IPsec over TCP-failover wanneer verkeer door ASA stroomt

Inhoud

Inleiding

Cisco VPN-clients die verbinding maken met een VPN-head-end met behulp van IPsec over TCP, kunnen verbinding maken met de head-end boete, maar de verbinding is na een tijdje mislukt. Dit document beschrijft hoe u via UDP of de native ESP IPsec-insluiting kunt overschakelen op IPsec om het probleem op te lossen.

Voordat u begint

Vereisten

Om dit specifieke probleem op te treden, moeten de Clients van Cisco VPN worden geconfigureerd om met een VPN-head-end apparaat te verbinden door IPsec over TCP te gebruiken. In de meeste gevallen configureren netwerkbeheerders de ASA om Cisco VPN-clientverbindingen via TCP-poort 1000 te accepteren.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco VPN-client.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Probleem

Wanneer de VPN-client is geconfigureerd voor IPsec over TCP (cTCP), reageert de VPN-

clientsoftware niet als er een dubbele TCP-ACK is ontvangen met het verzoek aan de VPN-client om gegevens opnieuw te verzenden. Er kan een dubbele ACK gegenereerd worden als er pakketverlies ergens tussen de VPN-client en het ASA-head-end is. Intermitterend pakketverlies is een redelijk gewone realiteit op het internet. Aangezien de VPN-endpoints het TCP-protocol echter niet gebruiken (herinneren dat ze cTCP gebruiken), blijven de endpoints verzenden en wordt de verbinding voortgezet.

In dit scenario, komt een probleem voor als er een ander apparaat zoals een firewall is die de TCP verbinding statelijk volgt. Aangezien het cTCP protocol geen TCP client volledig uitvoert en server duplicaat ACK's geen respons ontvangen, kan dit andere apparaten in-line met deze netwerkstroom veroorzaken om het TCP verkeer te laten vallen. Het pakketverlies moet op het netwerk gebeuren dat TCP segmenten veroorzaakt om te missen, wat het probleem veroorzaakt.

Dit is geen bug, maar een neveneffect van zowel pakketverlies op het netwerk als het feit dat cTCP geen echte TCP is. cTCP probeert het TCP protocol na te bootsen door de IPsec-pakketten in een TCP-header te wikkelen, maar dit is de reikwijdte van het protocol.

Dit probleem doet zich typisch voor wanneer netwerkbeheerders een ASA met een IPS uitvoeren, of een of ander soort van toepassing inspectie op de ASA uitvoeren die de firewall veroorzaakt om als volledige TCP-proxy van de verbinding te handelen. Als er pakketverlies is zal de ASA for de ontbrekende gegevens namens de cTCP server of client ACK, maar de VPN client zal nooit reageren. Aangezien de ASA nooit de data ontvangt die ze verwacht heeft, kan de communicatie niet doorgaan. Als resultaat hiervan faalt de verbinding.

Oplossing

Voer een van deze handelingen uit om dit probleem op te lossen:

- Schakelt van IPsec over TCP naar IPsec over UDP of native insluiting met het ESP-protocol.
- Schakelt over naar de AnyConnect-client voor VPN-beëindiging, waarbij een volledig geïmplementeerde TCP-protocolstack wordt gebruikt.
- Configureer de ASA om tcp-state-bypass toe te passen voor deze specifieke IPsec/TCP-stromen. Dit schakelt in feite alle veiligheidscontroles uit op de verbindingen die overeenkomen met het tcp-staat-bypass-beleid, maar zal het mogelijk maken dat de verbindingen werken totdat een andere resolutie uit deze lijst uitgevoerd kan worden. Raadpleeg voor meer informatie de TCP-richtsnoeren voor statelijke omzeilingen en beperkingen.
- Identificeer de bron van het pakketverlies en neem correctieve actie om te voorkomen dat de IPsec/TCP-pakketten op het netwerk vallen. Dit is meestal onmogelijk of extreem moeilijk omdat de oorzaak van de kwestie gewoonlijk het pakketverlies op het internet is, en de druppels kunnen niet worden voorkomen.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems