Contenu

Introduction

Ce document affiche comment employer la caractéristique faite sur commande du module de langage de description de paquet (PDLM) du Reconnaissance d'application fondée sur le réseau (NBAR) pour apparier sur le trafic non classifié ou pour trafiquer qui n'est pas spécifiquement pris en charge comme déclaration de match protocol.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Méthodologies de base de QoS
- Compréhension de base de NBAR

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 12.2(2)T de Cisco IOS®
- Routeur Cisco 7206

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Compréhension de la coutume PDLM

NBAR prend en charge un grand choix de charge statique et d'états de protocole. PDLMs permettent le nouveau support de protocole pour NBAR sans condition requise d'une mise à jour et d'un routeur rechargé de release IOS. Les releases ultérieures IOS incorporent le soutien de ces nouveaux protocoles.

La coutume PDLM te permet pour tracer des protocoles au Protocole UDP (User Datagram Protocol) et aux ports TCP statiques pour les protocoles qui ne sont pas actuellement pris en charge dans NBAR avec une déclaration de match protocol. En d'autres termes, il étend ou améliore la liste de protocoles identifiés par NBAR.

Voici les étapes à ajouter la coutume PDLM à votre routeur.

1. Localisez et téléchargez le NBAR PDLM de la page de téléchargement du logiciel (clients enregistrés seulement) en téléchargeant le **fichier custom.pdlm.**
2. Chargez le PDLM sur un bloc de mémoires de mémoire flash, tel que la carte PCMCIA dans les emplacements 0 ou 1, utilisant la commande ci-dessous.`7206-15(config)# ip nbar pdlm slot0:custom.pdlm`
3. Vérifiez le soutien des protocoles faits sur commande utilisant le **show ip nbar port-map | incluez la** commande **faite sur commande** (affichée ci-dessous) ou la commande de **show ip nbar pdlm**.
```
7206-16# show ip nbar port-map | include custom port-map custom-01            udp
0 port-map custom-01            tcp 0 port-map custom-02            udp 0 port-map custom-
02            tcp 0 port-map custom-03            udp 0 port-map custom-03            tcp 0
port-map custom-04            udp 0 port-map custom-04            tcp 0 port-map custom-05
udp 0 port-map custom-05            tcp 0 port-map custom-06            udp 0 port-map
custom-06            tcp 0 port-map custom-07            udp 0 port-map custom-07
tcp 0 port-map custom-08            udp 0 port-map custom-08            tcp 0 port-map
custom-09            udp 0 port-map custom-09            tcp 0 port-map custom-10
udp 0 port-map custom-10            tcp 0
```
4. Assignez les ports aux protocoles faits sur commande utilisant l'**ip nbar port-map coutume-DE X/Y {TCP|** commande. Par exemple, pour apparier sur le trafic au port TCP 8877, employez la commande du **TCP 8877 de l'ip nbar port-map custom-01**.

Classification des ports « non classifiés »

Selon votre trafic réseau, vous pouvez devoir utiliser des mécanismes de classification spéciale dans NBAR. Une fois que vous classifiez ce trafic, vous alors pouvez utiliser la coutume PDLM et apparier les nombres d'UDP et de port TCP à une port-MAP faite sur commande.

Par défaut, les mécanismes non classifiés NBAR ne sont pas activés. **Les non classifié-port-stats nbar de show ip** commandent des retours le message d'erreur suivant :

```
d11-5-7206-16# show ip nbar unclassified-port-stats Port Statistics for unclassified packets is
not turned on.
```

Sous des circonstances soigneusement commandées, utilisez l'**IP de débogage les non classifié-port-stats que nbar** commandent de configurer le routeur pour commencer le cheminement sur quels ports que les paquets arrivent. Utilisez alors le **show ip les non classifié-port-stats que nbar** commandent de vérifier l'information collectée. La sortie affiche maintenant un histogramme des ports les plus utilisés généralement.

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations

importantes sur des commandes de debug. Les commandes **nbar d'IP de débogage** devraient être activées seulement sous des circonstances soigneusement commandées.

