les paramètres de politique suivants :

• Politique de déchiffrement :

- Action par défaut Ne pas déchiffrer.
- Activer la journalisation
- Définissez Undecryptable Actions sur Block (blocage) pour la session SSL v2 et la session comprimée.
- Activez le déchiffrement TLS 1.3 dans les paramètres avancés de la politique.
- règle de déchiffrement : Activez la journalisation pour chaque règle, à l'exception de celles avec une action de règle Ne pas déchiffrer. (C'est à vous de décider; si vous souhaitez voir les informations sur le trafic qui n'est pas déchiffré, activez également la journalisation pour ces règles.)
- Politique de contrôle d'accès :
 - Associez votre politique de déchiffrement à une politique de contrôle d'accès. (Si vous ne faites pas cela, vos politique de déchiffrement et vos règles n'ont aucun effet.)
 - Définissez l'action de politique par défaut sur **Prévention des intrusions : sécurité et connectivité équilibrées**.
 - Activer la journalisation

Sujets connexes

Paramètres de Politique de déchiffrement, à la page 6 Paramètres de Règle de déchiffrement, à la page 21 Paramètres de politique de contrôle d'accès, à la page 8

Paramètres de Politique de déchiffrement

Configurer les paramètres recommandés pour les bonnes pratiques suivantes pour votre politique de déchiffrement :

- Action par défaut Ne pas déchiffrer.
- Activer la journalisation
- Définissez Undecryptable Actions sur Block (blocage) pour la session SSL v2 et la session comprimée.
- Activez le déchiffrement TLS 1.3 dans les paramètres avancés de la politique.

Procédure

Étape 1	Cliquez sur Politiques > Contrôle d'accès > Déchiffrem	ent.
Étape 2	Cliquez sur Edit (🖋) à côté de votre politique de déchiffi	rement.
Étape 3	Dans la liste des actions par défaut figurant au bas de la La figure suivante présente un exemple.	page, cliquez sur Ne pas déchiffrer .
	Default Action	Do not decrypt v

Étape 4 À la fin de la ligne, cliquez sur Se connecter (.....).

Étape 5 Cochez la case Log at End of Connection (journal à la fin de la connexion).

- Étape 6 Cliquez sur OK.
- Étape 7 Cliquez sur Save (enregistrer).
- Étape 8 Cliquez sur l'onglet Undecryptable Actions (actions non déchiffrables).
- Étape 9 Nous vous recommandons de définir l'action pour la session SSLv2 et la session comprimée sur Block (blocage).

Vous ne devez pas autoriser SSL v2 sur votre réseau et le trafic TLS/SSL comprimé n'est pas pris en charge, vous devez donc également bloquer ce trafic.

Consultez Options de traitement par défaut du trafic non déchiffrable pour plus d'informations sur la définition de chaque option.

La figure suivante présente un exemple.

SSL Policy Example	e	
Rules Trusted CA Certific	ates Undecryptable Actions	Advanced Settings
Decryption Errors	Block	v
Handshake Errors	Inherit Default Action	•
Session not cached	Inherit Default Action	•
Unsupported Cipher Suite	Inherit Default Action	•
Unknown Cipher Suite	Inherit Default Action	•
SSLv2 Session	Block	•
Compressed Session	Block	· /
	Revert to Defau	ilts

Étape 10 Cliquez sur l'onglet Advanced Settings (paramètres avancés).

Étape 11 Cochez la case **Enable TLS 1.3 Decryption** (activer le déchiffrement TLS 1.3). Pour plus d'informations sur les autres options, consultez Options avancées de Politique de déchiffrement.

Applies to 7.1.0 and later
Block flows requesting ESNI
Disable HTTP/3 advertisement
Propagate untrusted server certificates to clients
Applies to 7.2.0 and later
Enable TLS 1.3 Decryption
Applies to 7.3.0 and later
Enable adaptive TLS server identity probe
Advanced options are available only with Snort 3
Revert to Defaults

Étape 12 En haut de la page, cliquez sur Save(Enregistrer).

