F5 Load Balancer DNS-Weiterleitungskonfiguration für sicheren Zugriff

Inhalt

Problem

Die DNS-Auflösung funktionierte nicht, wenn bei der Migration von Umbrella zu Secure Access ein F5 Load Balancer als Client-DNS-Server verwendet wurde. Wenn DNS-Anfragen die virtuelle IP (VIP) erreichten, leitete der F5 Load Balancer erfolgreich Pakete an Back-End-DNS-Weiterleitungen weiter, die Hostnamen wurden jedoch nicht auf den Endgeräten aufgelöst. Die DNS-Auflösung funktionierte gut, wenn eine virtuelle Appliance direkt als Client-DNS-Server verwendet wurde. Dies zeigt an, dass das Problem spezifisch für die F5 Load Balancer-Konfiguration war.

Paketerfassungen ergaben, dass DNS-Antworten die IP-Adresse der virtuellen Appliance anstelle der erwarteten F5-VIP-Adresse verwendeten. Der Client-Computer erwartete DNS-Antworten von der F5-VIP-Adresse, erhielt jedoch stattdessen Antworten von der IP-Adresse der virtuellen Backend-Appliance.

Umwelt

- Cisco Umbrella to Secure Access-Migrationsumgebung
- F5 Load Balancer mit konfiguriertem DNS Load Balancing-VIP
- Mehrere DNS-Weiterleitungen als Backend-Server
- Virtuelle Appliances als DNS-Server
- Client-Endpunkte, die eine DNS-Auflösung über den Load Balancer erfordern

Auflösung

Das Problem wurde behoben, indem der F5 Load Balancer so konfiguriert wurde, dass er ordnungsgemäß als Proxy zwischen den Client-Computern und den virtuellen Appliances fungiert. Die wichtigste Konfigurationsänderung betrifft die Aktivierung von SNAT (Source Network Address Translation) mit automatischer Zuordnung.

Durchgeführte Diagnoseschritte

Schritt 1: DNS-Auflösungsverhalten überprüfen

Die DNS-Auflösung wurde sowohl mit dem F5 Load Balancer-VIP als auch mit direkten virtuellen Appliance-Verbindungen getestet, um das Problem zu isolieren.

Phase 2: Erfassung und Analyse von DNS-Datenverkehr

Paketerfassungen wurden durchgeführt, um den DNS-Anforderungs- und Antwortfluss über den F5 Load Balancer zu analysieren.

Schritt 3: Identifizieren der Nichtübereinstimmung der Quelladresse

Die Analyse ergab, dass die DNS-Antworten die IP-Adresse der virtuellen Appliance enthielten und nicht die F5-VIP-Adresse, was zu einer Client-Verwirrung führte.

Konfigurationsänderung

Schritt 1: F5 Load Balancer-Konfiguration aufrufen

Navigieren Sie zur Verwaltungsoberfläche des F5 Load Balancers, um die DNS-VIP-Konfiguration zu ändern.

Phase 2: Aktivieren der automatischen SNAT-Zuordnung

Konfigurieren Sie SNAT (Source Network Address Translation) für die automatische Zuordnung auf dem F5 Load Balancer. Dadurch wird sichergestellt, dass das F5-Gerät DNS-Anfragen und -Antworten zwischen Clients und Back-End-DNS-Servern ordnungsgemäß weiterleitet.

Schritt 3: Konfiguration überprüfen

Nach der Implementierung der automatischen SNAT-Zuordnungskonfiguration funktionierte die DNS-Auflösung über den F5 Load Balancer ordnungsgemäß.

Ursache

Die Ursache hierfür war die unsachgemäße SNAT-Konfiguration (Source Network Address Translation) auf dem F5 Load Balancer. Ohne die Aktivierung der automatischen SNAT-Zuordnung agierte das F5-Gerät nicht ordnungsgemäß als Proxy für den DNS-Datenverkehr. Dies führte dazu, dass DNS-Antworten direkt von den virtuellen Backend-Appliances an die Client-Computer gesendet wurden, wobei die IP-Adresse der virtuellen Appliance als Quelle anstatt der erwarteten F5-VIP-Adresse verwendet wurde. Client-Computer erwarteten, dass DNS-Antworten von derselben IP-Adresse ausgingen, an die sie ihre Anfragen gesendet hatten (die F5-VIP), aber Antworten von verschiedenen IP-Adressen (die Backend-Server) erhielten, was zu Fehlern bei der DNS-Auflösung führte.

Verwandte Inhalte

- F5 GTM-Lastenausgleich konfigurieren
- Technischer Support und Downloads von Cisco

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.