Contenu

Introduction

Ce document aborde les questions fréquemment posées (Foire aux questions) au sujet du Commutateur de services de contenu (CSS) de Cisco.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Q. Où peux-je trouver le MIB pour le CSS ?

A. Le MIB est déjà sur le CSS. Vous pouvez considérer le CSS un agent dans la structure du réseau de Protocole SNMP (Simple Network Management Protocol). Tout que vous devez faire est de configurer les paramètres SNMP sur le CSS. Référez-vous au document configurant le pour en savoir plus de Protocole SNMP (Simple Network Management Protocol).

Q. Quel est le nombre maximal de keepalives à base de script que le CSS prend en charge ?

A. Le nombre maximal de keepalives à base de script que le CSS prend en charge est 255. Référez-vous aux *nouvelles caractéristiques dans la version de logiciel 5.00* sections de la note en version pour le commutateur de services satisfaits de gamme Cisco 11000.

Q. Comment est-ce que je peux effacer ou retirer les fichiers image mémoire ?

A. Émettez la **principale** commande **claire**. La commande est disponible dans la version 5.00 et ultérieures de logiciel CSS, mettent au point dedans le mode. La syntaxe est la suivante :

```
css150(debug)#clear core filename CR
```

Q. Où peux-je trouver des traductions des messages de log ?

A. Pour des traductions des messages de log, référez-vous aux messages de log de document.

Q. Y a-t-il une commande qui contrôle combien de fois les pairs envoient des états de chargement entre eux ?

A. Vous pouvez utiliser la commande d'**intervalle de dn-pair**. Il y a également des commandes supplémentaires que vous pouvez configurer localement afin de réaliser une mesure plus rapide du chargement local :

- **ageout-temporisateur** ? Place la période (en quelques secondes) de l'ageout des informations éventées de chargement.
- **désinstallation-temporisateur** ? Fixe le délai prévu maximum (en quelques secondes) que le système attend d'envoyer à un état de désinstallation.

Q. Font-elles la modification de clés de licence avec des versions de code ?

A. Non, des clés de licence ne changent pas avec des versions de code.

Q. J'ai perdu ma clé de licence. Queest-ce que je fais ?

A. Envoyez un email avec le numéro de série de votre CSS à licensing@cisco.com. La

commande de **version** affiche le pack de fonctionnalités, mais pas la clé de licence.

Q. Quel est le délai par défaut pour la conservation d'une entrée dans une table Rémanente ?

A. À moins que vous utilisiez le Rémanent-inact-**délai d'attente de** commande, il n'y a aucun délai par défaut. La table Rémanente est gardée sur une base FIFO (32,000 ou 128,000 entrées, selon le type de périphérique et la mémoire disponibles), ou jusqu'à la réinitialisation du CSS.

Q. Comment est-ce que je configure le masque Rémanent afin de couvrir des demandes d'un méga-proxy comme America Online (AOL) ?

A. Si une application exige d'un utilisateur d'être coincé pour la vie entière de la session, considérez une couche 3 Rémanente. Une couche 3 Rémanente colle un utilisateur à un serveur sur la base de l'adresse IP d'utilisateur. Le CSS a une table Rémanente de 32,000, ainsi il signifie que quand 32,000 utilisateurs simultanés se trouvent sur le chantier, les bouclages de table et les premiers utilisateurs deviennent « décollés ». Cependant, le volume de votre site peut être tel que vous avez plus de 32,000 utilisateurs à la fois. Ou un grand pourcentage de vos clients peut être livré à vous par un méga-proxy. Dans des ces cas, considérez l'utilisation d'une méthode Rémanente différente (telle que le Témoin, le cookieurl, ou l'URL) ou une augmentation de votre masque Rémanent. Le masque Rémanent par défaut est 255.255.255.255, ainsi il signifie que chaque entrée dans la table Rémanente est une adresse IP individuelle. Certains des méga-proxys ont une situation dans lesquels l'utilisateur au cours de la vie d'une session utilise plusieurs différentes adresses IP dans une plage d'adresses. Cette situation fait être bloqué certaines des connexions TCP à un serveur, et peut faire être bloqué d'autres connexions à un serveur différent pour la même transaction. Un résultat peut être la perte de quelques éléments du panier d'épicerie. Si vous ne pouvez pas utiliser une des méthodes plus avancées de collage, utilisez le masque Rémanent de 255.255.240.0 quand votre base de client est livré par un de ces méga-proxys.

