Netwerkverkeer vastleggen en analyseren met Wireshark for Diagnostics

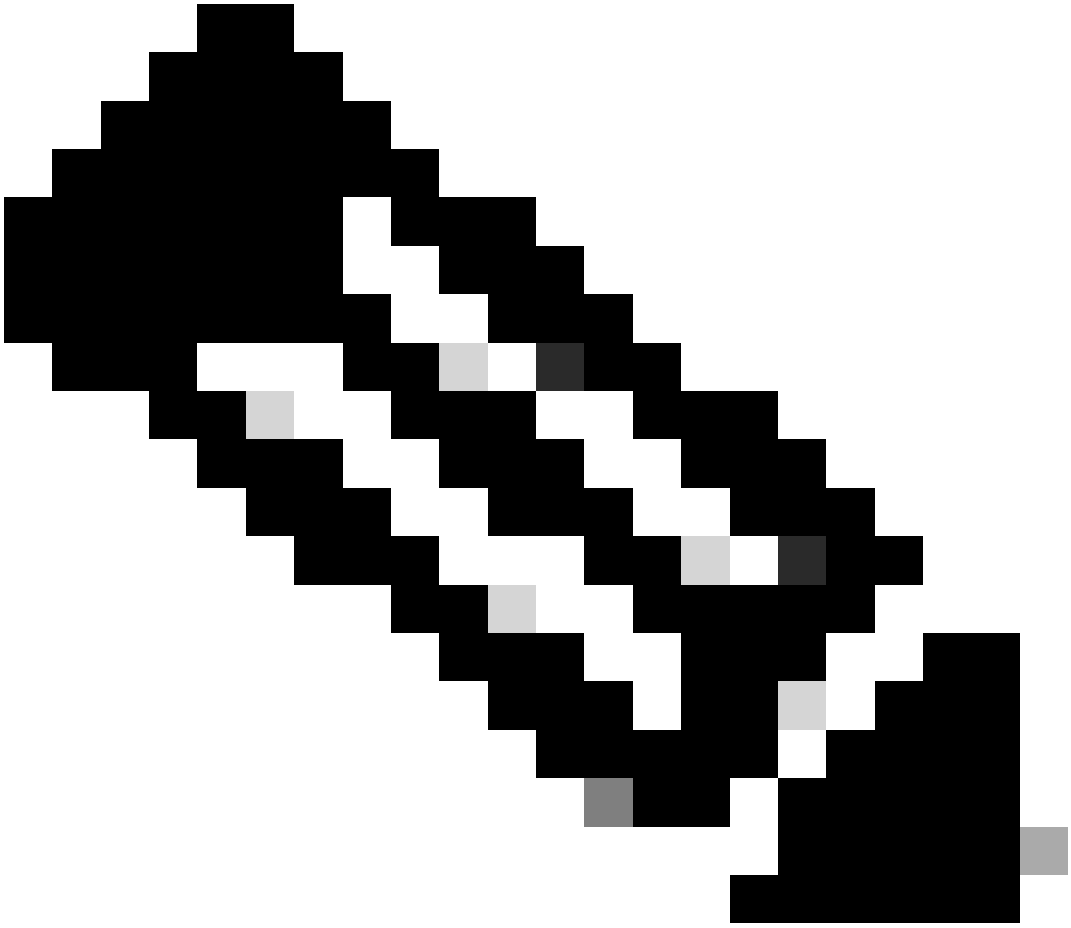
Inhoud

Inleiding

In dit document wordt beschreven hoe u Wireshark kunt gebruiken om netwerkverkeer vast te leggen en te analyseren voor diagnostische doeleinden.

Overzicht

Wireshark is een gratis applicatie die u kunt gebruiken om pakketopnames te lezen en te analyseren (ook wel "TCP dumps" genoemd). Packet Captures onthullen alle communicatie via een netwerkadapter op pakketniveau, waardoor het mogelijk is om DNS, HTTP, ping en andere verkeerstypen te bekijken. Packet captures zijn vooral waardevol als diagnostische stap voor het oplossen van diepe problemen en zijn met de introductie van SIG nu een fundamenteel onderdeel van het diagnostische proces.



Opmerking: Wireshark vangt al het verkeer op de geselecteerde adapter op. Omdat pakketopnames vaak persoonlijk identificeerbare informatie (PII) bevatten, moet u altijd een veilige methode gebruiken, zoals een Box-link, om vastlegbestanden te delen met ondersteuning.

