DNS-Doctoring auf ASA - Konfigurationsbeispiel

Inhalt

Einleitung

Dieses Dokument zeigt, wie DNS Doctoring auf der Adaptive Security Appliance (ASA) verwendet wird, um die eingebetteten IP-Adressen in DNS-Antworten (Domain Name System) zu ändern, sodass Clients sich mit der richtigen IP-Adresse von Servern verbinden können.

Voraussetzungen

Anforderungen

DNS Doctoring erfordert die Konfiguration der Network Address Translation (NAT) auf der ASA sowie die Aktivierung der DNS-Inspektion.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Adaptive Security Appliance.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

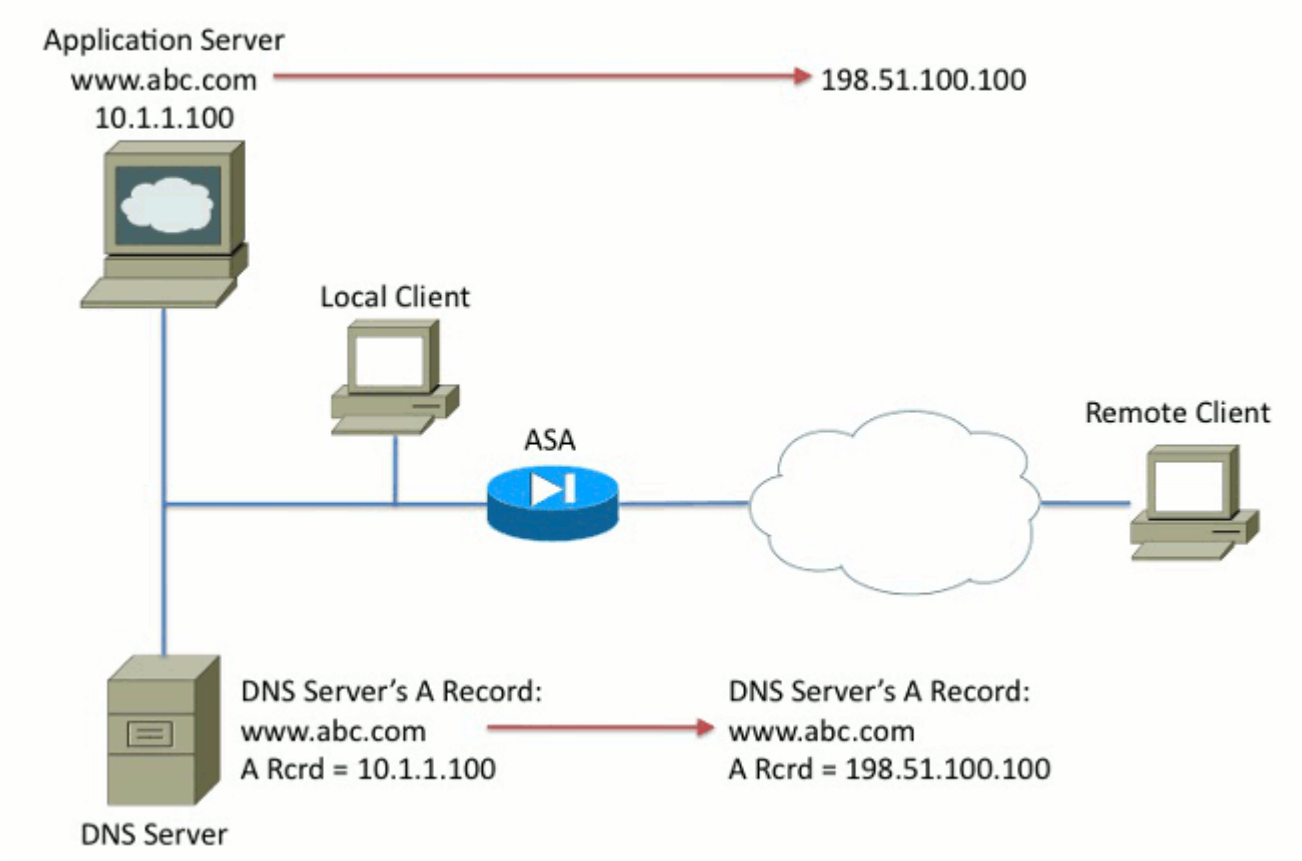
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Beispiele für DNS-Doctoring