Q. Pourquoi y a-t-il aucune option pour Rémanent quand j'utilise le Protocole SSL (Secure Socket Layer) d'avancé-équilibre ?

A. le SSL d'Avancé-équilibre est identique que le SSL Rémanent.

Q. Quel type de cryptage est-ce que le Protocole CAPP (Content and Application Peering Protocol) ou l'application Protocol scrutant (APP) utilise ?

A. Par défaut, CAPP n'utilise aucun cryptage. Vous pouvez configurer la session d'APP pour utiliser le Message Digest 5 (MD5). Le type de cryptage doit être identique sur les deux pairs pour que la session d'APP monte.

Q. Que le message « d'ARP gratuit » signifie-t-il ?

A. Quand le commutateur de sauvegarde ne détecte pas une pulsation du commutateur principal dans 3 secondes, les transitions de sauvegarde de commutateur à devenir le maître et envoie un message « d'ARP gratuit ». Le message indique une fiche d'envoi de Protocole ARP (Address Resolution Protocol) du nouveau commutateur principal. Le message contient l'adresse MAC du commutateur principal en cours. L'ARP gratuit est activé par la commande d'**ip gratuitous-arps** en mode de configuration globale. Il ne peut pas être activé sur une interface unique et la bloquer sur

d'autres interfaces.

Q. Comment est-ce que je synchronise des configurations au-dessus du CSS en mode de Basculement ?

A. Afin de synchroniser des configurations dans la version de logiciel 4.0, utilisez la commande de **sync de config de validation**. Afin de synchroniser des configurations en code de la version de logiciel 3.10, vous devez employer le FTP afin de déplacer la configuration d'un commutateur à l'autre. Afin de synchroniser des configurations dans les versions de logiciel 6.x et 7.x codez, utilisez le **commit_redundancy de** commande pour la Redondance d'active/standby ou de case-à-case. Ou vous pouvez utiliser le **commit_vip_redundancy de** commande pour la Redondance virtuelle IP (VIP) /interface. Vous pouvez employer le **commit_redundancy de script d'exposition de** commande afin de visualiser dans l'en-tête du script les options de ligne de commande disponibles pour le script de **commit_redundancy**. Le même s'applique à la commande de **commit_vip_redundancy**.

Q. Quelles configurations est-ce que je devrais utiliser dans un programme de terminal ?

A. Utilisez ces configurations :

- 9 600 bauds
- 8 bits
- Aucune parité
- 1 bit d'arrêt
- Aucun contrôle de flux

Q. Y a-t-il une manière de reprogrammer l'adresse MAC sur un CSS ?

A. Oui, il y a une manière.

Remarque: Vous pouvez trouver l'adresse MAC et le numéro de série au dos de l'unité.

Terminez-vous ces étapes afin de reprogrammer le numéro de série et l'adresse MAC. Cet exemple est pour une adresse MAC dans le châssis CS800 :

1. Ouvrez le **diagnostic monitor hors ligne (ODM)**.
2. Dans le menu principal ODM, **shift-T de** presse afin d'atteindre le menu de technicien.
3. Choisissez **1** (configurez).
4. Choisissez **5** (placez les informations de fabrication).
5. Choisissez **2** (placez les informations de fabrication du fond de panier).
6. Suivez la demande et saisissez les données qui correspondent, comme le numéro de série et l'adresse MAC. Vous pouvez trouver ces données sur le dessus du châssis CS800.
7. Redémarrez la case.

Q. Comment est-ce que j'apporte une modification prompte permanente sur le CSS ?

A. Ouvrez une session dans la case CSS comme utilisateur Fred, et utilisez vos qualifications de

procédure de connexion. Afin d'apporter une modification prompte permanente, émettez cette commande :

```
Css100#prompt Redsox <cr> Redsox#
```

Émettez cette commande de sauvegarder la modification :

```
Redsox#save_profile
```

Cette commande enregistre le profil utilisateur de sorte que chaque fois que l'utilisateur ouvre une session, le CSS utilise la même demande. Cette action, semblable de utiliser du **?. ?** les fichiers de ressources dans l'UNIX, crée un seul profil pour chaque utilisateur.