Prochaine étape

Configurez règles de déchiffrement et définissez chacun d'eux comme indiqué dans Paramètres de Règle de déchiffrement, à la page 21.

Paramètres de politique de contrôle d'accès

Comment configurer les paramètres recommandés selon les bonnes pratiques suivantes pour votre politique de contrôle d'accès :

- Associez votre politique de déchiffrement à une politique de contrôle d'accès. (Si vous ne faites pas cela, vos politique de déchiffrement et vos règles n'ont aucun effet.)
- Définissez l'action de politique par défaut sur Prévention des intrusions : sécurité et connectivité équilibrées.
- Activer la journalisation

Procédure

Étape 1 Cliquez sur Politiques > Contrôle d'accès.

- Étape 2 Cliquez sur Edit (🖉) à côté d'une politique de contrôle d'accès.
- Étape 3 (Si votre politique de déchiffrement n'est pas encore configurée, vous pouvez le faire ultérieurement.)
 - a) En haut de la page, cliquez sur **Decryption** (déchiffrement), comme le montre la figure suivante.



- b) Dans la liste, cliquez sur le nom de votre politique de déchiffrement.
- c) Cliquez sur Apply.

Default Action

- d) En haut de la page, cliquez sur Save(Enregistrer).
- Étape 4 Dans la liste Default Action (Actions par défaut) située au bas de la page, cliquez sur Intrusion Prevention:
 Balanced Security and Connectivity (Prévention des intrusions : Sécurité et connectivité équilibrées).
 La figure suivante présente un exemple.

Intrusion Prevention: Balanced Security and Connectivit 💌 🖃 📱

Étape 5	Cliquez sur Se connecter ().
Étape 6	Cochez la case Log at End of Connection (Journaliser à la fin de la connexion) et cliquez sur OK.
Étape 7	Cliquez sur Save (enregistrer).

Prochaine étape

Consultez Exemples de Règle de déchiffrement, à la page 9.

Exemples de Règle de déchiffrement

Cette section fournit un exemple de règle de déchiffrement qui illustre nos bonnes pratiques.

Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Trafic vers le préfiltre, à la page 9

PremierRègle de déchiffrement : Ne pas déchiffrer le trafic spécifique, à la page 9 Régles de déchiffrement suivantes : déchiffrer un trafic de test spécifique, à la page 10 Ne pas déchiffrer les catégories, les réputations ou les applications à faible risque, à la page 11 Créer une règle de déchiffrement - nouvelle signature pour les catégories, à la page 13 Dernières Régles de déchiffrement : bloquer ou surveiller les certificats et les versions de protocole, à la page 14

Trafic vers le préfiltre

Le *préfiltrage* est la première phase du contrôle d'accès, avant que le système effectue des évaluations plus exigeantes en ressources. Le préfiltrage est simple, rapide et précoce par rapport à l'évaluation ultérieure, qui utilise des en-têtes internes et possède des capacités d'inspection plus robustes.

En fonction de vos besoins de sécurité et de votre profil de trafic, vous devriez envisager de préfiltrer et, par conséquent, d'exclure de toute politique et inspection les éléments suivants :

- Applications internes courantes telles que Microsoft Outlook 365
- Flux éléphants, comme les sauvegardes de serveur

Sujets connexes

Préfiltrage ou contrôle d'accès Bonnes pratiques de préfiltrage Fastpath

PremierRègle de déchiffrement : Ne pas déchiffrer le trafic spécifique

Le premier règle de déchiffrement dans l'exemple ne déchiffre pas le trafic qui va vers un réseau interne (défini par **intranet**). Les actions liées aux règles**Ne pas déchiffrer** sont mises en correspondance pendant ClientHello de sorte qu'elles sont traitées très rapidement.

