시스코 4D SD-WAN (Viptela) v1

마지막 업데이트: 2017 년 9 월 1 일

본 데모에 대하여

미리 구성되어 있는 본 데모는 아래 내용을 포함합니다.

준비 사항

아래 항목은 데모를 진행하는데 필요한 구성요소입니다.

테이블 1. 준비 사항

필수	옵션
●개인용 컴퓨터	● 시스코 AnyConnect®

아젠다 – 본 데모의 목표

이 가이드는 아래와 같은 시나리오의 내용을 포함하고 있습니다.

시나리오 1 – SD-WAN vManage 대시 보드 개요 및 Zero Touch Provisioning (ZTP) 기능에 대해 토론합니다. 디자인 모범 사례를 통해 제로 터치(Zero Touch) 프로비저닝 및 중앙 집중식 구성을 이용한 자동화를 활용해 지사 라우터를 손쉽게 프로비저닝 할 수 있습니다. 중앙 집중식 구성은 장치 배포 전 사전에 정의해 놓을 수 있는 템플릿을 사용합니다.

시나리오 2 – 다양한 방식의 WAN 전송을 통해 하이브리드 WAN 연결을 사용합니다. 연결은 어떤 종류의 전송 방식 또는 응용 프로그램에 대해서도 수립될 수 있습니다. IP 를 이용해 Full-Mesh 및 Hub-n-Spoke 또는 그 밖의 다른 구성 형태까지도 지원 가능한 데이터 플레인을 생성하여 데이터를 전송합니다.

시나리오 3 – 중앙 집중식 정책을 사용하여 비즈니스 요구사항에 맞는 서비스 (FW, IPS, IDS 등) 를 포함시킵니다. 이 서비스는 물리적 구성 형태와 상관없이 유연하게 배포 가능하며 간단한 방식의 정책 적용을 통해 응용 프로그램 및 사이트에 대해 선택적 서비스 기능을 수행할 수 있습니다.

시나리오 4 – 중앙 집중형 애플리케이션 방화벽 정책을 얼마나 손쉽게 사용할 수 있는지 보여줍니다. 사이트간 애플리케이션 및 / 또는 플로우는 허용되지 않습니다. 간단히 정책을 활성화시켜 오버레이 환경을 통해 모든 사이트에 정책을 적용할 수 있습니다.

시나리오 5 - 임의의 네트워크 구성에 대해 애플리케이션 인식 라우팅을 사용하여 응용 프로그램 분류(classification), 연결 및 QoS 프로비저닝을 확인합니다. 애플리케이션 퍼포먼스 설정에 대해 논의하면서 일관된 애플리케이션 경험을 유지할 수 있도록 네트워크가 동적으로 경로를 전환하는 능력을 강조하십시오.

시나리오 6 – 각 브랜치 사이트별로 정책을 기반으로 한 데이터센터 선택. 일부 하위 브랜치 사이트들은 해당 지역에 대한 인터넷 게이트웨이로 특정 데이터 센터를 선호할 수 있습니다.

노트: 본 데모는 표준 디바이스 레벨 QoS, 라우팅 프로토콜, 네트워크 관리 인터페이스 등의 일반적인 SD-WAN 의 이용 사례에는 초점을 맞추지 않습니다. 본 데모는 중앙 집중형 제어 및 정책 기반의 고급 SD-WAN 의 기능을 보여주는 것입니다.

노트: 클라우드 익스프레스 (SaaS 솔루션) 및 클라우드 온램프(On-Ramp) (IaaS 솔루션)는 본 데모에 포함되지 않습니다.

이 시나리오를 통해 다음을 수행 할 수 있습니다:

- SD-WAN vManage 기능 데모.
- 고객의 환경 및 계획에 대한 연관성 확인.
- 최대한 간단하게 진행하며 본 솔루션에 대한 심화 과정은 다루지 않음.
- 단순화된 관리 기능을 강조.
- 프로비저닝, 구성 관리, 정책 관리, 모니터링 및 문제 해결을 위해 중앙 집중식 GUI 인터페이스를 제공.

데모 진행 시 고객과의 대화는 전체적인 비용 및 구성 환경의 복잡성을 축소시킬 수 있다는 점에 초점을 맞추십시오. 본 가이드는 일반적인 과제, 솔루션 이점 및 관련 데모 플로우를 포함하고 있습니다.

과제(Challenges)

비용 및 복잡성.

- 리모트 사이트의 네트워크 구성에는 많은 시간과 비용이 소모
- 애플리케이션 정책을 네트워크 인프라 구성에 그대로 적용하기가 쉽지 않음
- WAN 전송 상태 및 그에 따른 애플리케이션 영향도에 대한 가시성 부족
- 엔드-투-엔드 WAN 구성의 복잡성
- 중앙 집중형 구성 및 정책 관리, 모니터에 대한 기능 부족

효과(Benefits)

비용 및 복잡성의 감소

- 서비스 제공을 위한 시간을 단축하고 비용을 절감 할 수 있도록 자동화된 제로 터치 프로비저닝
- 템플릿 사용을 통해 모든 네트워크 디바이스 구성을 중앙 집중형으로 관리
- 중앙 집중식 vManage 를 통해 비즈니스 정책을 정의 및 활성화
- 중앙 집중식 vManage 를 통해 애플리케이션 및 WAN 전송 상태에 대한 가시성 확보
- 운영 단순성

데모 환경에 대한 참고 사항

이 가이드는 AM 및 SE 가 Cisco SD-WAN 의 주요 기능을 손쉽게 데모해볼 수 있도록 만들어졌습니다. 여기에는 제로 터치 프로비저닝 (Zero touch provisioning), 퍼포먼스 기반 애플리케이션 경로 선택(Performance based Application path selection) 지역 및 다이렉트 인터넷 액세스(Regional and Direct Internet Access), 정책 기반 토폴로지 생성, vManage (관리 , 오케스트레이션)를 포함하고 있습니다.

이 데모는 dCloud 를 통해 제공되며 다음과 같이 구성됩니다:

- ZTP, vManage, 애플리케이션 인식 라우팅 데모
- 데모 시뮬레이션용 데이터
  - 데이터는 수정 불가
  - 장치 프로비저닝 애플리케이션 또는 기타 변경 사항은 적용됨
  - 일부 고급 SD-WAN 이용 사례를 보여주기 위해 사용

이 데모는 일부 기능 구현을 위한 용도로 범위가 제한됩니다. Cloud Express 및 Cloud On-Ramp 는 데모에 포함되지 않습니다.

Cisco Intelligent SD-WAN 은 모든 종류의 전송 방식을 통해 뛰어난 사용자 경험을 제공하고 비용을 절감 및 운영을 단순하게 만들어 네트워크 규모에 맞게 비지니스를 수행할 수 있게끔 합니다. 이제 IT 부서는 예상치 못한 비용, 다운 타임 및 의도하지 않은 시스템 복잡성을 방지하는데 필요한 모든 차세대 WAN 기능의 요구 사항을 보장함과 동시에 최고의 성능, 안정성 및 보안 기능으로 WAN 에 대한 투자를 최대한 활용할 수 있습니다.