Quand vous retournez au CSS et à la procédure de connexion comme admin, la demande ne reflète pas ces modifications. Les modifications sont utilisateur-particularité, ainsi vous devez émettre les commandes **promptes** et **save_profile** pour chaque utilisateur qui veut faire refléter la demande la nouvelle modification.

Q. Quelle est la différence entre l'éclair opérationnel et verrouillé ?

A. Cet exemple affiche les différents types d'éclair que la commande de **show version** affiche :

```
CSS150-2#show versionVersion:              ap0401049s (4.01 Build 49) Flash (Locked):        3.10 Build
33!--- This image is the original image that was installed on the CSS. !--- The image serves as a backup
in the event that the CSS is not able !--- to boot from the operational Flash because of an image
corruption.Flash (Operational):   5.00 Build 10-!--- This is the image that currently runs on the CSS.
Type: PRIMARY Licensed Cmd Set(s): Standard Feature Set Enhanced Feature Set SSH Server
```

Q. Pourquoi y a-t-il des différentes versions d'éclair ?

A. L'éclair verrouillé affiche la version de logiciel qui a été initialement installé sur ce CSS. La version demeure la même et sert seulement de sauvegarde. La version dans l'éclair opérationnel est la version qui fonctionne actuellement sur ce CSS.

Q. Pourquoi est-ce que je ne peux pas accéder au port de gestion du CSS d'un port distant ?

A. Dans toutes les versions de Cisco WebNS qui sont plus tôt que 5.03, le port de gestion n'est pas une interface routable. Dans la version 5.03, vous pouvez ajouter une passerelle par défaut au port de gestion afin de faire au port une interface routable.

Q. Le support technique de Cisco prend en charge-il le Keepalives de script personnalisé que le client écrit ?

A. Non, support technique de Cisco ne prend en charge pas les scripts de keepalive qu'un client écrit.

Q. Comment est-ce que je retire les fichiers image mémoire à partir du disque CSS ?

A. Si, après que vous émettiez la commande de **noyau d'exposition**, vous trouvez une liste de fichiers image mémoire, vous pouvez retirer les fichiers dans une de deux manières :

Remarque: La méthode que vous utilisez dépend de la version du code.

- CSS50-1(config)#**llama** *!--- This command places the CSS in debug mode.* CSS50-1(debug)#**clear core** corefilename

ou

- CSS50-1(config)#**llama** *!--- This command places the CSS in debug mode.*CSS50-1(debug)#**dir c:/Core/?** *!--- This command lists the names of all the core !--- files in the c:/Core directory.*CSS50-1(debug)#**ap_file delete c:/Core/** corefilename *!--- This command deletes the specified core file.*

Q. Quand j'authentifie à un serveur de RAYON avec mon CSS, j'obtiens le "RADIUS-4 : Échec de l'authentification de RAYON avec le message d'erreur de code de raison 2". Que signifie ce message ?

A. Ce message d'erreur indique que la réponse a atteint le CSS et il y a un problème. Un manque de placer l'attribut de type de service à administratif sur le serveur de RAYON peut être la cause du problème. Vérifiez le serveur de RAYON et vérifiez les attributs de type de service.

Q. Combien grande est la table Rémanente, et ce qui entraîne la suppression des entrées ?

A. Le CSS a (qui dépend du type de modèle et de la mémoire disponibles) une table 32,000 ou 128,000 Rémanente qui contient des entrées pour le **source-ip Rémanent** et le Protocole SSL (Secure Socket Layer) Rémanent. La table Rémanente ne met pas à jour les Témoins Rémanents sur le CSS. La suppression des entrées dans la table Rémanente sur le CSS se produit dans ces situations :