Si ces informations ne sont pas suffisantes, vous pouvez activer la capacité de capture, qui fournit une méthode facile de capturer des tracés de paquets de nouveaux protocoles. Utilisez les commandes de **débogage** suivantes, comme affiché ci-dessous.

```
debug ip nbar filter destination_port tcp XXXX debug ip nbar capture 200 10 10 10
```

La première commande définit les paquets en lesquels vous êtes intéressé pour la capture. La deuxième commande met NBAR dans le mode de capture. Les arguments de l'ordre de **capture** sont comme suit :

- Nombre d'octets aux capturer par paquet.
- Nombre de commencer des paquets pour capturer, en d'autres termes, combien de paquets pour capturer après le paquet de synchronisation TCP/IP.
- Nombre de paquets finaux aux capturer, en d'autres termes, de combien de paquets à la fin de l'écoulement pour lequel l'espace devrait être réservé.
- Nombre de paquets totaux aux capturer.

Remarque: Spécifiant commencer et les paramètres finaux de paquet capture seulement les paquets appropriés dans un long écoulement.

Utilisez l'ordre **nbar de capture de show ip** de visualiser l'information collectée. Par défaut, le mode de capture attend un paquet de synchronisation pour arriver et puis commence capturer les paquets sur cet écoulement bidirectionnel.

Blocage de Gnutella avec la coutume PDLM

Regardons un exemple de la façon utiliser la coutume PDLM. Nous utilisons Gnutella comme le trafic que nous voulons classifier et puis appliquer une stratégie QoS qui bloque ce trafic.

Gnutella utilise six ports TCP réputés - 6346, 6347, 6348, 6349, 6355, et 5634. D'autres ports peuvent être détectés comme des puanteurs sont reçues. Si les utilisateurs spécifient d'autres ports pour l'usage dans le partage de fichier de Gnutella, vous pouvez ajouter ces ports à votre déclaration faite sur commande de match protocol.

Voici les étapes à créer une stratégie de service QoS que les correspondances en fonction et relâche le trafic de Gnutella.

1. Comme remarquable ci-dessus, utilisez le **show ip les non classifié-port-stats que nbar** commandent de visualiser trafic le « non classifié » NBAR. Si votre réseau transporte le trafic de Gnutella, vous verrez la sortie semblable au suivant.`debug ip nbar filter destination_port tcp XXXX debug ip nbar capture 200 10 10 10`
2. Utilisez la commande **faite sur commande d'ip nbar port-map** de définir une port-MAP faite sur commande cette des correspondances sur les ports de Gnutella.`ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355` **Remarque:** Actuellement, vous devez utiliser un nom tel que la coutume-xx. Des noms définis par l'utilisateur pour PDLMs fait sur commande seront pris en charge dans une prochaine version de logiciel de Cisco IOS.
3. Utilisez le **show ip les stats que nbar de protocole** commandent de confirmer des correspondances à la déclaration faite sur commande.`2620# show ip nbar protocol stats byte-count FastEthernet0/0 Input Output Protocol Byte Count Byte Count ----------------------------------------------- custom-02`

```
43880517            52101266
```

4. Créez une stratégie de service QoS utilisant les commandes de l'Interface MQC (Modular QoS CLI).`d11-5-7206-16(config)# **class-map gnutella** d11-5-7206-16(config-cmap)# **match protocol custom-02** d11-5-7206-16(config-cmap)# **exit** d11-5-7206-16(config)# **policy-map sample** d11-5-7206-16(config-pmap)# **class gnutella** d11-5-7206-16(config-pmap-c)# **police 1000000 31250 31250 conform-action drop exceed-action drop violate-action drop`**Référez-vous utilisant la reconnaissance Fondé(e) sur le réseau et les listes de contrôle d'accès d'application pour bloquer le ver de « Code Red » pour que d'autres commandes de configuration bloquent Gnutella et tout autre trafic non désiré.

Informations connexes

- Ressources en support QoS
- Support technique - Cisco Systems