노트: vManage 대시 보드를 통해 통계값을 보기 위해서는 dCloud 세션이 30 분 이상 가동되어야 합니다.
그에 따라 데모를 계획하십시오.

솔루션 구성 요소

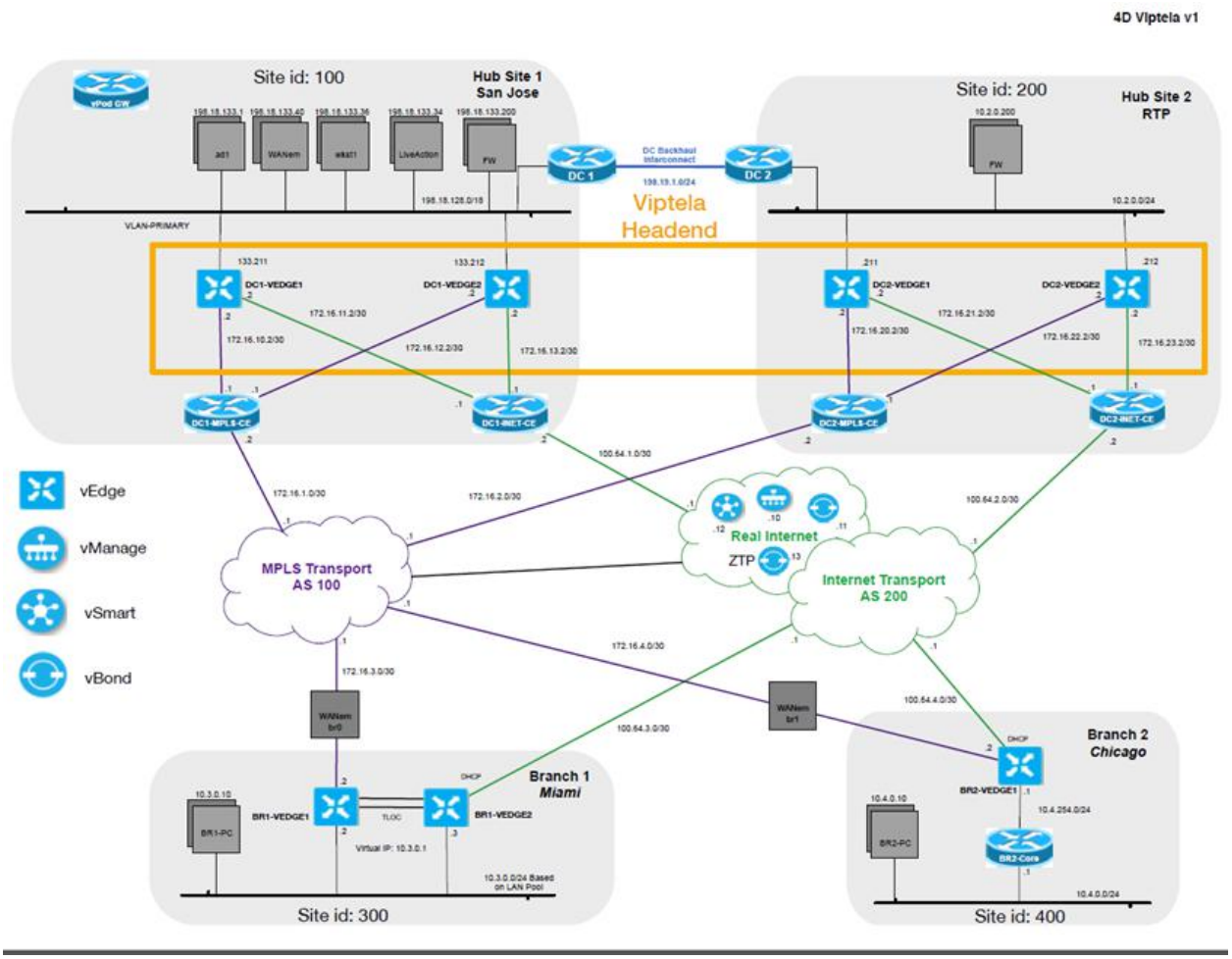
솔루션의 주요 구성 요소

- Orchestrator 는 모든 SD-WAN 구성 요소 (vBond) 간의 보안 통신을 조정
- 중앙 관리 및 프로비저닝 시스템 (vManage)
- 라우팅 및 정책 컨트롤러 (vSmart) 용 중앙 집중식 컨트롤러
- 데이터 플레인 라우터 (vEdge)

토폴로지

본 데모는 시나리오의 원활한 진행 및 솔루션이 제공하는 각 기능들의 동작 확인을 위해 사전에 미리 설정된 구성요소들을 포함하고 있습니다. 대부분의 구성요소들은 별도로 제공되는 관리자 계정을 통해 설정이 가능하며 **토폴로지** 메뉴에 있는 각 구성요소 아이콘을 클릭하면 접속하기 위한 IP 어드레스 및 계정 정보를 확인할 수 있습니다.

Figure 1. dCloud 토폴로지



OSPF 는 DC 와 Branch 1 에서 실행됩니다.

데이터 플레인 연결 테스트를 위해 다음 호스트 IP 정보를 사용하십시오.

- DC1 : 198.18.133.1
- DC2 : 10.2.0.1
- Branch 1 : 10.3.0.1
- Branch 2 : 10.4.254.254

데모 시작하기

시작하기에 앞서

고객 및 파트너를 대상으로 데모시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다.

데모 완료 후 새로이 구성을 해야 하는 경우는 세션을 새로 예약하십시오.

사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.

세션 예약 및 데모환경을 준비하기 위하여 아래 절차를 따라 주십시오..

1. dCloud 세션 시작. [Show Me How]

노트: 세션 예약 후 시나리오의 랩이 활성화 되기까지 최대 45 분 소요됩니다..

2. 보다 빠른 환경으로 시나리오 진행을 원하는 경우는 **시스코 AnyConnect VPN 클라이언트 클라이언트** [가이드] 및 **이용자 컴퓨터에 있는 로컬 RDP 클라이언트를** 이용해 접속하십시오. [가이드]

   - Workstation 1: **198.18.133.36**, Username: **dcloud\administrator**, Password: **C1sco12345**

노트 : 클라우드의 원격 트레스웨어 클라이언트 [가이드]를 접속할 수 있습니다. dCloud 를 제공하는 원격 데스크톱 컴퓨터는 최소한의 시스템 워크로드를 사용하여 원격 환경에서 환경을 제공합니다

참고: vManage 대시 보드를 통해 통계값을 확인하려면 dCloud 세션이 30 분 이상 작동해야 합니다. 그에 따라 계획하십시오.

시나리오 1. 설명

포인트 투 포인트 연결 뿐만 아니라 모든 종류의 전송 방식에 대한 대역폭 증가 이슈를 고려해야 한다면 전반적인 비즈니스 전략의 일환으로 SD-WAN 을 수용하여 조직 전반의 비용 절감, 투자 극대화, 애플리케이션 경험 향상 및 조직 전반의 혁신적인 서비스 제공, 민첩성을 갖출 수 있습니다.

