ASA 컨피그레이션에 대한 DNS Doctoring 예

목차

소개

이 문서에서는 클라이언트가 서버의 올바른 IP 주소에 연결할 수 있도록 DNS(Domain Name System) 응답에서 포함된 IP 주소를 변경하기 위해 ASA(Adaptive Security Appliance)에서 DNS Doctoring을 사용하는 방법을 보여 줍니다.

사전 요구 사항

요구 사항

DNS Doctoring을 사용하려면 ASA에서 NAT(Network Address Translation)를 구성하고 DNS 검사를 활성화해야 합니다.

사용되는 구성 요소

이 문서의 정보는 Adaptive Security Appliance를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

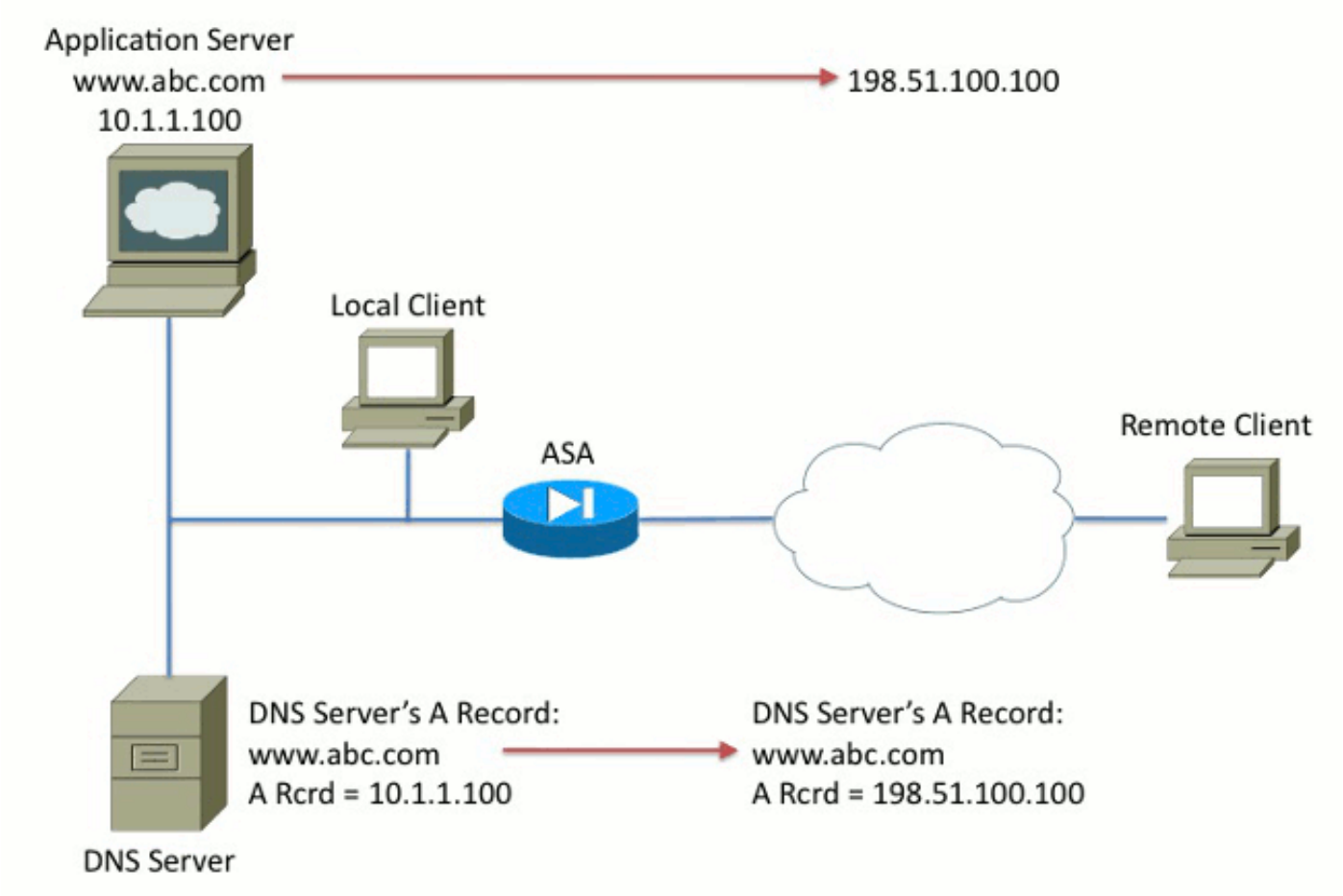
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