DNS-Server auf der Innenseite der ASA

Abbildung 1



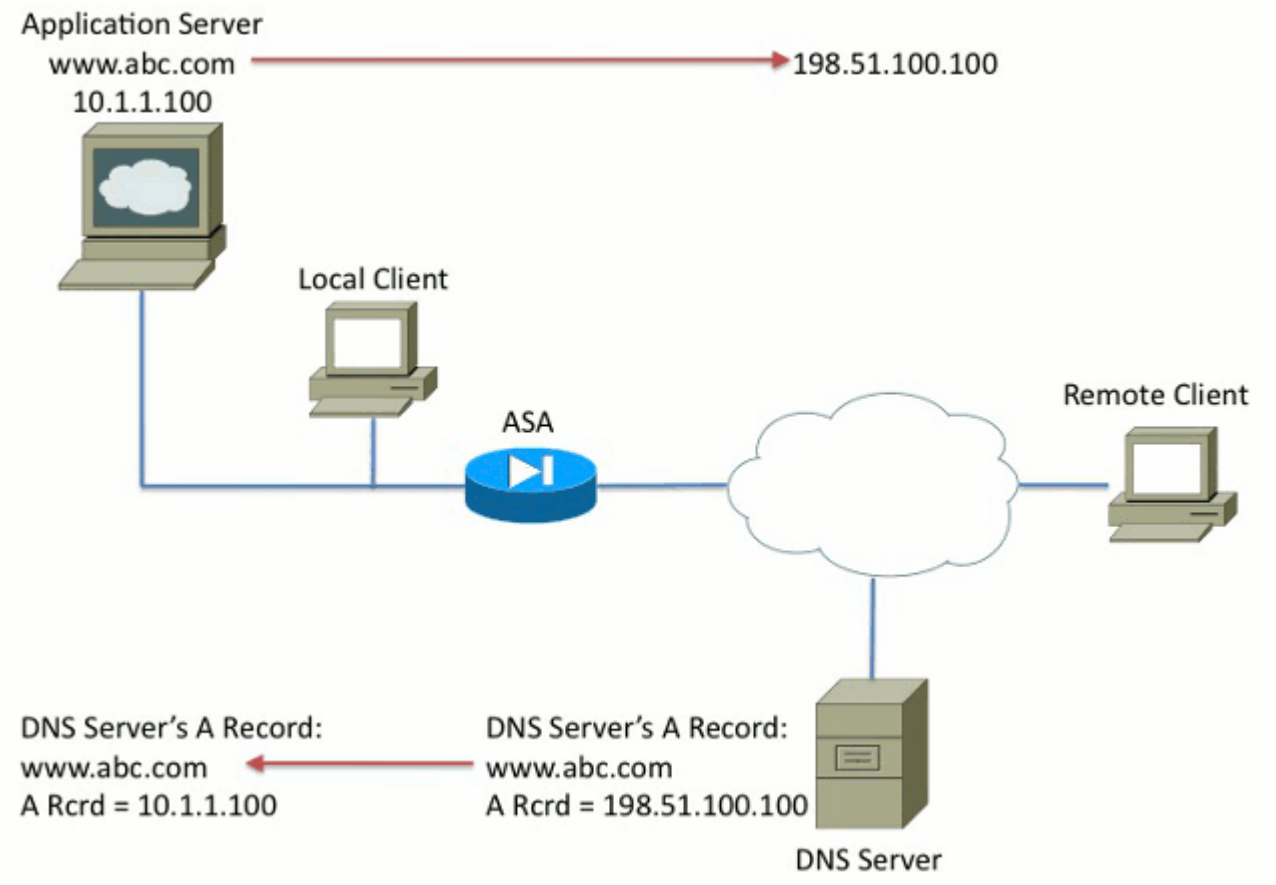

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

In Abbildung 1 wird der DNS-Server vom lokalen Administrator gesteuert. Der DNS-Server sollte eine private IP-Adresse angeben, d. h. die *tatsächliche* IP-Adresse, die dem Anwendungsserver zugewiesen wurde. Dadurch kann der lokale Client direkt mit dem Anwendungsserver verbunden werden.