관리 솔루션은 Fast IT 를 실현하기 위한 중요한 부분입니다. Cisco-SD Wan 솔루션은 온 프레미스, 클라우드 또는 서비스 사업자 형태의 솔루션 방식을 통해 효과적으로 관리 할 수 있습니다. 단순해진 제어방식 요구를 만족시키기 위해 중요한 솔루션 기능을 간과해서는 안됩니다. Cisco SD WAN 은 단순히 귀사의 요구사항만을 만족시킬 뿐만 아니라 애플리케이션 인식 라우팅 및 제로 터치 프로비저닝을 경험할 수 있도록 합니다. vManage 는 네트워크를 효율적으로 관리하고 운영하기 위해 단일 관리 플랫폼을 제공합니다. vMange 는 핵심 네트워크 자동화 솔루션 및 효율적인 운영을 주도하는 개방형 Northbound REST API 를 제공합니다.

또한 vEdge 라우터는 귀사가 Greenfield 및 Brownfield 환경에 솔루션의 가치를 전달할 수 있도록 여러 가지의 South-bound 프로토콜을 지원합니다.
제로 터치 프로비저닝 및 중앙 집중식 정책 제어를 이용해 브랜치 사이트에 대한 민첩성 제공을 간단한 데모를 통해 확인하겠습니다.
이 시나리오는 ZTP 오토메이션 기능을 이용해 어떻게 장비가 안전하게 탐지되고 프로비저닝 됐는지를 보여주는 브랜치 사이트 구성요소에 대한 오버뷰를 제공합니다.

NOTE: vManage 는 정기적으로 장치에서 통계 데이터를 수집합니다. vManage 대시보드에 그래픽 데이터를 올바르게 표시하려면 데모를 진행하기 전에 dcloud 세션을 최소 45 분 동안 실행 상태로 놔두십시오.

처음 BR2-vEDGE1 을 가동하는 경우도 마찬가지로 디바이스 대시보드에 플로우 및 DPI 그래픽 데이터를 표시하려면 최대 20~30 분이 소요될 수 있습니다.

과제

- 원격 사이트 네트워크 설치는 시간이 많이 소요되고 비용이 많이 소요됩니다.

