Fehlerbehebung bei der Port-Erschöpfung bei der Verwendung der Port-Adressumwandlung mit Umbrella-Komponenten

Inhalt

Einleitung

In diesem Dokument werden Umbrella-Kunden beschrieben, die Roaming-Clients und/oder virtuelle Appliances verwenden und bei Firewalls, die die Port-Adressumwandlung verwenden, auf Probleme mit der Port-Erschöpfung stoßen. Dies ist am wahrscheinlichsten in Umgebungen mit einer großen Anzahl an Roaming-Clients und/oder einem hohen Datenverkehrsvolumen, das durch die VAs läuft. Zu den Symptomen können langsame DNS-Abfragen oder Zeitüberschreitungen gehören.

Ursachen

Antworten auf DNS-Abfragen werden weder von Roaming-Clients noch von virtuellen Appliances zwischengespeichert. Darüber hinaus senden Roaming-Clients häufige DNS-Anfragen, um die Netzwerkumgebung zu analysieren und ihre Integrität zu überprüfen.

Empfehlungen

- Stellen Sie sicher, dass Ihre internen Domänen im Domänenmanagement auf Ihrem Umbrella Dashboard ordnungsgemäß konfiguriert sind. Sie müssen Ihre Active Directory-Zone (und/oder andere interne Zonen) enthalten, um die Anzahl der Abfragen mit hoher Häufigkeit zu reduzieren.
- Überprüfen Sie einige der PAT-Einstellungen auf der Firewall:
    - Ein langes Timeout für UDP-Sitzungen kann ein Problem sein. In der Regel empfehlen wir UDP-Sitzungs-Timeouts von etwa 15 Sekunden. Beachten Sie jedoch, dass UDP, wenn es stark von anderen Anwendungen in Ihrem Netzwerk genutzt wird, längere Zeitüberschreitungen aufweisen kann, die Sie berücksichtigen müssen.
    - Je nach Firewall ist es möglich, den PAT-Pool zu vergrößern, um die Anzahl der gleichzeitigen Verbindungen zu erhöhen.
- Wenn Sie über IP-Adressen verfügen, die Sie den VAs zuweisen können, verwenden Sie 1:1

NAT anstelle von PAT in der Firewall. Anmerkung: "1:1 NAT" wird manchmal auch als "Direct NAT" bezeichnet, es handelt sich jedoch um eine Fehlbezeichnung. der korrekte Fachausdruck lautet "1:1 NAT".
- Überprüfen Sie Ihre Pro-IP-Verbindungslimits. Häufig führt eine Richtlinie, die nicht für das fragliche Gerät gelten soll, tatsächlich zu einer Beschränkung. Im nächsten Abschnitt erfahren Sie, wie Sie die Bestätigung durchführen.

Überprüfen Sie, ob auf einer ASA IP-basierte Verbindungslimits gelten.

Führen Sie die folgenden Schritte aus:

- Konfigurieren Sie die ASA mit einer Erfassung, um zu sehen, warum Pakete von der Firewall verworfen wurden:

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

- Suchen Sie nach Paketen, die für die betreffende IP verworfen werden. Der Grund für die Verbindungsbeschränkung wird als "Ablehnungsgrund: (Verbindungslimit)"
- Untersuchen Sie die Hostverbindungsgrenze mithilfe des folgenden Befehls:

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

    - Ist diese Zahl an einem bestimmten Grenzwert (also 999) konstant und steigt sie nie an? Ist dies der Fall, wird eine Verbindungsbeschränkung angezeigt.
- Suchen Sie nach einer Dienstrichtlinie, die diese Richtlinie anwendet. Wenn Sie sie finden, überprüfen Sie ihre Richtlinienzuordnung:

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

    - Wenn Sie eine Richtlinienzuordnung "NAME" finden, die die maximale Anzahl von Verbindungen pro Host auf 1.000 setzt, werden dadurch alle neuen DNS-Pakete vom Gerät verworfen, bis weitere Verbindungen verfügbar sind. UDP ist stateless und wird nicht wiederholt.
- Entfernen Sie zum Auflösen diese Dienstrichtlinie (kein Name der Dienstrichtlinie enthalten). Verbindungen müssen die Grenze von 1.000 überschreiten (aus unserem Beispiel). Dies geschieht bei einer VA schneller als bei einem Roaming-Client.

Weitere Empfehlungen

Wenn diese Empfehlungen nicht helfen, wäre eine mögliche Problemumgehung:

1. Verwenden Sie den Umbrella Dashboard —> Reporting —> Top Destinations-Bericht, um

eine oder mehrere Domänen zu identifizieren, die eine große Anzahl von Anfragen innerhalb der letzten 24 Stunden haben.
2. Fügen Sie im Umbrella Dashboard —> Configuration —> Domain Management (Domänenmanagement) eine oder mehrere der Domänen mit hohem Volumen zur Liste hinzu, und legen Sie "Applies to" (Anwendbar auf) auf "All Appliances and Devices" (Alle Anwendungen und Geräte) fest.
3. Danach werden Abfragen für diese Domänen von den VAs an den lokalen DNS weitergeleitet. Im Idealfall muss der lokale DNS so konfiguriert werden, dass er an Umbrella DNS unter 208.67.220.220/208.67.222.222 weitergeleitet wird. Sie können jedoch so konfiguriert werden, dass sie an einen beliebigen externen DNS weitergeleitet werden.
4. Der lokale DNS verarbeitet Abfragen für alle Domänen, für die sie autoritär sind.
5. Wenn der lokale DNS Abfragen für nicht lokale Domänen zulässt, werden die Abfragen für diese anderen Domänen an den externen DNS weitergeleitet.

Dies liegt daran, dass der lokale DNS DNS DNS-Ergebnisse zwischenspeichern kann, während die Roaming-Clients und virtuellen Appliances keine Zwischenspeicherung durchführen. Beachten Sie, dass diese Problemumgehung zu mehr Datenverkehr und einer höheren Auslastung des internen DNS führt. Überwachen Sie diese daher sorgfältig, um sicherzustellen, dass sie nicht überlastet sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.