터미널 서비스, Citrix 및 Umbrella와 Active Directory 통합 이해

목차

소개

이 문서에서는 터미널 서비스, Citrix 및 Active Directory와의 Umbrella Integration에 대해 설명합니다.

개요

적용 대상: Windows 터미널 서비스 및 원격 데스크톱 서비스, Windows 10 Enterprise 다중 세션, Citrix XenApp 및 XenDesktop

터미널 서비스 및 Citrix 서버는 여러 개의 동시 클라이언트 세션을 단일 서버에서 호스팅할 수 있는 기능을 제공합니다. 다음 두 가지 구성이 있습니다.

- RDS(원격 데스크톱 서비스). 여러 사용자가 동일한 서버의 단일 가상 머신에서 세션을 실행합니다. 이러한 세션은 모두 동일한 OS 및 IP 주소를 공유합니다. 이를 일반적으로 터미널 서비스라고 합니다.
- 가상 데스크톱 인프라(VDI). 서버는 가상 머신 풀을 실행하며 각 사용자는 고유한 운영 체제 및 IP 주소를 사용하여 고유한 VM에 연결합니다

웹 정책: RDS 및 VDI에 적용 가능

PAC 파일, CDFW 터널 및 프록시 체인을 통한 SAML 쿠키 기반 인증을 사용하는 보안 웹 게이트웨이는 단일 IP 주소에 대해 여러 사용자를 지원합니다. 즉, 사용자 웹 정책 시행별로 가상 데스크톱(Citrix/TS)이 지원됩니다.

DNS 정책: AD가 통합된 RDS

사용자 단위 식별을 위해 RDS/원격 데스크톱 세션 호스트/터미널 서버를 지원하지 않습니다. 여기에는 Azure 전용 Windows 10 Enterprise 다중 세션 OS가 포함됩니다.

이러한 서버에서 호스팅되는 클라이언트 세션은 단일 IP 주소를 공유합니다. 호스트 컴퓨터에 속하는 AD(Umbrella Active Directory)와 VA(가상 어플라이언스)의 통합은 올바르게 작동하기 위해 고유한 사용자-IP 주소 매핑에 의존합니다. 즉, 사용자가 동일한 소스 IP 주소를 공유하는 어떤 상황에서도 사용자별 식별이 가능하지 않음을 의미합니다.

로그인한 여러 사용자가 동일한 IP를 공유하는 경우 정책 애플리케이션 및 보고에 부정적인 영향을 미칩니다. 모든 사용자는 동일한 정책을 받으며, 식별된 사용자는 마지막으로 로그온한 사용자를 기반으로 지속적으로 변경할 수 있습니다.

DNS 정책: 솔루션 - RDS(AD 통합)

이 문제를 해결하는 가장 좋은 방법은 터미널 서버 또는 Citrix 서버의 IP 주소에 대한 고유한 정책을 구성하는 것입니다. 이는 터미널 서버의 모든 사용자가 동일한 일관된 정책을 수신함을 의미합니다.

1. 'Deployments(구축) > Internal Networks(내부 네트워크)'에서 내부 네트워크를 생성합니다. 터미널 서버의 /32 IP 주소를 다룹니다. 해당 가상 어플라이언스와 동일한 Umbrella 사이트에 네트워크를 할당합니다.
2. 정책 마법사로 이동하여 새 정책을 생성합니다.
3. ID 선택 섹션에서 '사이트'를 클릭한 다음 관련 Umbrella 사이트를 엽니다.
4. 이전에 생성한 내부 네트워크 ID를 선택합니다
5. 평소와 같이 정책을 구성합니다
6. 터미널 서버에 대한 정책을 생성한 후에는 모든 사용자 기반 정책보다 우선하도록 정책 목록의 맨 위에 이 정책을 정렬해야 합니다.

또는 AD 컴퓨터 ID를 기반으로 터미널 서버에 대한 정책을 만들 수 있습니다. 이 방법은 동일한 방식으로 작동합니다. 서버의 모든 사용자는 터미널 서버 컴퓨터 이름으로 식별됩니다. 그러나 이 기능이 일관성 있게 작동하려면 호스트-IP 매핑을 최적화하는 방식으로 VA를 구성해야 합니다. 자세한 내용은 AD 호스트 GUID 시간 초과 지침을 참조하거나 Umbrella 지원에 문의하십시오.

DNS 정책: AD 통합에 VDI 사용

각 사용자에 대해 실행되는 고유한 가상 머신이 있는 VDI 유형 구축은 사용자별 ID를 계속 수신할 수 있습니다. 요구 사항은 다음과 같습니다.

- 가상 어플라이언스 - 각 사용자는 가상 어플라이언스에 표시되는 고유한 소스 IP를 가져야 합니다. 소스 IP는 어플라이언스에 도달하기 전에 "Source NATing"의 대상이 아니어야 합니다.
- 로밍 클라이언트 - 로밍 클라이언트가 각 가상 컴퓨터에 설치되어 있는 경우 로밍 클라이언트에서의 AD 통합이 가능합니다. 이러한 방식으로 구축하는 것은 각각의 사용자가 지속성을 가질 때 더 실현 가능하다(예를 들어, 가상 머신.

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.