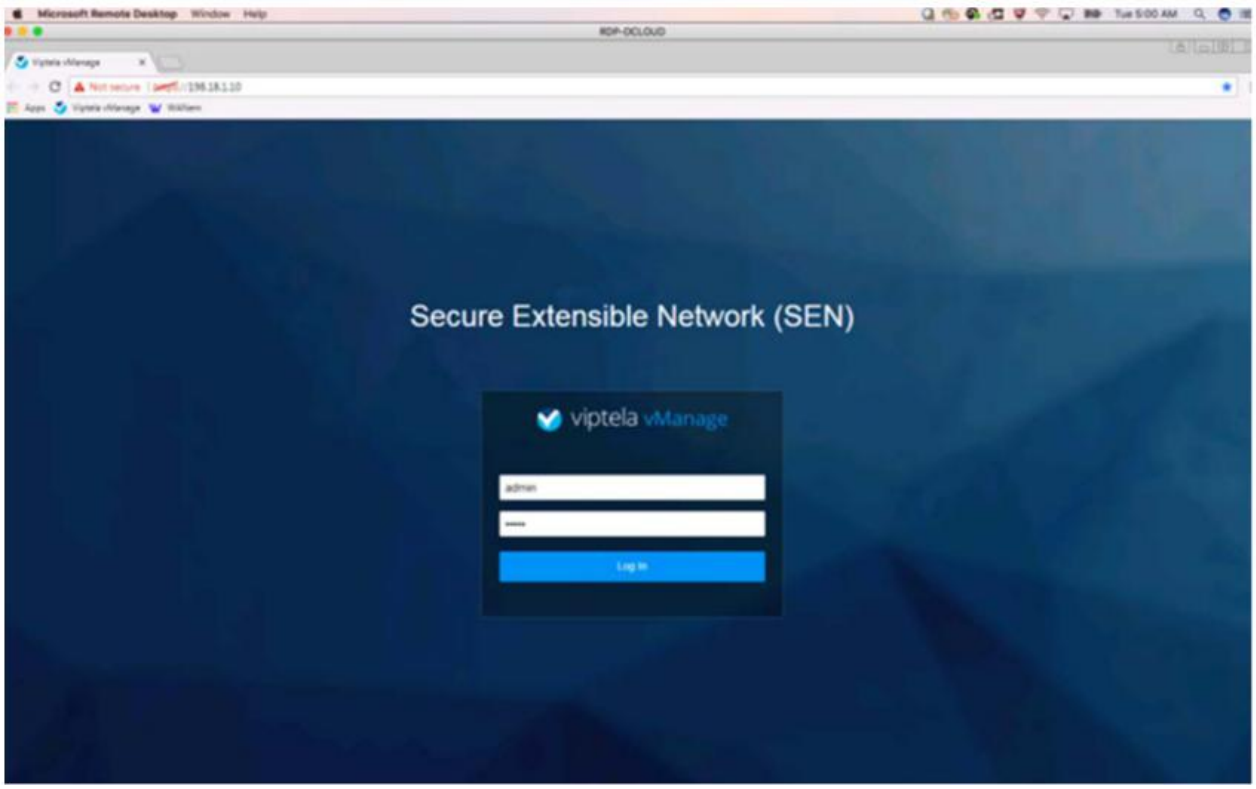
효과 – 비용 및 복잡성 감소

- 신속한 서비스를 위해 시간 단축 및 비용 절감을 위한 자동화 및 적응형 프로비저닝

스텝

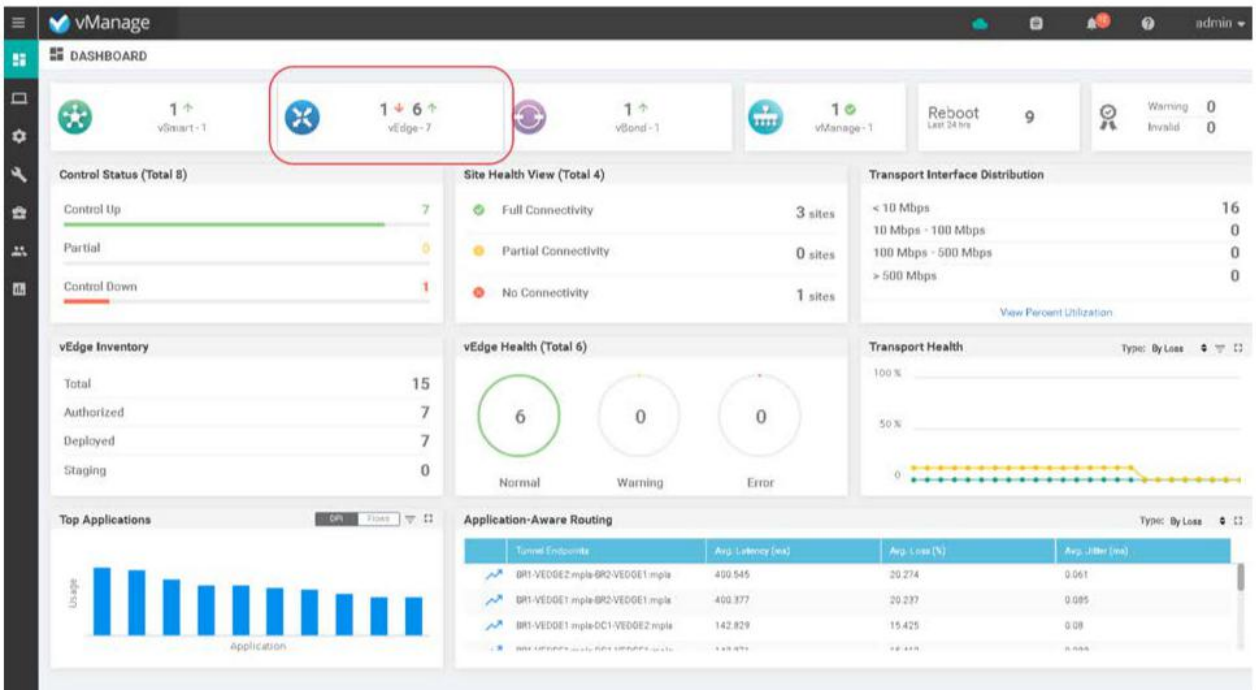
vManage 구성 템플릿 및 Viptela 의 ZTP (Zero Touch Provisioning) 서비스를 이용하여 브랜치를 구성합니다. 이 랩에서는 일부 시스템 레벨 구성을 제외한 모든 구성 프로세스를 제거하여 ZTP 프로세스를 시뮬레이션합니다. ZTP 포트 (ge0 / 1)는 Shut-down 상태입니다. vEdge 연결을 위해 “no shut” 을 수행합니다.

Workstation 1 에 접속하여 Chrome 브라우저를 실행하십시오. 보안 경고를 클릭하고 vManage 서비스에 접속합니다. 사용자 이름 및 암호로 admin / admin 을 사용하여 vManage 에 로그인 한 다음 Enter 키를 누릅니다.

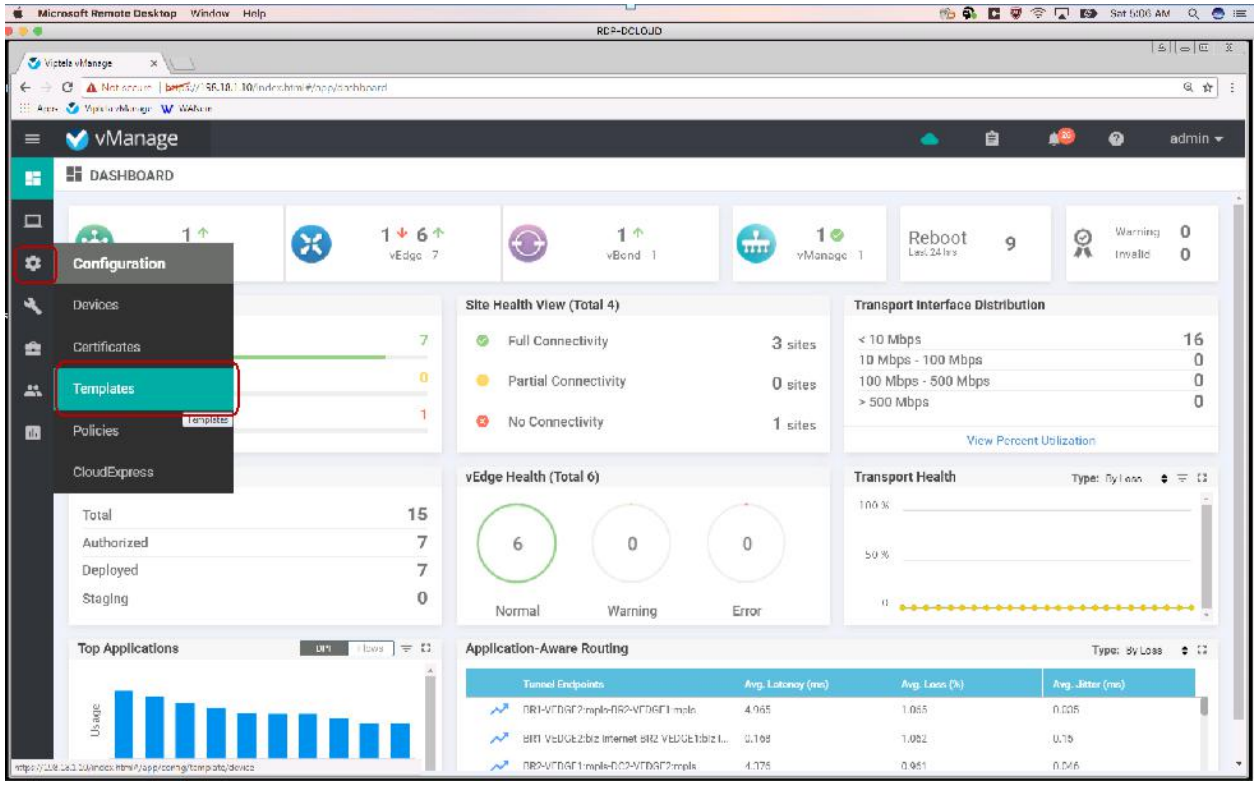


vManage 대시 보드로 이동합니다. 대시 보드에는 컨트롤러가 동작 중이며 가동 중인 6 개의 vEdge 가 있습니다. vEdge 중 하나는 지점 2 에 아직 제공되지 않습니다.