Haal Wireshark

U kunt Wireshark voor Windows, macOS of Linux downloaden op: https://www.wireshark.org/

Pakket vastleggen

1. Kies de netwerkadapter die is verbonden met internet en start de opname in Wireshark.
2. Tijdens het vastleggen reproduceert u het probleem dat u wilt diagnosticeren.
3. Stop de opname wanneer deze is voltooid en sla het bestand op als a `.pcap`.

Basispoorten en protocollen

- De meeste pakketten communiceren op de transportlaagprotocollen TCP of UDP
  - Bijvoorbeeld, "DNS" draait standaard "bovenop" UDP. Het schakelt naar UDP als TCP mislukt.
- HTTP en DNS zijn gangbare protocollen die draaien op een combinatie van transportprotocol + poorten.

Transport Layer Protocol	Port	protocolnaam	gebruik
TCP	22	SSH	Remote VA Access
TCP	25	SMTP	VA-bewaking
IP	50	ESP (Inkapselen van beveiligingslading)	Vertrouwelijkheid, gegevensintegriteit, authenticatie van oorsprong
IP	51	AH (koptekst voor verificatie)	Gegevensintegriteit, oorsprongverificatie
UDP	53	DNS	DNS-standaard
TCP	53	DNS	DNS-failover
TCP	80	HTTP	Webverkeer (niet-gecodeerd), API's
UDP	123	NTP	VA-tijdsynchronisatie
TCP	443	HTTPS	Gecodeerd webverkeer, API's, AD-connectors naar VA's
UDP	443	HTTPS	RC Encrypted DNS queries
UDP	500	IKE	Onderhandelingen over de IPsec-tunnel
UDP	4500	NAT-T	NAT-traversal voor IPsec-tunnels
TCP	8080	HTTP	AD-connectors voor VA-communicatie

Het kennen van protocolnamen, poorten en hun gebruik helpt u bij het identificeren en analyseren van relevant verkeer in Wireshark.

Basisoperatoren

Gebruik bij het bouwen van filtersnaren in Wireshark de volgende operatoren:

- `==`: Gelijk aan (voorbeeld: `ip.dst==1.2.3.4`)
- `!=`: Niet gelijk (voorbeeld: `ip.dst!=1.2.3.4`)
- `&&`: en (Voorbeeld: `ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`: Of (Voorbeeld: `ip.dst==1.2.3.4 || ip.dst==1.2.3.5`)

Raadpleeg voor geavanceerde filteropties de documentatie van Wireshark: [6.4. Weergavefilterexpressies bouwen]

Filters

Packet captures kunnen duizenden pakketten bevatten. Filters helpen u zich te concentreren op specifieke verkeerstypen:

- Per protocol:
    - `dns` — Alleen DNS-verkeer weergeven
    - `http || dns` — HTTP- of DNS-verkeer weergeven
- Op IP-adres:
    - `ip.addr==<IP>` — Al het verkeer van/naar `<IP>`
    - `ip.src==<IP>` — Al het verkeer van `<IP>`
    - `ip.dst==<IP>` — Al het verkeer naar `<IP>`
- Diversen:
    - `tcp.flags.reset==1` — Controleren op TCP-resets (time-outs)
    - `dns.qry.name bevat "[domein]"` — DNS-query's die overeenkomen met een domein
    - `tcp.port==80 || udp.port==80` — TCP- of UDP-verkeer op poort 80

Pakketten bekijken en analyseren

Nadat u een pakket hebt gevonden, breidt u de segmenten binnen Wireshark uit om details te analyseren. Vertrouwdheid met de protocolstructuur helpt u deze details te interpreteren en zelfs gegevens te reconstrueren als dat nodig is.

Na een gegevensstroom

Gebruik de pakketlijst om vraag- en antwoordparen te vinden. Klik met de rechtermuisknop op een pakket en selecteer Volgen **>** TCP Stream, UDP Stream, TLS Stream of HTTP Stream om de bijbehorende reeksen verzoeken en antwoorden te bekijken.

- Dit is nuttiger bij protocollen die meerdere exchanges hebben (bijvoorbeeld HTTP) dan bij single-request protocollen (bijvoorbeeld DNS).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.