Ente	er Description												
R	ules Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ttings								
									+ /	Add Category	+ Add Rule	Q Search I	Rules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Ad	Iministrator Rules												
T	nis category is empty												
Sta	andard Rules												
•	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕝 Do no
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decry Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo	any	any	any	any	🛛 Do ni
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Pho	any	any	any	any	🕑 Do ni
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decr Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	алу	any	3 Protocol Versi	Block
Ro	ot Rules												
TP	his category is empty												

Remarque

Si du trafic va des serveurs DNS internes vers des résolveurs DNS internes (comme des périphériques virtuels Cisco Umbrella), vous pouvez également ajouter des règles **Ne pas déchiffrer** pour ces derniers. Vous pouvez même les ajouter aux politiques de préfiltre si les serveurs DNS internes effectuent leur propre journalisation.

Cependant, nous vous recommandons fortement de *ne pas* utiliser les règles **Ne pas déchiffrer** ou le préfiltre pour le trafic DNS qui va à Internet, comme les serveurs racine Internet (par exemple, les résolveurs DNS internes de Microsoft intégrés à Active Directory). Dans ce cas, vous devez inspecter entièrement le trafic ou même envisager de le bloquer.

ame		Move				
DND internal source network	🗹 Enabled	below rule	v 1			
ction						
Do not decrypt						
Zones Networks VLAN Tag	gs Users A	opplications Ports	Category Certificate DM	N Cert Status	Cipher Suite Version	Logging
ailable Networks C	+		Source Networks (1)		Destination Networks (0)	
Search by name or value			Intranet	Ì	any	
Networks Geolocation						
inv						
Pv4-Private-All-RFC1918						
ny-ipv4						
iny-ipv6						
lefaultgateway						
nsidesubnet						
ntranet			Enter an IP address	Add	Enter an IP address	Add
Pv4-Benchmark-Tests						

Régles de déchiffrement suivantes : déchiffrer un trafic de test spécifique

La règle suivante est *facultative* dans cet exemple; Vous pouvez l'utiliser pour déchiffrer et surveiller des types limités de trafic avant de déterminer s'il faut l'autoriser ou non sur votre réseau.

	Rules Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings								
									+ A	dd Category	+ Add Rule	Q Search F	Rules
	# Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
	Administrator Rules												
	This category is empty												
	Standard Rules												
	1 DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	OD not decry
>	2 Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign
	3 0 Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo	any	any	any	any	OD not decry
	4 Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Pho	any	any	any	any	🕑 Do not decry
	5 Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign
	6 0 Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
	7 0 Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block

Détails de la règle :

ame										
Decrypt test site	Enabled	Move								
tion										
🗃 Decrypt - Resign 🔹 w	vith IntCA		*	C 🔽 R	eplace Key Onl	У				
Zones Networks VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
ategories C		Reputations						Selected Catego	ories (1)	
Search by name or value		Any						Astrology (Any	reputation)	i
Any (Except Uncategorized)										
Uncategorized										
Adult										
Advertisements										
Alcohol										
Animals and Pets										
Arts										
Astrology		Mapply to u	unknown re	putation						
✓ Viewing 1-100 of 125 > >	>									

Ne pas déchiffrer les catégories, les réputations ou les applications à faible risque

Évaluez le trafic sur votre réseau pour déterminer lequel correspondrait aux catégories à faible risque, aux réputations ou aux applications, et ajoutez ces règles avec une action **Ne pas déchiffrer**. Placez ces règles *après* d'autres règles plus spécifiques au mode **Ne pas déchiffrer**, car le système a besoin de plus de temps pour traiter le trafic.

Voici un exemple.