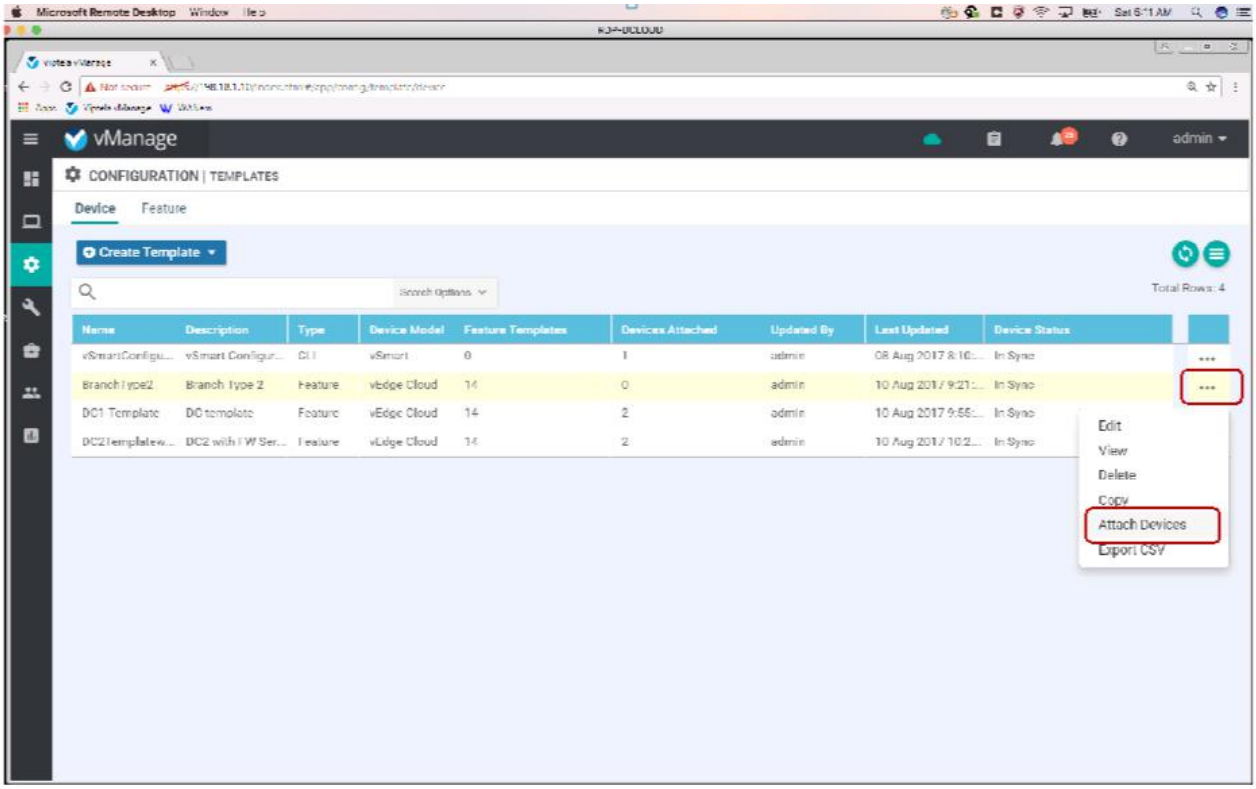
노트: 위쪽 화살표는 작동중인 vEdge Boxes 를 표시하고 아래쪽 화살표는 작동하지 않는 vEdge Boxes 를 표시합니다.



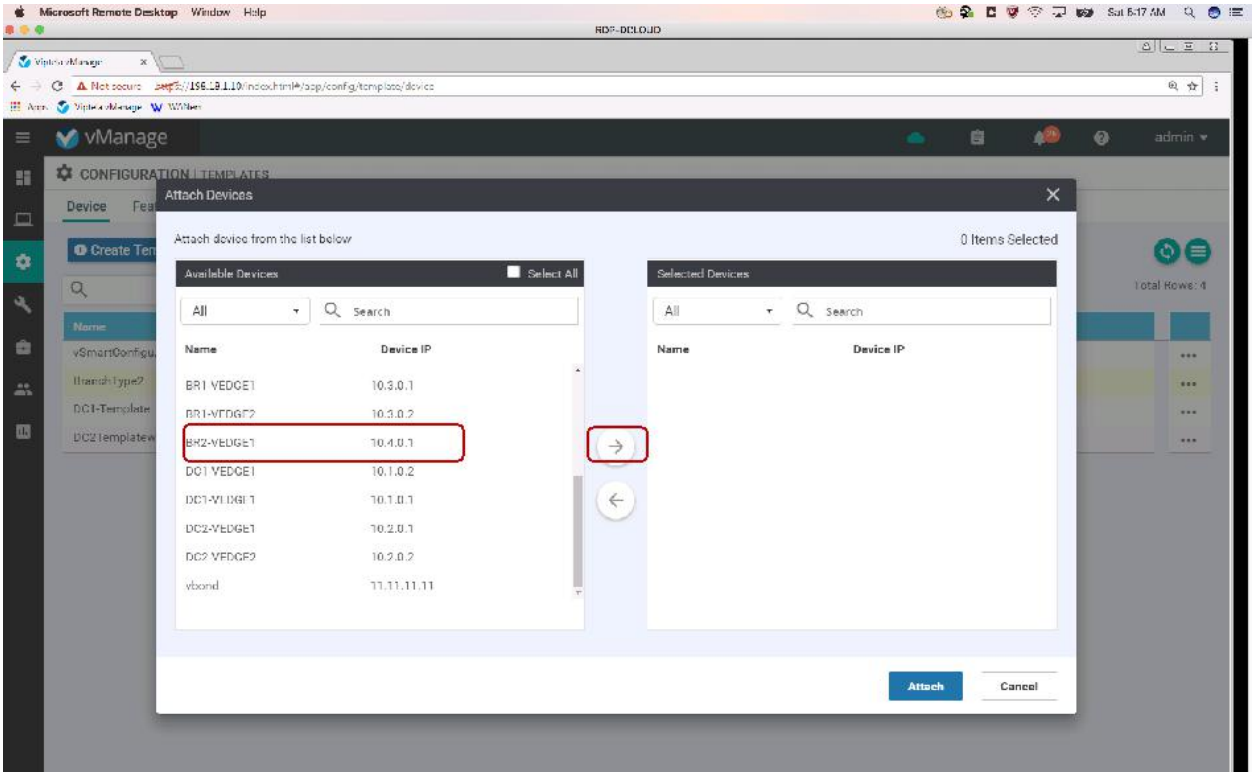
구성 아이콘을 클릭하고 드롭 다운 메뉴에서 템플릿을 선택하십시오.



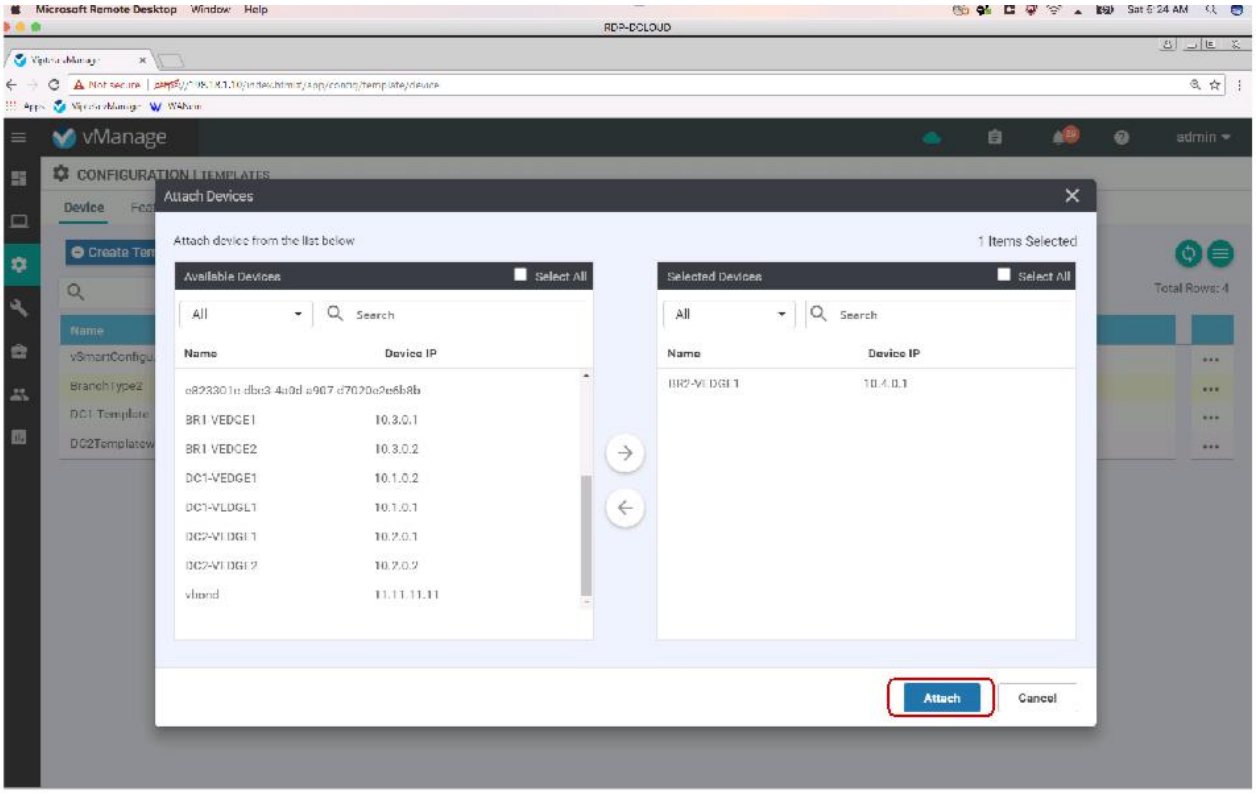
다양한 템플릿이 표시됩니다. 이제 이 원격 사이트를 위해 BranchType2 라는 템플릿을 선택합니다. 사전 구성된 이 템플릿은 고객이 새 브랜치를 롤아웃할 때 설정할 템플릿입니다. 드롭 다운에서 Attach Devices 옵션을 선택하십시오.



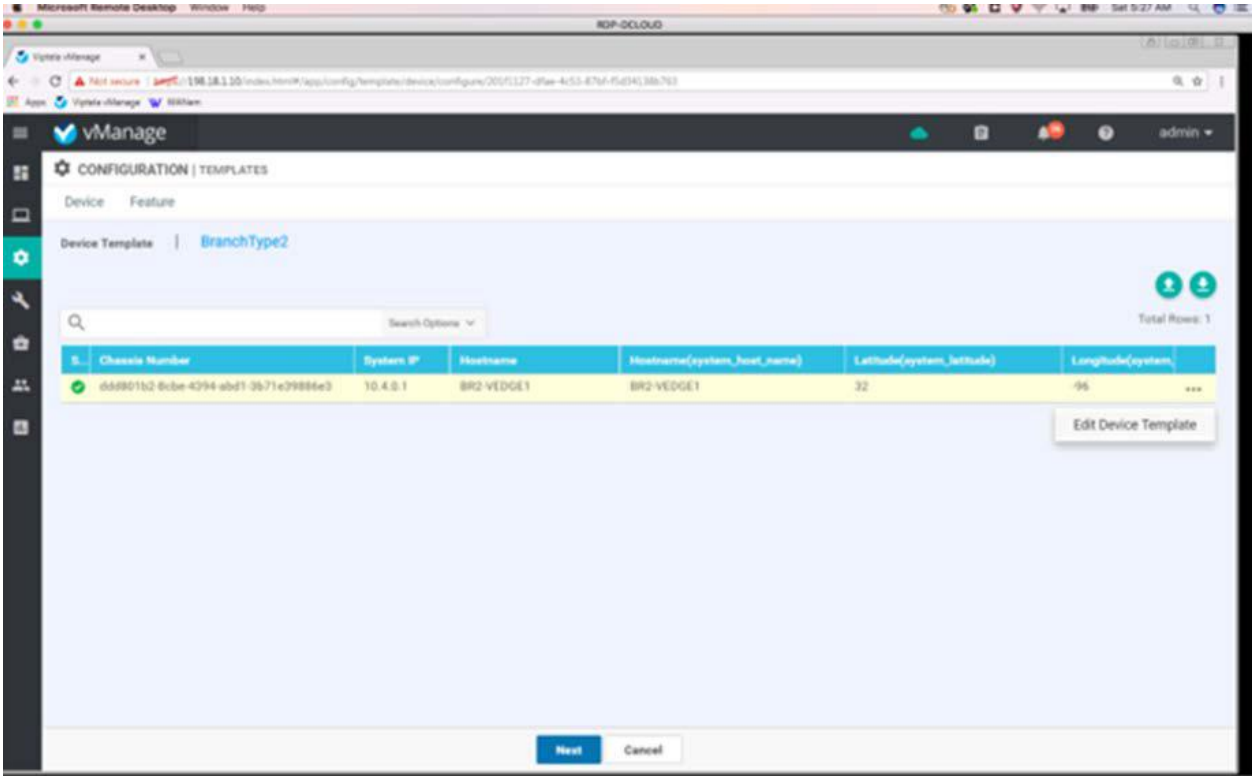
사용 가능한 장치라고 표시된 왼쪽 창에서 BR2-VEDGE1 을 찾습니다. 시스템 IP 가 10.4.0.1 인 BR2-VEDGE1 을 선택하십시오. 실제 배포 시나리오에서는 vEdge 의 이름이 나타나지 않으며 샤시 번호와 일치해야 합니다. 선택한 장치를 오른쪽 화살표 단추를 클릭하여 오른쪽 창으로 이동하십시오.



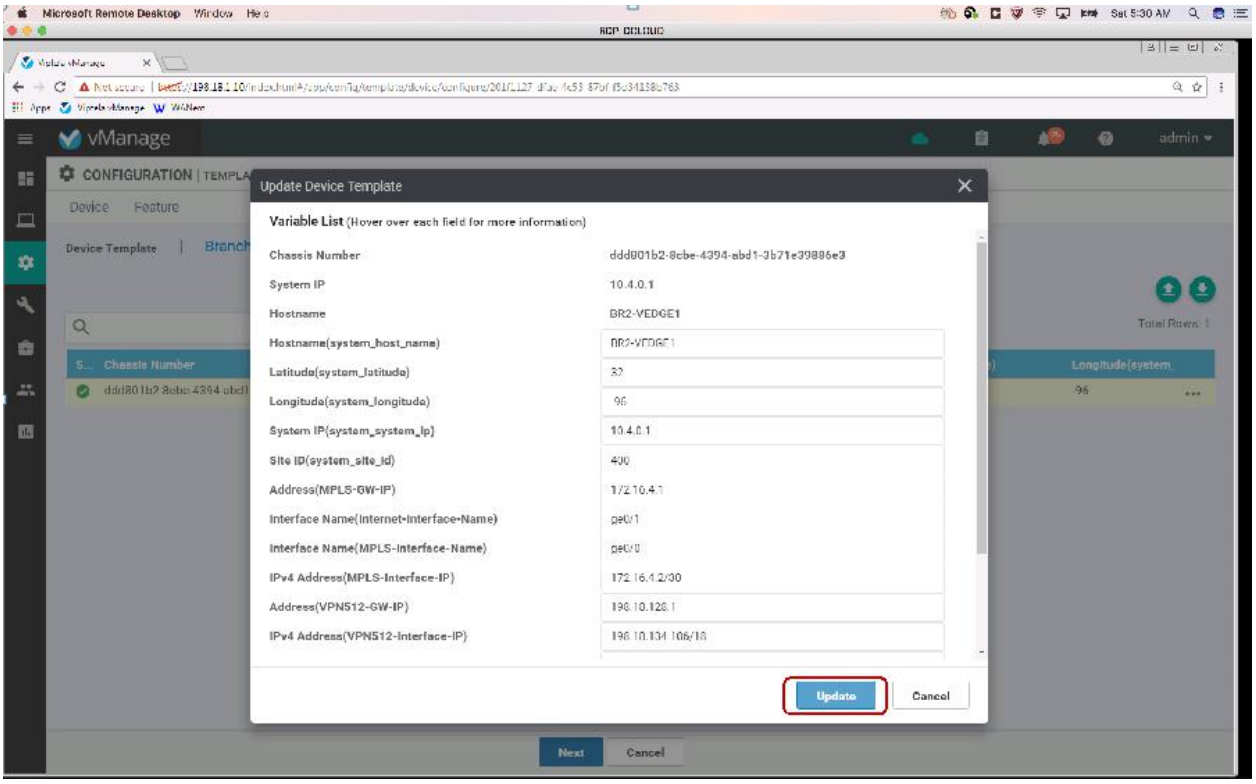
장치가 오른쪽 창으로 이동되면 Attach 버튼을 클릭하십시오.



