Utilisation de la commande tcpdump dans le logiciel ACNS

Contenu

Introduction

L'application de Cisco et le logiciel réseau de Réseau de diffusion de contenu (ACNS) 4.2.1 ont introduit la commande de **tcpdump**. Ce commandes enables vous pour recueillir un tracé de renifleur sur l'engine, le routeur de contenu, ou le Content Distribution Manager satisfait afin du dépannage, une fois demandé de recueillir les données par le support technique de Cisco. Cet utilitaire est très semblable à la commande de **tcpdump de** Linux/Unix.

Conditions préalables

Conditions requises

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

- FTP
- ACNS
- Interface de ligne de commande (CLI) d'ACNS

Composants utilisés

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

- Logiciel ACNS 4.2.1 et plus tard
- Toutes les Plateformes qui exécutent ACNS 4.2.X et en haut

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

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

Capturer des paquets

Le CLI sur ACNS permet maintenant à l'administrateur (doit être l'admin d'utilisateur) pour capturer des paquets des Ethernets. Sur la gamme satisfaite d'Engine 500, les noms d'interface sont eth0 et eth1. Sur toutes les Plateformes ACNS, il est recommandé que vous spécifiez un chemin/nom du fichier dans le répertoire local1.

Vous pouvez faire un vidage mémoire droit d'en-tête de paquet à l'écran si vous émettez la commande de **tcpdump** sur le CLI. Presse **CTRL-C** afin d'arrêter le vidage mémoire.

Options

La commande de **tcpdump** a ces options :

- **- *nom du fichier* W** — Écrit la sortie crue de capture de paquet à un fichier.
- **- *compte* s** — Capture les premiers octets de <count> de chaque paquet.
- **- *interface* I** — Te permet pour spécifier une interface spécifique pour l'utiliser pour capturer les paquets.
- **- *compte* c** — Limite la capture *pour compter des* paquets.

C'est une commande d'échantillon :

tcpdump - W /local1/dump.pcap - I eth0 - s 1500 - c 10000

Cette commande capture les 1500 premiers octets des 10,000 prochains paquets des Ethernet 0 d'interface, et met la sortie dans un fichier nommé **dump.pcap dans le** répertoire local1 sur l'engine satisfaite.

Remarque: Assurez-vous que vous spécifiez l'option **– s** de placer le snaplength de paquet. La valeur par défaut capture seulement 64 octets, et ceci enregistre seulement des en-têtes de paquet dans le fichier de capture. Pour le dépannage des paquets réorientés ou du trafic de plus haut niveau (HTTP, authentification, et ainsi de suite), une copie des paquets complets est nécessaire.

Vous pouvez également exécuter le **tcpdump** et le filtre sur une adresse IP particulière :

- Ajoutez l'**hôte 10.255.1.34 à l'**extrémité de la ligne de **tcpdump**. **Remarque:** Remplacez **10.255.1.34** par l'adresse IP que le client utilise.
- En outre, employez 1600 comme taille afin d'attraper les mauvais paquets qui peuvent être plus grands que 1500 octets.

Voici un exemple :

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

FTP

Après que le vidage mémoire de TCP ait été collecté, vous devez déplacer le fichier de l'engine satisfaite à un PC de sorte qu'il puisse être visualisé par un décodeur de renifleur.

```
ftp <ip address of the CE>
 !--- Log in with the admin username and password. cd local1 bin hash get <name of the file> !--
- Using the previous example, it is dump.pcap.

     bye
```

Éthéré

Éthérée est l'application logicielle recommandée pour lire le vidage mémoire de TCP, due à l'ampleur de ses caractéristiques et de leur utilisation avec le Réseau de diffusion de contenu, y compris la capacité de décoder les paquets qui sont encapsulés dans un tunnel GRE, utilisés par redirection WCCP. Référez-vous au pour en savoir plus de site Web de Wireshark.

Remarque: Dans la plupart des cas, les paquets réorientés capturés par l'installation de **tcpdump** disponible avec l'ACNS CLI diffèrent des données reçues sur l'interface. En raison de l'implémentation interne et de la manipulation des paquets réorientés, du nombre d'adresse IP de destination et de port TCP sont modifiés pour refléter l'adresse IP et le numéro de port 8999 de périphérique.

Informations connexes

- Application de Cisco et support logiciel du logiciel réseau de Réseau de diffusion de contenu (ACNS)
- Support et documentation techniques - Cisco Systems