Contenu

Introduction

Ce document décrit comment effectuer des captures de paquet sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de Cisco ESA.

Composants utilisés

Les informations dans ce document sont basées sur Cisco ESA qui exécutent n'importe quelle version d'AsyncOS.

Informations générales

Quand vous entrez en contact avec le support technique d'IronPort avec une question, vous pourriez être invité à fournir la vue dans l'activité réseau sortante et d'arrivée de l'ESA. L'appliance fournit la capacité d'intercepter et afficher le TCP, l'IP, et d'autres paquets qui sont transmis ou reçus au-dessus du réseau auquel l'appliance est reliée. Vous pourriez vouloir exécuter une capture de paquet afin de mettre au point la configuration réseau et afin de vérifier le trafic réseau qui atteint ou part de l'appliance.

Remarque: Ce document met en référence le logiciel qui n'est pas mis à jour ou est pris en

charge par IronPort. Les informations sont données comme courtoisie pour votre commodité. Pour davantage d'assistance, contactez s'il vous plaît le fournisseur de logiciels.

Il est important de noter que la commande précédemment utilisée CLI de **tcpdump** est remplacée par la nouvelle commande de **packetcapture** dans des versions 7.0 et ultérieures d'AsyncOS. Cette commande offre la fonctionnalité semblable à la commande de **tcpdump**, et elle est également disponible pour l'usage sur le GUI.

Si vous exécutez la version 6.x ou antérieures d'AsyncOS, référez-vous aux instructions sur la façon dont utiliser la commande de **tcpdump** dans les **saisies de paquet sur la** section de **versions 6.x et antérieures d'AsyncOS de** ce document. En outre, les options de filtre qui sont décrites dans les **filtres de capture de paquet** sectionnent sont valides pour la nouvelle commande de **packetcapture** aussi bien.

Saisies de paquet sur des versions 7.x et ultérieures d'AsyncOS

Cette section décrit le processus de saisie de paquet sur des versions 7.x et ultérieures d'AsyncOS.

Commencez ou arrêtez une capture de paquet

Afin de commencer une capture de paquet avec le GUI, naviguez vers le support et le menu Help, **capture** choisie de **paquet**, et puis cliquez sur la **capture de début**. Afin d'arrêter le processus de capture de paquet, **capture d'arrêt de** clic.

Remarque: Une capture qui commence dans le GUI est préservée entre les sessions.

Afin de commencer une capture de paquet avec le CLI, sélectionnez la commande de **packetcapture > de début**. Afin d'arrêter le processus de capture de paquet, sélectionnez la commande de **packetcapture > d'arrêt**, et l'ESA arrête la capture de paquet quand la session finit.

Fonctionnalité de capture de paquet

Voici une liste des informations utiles que vous pouvez employer afin de manipuler les captures de paquet :

- L'ESA enregistre l'activité capturée de paquet à un fichier et enregistre le fichier localement. Vous pouvez configurer la taille de fichier maximum de capture de paquet, la durée pour laquelle la capture de paquet fonctionne, et sur quelle interface réseau la capture exécute. Vous pouvez également utiliser un filtre afin de limiter la capture de paquet pour trafiquer par un port spécifique ou pour trafiquer d'un client spécifique ou de l'adresse IP du serveur.

- Naviguez **pour le prendre en charge et aide > capture de paquet du** GUI afin de visualiser une liste complète des fichiers de capture de paquet qui sont enregistrés sur le disque dur. Quand une capture de paquet s'exécute, la page de capture de paquet affiche le statut de la capture

en cours avec les statistiques en cours, telles que la taille de fichier et le temps s'est écoulé.

- Cliquez sur le bouton de **fichier téléchargé** afin de télécharger un fichier de capture de paquet. Vous pouvez l'expédier dans un email au support technique d'IronPort afin de mettre au point et dépanner toutes les questions.

- Afin de supprimer un fichier de capture de paquet, sélectionnez un ou plusieurs fichiers et cliquez sur Delete les **fichiers sélectionnés**.