Leider kann der Remoteclient nicht mit der privaten Adresse auf den Anwendungsserver zugreifen. Daher wird DNS Doctoring auf der ASA konfiguriert, um die eingebettete IP-Adresse im DNS-Antwortpaket zu ändern. Dadurch wird sichergestellt, dass der Remote-Client, wenn er eine DNS-Anfrage für www.abc.com stellt, die Antwort für die übersetzte Adresse des Anwendungsservers erhält. Ohne das DNS-Schlüsselwort in der NAT-Anweisung versucht der Remoteclient, eine Verbindung mit 10.1.1.100 herzustellen, was nicht funktioniert, da diese Adresse nicht im Internet geroutet werden kann.

DNS-Server außerhalb der ASA

Abbildung 2



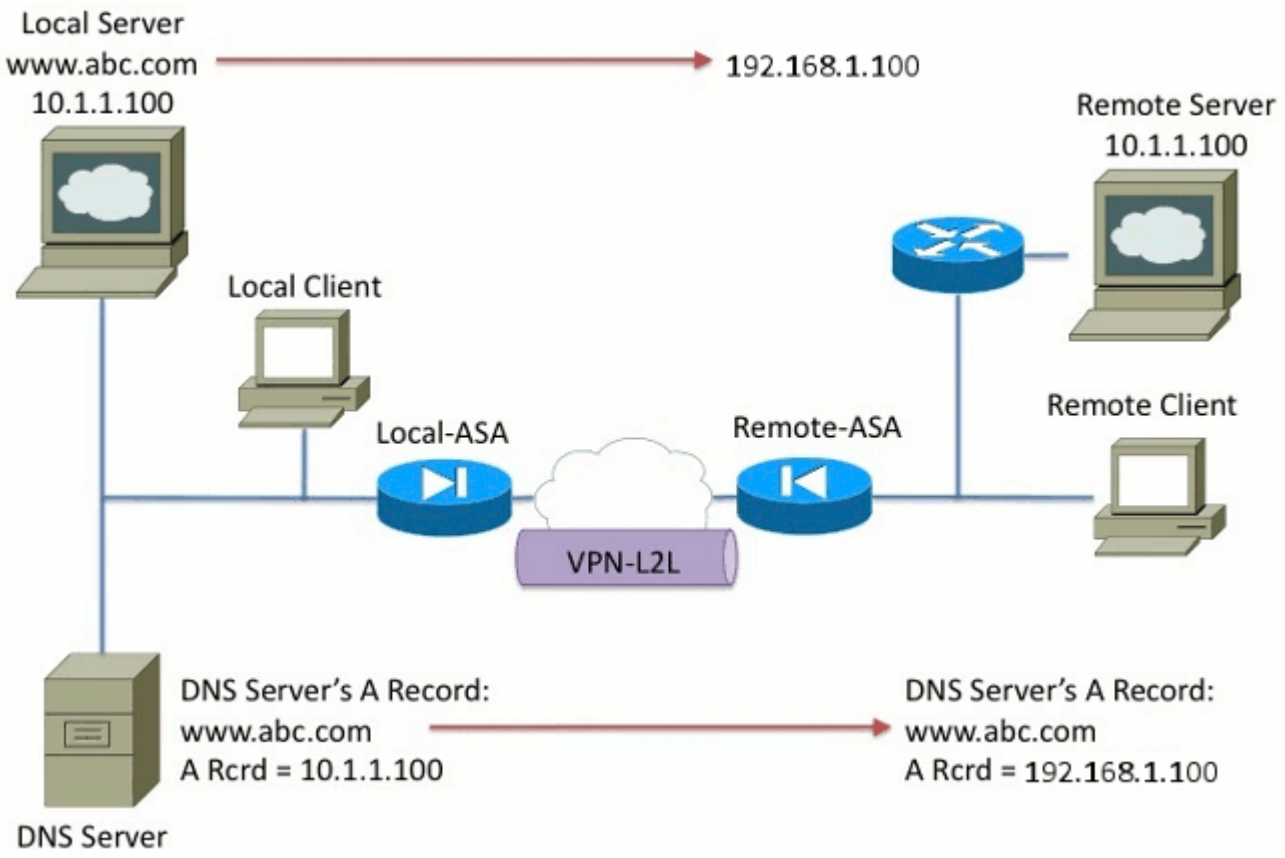

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

In Abbildung 2 wird der DNS-Server vom ISP oder einem ähnlichen Service Provider gesteuert. Der DNS-Server sollte die öffentliche IP-Adresse, d.h. die *übersetzte* IP-Adresse des Anwendungsservers, angeben. Dies ermöglicht allen Internetnutzern, über das Internet auf den Anwendungsserver zuzugreifen.

Leider kann der lokale Client nicht mit der öffentlichen Adresse auf den Anwendungsserver zugreifen. Daher wird DNS Doctoring auf der ASA konfiguriert, um die eingebettete IP-Adresse im DNS-Antwortpaket zu ändern. Dadurch wird sichergestellt, dass die empfangene Antwort die tatsächliche Adresse des Anwendungsservers ist, wenn der lokale Client eine DNS-Anfrage für www.abc.com stellt. Ohne das DNS-Schlüsselwort in der NAT-Anweisung versucht der lokale Client, eine Verbindung mit 198.51.100.100 herzustellen. Dies funktioniert nicht, da dieses Paket an die ASA gesendet wird, die das Paket verwirft.

VPN NAT und DNS Doctoring

Abbildung 3



