Risoluzione dei problemi di esaurimento delle porte quando si utilizza Port Address Translation con i componenti Umbrella

Sommario

Introduzione

In questo documento vengono descritti i clienti Umbrella che utilizzano client in roaming e/o appliance virtuali e i problemi di esaurimento delle porte nei firewall che utilizzano Port Address Translation. Ciò è molto probabile in ambienti che dispongono di un numero elevato di client di roaming e/o di un volume elevato di traffico che attraversa i VA. I sintomi possono includere query DNS con ritorno lento o timeout.

Cause

Le risposte alle query DNS non vengono memorizzate nella cache né dai client in roaming né dalle appliance virtuali. Inoltre, i client di roaming inviano frequenti richieste DNS "probe" per analizzare l'ambiente di rete e come controlli di integrità.

Consigli

- Verificare che i domini interni siano configurati correttamente in Gestione domini nel dashboard Umbrella. Devono contenere la zona di Active Directory e/o altre zone interne per ridurre il volume delle query ad alta frequenza.
- Verificare alcune impostazioni PAT sul firewall:
    - Un timeout di sessione UDP prolungato può rappresentare un problema. In genere, si consiglia un timeout della sessione UDP di circa 15 secondi. Tuttavia, se UDP viene utilizzato in modo intensivo da altre applicazioni sulla rete, è possibile che abbiano timeout più lunghi, di cui è necessario tenere conto.
    - A seconda del firewall, è possibile aumentare le dimensioni del pool PAT per aumentare il numero di connessioni simultanee.
- Se si dispone di un indirizzo IP che è possibile dedicare ai VA, utilizzare un NAT 1:1 anziché PAT sul firewall. Nota: Il termine "NAT 1:1" viene talvolta chiamato "NAT diretto", ma si tratta di un termine improprio; il termine tecnico corretto è "1:1 NAT".

- Controllare i limiti delle connessioni per IP. Spesso, una politica che non dovrebbe essere applicata al dispositivo in questione sta in effetti applicando un limite. Per informazioni sulla conferma, vedere la sezione successiva.

Verifica dei limiti delle connessioni per IP su un'appliance ASA

Attenersi alla procedura seguente:

- Configurare l'appliance ASA con un'acquisizione per verificare il motivo per cui i pacchetti sono stati scartati dal firewall:

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

- Cercare i pacchetti ignorati per l'IP in questione. Un motivo per il limite della connessione viene visualizzato come "Motivo perdita: (conn-limit)"
- Esaminare il limite di connessioni host utilizzando il comando:

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

    - Questo numero è statico a un certo limite (cioè 999) e non aumenta mai? In tal caso, indica un limite di connessioni.
- Verificare la presenza di una politica dei servizi che applica questo criterio; se disponibile, verificare la mappa dei criteri:

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

    - Se si trova un "NAME" della mappa dei criteri che imposta il limite di connessioni per host su 1000 (ad esempio), tutti i nuovi pacchetti DNS del dispositivo verranno eliminati finché non saranno disponibili più connessioni. UDP è senza stato e non riprova.
- Per risolvere il problema, rimuovere il criterio servizio (non è presente il NOME del criterio servizio). Le connessioni devono iniziare a superare il limite di 1K (dal nostro esempio). Ciò si verifica più rapidamente per un VSA rispetto a un client mobile.

Ulteriori raccomandazioni

Se tali suggerimenti non sono utili, è possibile implementare una soluzione che consenta di:

1. Utilizzare il dashboard Umbrella —> Report —> Report prime destinazioni per identificare uno o più domini che hanno un numero elevato di richieste nelle ultime 24 ore.
2. Nel dashboard Umbrella —> Configuration —> Domain Management, aggiungere uno o più domini con volumi elevati all'elenco, impostando "Si applica a" su "Tutti gli accessori e i dispositivi".
3. In seguito, le query per tali domini vengono inoltrate dai VA al DNS locale. Idealmente, il

DNS locale deve essere configurato per l'inoltro al DNS Umbrella all'indirizzo 208.67.220.220/208.67.222.222, ma potrebbe essere configurato per l'inoltro a qualsiasi DNS esterno.

4. Il DNS locale gestisce le query per tutti i domini di cui è autorevole.
5. Presumendo che il DNS locale non accetti query per domini non locali, le query per questi altri domini vengono inoltrate al DNS esterno.

Ciò è dovuto al fatto che il DNS locale può memorizzare nella cache i risultati DNS, mentre i client in roaming e le appliance virtuali non memorizzano nella cache. Si noti che questa soluzione consente di aumentare il traffico e il carico sul DNS interno, quindi monitorarli attentamente per verificare che non siano sovraccarichi.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).