- Par défaut, avec une méthode FIFO. Les entrées demeurent dans la table jusqu'aux 32,000 ou aux 128,000 que la mémoire tampon est pleine. À ce moment, toutes les nouvelles entrées font retirer le CSS une entrée sur la base du FIFO.
- minutes de Rémanent-inact-**délai d'attente**. Dans une règle de contenu, vous pouvez spécifier la temporisation d'inactivité par laquelle le CSS retire une entrée Rémanente, comme indiqué dans cet exemple :CSS50-1(config)#**llama** *!--- This command places the CSS in debug mode.*CSS50-1(debug)#**dir c:/Core/?** *!--- This command lists the names of all the core !--- files in the c:/Core directory.*CSS50-1(debug)#**ap_file delete c:/Core/** corefilename *!--- This command deletes the specified core file.***Remarque:** Le CSS rejette la prochaine demande Rémanente dans un cas quand tous ces éléments sont vrais :Le paramètre de Rémanent-inact-**délai d'attente** est utilisé.Le CSS a rempli mémoire tampon 32,000 ou 128,000.Aucune entrée n'est environ au délai d'attente.
- Règle de contenu. Avec la suspension et la réactivation d'une règle de contenu, la suppression des entrées de table Rémanentes qui s'appliquent à cette règle se produit.

Le pour en savoir plus, se rapportent au document configurant des paramètres Rémanents pour des règles de contenu.

Q. Comment est-ce que je peux prendre un service hors de la rotation ?

A. Avec la configuration de la règle de contenu (la couche 3, la couche 4, ou posez 5) comme base, le CSS se comporte différemment avec la suspension manuelle d'un service, qui prend un serveur hors service. Beaucoup de fois, les développeurs web doivent temporairement interrompre un service et apporter des modifications de gestion aux pages Web. Puisque ces modifications de Web peuvent se produire pendant des heures de production, vous ne voulez pas détruire les connexions qui existent au service ou aux services quand la suspension manuelle de

service se produit. Exécutez les mises à jour à un service pendant la suspension manuelle de service.

Cet exemple affiche la couche 5 témoin, la couche 4, et pose 3 règles de contenu :

```
CSS50-1(config)#llama                                          !--- This command places the
CSS in debug mode.CSS50-1(debug)#dir c:/Core/?                                  !--- This command
lists the names of all the core !--- files in the c:/Core directory.CSS50-1(debug)#ap_file delete
c:/Core/ corefilename    !--- This command deletes the specified core file.
```

Le CSS détourne les connexions qui existent quand les règles de contenu sont la couche 3 ou la couche 4. Si la suspension d'un service selon une règle de contenu de la couche 3 ou de la couche 4 se produit, le CSS détourne n'importe quelle connexion qui existe et en avant tout le TCP ultérieur demande au service actif selon cette règle de contenu respective.

Avec la suspension manuelle d'un service qui réside selon une règle de contenu de la couche 5, le CSS remet à l'état initial tout ou une partie de connexions qui associent avec ce service.

Q. La pièce de proximité de réseau de la fonction améliorée est-elle placée ?

A. Les caractéristiques de proximité de réseau ne sont pas une partie de la fonction améliorée réglée et exigent une licence supplémentaire. Si vous essayez d'émettre des commandes de **proximité** sur le CSS sans permis approprié, vous recevez ce message d'erreur :

```
CSS50-1(config)#proximity db 0 tier1                          ^ %% Invalid License to execute
command. This command belongs to the Proximity Database.  Refer to the user manual or contact Cisco
Systems, Inc for further information concerning license keys.
```

Afin d'acheter un permis, voir le votre revendeur local Cisco. Si vous achetiez un permis et avez besoin d'un remplacement, envoyez un email à licensing@cisco.com.

Q. Quels détails la commande DOS d'exposition fournit-elle ?

A. Le Cisco CSS peut afficher des détails au sujet des événements d'attaque les plus récents, qui incluent :

- Adresses IP de source et de destination
- Le type d'événement
- Occurrences totales

Si plusieurs les attaques se produisent avec le mêmes type et adresse source et de destination du Déni de service (DOS), il y a une tentative de les fusionner en tant qu'un événement. Cette fusion réduit l'affichage des événements.

