Problemen met uitputting van poorten oplossen bij het vertalen van poortadressen met paraplu-onderdelen

Inhoud

Inleiding

In dit document wordt beschreven hoe klanten die gebruikmaken van roamingclients en/of virtuele apparaten problemen ondervinden met de uitputting van poorten in firewalls die gebruikmaken van Port Address Translation. Dit is waarschijnlijk het geval in omgevingen met een groot aantal roamingklanten en/of een grote hoeveelheid verkeer dat door de VA's loopt. Symptomen kunnen zijn DNS-query's die langzaam terugkeren of timing-out.

Oorzaken

Noch roamingclients, noch virtuele apparaten cachen antwoorden op DNS-query's. Bovendien sturen roamingklanten vaak "sonde" DNS-verzoeken om de netwerkomgeving te analyseren en als gezondheidscontroles.

Aanbevelingen

- Zorg ervoor dat uw interne domeinen correct zijn geconfigureerd binnen Domeinbeheer op uw Umbrella-dashboard. Ze moeten uw Active Directory-zone (en/of andere interne zones) bevatten om het volume van query's met een hoge frequentie te verminderen.
- Bekijk enkele van de PAT-instellingen op de firewall:
    - Een lange UDP sessie time-out kan een probleem zijn. We raden meestal UDP sessie time-outs van ongeveer 15 seconden. Houd er echter rekening mee dat als UDP zwaar wordt gebruikt door andere toepassingen op uw netwerk, ze langere time-outs kunnen hebben waarmee u rekening moet houden.
    - Afhankelijk van uw firewall is het mogelijk om de grootte van de PAT-pool te vergroten om het aantal gelijktijdige verbindingen te vergroten.
- Als u een IP-adres hebt dat u kunt toewijzen aan de VA's, gebruikt u 1: 1 NAT in plaats van PAT op de firewall. Opmerking: "1:1 NAT" wordt soms aangeduid als "Direct NAT", maar dit is een verkeerde benaming; de juiste technische term is "1:1 NAT".

- Controleer de limieten per IP-verbinding. Vaak is een beleid dat naar verwachting niet van toepassing is op het apparaat in kwestie inderdaad een limiet van toepassing. Zie de volgende sectie voor het bevestigen.

Controleren op per-IP-verbindingslimieten op een ASA

Voer de onderstaande stappen uit:

- Configureer de ASA met een capture om te zien waarom pakketten werden gedropt door de firewall:

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- Zoek naar pakketten die worden gedropt voor het betreffende IP-adres. Een reden voor de verbindingslimiet wordt weergegeven als "Drop-reason: (conn-limit)"
- Controleer de limiet voor de hostverbinding met behulp van de opdracht:

```
show local-host detail | begin <IP Address of VA or roaming client>
```

    - Is dit getal statisch op een bepaalde limiet (dat is 999) en neemt het nooit toe? Als dit het geval is, wordt een verbindingslimiet aangegeven.
- Controleer of er een servicebeleid is dat dit toepast; als u dit vindt, raadpleegt u de beleidskaart:

```
show run service-policy, show policy-map NAME
```

    - Als u een beleidskaart "NAME" vindt die de limiet voor de verbinding per host instelt op 1000 (bijvoorbeeld), worden nieuwe DNS-pakketten van het apparaat verwijderd totdat er meer verbindingen beschikbaar zijn. UDP is staatloos en probeert het niet opnieuw.
- Om dit probleem op te lossen, verwijdert u dat servicebeleid (geen naam voor servicebeleid in). Verbindingen moeten over de 1K-limiet gaan (uit ons voorbeeld). Dit gebeurt sneller voor een VA dan voor een roamingclient.

Verdere aanbevelingen

Als deze aanbevelingen niet helpen, is een mogelijke oplossing:

1. Gebruik het Umbrella Dashboard --> Reporting --> Top Destinations-rapport om een of meer domeinen te identificeren die de afgelopen 24 uur een groot aantal verzoeken hebben ontvangen.
2. Voeg in het Umbrella-dashboard --> Configuration --> Domain Management een of meer van de domeinen met een hoog volume toe aan de lijst en stel "Van toepassing op" in op "Alle apparaten en apparaten".

3. Daarna worden query's voor die domeinen door de VA's doorgestuurd naar de lokale DNS. Idealiter moet de lokale DNS worden geconfigureerd om door te sturen naar de Umbrella DNS op 208.67.220.220/208.67.222.222, maar ze kunnen worden geconfigureerd om door te sturen naar een externe DNS.
4. De lokale DNS behandelt query's voor alle domeinen waarvoor ze gezaghebbend zijn.
5. Als de lokale DNS query's voor niet-lokale domeinen accepteert, worden query's voor die andere domeinen doorgestuurd naar de externe DNS.

Dit komt omdat de lokale DNS-cache DNS-resultaten kan bevatten, terwijl de zwervende clients en virtuele apparaten geen cache hebben. Houd er rekening mee dat het gebruik van deze tijdelijke oplossing resulteert in meer verkeer en een zwaardere belasting van de interne DNS, dus houd ze zorgvuldig in de gaten om ervoor te zorgen dat ze niet overbelast zijn.

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.