DNS 문서화 예

ASA 내부의 DNS 서버

그림 1



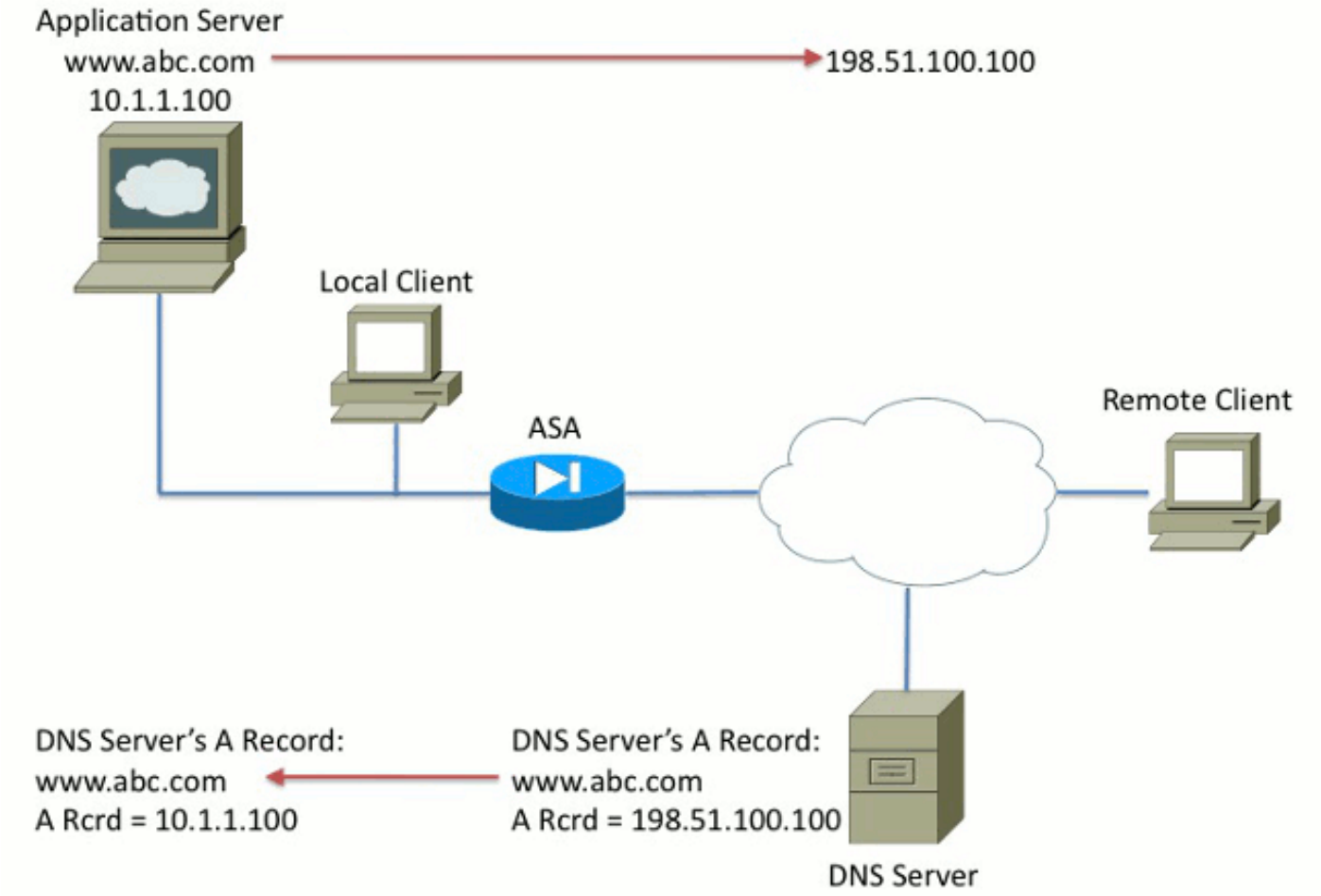

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

그림 1에서 DNS 서버는 로컬 관리자에 의해 제어됩니다. DNS 서버는 애플리케이션 서버에 할당된 실제 IP 주소인 개인 IP 주소를 제공해야 합니다. 이렇게 하면 로컬 클라이언트가 응용 프로그램 서버에 직접 연결할 수 있습니다.

죄송합니다. 원격 클라이언트가 개인 주소로 애플리케이션 서버에 액세스할 수 없습니다. 그 결과 DNS 응답 패킷 내에 포함된 IP 주소를 변경하기 위해 ASA에서 DNS Doctoring이 구성됩니다. 이렇게 하면 원격 클라이언트가 www.abc.com에 대한 DNS 요청을 할 때 애플리케이션 서버의 변환된 주소에 대한 응답을 받게 됩니다. NAT 문에 DNS 키워드가 없으면 원격 클라이언트는 10.1.1.100에 연결을 시도합니다. 10.1.100은 해당 주소를 인터넷에서 라우팅할 수 없으므로 작동하지 않습니다.