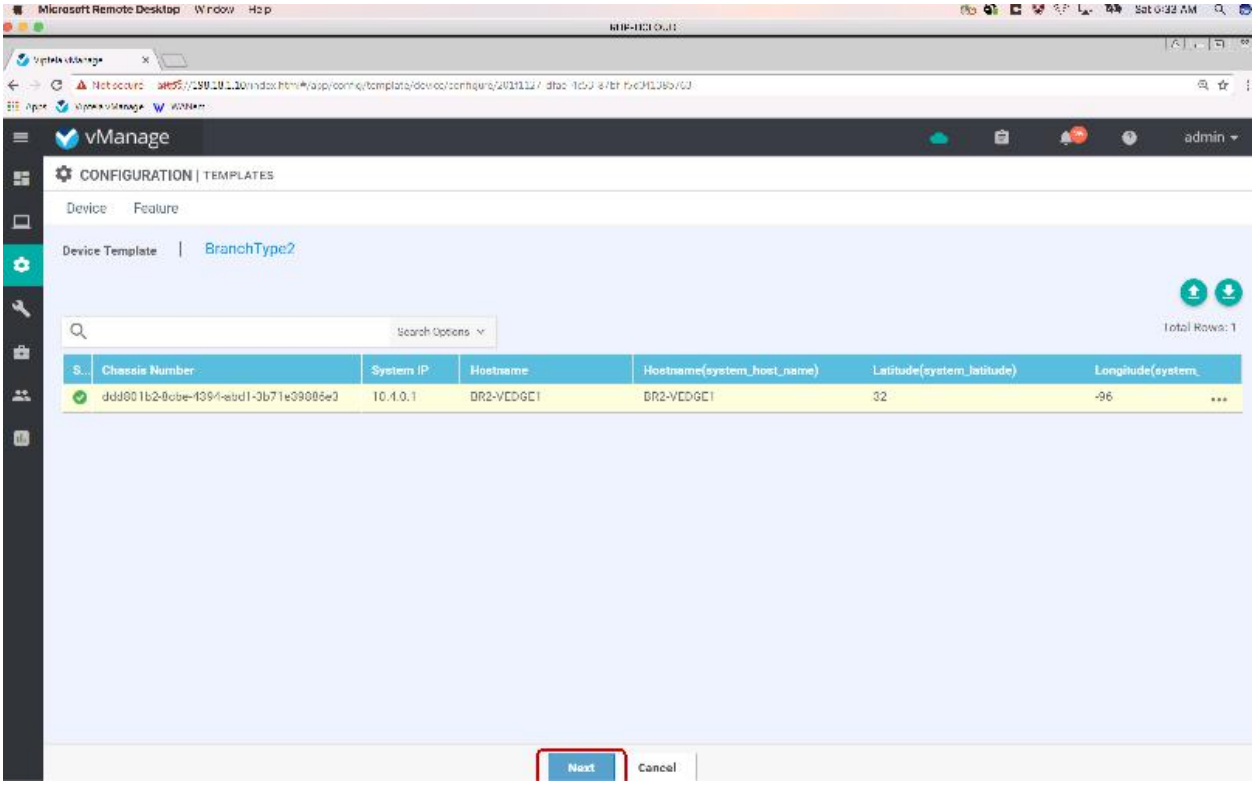
가장 오른쪽 열을 클릭하고 Edit Device Template 을 선택하십시오.



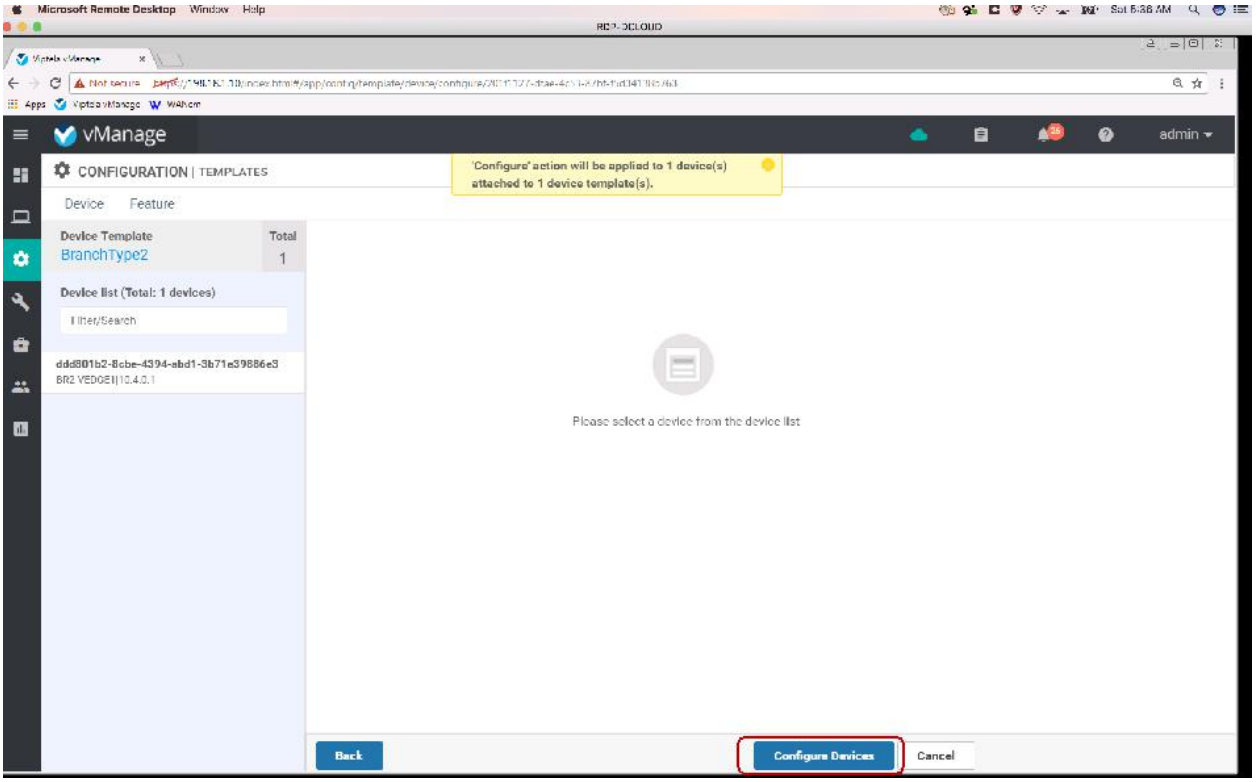
Edit Device Template 은 브랜치 2 vEdge 에 관한 설정값을 업데이트하기 위한 옵션을 제공합니다. Update 버튼을 클릭하십시오.