_		ondecrypta	ble Actions	Advanced Se	stungs								
									+ Ac	d Category	+ Add Rule	Q Search F	Rules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Ad	ministrator Rules												
Th	is category is empty												
Sta	indard Rules												
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🖉 Do not i
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not
4	Do not decrypt applications	any	any	any	any	алу	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	🕑 Do not
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decryp Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block

Détails de la règle :

Name Do not decrypt low risk ✓ Enabled Move Action <	
Do not decrypt low risk ✓ Enabled Move Action Cons Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Lo Application Filters C Clear All Filters Available Applications (1483) C Selected Applications and Filters (1) Filters Search by name Q. Search by name Q. Search by name Filters Risks:/Very Low, Low Very Low 538 181 Internet 0 Add to Rule Risks:/Very Low, Low High 139 12300-Filowers 0 123Movies 0 Very High 70 123Movies 0 1246.com 0	
Action	
e Do not decrypt Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Clipher Suite Version L Applications Risks (Any Selected)	
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Clipher Suite Version L Application Filters C Clear All Filters Available Applications (1483) C Selected Applications and Filters (1) Selected Applications and Filters (1) © Search by name © Search by name Filters Risks (Any Selected) Filters Risks: Very Low, Low Filters Very Low 538 1-800-Filowers 0 Add to fluite Risks: Very Low, Low Filters Medium 282 1000mercis 0 123Movies 0 Filters Very High 70 123Movies 0 126.com 0 Filters	
Application Filters C Clear All Filters Available Applications (1483) C Selected Applications and Filters (1) Q. Search by name Q. Search by name Filters Filters Very Low 538 181 Internet Ist Internet Filters Medium 282 1000mercis Ist Internet Filters High 139 12306.cn Ist	jging
Q. Search by name Q. Search by name Filters Risks (Any Selected) 050plus Image: Constraint of the second sec	
• Risks (Any Selected) 050plus • Add to Rule Risks:Very Low, Low · Very Low 538 18.1 Internet • · Low 454 1-800-Flowers • · Medium 282 1000mercis • · High 139 12306.cn • · Very High 70 123Movies • • Business Relevance (Any Selected) 126.com •	
Very Low 538 1&1 Internet Low 454 1-800-Flowers Medium 282 1000mercis High 139 12306.cn Very High 70 123Movies Very Selevance (Any Selected) 126.com	Ì
Low 454 1-800-Flowers Medium 282 1000mercis High 139 12306.cn Very High 70 123Movies v Business Relevance (Any Selected) 126.com	
Medium 282 1000mercis High 139 12306.cn Very High 70 123Movies Business Relevance (Any Selected) 126.com	
High 139 12306.cn Very High 70 123Movies Business Relevance (Any Selected) 126.com	
Very High 70 123Movies v Business Relevance (Any Selected) 126.com	
Business Relevance (Any Selected) 126.com	
Very Low 580 17173.com •	
< < Viewing 1-100 of 1483 > >	
Canal	20140

Régles de déchiffrement et exemple de politique

Cancel

Add Rule		0
Name Do not decrypt applications Control decrypt Do not decrypt	Insert ed Into Category • Standard Rules	v
Application Filters Clear All Filters > Q. pinn X V. Risks (Any Selected) V. Business Relevance (Any Selected) V. Types (Any Selected) V. Categories (Any Selected) V. Tags (1 Selected) V. Tags (1 Selected) V. Tags (1 Selected) V. Tags (1 Selected)	Available Applications (0) C Q. faceb X All apps matching the filter Add to Rule	Selected Applications and Filters (4) Filters Tags:pinned certificate Filter:"faceb" Applications Facebook Face

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications Recommandations pour le contrôle des applications

Créer une règle de déchiffrement - nouvelle signature pour les catégories

Cette rubrique donne un exemple de création d'un règle de déchiffrement avec une action **Déchiffrer** – **Resigner** pour tous les sites sauf les non catégorisés. La règle utilise l'option facultative **Remplacer la clé uniquement**, que nous recommandons toujours avec une action de règle **Déchiffrer - Resigner**.

Avec le **remplacement de la clé uniquement**, l'utilisateur voit un avertissement de sécurité dans le navigateur Web lorsqu'il navigue vers un site qui utilise un certificat autosigné, l'informant qu'il communique avec un site non sécurisé.

En mettant cette règle près du bas de la liste, vous obtenez le meilleur des deux mondes : vous pouvez déchiffrer et éventuellement inspecter le trafic tout en n'affectant pas autant les performances que si vous aviez mis la règle plus tôt dans la politique.