ASA 외부의 DNS 서버

그림 2



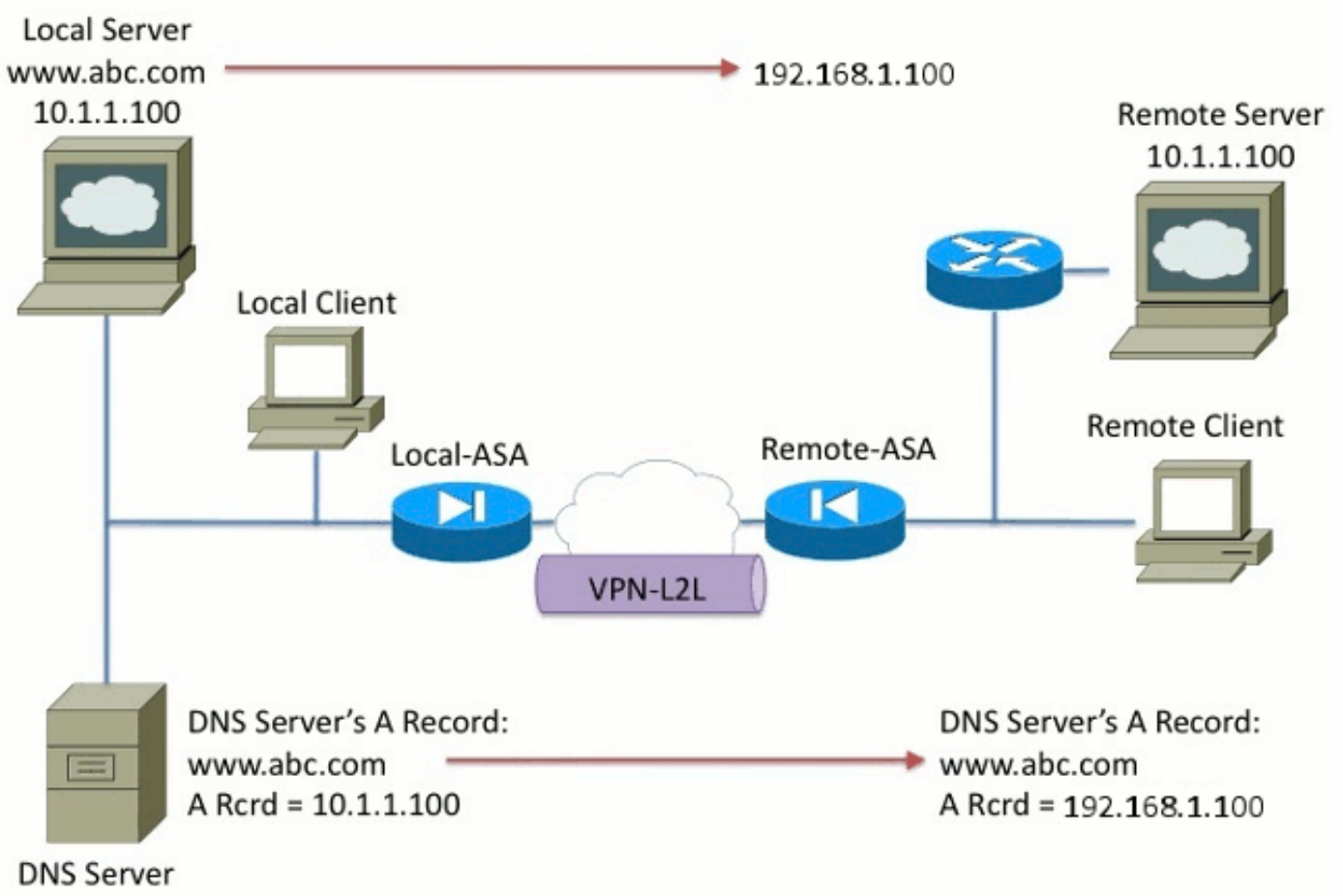

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

그림 2에서 DNS 서버는 ISP 또는 유사한 서비스 공급자에 의해 제어됩니다. DNS 서버는 공용 IP 주소, 즉 애플리케이션 서버의 변환된 IP 주소를 제공해야 합니다. 이렇게 하면 모든 인터넷 사용자가 인터넷을 통해 애플리케이션 서버에 액세스할 수 있습니다.

죄송합니다. 로컬 클라이언트가 공용 주소를 사용하여 애플리케이션 서버에 액세스할 수 없습니다. 그 결과 DNS 응답 패킷 내에 포함된 IP 주소를 변경하기 위해 ASA에서 DNS Doctoring이 구성됩니다. 이렇게 하면 로컬 클라이언트가 www.abc.com에 대한 DNS 요청을 할 때 수신된 응답이 애플리케이션 서버의 실제 주소가 됩니다. NAT 문에 DNS 키워드가 없으면 로컬 클라이언트는 198.51.100.100에 연결을 시도합니다. 이 패킷은 ASA로 전송되어 패킷을 삭제하므로 작동하지 않습니다.

VPN NAT 및 DNS 문서화

그림 3



네트워크가 겹치는 상황을 고려해 보십시오. 이 조건에서 주소 10.1.1.100은 원격 측과 로컬 측에 모두 상주합니다. 따라서 원격 클라이언트가 IP 주소 192.1.1.100을 사용하여 계속 액세스할 수 있도록 로컬 서버에서 NAT를 수행해야 합니다. 이 기능이 제대로 작동하려면 DNS Doctoring이 필요합니다.

이 함수에서는 DNS Doctoring을 수행할 수 없습니다. DNS 키워드는 개체 NAT 또는 소스 NAT의 끝에만 추가할 수 있습니다. Twice NAT는 DNS 키워드를 지원하지 않습니다. 가능한 컨피그레이션에는 두 가지가 있으며 둘 다 실패합니다.

실패한 컨피그레이션 1: 하위 라인을 구성하면 원격 클라이언트뿐만 아니라 인터넷에 있는 모든 사용자에 대해 10.1.1.1에서 192.1.1.1로 변환됩니다. 192.1.1.1은 인터넷 라우팅이 가능하지 않으므로 인터넷에 있는 사용자는 로컬 서버에 액세스할 수 없습니다.

```
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
```

실패한 컨피그레이션 2: 필요한 Twice NAT 라인 다음에 DNS Doctoring NAT 라인을 구성하면 DNS Doctoring이 작동하지 않는 상황이 발생합니다. 그 결과, 원격 클라이언트는 IP 주소 10.1.1.100을 사용하여 www.abc.com에 액세스하려고 시도하지만 작동하지 않습니다.

```
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
```

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco ASA 5500 Series Adaptive Security Appliance > 소프트웨어 다운로드
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.