Configurazione inoltro DNS servizio di bilanciamento del carico F5 per l'accesso sicuro

Sommario

Problema

La risoluzione DNS non funziona quando si utilizza un servizio di bilanciamento del carico F5 come server DNS client durante la migrazione da Umbrella a Secure Access. Quando le richieste DNS raggiungono l'indirizzo IP virtuale (VIP), il servizio di bilanciamento del carico F5 ha inoltrato i pacchetti ai server di inoltro DNS back-end, ma i nomi host non sono stati risolti nei computer endpoint. La risoluzione DNS ha funzionato correttamente quando si utilizza un dispositivo virtuale direttamente come server DNS client, indicando che il problema era specifico della configurazione del bilanciamento del carico F5.

Le acquisizioni dei pacchetti hanno rilevato che le risposte DNS utilizzavano l'indirizzo IP dell'appliance virtuale anziché l'indirizzo VIP F5 previsto. Il computer client prevedeva che le risposte DNS provenissero dall'indirizzo VIP F5, ma ha invece ricevuto risposte dall'indirizzo IP dell'appliance virtuale back-end.

Ambiente

- Ambiente di migrazione da Cisco Umbrella a Secure Access
- Bilanciamento del carico F5 con VIP di bilanciamento del carico DNS configurato
- Più server di inoltro DNS come server back-end
- Appliance virtuali che fungono da server DNS
- Endpoint client che richiedono la risoluzione DNS tramite il servizio di bilanciamento del carico

Risoluzione

Il problema è stato risolto configurando il servizio di bilanciamento del carico F5 in modo che agisca correttamente come proxy tra i computer client e le appliance virtuali. La modifica alla configurazione principale ha comportato l'abilitazione di Source Network Address Translation (SNAT) con funzionalità di mappatura automatica.

Passi diagnostici eseguiti

Passaggio 1: Verifica comportamento risoluzione DNS

La risoluzione DNS è stata testata utilizzando sia il VIP del servizio di bilanciamento del carico F5 che le connessioni dirette dei dispositivi virtuali per isolare il problema.

Passaggio 2: Acquisire e analizzare il traffico DNS

Le acquisizioni dei pacchetti sono state eseguite per analizzare il flusso di richiesta e risposta DNS tramite il bilanciamento del carico F5.

Passaggio 3: Identifica indirizzo di origine non corrispondente

L'analisi ha rilevato che le risposte DNS contenevano l'indirizzo IP dell'appliance virtuale anziché l'indirizzo VIP F5, causando confusione nei client.

Modifica della configurazione

Passaggio 1: Accesso alla configurazione del servizio di bilanciamento del carico F5

Passare all'interfaccia di gestione del bilanciamento del carico F5 per modificare la configurazione VIP DNS.

Passaggio 2: Abilita mapping automatico SNAT

Configurare SNAT (Source Network Address Translation) per eseguire il mapping automatico sul bilanciamento del carico F5. Ciò garantisce che il dispositivo F5 invii correttamente tramite proxy le richieste e le risposte DNS tra client e server DNS back-end.

Passaggio 3: Verifica della configurazione

Dopo aver implementato la configurazione della mappa automatica SNAT, la risoluzione DNS ha iniziato a funzionare correttamente tramite il bilanciamento del carico F5.

Causa

La causa principale è stata una configurazione SNAT (Source Network Address Translation) non corretta nel bilanciamento del carico F5. Senza la mappatura automatica SNAT abilitata, il dispositivo F5 non agiva correttamente come proxy per il traffico DNS. Di conseguenza, le risposte DNS vengono inviate direttamente dai dispositivi virtuali back-end ai computer client, utilizzando come origine l'indirizzo IP del dispositivo virtuale anziché l'indirizzo VIP F5 previsto. I computer client prevedevano che le risposte DNS provenissero dallo stesso indirizzo IP a cui hanno inviato le richieste (VIP F5), ma ricevevano risposte da indirizzi IP diversi (server back-end), causando errori di risoluzione DNS.

Contenuto correlato

- Configura load balancing F5 GTM
- Supporto tecnico Cisco e download

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).