Procédure

Étape 1	Si vous ne l'avez pas encore fait, téléchargez une autorité de certification (CA) interne dans Cisco Secure Firewall Management Center (Objects (objets) > Object Management (gestion des objets), puis des PKI > certification internes).
Étape 2	Cliquez sur Politiques > Contrôle d'accès > Déchiffrement .
Étape 3	Cliquez sur Edit () à côté de votre politique SSL.
Étape 4	Cliquez sur Add Rule (ajouter une règle).
Étape 5	Dans le champ Name, saisissez un nom pour identifier la règle.
Étape 6	Dans la liste Action, cliquez sur Decrypt - Resign (Déchiffrer - Resigner).
Étape 7	Dans la liste avec (avec), cliquez sur le nom de votre autorité de certification interne.
Étape 8	Cochez la case Replace Key Only (remplacement de la clé seulement).

La figure suivante présente un exemple.

Name		Insert		
DR rule sample	Enabled	below rule	▼ 8	
Action				
🚰 Decrypt - Resign	▼ with IntCA	• C	🗸 Replace Key Only	

- Étape 9 Cliquez sur la page à l'onglet Catégorie (Catégorie).
- Étape 10 En haut de la liste des catégories, cliquez sur Any (exceptUncatégorized) (Toutes (sauf non catégorisées)).
- Étape 11 Dans la liste des réputations, cliquez sur Any (Toutes).
- Étape 12 Cliquez sur Add Rule (ajouter une règle).

La figure suivante présente un exemple.

ecrypt all except trusted cat C Enable	ed <u>Move</u>				
on					
Decrypt - Resign vith IntCa	A •	C Replace Key On	ly		
ones Networks VLAN Tags Users	Applications Ports	Category Certificate	DN Cert Status	Cipher Suite Version	Logging
egories C	Reputations			Selected Categories (1)	
Search by name or value	Any			Any (Except Uncategorized) (F	Reputations 1 🗑
ny (Except Uncategorized)	5 - Trusted				
ncategorized	4 - Favorable				
dult	3 - Neutral				
dvertisements	2 - Questionable				
cohol	1 - Untrusted				
nimals and Pets					
ts					
strology	Apply to unknown rep	outation			

Sujets connexes

Objets Autorité de certification interne

Dernières Régles de déchiffrement : bloquer ou surveiller les certificats et les versions de protocole

Les dernières règles de déchiffrement, parce qu'elles sont les plus spécifiques et nécessitent le plus grand nombre de traitements, sont des règles qui surveillent ou bloquent les mauvais certificats et les versions de protocole non sécurisées.

	ules Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings								
-													
									+ /	Add Category	+ Add Rule	Q Search I	lules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Ad	Iministrator Rules												
Т	his category is empty												
Sta	andard Rules												
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕑 Do not d
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	🕑 Do not d
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	🕑 Do not d
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block

Détails de la règle :

Editing Rule - Block bad cert status

Name Block bad cert status			Enabled	Move								
Action												
Block		•										
Zones Networks	VLAN	Tags	Users	Applications Ports	Category		Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any					Revert to Defaults
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any					
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any					
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any					
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any					

Cancel	Save

0

Editing Ru	ule - Block S	SSLv3. TL	S 1.0										0
Name				Move									
Block SSL	v3. TLS 1.0		Enabled	into	Category		▼ St	andard R	ules	¥			
Action													
Block		•											
Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logg	ging
SSL v3.	0												
TLS v1.	0												
TLS v1.	1												
TLS v1.	2												
Revert to	Defaults												
											C	Cancel	ave

Sujets connexes

Exemple : Règle de déchiffrement pour surveiller ou bloquer l'état d'un certificat, à la page 16 Exemple : Règle de déchiffrement pour surveiller ou bloquer des versions de protocole, à la page 18 Exemple facultatif : Règle de déchiffrement pour surveiller ou bloquer le certificat nom distinctif, à la page 20

Exemple : Règle de déchiffrement pour surveiller ou bloquer l'état d'un certificat

Les dernières règles de déchiffrement, parce qu'elles sont les plus spécifiques et nécessitent le plus grand nombre de traitements, sont des règles qui surveillent ou bloquent les mauvais certificats et les versions de protocole non sécurisées. L'exemple de cette section montre comment surveiller ou bloquer le trafic par état de certificat.



