Erfahren Sie, warum Abfragen für interne Domänen in Umbrella Insights nicht angemeldet sind.

Inhalt

Einleitung

In diesem Dokument wird beschrieben, warum Abfragen für interne Domänen nicht protokolliert werden.

Überblick

Bei Verwendung von Umbrella Insights, das die virtuelle Appliance (VA) beinhaltet, dürfen alle Workstations nur mit ihren DNS-Servereinstellungen auf die VAs verweisen. Die VAs müssen für die Verwendung Ihrer vorhandenen internen DNS-Server konfiguriert werden. Im Dashboard können Sie eine Liste der internen Domänen eingeben, sodass die VA die Anforderung an einen der internen DNS-Server weiterleitet, wenn der Client eine DNS-Abfrage für eine interne Ressource durchführt. Gelegentlich werden wir gefragt, warum keine dieser internen Anfragen in der Protokollierung auftaucht.

Erläuterung

Wie oben beschrieben, werden von der VA empfangene interne DNS-Anfragen während der Einrichtung an einen der in der VA konfigurierten internen DNS-Server weitergeleitet. Diese werden in der Konsole angezeigt. Der interne DNS-Server gibt eine Antwort aus, und die VA leitet diese an den Client weiter.

Wenn der Client eine DNS-Anfrage für eine Ressource stellt, die NICHT in der Liste der internen Domänen aufgeführt ist, leitet er diese an die Umbrella Anycast IP-Adressen weiter. Diese Anfrage enthält zusätzliche Daten in der DNS-Anfrage an unsere Resolver, wodurch die Anfrage an einen Ursprung zurückgebunden werden kann. Der Ursprung kann beispielsweise ein UserID-Hash, eine Quell-IP oder eine Reihe anderer Identifizierungsfaktoren sein, die in diesem erweiterten DNS-Paket enthalten sind. Diese zusätzlichen Daten können angezeigt werden, indem eine bestimmte DNS-Abfrage über eine Befehlszeile ausgeführt wird:

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

Die eigentliche Protokollierung von DNS-Anfragen erfolgt auf unseren Resolvern. Die Protokollierung basiert darauf, dass diese eindeutigen Informationen an das DNS-Paket angehängt werden. Die VA protokolliert die DNS-Anfragen nicht, an die sie weitergeleitet wird. Er ist in erster Linie ein rekursiver DNS-Server. Sobald unsere öffentlichen Resolver eine DNS-Abfrage empfangen, verwendet sie die erweiterten Daten, die mit der eigentlichen Abfrage gesendet wurden, um die Quelle zu identifizieren, die entsprechende Richtlinie anzuwenden und die Informationen der Anforderung zu protokollieren. Wenn diese zugelassen oder blockiert wurde, wird diese im Dashboard angezeigt. Da interne DNS-Abfragen unsere Resolver nie sehen, ist deren Protokollierung nicht möglich.

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.