Émettez la commande **DOS d'exposition** afin d'afficher :

- Le nombre total d'attaques puisque le démarrage du CSS
- Les types d'attaques et le nombre maximal de ces attaques par seconde
- La première et dernière occurrence d'une attaque

Cet exemple affiche la sortie de la commande **DOS d'exposition** :

```
CSS50-1#show dosDenial of Service Attack Summary: Total Attacks: 0 SYN Attacks:
0 Maximum per second:                  0 LAND Attacks:                        0 Maximum per second:
0 Zero Port Attacks:                   0 Maximum per second:                  0 Illegal Src Attacks:
0 Maximum per second:                  0 Illegal Dst Attacks:                 0 Maximum per second:
0 Smurf Attacks:                       0 Maximum per second:                  0   No attacks detected
```

Cette liste fournit une brève description de chacun des champs que la commande affiche :

- `Attaques totales` ? Le nombre total d'attaques DoS qui ont été détectées puisque le démarrage de la case. Vous pouvez trouver une description du type d'attaques qui apparaissent dans la liste, avec le nombre d'occurrences, ci-dessous.
- `Attaques de synchronisation` ? Les connexions TCP qu'une source initie mais qui ne sont pas suivies avec une trame d'accusé de réception afin de se terminer la prise de contact à trois voies de TCP.
- `Attaques de TERRE` ? Tous paquets qui ont la source et les adresses de destination identiques. Le CSS ne permet pas aux adresses IP internes pour être l'adresse source d'un écoulement. En outre, le CSS ne permet pas à la source et aux adresses de destination des trames pour être égal.
- `Attaques zéro de port` ? Vues qui contiennent le TCP de source ou de destination ou les ports de Protocole UDP (User Datagram Protocol) qui sont égaux à zéro.**Remarque:** Un logiciel plus ancien de SmartBits peut envoyer les trames qui contiennent la source ou les destinations port égalent à zéro. Le CSS se connecte les comme attaques DoS et relâche ces trames.
- `Attaques illégales de Src` ? Adresses sources illégales.
- `Attaques illégales de Dst` ? Adresses de destination illégales.
- `Attaques smurf` ? Pings avec une adresse de destination d'émission. Le CSS ne permet pas des diffusions dirigées par défaut. `Une attaque smurf` utilise un écho de Protocole ICMP (Internet Control Message Protocol) à une adresse d'émission. Le CSS peut bloquer l'accès aux ports d'écho d'UDP par l'intermédiaire du Listes de contrôle d'accès (ACL).
- `Maximum par seconde` ? Le nombre maximal d'événements par seconde. Employez les maximum-événement-par-deuxièmes informations pour placer des valeurs seuil de déroutement de Protocole SNMP (Simple Network Management Protocol).**Remarque:** Le nombre maximal d'événements par seconde est le maximum par Small Form Factor enfichable (SFP). Pour un CSS 11800, par exemple, qui peut avoir jusqu'à quatre SFP, le débit maximum par seconde peut être aussi élevé que quatre fois le nombre qui apparaît dans l'affichage.**Remarque:** Une autre Foire aux questions demande si vous pouvez désactiver la protection DOS sur le CSS. La réponse est non. La protection DOS fait partie du processus d'admission d'écoulement. L'intention de protection DOS est de protéger les ressources dans le CSS aussi bien que les serveurs derrière le CSS. Le DOS n'est pas un élément configurable. L'intention est pour que le DOS soit transparent quand les protocoles fonctionnent correctement. La procédure d'installation d'écoulement implique profondément les caractéristiques DOS. L'aide de caractéristiques le CSS économisent des ressources en chemin rapide et protègent les périphériques que le CSS atteint. Les caractéristiques sont toujours présentes dans la version de logiciel 3.0 et plus tard.

Considérez également l'installation de certains déroutements SNMP pour la détection des attaques DoS possibles. Les déroutements disponibles sont :

- **entreprise de déroutement-type SNMP** ? Afin d'activer des déroutements d'entreprise SNMP et configurer des types de déroutement, émettez la commande d'**entreprise de déroutement-type SNMP**. N'émettez l'**aucune** commande d'**entreprise de déroutement-type SNMP** afin de désactiver tous les déroutements. Vous devez activer des déroutements d'entreprise avant que vous configuriez une option de déroutement d'entreprise. Vous pouvez permettre au CSS de générer des déroutements d'entreprise quand les événements d'attaque DoS se produisent, une procédure de connexion échoue, ou un état de transitions de service CSS.