Remarque

Utilisez les conditions de règle **Suite de chiffrement** et **version** *uniquement* dans les règles avec l'action de règle **Bloquer** ou **Bloquer avec réinitialisation**. L'utilisation de ces conditions dans des règles avec d'autres actions liées à des règles peut interférer avec le traitement ClientHello du système, ce qui entraîne un rendement imprévisible.

Procédure

Étape 1	Connectez-vous au Cisco Secure Firewall Management Center si vous ne l'avez pas encore fait.
Étape 2	Cliquez sur Politiques > Contrôle d'accès > Déchiffrement.
Étape 3	Cliquez sur Edit (🖍) à côté de votre politique SSL.
Étape 4	Cliquez sur Edit (<i>I</i>) à côté de règle de déchiffrement.
Étape 5	Cliquez sur Add Rule (ajouter une règle).
Étape 6	Dans la boîte de dialogue Add Rule (ajouter une règle), saisissez un nom pour la règle dans le champ Name (Nom).

Étape 7 Étape 8	Cliquez sur Cert Status (État du certificat). Pour chaque état de certificat, vous avez les options suivantes :
	• Cliquez sur Yes (oui) pour vérifier la présence de l'état de ce certificat.
	• Cliquez sur No (non) pour vérifier l'absence de cet état de certificat.
	• Cliquez sur Any (tous) pour ignorer la condition lors de la mise en correspondance de la règle. En d'autres termes, si vous sélectionnez Any (tous), la règle est respectée si l'état du certificat est présent ou absent.
Étape 9	Dans la liste Action , cliquez sur Monitor (surveillance) pour surveiller et journaliser uniquement le trafic qui correspond à la règle ou cliquez sur Block (Bloquer) ou sur Block with Reset (Bloquer avec réinitialisation) pour bloquer le trafic et réinitialiser la connexion (facultatif).
Étape 10	Pour enregistrer les modifications à la règle, au bas de la page, cliquez sur Save (Enregistrer).
Étape 11	Pour enregistrer les modifications apportées à la politique, en haut de la page, cliquez sur Save (Enregistrer).

Exemple

L'organisation fait confiance à l'autorité de certification de l'autorité vérifiée. L'organisation ne fait pas confiance à l'autorité de certification de l'autorité des Spammeurs. L'administrateur du système téléverse le certificat de l'autorité vérifiée et un certificat d'autorité de certification intermédiaire émis par l'autorité vérifiée dans le système. Étant donné que l'autorité vérifiée a révoqué un certificat qu'elle avait précédemment délivré, l'administrateur système téléverse la CRL fournie par l'autorité vérifiée.

La figure suivante montre une condition de règle d'état de certificat qui vérifie si des certificats valides sont valides; ceux émis par une autorité vérifiée, ne figurent pas sur la liste de révocation de certificats et sont toujours entre les dates de validité et de fin de validité. En raison de la configuration, le trafic chiffré avec ces certificats n'est pas déchiffré et inspecté par le contrôle d'accès.



La figure suivante montre une condition de règle d'état de certificat qui vérifie l'absence d'état. Dans ce cas, en raison de la configuration, elle compare le trafic crypté avec un certificat qui n'a pas expiré et surveille ce trafic.

Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any

Dans l'exemple suivant, le trafic correspondrait à cette condition de règle si le trafic entrant utilise un certificat qui a un émetteur non valide, qui est autosigné, a expiré et qu'il s'agit d'un certificat non valide.

Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any

Le graphique suivant illustre une condition de règle d'état de certificat qui correspond si le SNI de la demande correspond au nom du serveur ou si la liste de révocation de certificats n'est pas valide.

Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any

Exemple : Règle de déchiffrement pour surveiller ou bloquer des versions de protocole

Cet exemple montre comment bloquer les protocoles TLS et SSL sur votre réseau qui ne sont plus considérés comme sécurisés, comme TLS 1.0, TLS 1.1 et SSLv3. Il est inclus pour vous donner un peu plus de détails sur le fonctionnement des règles de version de protocole.

Vous devez exclure les protocoles non sécurisés de votre réseau, car ils sont tous exploitables. Dans cet exemple :

- Vous pouvez bloquer certains protocoles à l'aide de la page Version de la règle SSL.
- Comme le système considère SSLv2 comme non déchiffrable, vous pouvez la bloquer à l'aide de l'option Undecryptable Actions (Actions indéchiffrables) dans la politique SSL.
- De même, parce que les TLS/SSL compressés ne sont pas pris en charge, vous devez également les bloquer.

Remarque

Utilisez les conditions de règle Suite de chiffrement et version uniquement dans les règles avec l'action de règle Bloquer ou Bloquer avec réinitialisation. L'utilisation de ces conditions dans des règles avec d'autres actions liées à des règles peut interférer avec le traitement ClientHello du système, ce qui entraîne un rendement imprévisible.

Procédure

Étape 1	Cliquez sur Politiques > Contrôle d'accès > Déchiffrement .
Étape 2	Cliquez sur Edit () à côté de votre politique SSL.
Étape 3	Cliquez sur Edit () à côté de règle de déchiffrement.
Étape 4	Cliquez sur Add Rule (ajouter une règle).
Étape 5	Dans le champ Name (Nom) de la boîte de dialogue Add Rule (Ajouter une règle), saisissez un nom pour la règle.
Étape 6	Dans la liste Action, cliquez sur Block (Bloquer) ou sur Block with reset (Bloquer avec réinitialisation).
Étape 7	Cliquez sur Version (version).
Étape 8	Cochez les cases des protocoles qui ne sont plus sécurisés, comme SSL v3.0 , TLS 1.0 et TLS 1.1 . Décochez les cases des protocoles toujours considérés comme sécurisés.
	La figure suivante présente un exemple.

AFT168												
	-2 TIC 1 0		Trabled	Maria								
BIOCK SSL	v3. ILS 1.0		Enabled	Move								
ction												
Block		•										
Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Loggin
SSL v3.	0											
TLS v1.	0											
TLS v1.	1											
TLS v1.	2											
Revert to	Defaulte											
Novent to I	Deraulta											
												_
											Can	cel Sav

Étape 9 Choisissez d'autres conditions de règle si nécessaire. Étape 10 Cliquez sur Save (enregistrer).

Exemple facultatif : Règle de déchiffrement pour surveiller ou bloquer le certificat nom distinctif

Cette règle est incluse pour vous donner une idée sur la façon de surveiller ou de bloquer le trafic en fonction du nom distinctif du certificat de serveur. Elle est incluse pour vous donner un peu plus de détails.

Le nom distinctif peut consister en un code de pays, un nom usuel, l'organisation et l'unité organisationnelle, mais consiste généralement en un nom usuel uniquement. Par exemple, le nom usuel dans le certificat pour https://www.cisco.com est cisco.com. (Cependant, ce n'est pas toujours aussi simple; Conditions de règles de noms distinctifs (DN) montre comment trouver des noms communs.)

La partie nom d'hôte de l'URL dans la demande du client constitue l'indication SNI (Server Name Indication). Le client spécifie le nom d'hôte auquel il souhaite se connecter (par exemple, auth.amp.cisco.com) en utilisant l'extension SNI dans l'établissement de liaison TLS. Le serveur sélectionne ensuite la clé privée et la chaîne de certificats correspondantes, qui sont nécessaires pour établir la connexion tout en hébergeant tous les certificats sur une seule adresse IP.