- Afin d'éditer les configurations de capture de paquet avec le GUI, la **capture** choisie de **paquet du** support et le menu Help et cliquer sur Edit des **configurations**.

- Afin d'éditer les configurations de capture de paquet avec le CLI, sélectionnez le **packetcapture > la commande setup**.

Remarque: Le GUI affiche seulement les captures de paquet qui commencent dans le GUI, pas ceux qui commencent par le CLI. De même, le CLI affiche seulement le statut d'une capture en cours de paquet qui a commencé dans le CLI. Seulement une capture peut s'exécuter à la fois.

Conseil : Pour des informations supplémentaires sur des options et des paramètres de filtre de capture de paquet, référez-vous à la section de **filtres de capture de paquet de** ce document. Afin d'accéder à l'aide en ligne d'AsyncOS le du GUI, naviguer **pour aider et prendre en charge l'aide de >Online > l'index > le P > la capture de paquet**.

Saisies de paquet sur des versions 6.x et antérieures d'AsyncOS

Cette section décrit le processus de saisie de paquet sur des versions 6.x et antérieures d'AsyncOS.

Commencez ou arrêtez une capture de paquet

Vous pouvez employer la commande de **tcpdump** afin de capturer le TCP/IP et d'autres paquets qui sont transmis ou reçus au-dessus d'un réseau auquel l'ESA est relié.

Terminez-vous ces étapes afin de commencer ou arrêter une capture de paquet :

1. Entrez dans le **diagnostique >** commande de **réseau > de tcpdump** dans le CLI de l'ESA. Voici un exemple de sortie :

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
```

```
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. Placez l'interface (données 1, données 2, ou Gestion) et le filtre.

   Remarque: Le filtre utilise le même format que la commande de **tcpdump d'**Unix.
3. Sélectionnez le **DÉBUT** afin de commencer la capture et l'**ARRÊT** afin de le finir.

   Remarque: Ne quittez pas le menu de tcpdump tandis que la capture est en cours. Vous devez employer une deuxième fenêtre CLI afin d'exécuter toutes les autres commandes. Une fois le processus de capture est complet, vous devez employer le Secure Copy (SCP) ou le Protocole FTP (File Transfer Protocol) de votre appareil de bureau local afin de télécharger les fichiers à partir du répertoire nommé Diagnostic (référez-vous à la section de **filtres de capture de paquet** pour des détails). Le format de la capture de paquet d'utilisation de fichiers (PCAP) et peut être passé en revue avec un programme tel qu'éthéré ou Wireshark.

Filtres de capture de paquet

Le diagnostique > commande CLI de **NET** utilise la syntaxe standard de filtre de tcpdump. Cette section fournit des informations en vue de la capture de tcpdump filtre et fournit quelques exemples.

Ce sont les filtres standard qui sont utilisés :

- **IP -** Filtres pour tout le trafic de protocole IP
- **TCP -** Filtres pour tout le trafic de protocole TCP
- **hôte d'IP** - Filtres pour une source ou une destination spécifique d'adresse IP

Voici quelques exemples des filtres en service :

- **hôte 10.1.1.1 d'IP** - Ce filtre capture n'importe quel trafic qui inclut 10.1.1.1 comme source ou destination.
- **hôte 10.1.1.1 d'IP ou hôte 10.1.1.2 d'IP** - ce filtre capture le trafic qui contient 10.1.1.1 ou 10.1.1.2 comme source ou la destination.

Pour la récupération du fichier capturé, naviguez vers **distributeur intégrant son logiciel au matériel > log > diagnostic** ou **données > bar > diagnostic** afin d'atteindre le répertoire diagnostique.

Remarque: Quand cette commande est utilisée, elle peut faire remplir votre espace disque ESA, et peut également entraîner la dégradation de représentation. Cisco recommande que vous utilisiez seulement cette commande avec l'assistance d'un ingénieur d'assistance clientèle d'IronPort Cisco.