- ***dos_attack_type*** ? Génère des déroutements d'entreprise SNMP quand un événement d'attaque DoS se produit. Une génération de déroutement se produit chaque seconde où le nombre d'attaques pendant le cela dépasse en second lieu le seuil pour la configuration d'attaque-type DOS. Les options sont :**DOS-illégal-attaque** ? Génère des déroutements pour des adresses illégales, source ou destination. Les adresses illégales sont :Adresses sources de bouclageAdresses sources d'émissionAdresses de destination de bouclageAdresses sources multicastsDes adresses sources ces vous possédezLe seuil par défaut de déroutement pour ce type d'attaque est un par seconde.**DOS-terre-attaque** ? Génère des déroutements pour les paquets qui ont la source et les adresses de destination identiques. Le seuil par défaut de déroutement pour ce type d'attaque est un par seconde.**DOS-ping-attaque** ? Génère des déroutements quand le nombre de pings dépasse la valeur seuil. Le seuil par défaut de déroutement pour ce type d'attaque est 30 par seconde.**Remarque:** Cette option ne dépiste pas des attaques DoS de pings de la mort.**DOS-smurf-attaque** ? Génère des déroutements quand le nombre de pings avec une adresse de destination d'émission dépasse la valeur seuil. Le seuil par défaut de déroutement pour ce type d'attaque est un par seconde.**DOS-synchronisation-attaque** ? Génère des déroutements quand le nombre de connexions TCP qu'une source initie mais qui ne sont pas suivis avec une trame d'accusé de réception pour se terminer la prise de contact à trois voies de TCP dépasse la valeur seuil. Le seuil par défaut de déroutement pour ce type d'attaque est 10 par seconde.

Q. Est-ce que je peux arrêter la caractéristique de protection du Déni de service (DOS) sur la ligne CSS des Commutateurs ?

A. Dans la ligne actuelle de logiciel pour le CSS (Cisco WebNS), il n'y a aucune option de désactiver la configuration de protection DOS.

Q. Est-ce que je peux arrêter les compteurs de protection du Déni de service (DOS) ?

A. Il n'y a aucune option de désactiver les compteurs qui se connectent des attaques DoS/SYN.

Remarque: Pour plus d'informations sur des attaques DOS et de synchronisation, voyez que la réponse à la Foire aux questions quels détails fait la commande **DOS d'exposition** fournissez ?.

Q. Comment est-ce que j'utilise des plages de port dans les Listes d'accès ?

A. L'utilisation des plages de port dans des aides d'une liste de contrôle d'accès (ACL) simplifient le nombre d'ACLs que vous configurez, donné une situation dans laquelle vous voulez bloquer l'accès client pour des ports de Protocole UDP (User Datagram Protocol) certain TCP/. Par exemple, supposez que vous voulez bloquer les ports 20 à 23 pour tous les utilisateurs qui entrent dans la case de l'extérieur de votre réseau. D'abord, supposez que le réseau extérieur ou le côté public du CSS est dans le VLAN 2. Supposez également que l'interne ou le côté serveur du réseau est sur le VLAN 1. La configuration d'ACL est :

```
CSS50-1#show dosDenial of Service Attack Summary: Total Attacks: 0 SYN Attacks:
0 Maximum per second:                  0 LAND Attacks:                        0 Maximum per second:
0 Zero Port Attacks:                   0 Maximum per second:                  0 Illegal Src Attacks:
0 Maximum per second:                  0 Illegal Dst Attacks:                 0 Maximum per second:
0 Smurf Attacks:                       0 Maximum per second:                  0   No attacks detected
```

Informations connexes

- Fin d'annonce de vente pour la gamme 11000 de Cisco CSS
- Bulletins de Commutateurs de services de contenu de la gamme Cisco CSS 11000
- Soutien technique de Commutateurs de services satisfaits de gamme 11000 CSS
- Centre de logiciel (téléchargements) - Réseau de diffusion de contenu (enregistrés seulement
- Support et documentation techniques - Cisco Systems