Capture et analyse du trafic réseau avec Wireshark pour les diagnostics

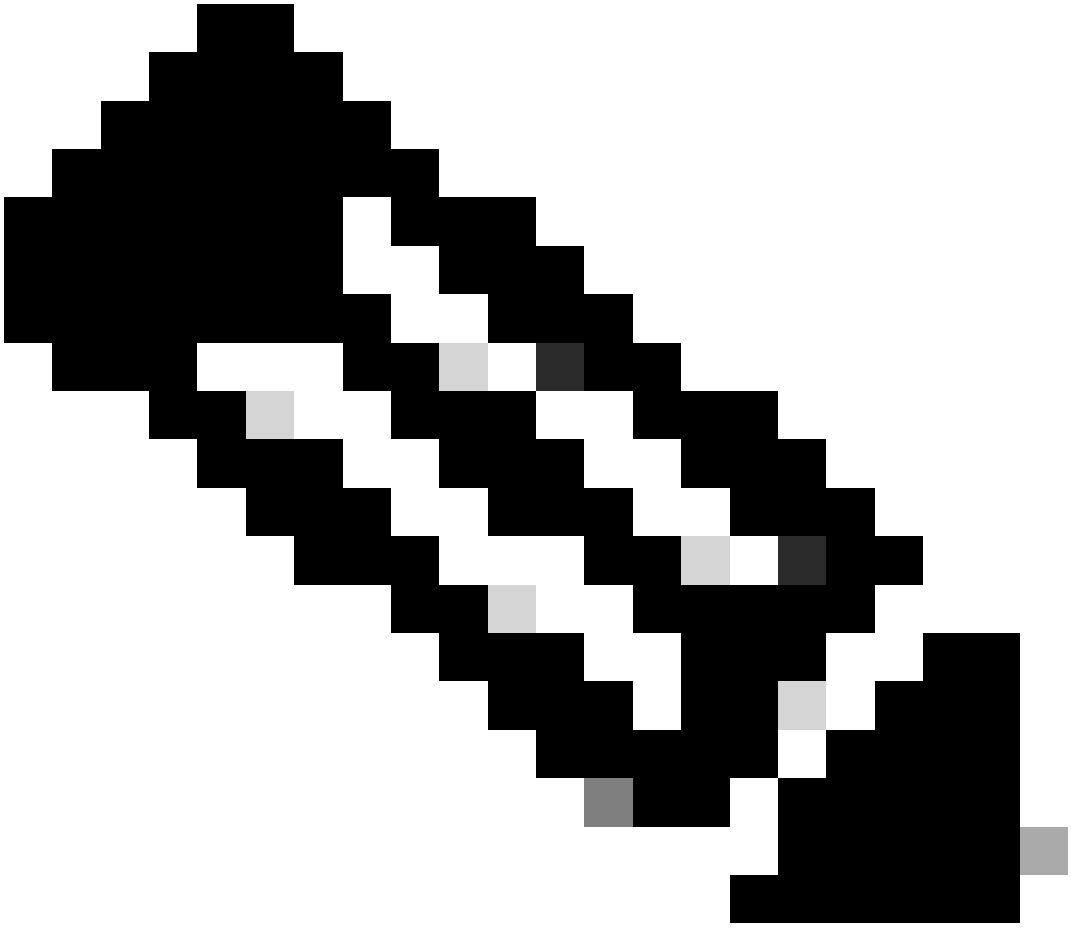
Table des matières

Introduction

Ce document décrit comment utiliser Wireshark pour capturer et analyser le trafic réseau à des fins de diagnostic.

Aperçu

Wireshark est une application gratuite que vous pouvez utiliser pour lire et analyser les captures de paquets (également appelée « vidages TCP »). Les captures de paquets révèlent toutes les communications via une carte réseau au niveau des paquets, ce qui permet d'afficher les types de trafic DNS, HTTP, ping et autres. Les captures de paquets sont particulièrement utiles en tant qu’étape de diagnostic pour le dépannage en profondeur et, avec l’introduction de SIG, elles constituent désormais une partie fondamentale du processus de diagnostic.



