Cisco Secure Access Fragmented ICMP-pakketverwerking

Inhoud

uitgeven

ICMP-echoverzoeken die groter zijn dan de MTU ontvangen geen antwoorden wanneer ze worden verzonden met de DF-bit (Don't Fragment) uitgeschakeld. Dit gebeurt in twee specifieke scenario's:

- Van RAVPN-eindpunten via de VPN-interface bij het verzenden van ICMP-pakketten die de MTU-grootte van de VPN-interface overschrijden met de DF-bit gewist
- Van on-premise eindpunten via een IPsec-tunnel tussen een site-router en Cisco Secure Access (CSA) bij het verzenden van ICMP-pakketten die de MTU-grootte van de IPsec-tunnelinterface overschrijden met de DF-bit gewist

In beide gevallen worden er geen ICMP-antwoorden ontvangen, wat leidt tot vragen over de vraag of CSA gefragmenteerde pakketten laat vallen met de DF-bit uitgeschakeld.

milieu

- Cisco Secure Access (CSA)
- RAVPN-eindpunten (Remote Access VPN)
- IPsec-tunnels tussen site routers en CSA
- ICMP-verkeer groter dan MTU-interfacegroottes
- Gefragmenteerde pakketscenario's met DF-bit gewist

resolutie

Cisco Secure Access laat gefragmenteerde pakketten vallen in zowel underlay- als overlay-

scenario's. Dit gedrag wordt gedocumenteerd in de Cisco Secure Access Help-documentatie, waarin expliciet staat: "Gefragmenteerde pakketten in de onderlaag of overlay worden verwijderd."

verwacht gedrag

Cisco Secure Access is ontworpen om gefragmenteerde pakketten te laten vallen, ongeacht of ze zich voordoen in het onderliggende of overlay-netwerk. Dit geldt voor:

- ICMP-pakketten verzonden vanaf RAVPN-eindpunten die de VPN-interface overschrijden MTU met DF-bit gewist
- ICMP-pakketten verzonden vanaf on-premise eindpunten via IPsec-tunnels die de tunnelinterface MTU met DF-bit overschrijden

Dit gedrag is consistent in alle scenario's met betrekking tot gefragmenteerde pakketten binnen de Cisco Secure Access-infrastructuur.

Aanvraag voor functie CSE-I-5739 is hiervoor gemaakt.

Oorzaak

Cisco Secure Access is ontworpen om gefragmenteerde pakketten te laten vallen als een beslissing over het ontwerp van beveiliging en prestaties. Dit gedrag wordt geïmplementeerd om potentiële beveiligingslekken en verwerkingsoverhead te voorkomen die verband houden met het opnieuw samenvoegen van pakketten in zowel onderliggende als overlay-netwerkscenario's.

Verwante inhoud

- Cisco Secure Access Help-documentatie - Versnipperde pakketverwerking
- Cisco Technical Support en downloads

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.