Procédure

Étape 1	Cliquez sur Politiques > Contrôle d'accès > Déchiffrement.
Étape 2	Cliquez sur Edit () à côté de votre politique SSL.
Étape 3	Cliquez sur Edit () à côté de règle de déchiffrement.
Étape 4	Cliquez sur Add Rule (ajouter une règle).
Étape 5	Dans le champ Name (Nom) de la boîte de dialogue Add Rule (Ajouter une règle), saisissez un nom pour la règle.
Étape 6	Dans la liste Action, cliquez sur Block (Bloquer) ou sur Block with reset (Bloquer avec réinitialisation).
Étape 7	Cliquez sur DN .
Étape 8	Recherchez les noms distinctifs que vous souhaitez ajouter parmi les noms distinctifs disponibles , comme suit :
	• Pour ajouter un objet de nom unique à la volée, que vous pouvez ensuite ajouter à la condition, cliquez
	sur Ajouter (+) au-dessus de la liste des noms distinctifs (DN) disponibles .
	• Pour rechercher des objets de nom unique et des groupes à ajouter, cliquez sur l'invite Search by Name or value (Rechercher par nom ou par valeur) au-dessus de la liste DN disponibles , puis saisissez le nom de l'objet ou une valeur de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.
Étape 9	Pour sélectionner un objet, cliquez dessus. Pour sélectionner tous les objets, cliquez avec le bouton droit, puis sélectionnez tout.
Étape 10	Cliquez sur Add to Subject (Ajouter au sujet) ou Add to Issuer (Ajouter à l'émetteur).
	Astuces Vous pouvez également faire glisser et déposer les objets sélectionnés.
Étape 11	Ajoutez les noms communs (CN) ou noms uniques littéraux que vous souhaitez définir manuellement. Cliquez sur l'invite Saisissez le DN ou CN sous la liste des DN des sujets ou des DN de l'émetteur ; saisissez un nom usuel ou un nom distinctif et cliquez sur Add (Ajouter).
	Bien que vous puissiez ajouter un nom distinctif ou usuel à l'une ou l'autre des listes, il est plus courant de les ajouter à la liste des noms distinctifs des sujets .

L

Étape 12 Ajoutez la règle ou continuez à la modifier.

Étape 13 Lorsque vous avez terminé, pour enregistrer les modifications à la règle, cliquez sur **Save** (Enregistrer) au bas de la page.

Étape 14 Pour enregistrer les modifications à la politique, cliquez sur Save (Enregistrer) en haut de la page.

Exemple

La figure suivante montre une condition de règle de nom distinctif recherchant les certificats émis pour bonneboulangerie.exemple.com ou émis par bonca.exemple.com. Le trafic chiffré avec ces certificats est autorisé, sous réserve du contrôle d'accès.

Subject DNs (1)		Issuer DNs (1)	
GoodBakery	Ĩ	CN=goodca.example.com	Ĩ
Enter DN or CN	Add	Enter DN or CN	Add

Paramètres de Règle de déchiffrement

Comment configurer les paramètres de bonnes pratiques pour votre règles de déchiffrement?

règle de déchiffrement : Activez la journalisation pour chaque règle, à l'exception de celles avec une action de règle **Ne pas déchiffrer**. (C'est à vous de décider; si vous souhaitez voir les informations sur le trafic qui n'est pas déchiffré, activez également la journalisation pour ces règles.)

Procédure

Étape 1	Cliquez sur Politiques > Contrôle d'accès > Déchiffrement .
Étape 2	Cliquez sur Edit () à côté de votre politique SSL.
Étape 3	Cliquez sur Edit () à côté de règle de déchiffrement.
Étape 4	Cliquez sur l'onglet Logging (Journalisation).
Étape 5	Cliquez sur Journaliser à la fin de la connexion.
Étape 6	Cliquez sur Save (enregistrer).

Étape 7 En haut de la page, cliquez sur Save(Enregistrer).

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.