Comprendere perché le query per i domini interni non sono registrate in Umbrella Insights

Sommario

Introduzione

In questo documento viene descritto il motivo per cui le query per i domini interni non vengono registrate.

Panoramica

Quando si utilizza Umbrella Insights, che include Virtual Appliance (VA), tutte le workstation devono avere solo le impostazioni del server DNS che puntano ai VA. I VA devono essere configurati per utilizzare i server DNS interni preesistenti. Il dashboard consente di immettere un elenco di "domini interni" in modo che, quando il client esegue una query DNS per una risorsa interna, la richiesta venga inoltrata a uno dei server DNS interni. A volte ci viene chiesto perché nessuna di queste richieste interne appare nella registrazione.

Spiegazione

Come descritto in precedenza, le richieste DNS interne ricevute dal VA vengono inoltrate a uno dei server DNS interni configurati sul VA durante l'installazione. che possono essere visualizzati sulla console. Tutto sommato, il server DNS interno invia una risposta e il VA la ritrasmette al client.

Quando il client effettua una richiesta DNS per una risorsa che NON è presente nell'elenco dei domini interni, la inoltra agli indirizzi IP Anycast Umbrella. Questa richiesta include dati aggiuntivi nella query DNS per i nostri resolver, il che consente di associare la richiesta a un'origine. L'origine potrebbe essere, ad esempio, un hash UserID, un indirizzo IP di origine o una serie di altri fattori di identificazione inclusi in questo pacchetto DNS esteso. Questi dati aggiuntivi possono essere visualizzati eseguendo una query DNS specifica da una riga di comando:

```
nslookup -server=208.67.222.222 -type=txt debug.opendns.com.
```

La registrazione effettiva delle richieste DNS viene eseguita sui nostri resolver. La registrazione si

basa su queste informazioni univoche aggiunte al pacchetto DNS. Il VSA non registra le richieste DNS inoltrate. Si tratta innanzitutto di un server DNS ricorsivo. Una volta che i nostri resolver pubblici ricevono una query DNS, utilizza i dati estesi inviati con la query effettiva per identificare l'origine, applicare il criterio appropriato e registrare le informazioni della richiesta e se è stata consentita o bloccata, che quindi viene visualizzata nel dashboard. Poiché le query DNS interne non vedono mai i nostri resolver, non è possibile registrarli.

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).