Déterminer le trafic non reconnu par NBAR

Contenu

Introduction

Ce document montre comment utiliser la fonctionnalité PDLM (Packet Description Language Module) personnalisée de Network-Based Application Recognition (NBAR) pour faire correspondre le trafic non classifié ou le trafic qui n'est pas spécifiquement pris en charge en tant qu'instruction de protocole de correspondance.

Conditions préalables

Conditions requises

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

- Méthodes QoS de base
- Compréhension de base de NBAR

Components Used

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

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Présentation du PDLM personnalisé

NBAR prend en charge divers protocoles statiques et avec état. Les PDLM permettent la prise en charge de nouveaux protocoles pour NBAR sans mise à niveau de version IOS ni rechargement du routeur. Les versions IOS suivantes intègrent la prise en charge de ces nouveaux protocoles.

Le PDLM personnalisé vous permet de mapper les protocoles au protocole UDP (User Datagram Protocol) statique et aux ports TCP pour les protocoles qui ne sont pas actuellement pris en charge dans NBAR avec une instruction de protocole de correspondance. En d'autres termes, il étend ou améliore la liste des protocoles reconnus par NBAR.

Voici les étapes à suivre pour ajouter le PDLM personnalisé à votre routeur.

1. Localisez et téléchargez le PDLM NBAR à partir de la page de téléchargement de logiciel (clients enregistrés uniquement) en téléchargeant le **fichier custom.pdlm**.
2. Chargez le PDLM sur un périphérique de mémoire Flash, tel que la carte PCMCIA dans les logements 0 ou 1, à l'aide de la commande ci-dessous.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. Vérifiez la prise en charge des protocoles personnalisés à l'aide de la **commande show ip nbar port-map | include custom** (voir ci-dessous) ou la commande **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. Affectez des ports aux protocoles personnalisés à l'aide de la commande **ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}**. Par exemple, pour faire correspondre le trafic au port TCP 8877, utilisez la commande **ip nbar port-map custom-01 tcp 8877**.

Classification des ports « non classifiés »

Selon le trafic réseau, vous devrez peut-être utiliser des mécanismes de classification spéciaux dans NBAR. Une fois que vous avez classifié ce trafic, vous pouvez utiliser le PDLM personnalisé et faire correspondre les numéros de port UDP et TCP à une carte de port personnalisée.

Par défaut, les mécanismes non classifiés NBAR ne sont pas activés. La commande **show ip nbar unclassifié-port-stats** renvoie le message d'erreur suivant :

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

Dans des circonstances contrôlées avec soin, utilisez la commande **debug ip nbar unclassifié-port-stats** pour configurer le routeur afin de commencer le suivi sur les ports sur lesquels les paquets arrivent. Ensuite, utilisez la commande **show ip nbar unclassifié-port-stats** pour vérifier les informations collectées. Le résultat affiche maintenant un histogramme des ports les plus couramment utilisés.

Remarque : avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage. Les commandes **debug ip nbar** ne doivent être activées que dans des circonstances soigneusement contrôlées.

Si ces informations ne sont pas suffisantes, vous pouvez activer la fonctionnalité de capture, qui fournit un moyen facile de capturer les traces de paquets de nouveaux protocoles. Utilisez les commandes **debug** suivantes, comme indiqué ci-dessous.

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

La première commande définit les paquets dans lesquels vous êtes intéressé pour la capture. La deuxième commande place NBAR en mode capture. Les arguments de la commande **capture** sont les suivants :

- Nombre d'octets à capturer par paquet.
- Nombre de paquets de démarrage à capturer, en d'autres termes, combien de paquets à capturer après le paquet SYN TCP/IP.
- Nombre de paquets finaux à capturer, en d'autres termes, combien de paquets à la fin du flux pour lesquels l'espace doit être réservé.
- Nombre total de paquets à capturer.

Remarque : La spécification des paramètres de début et de fin du paquet capture uniquement les paquets pertinents dans un flux long.

Utilisez la commande **show ip nbar capture** pour afficher les informations collectées. Par défaut, le mode capture attend l'arrivée d'un paquet SYN, puis commence à capturer les paquets sur ce flux bidirectionnel.

Blocage de Gnutella avec le PDLM personnalisé

Examinons un exemple d'utilisation du PDLM personnalisé. Nous utilisons Gnutella comme trafic que nous voulons classifier, puis appliquons une stratégie QoS qui bloque ce trafic.

Gnutella utilise six ports TCP connus : 6346, 6347, 6348, 6349, 6355 et 5634. D'autres ports peuvent être détectés lors de la réception des pongs. Si les utilisateurs spécifient d'autres ports à utiliser dans le partage de fichiers Gnutella, vous pouvez ajouter ces ports à votre instruction de protocole de correspondance personnalisée.

Voici les étapes à suivre pour créer une stratégie de service QoS qui correspond au trafic Gnutella et le supprime.

1. Comme indiqué ci-dessus, utilisez la commande **show ip nbar unclassifié-port-stats** pour afficher le trafic NBAR « non classifié ». Si votre réseau transporte du trafic Gnutella, vous obtiendrez des résultats similaires à ceux qui suivent.
```
Port    Proto    # of Packets
------- -------- -------
6346    tcp      347679
27005   udp      55043
```
2. Utilisez la commande **ip nbar port-map custom** pour définir une carte de port personnalisée qui correspond aux ports Gnutella.

   ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355

   Remarque : Actuellement, vous devez utiliser un nom tel que custom-xx. Les noms définis par l'utilisateur pour les PDLM personnalisés seront pris en charge dans une prochaine version du logiciel Cisco IOS.
3. Utilisez la commande **show ip nbar protocol stats** pour confirmer les correspondances avec l'instruction personnalisée.
```
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 à l'aide des commandes de l'interface de ligne de commande QoS modulaire (MQC).
```
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
```

   Reportez-vous à Utilisation de listes de contrôle d'accès et de reconnaissance d'applications basées sur le réseau pour bloquer le ver « Code Red » pour d'autres commandes de configuration afin de bloquer Gnutella et tout autre trafic indésirable.

Informations connexes

- Ressources d'assistance QoS
- Support technique - Cisco Systems