Stellen Sie sich eine Situation vor, in der sich Netzwerke überschneiden. In diesem Zustand befindet sich die Adresse 10.1.1.100 sowohl auf der Remote-Seite als auch auf der lokalen Seite. Daher müssen Sie NAT auf dem lokalen Server ausführen, damit der Remote-Client weiterhin mit der IP-Adresse 192.1.1.100 darauf zugreifen kann. Damit dies richtig funktioniert, ist DNS Doctoring erforderlich.

Die DNS-Dokumentation kann in dieser Funktion nicht ausgeführt werden. Das DNS-Schlüsselwort kann nur am Ende einer Objekt-NAT oder Quell-NAT hinzugefügt werden. Das Schlüsselwort double NAT unterstützt das DNS-Schlüsselwort nicht. Es gibt zwei mögliche Konfigurationen, und beide sind fehlerhaft.

Fehlgeschlagene Konfiguration 1: Wenn Sie das Endergebnis konfigurieren, wird 10.1.1.1 in 192.1.1.1 übersetzt, und zwar nicht nur für den Remote-Client, sondern für alle Benutzer im Internet. Da 192.1.1.1 nicht über das Internet routbar ist, kann niemand im Internet auf den lokalen Server zugreifen.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Fehlgeschlagene Konfiguration 2: Wenn Sie die DNS Doctoring NAT-Leitung nach der erforderlichen doppelten NAT-Leitung konfigurieren, führt dies zu einer Situation, in der die DNS Doctoring nie funktioniert. Als Ergebnis versucht der Remote-Client, über die IP-Adresse 10.1.1.100 auf www.abc.com zuzugreifen, was nicht funktioniert.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Zugehörige Informationen

- **Cisco Adaptive Security Appliances der Serie ASA 5500**
- **Cisco Adaptive Security Appliances der Serie ASA 5500 > Software-Downloads**
- **Technischer Support und Dokumentation für Cisco Systeme**

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.