Remarque : Wireshark capture tout le trafic sur la carte sélectionnée. Comme les captures de paquets contiennent souvent des informations d'identification personnelle (PII), utilisez toujours une méthode sécurisée, telle qu'un lien Box, pour partager les fichiers de capture avec l'assistance.

Obtenir Wireshark

Vous pouvez télécharger Wireshark pour Windows, macOS ou Linux à l'adresse : https://www.wireshark.org/

Collecter une capture de paquets

1. Choisissez la carte réseau connectée à Internet et lancez la capture dans Wireshark.
2. Lors de la capture, reproduisez le problème que vous souhaitez diagnostiquer.
3. Arrêtez la capture lorsque vous avez terminé et enregistrez le fichier en tant que fichier `.pcap`.

Ports et protocoles de base

- La plupart des paquets communiquent sur les protocoles TCP ou UDP de la couche transport
    - Par exemple, « DNS » exécute « sur » UDP par défaut. Il passe au protocole UDP si le protocole TCP échoue.
- HTTP et DNS sont des protocoles courants qui s'exécutent sur une combinaison de protocole de transport et de ports.

Protocole de couche transport	Port	Nom du protocole	Utilisation
TCP	22	SSH	Accès VA distant
TCP	25	SMTP	Surveillance VA
IP	50	ESP (Encapsulating Security Payload)	Confidentialité, intégrité des données, authentification de l'origine
IP	51	AH (Authentication Header)	Intégrité des données, authentification de l'origine
UDP	53	DNS	DNS par défaut
TCP	53	DNS	Basculement DNS
TCP	80	HTTP	Trafic Web (non chiffré), API
UDP	123	NTP	Synchronisation du temps VA
TCP	443	HTTPS	Trafic Web chiffré, API, connecteurs AD vers VA
UDP	443	HTTPS	Requêtes DNS chiffrées RC
UDP	500	IKE	Négociations de tunnel IPsec
UDP	4500	NAT-T	Traversée NAT pour tunnels IPsec
TCP	8080	HTTP	Connecteurs AD pour les communications VA

La connaissance des noms de protocole, des ports et de leurs utilisations vous aide à identifier et à analyser le trafic pertinent dans Wireshark.

Opérateurs de base

Lorsque vous créez des chaînes de filtre dans Wireshark, utilisez les opérateurs suivants :

- `==`: Égal à (exemple : `ip.dst==1.2.3.4`)
- `!=`: Non égal (exemple : `ip.dst!=1.2.3.4`)
- `&`: Et (Exemple : `ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`: Ou (Exemple : `ip.dst==1.2.3.4 || ip.dst==1.2.3.5`)

Pour connaître les options de filtrage avancées, reportez-vous à la documentation Wireshark : 6.4.

[Création d’expressions de filtre d’affichage]

Filtres

Les captures de paquets peuvent contenir des milliers de paquets. Les filtres vous aident à vous concentrer sur des types de trafic spécifiques :

- Par protocole :
  - `dns` : affiche uniquement le trafic DNS
  - `http || dns` : affiche le trafic HTTP ou DNS
- Par adresse IP :
  - `ip.addr==<IP>`— Tout le trafic vers/depuis`<IP>`
  - `ip.src==<IP>`— Tout le trafic provenant de`<IP>`
  - `ip.dst==<IP>`— Tout le trafic vers`<IP>`
- Divers :
  - `tcp.flags.reset==1`— Vérifier les réinitialisations TCP (délais d'expiration)
  - `dns.qry.name contient "[domaine]"` : requêtes DNS correspondant à un domaine
  - `tcp.port==80 || udp.port==80` — Trafic TCP ou UDP sur le port 80

Affichage et analyse des paquets

Après avoir localisé un paquet, développez les segments dans Wireshark pour analyser les détails. La connaissance de la structure du protocole vous aide à interpréter ces détails et même à reconstruire les données si nécessaire.

Suivi d'un flux de données

Utilisez la liste de paquets pour localiser les paires requête/réponse. Cliquez avec le bouton droit sur un paquet et sélectionnez Follow > TCP Stream, UDP Stream, TLS Stream, or HTTP Stream pour afficher la séquence de requête et de réponse associée.

- Cela est plus utile avec les protocoles qui ont plusieurs échanges (par exemple, HTTP) qu'avec les protocoles à demande unique (par exemple, DNS).

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.