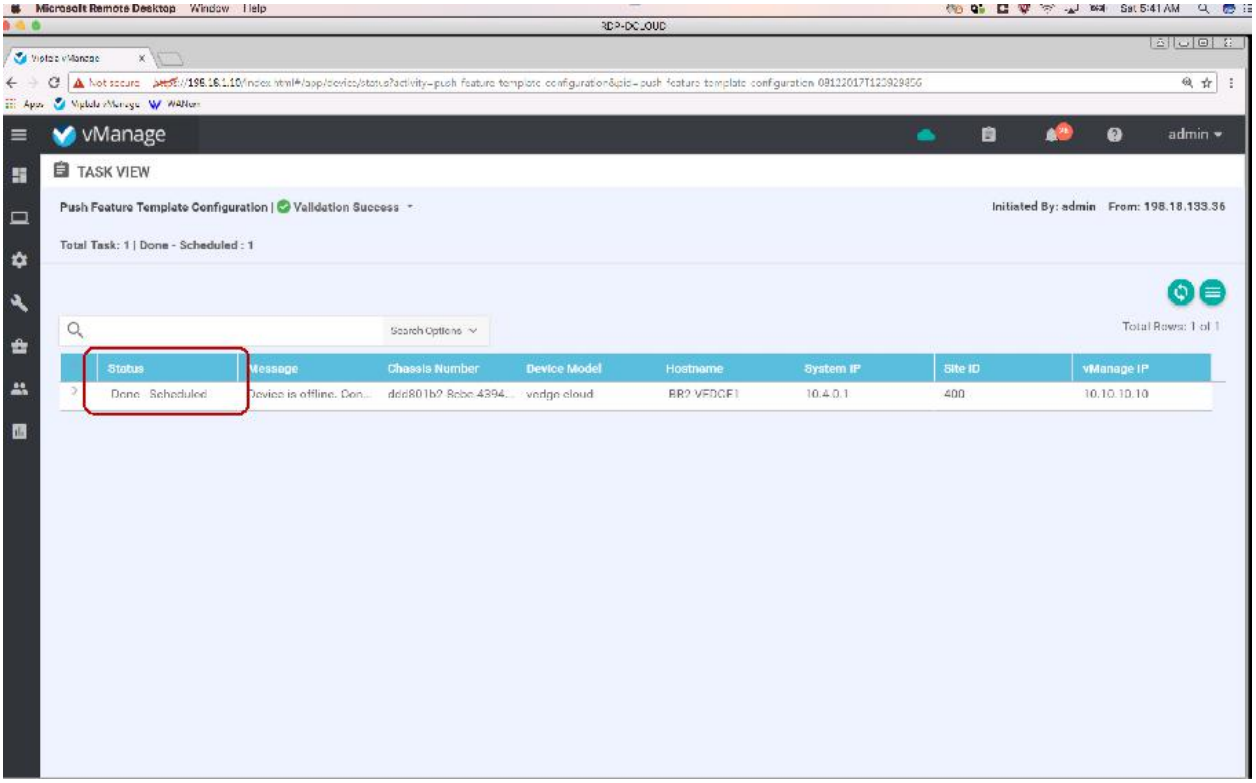
다음 화면에서 Next button 을 클릭하십시오.



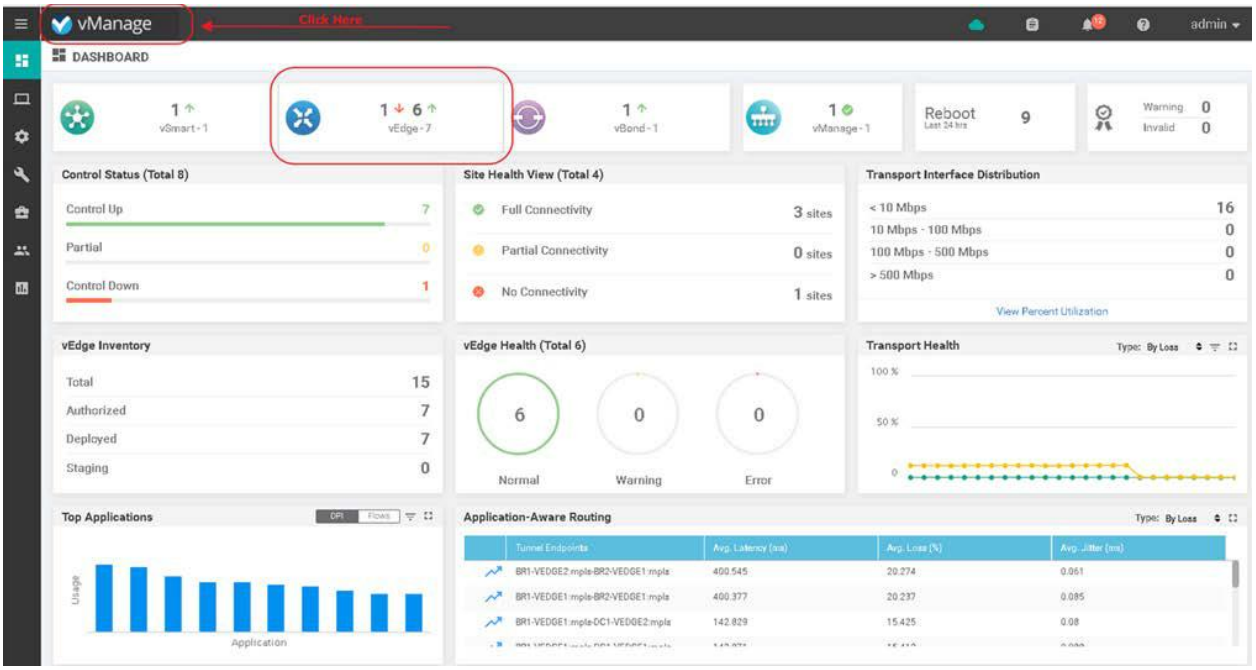
Configure Devices 를 클릭하십시오.



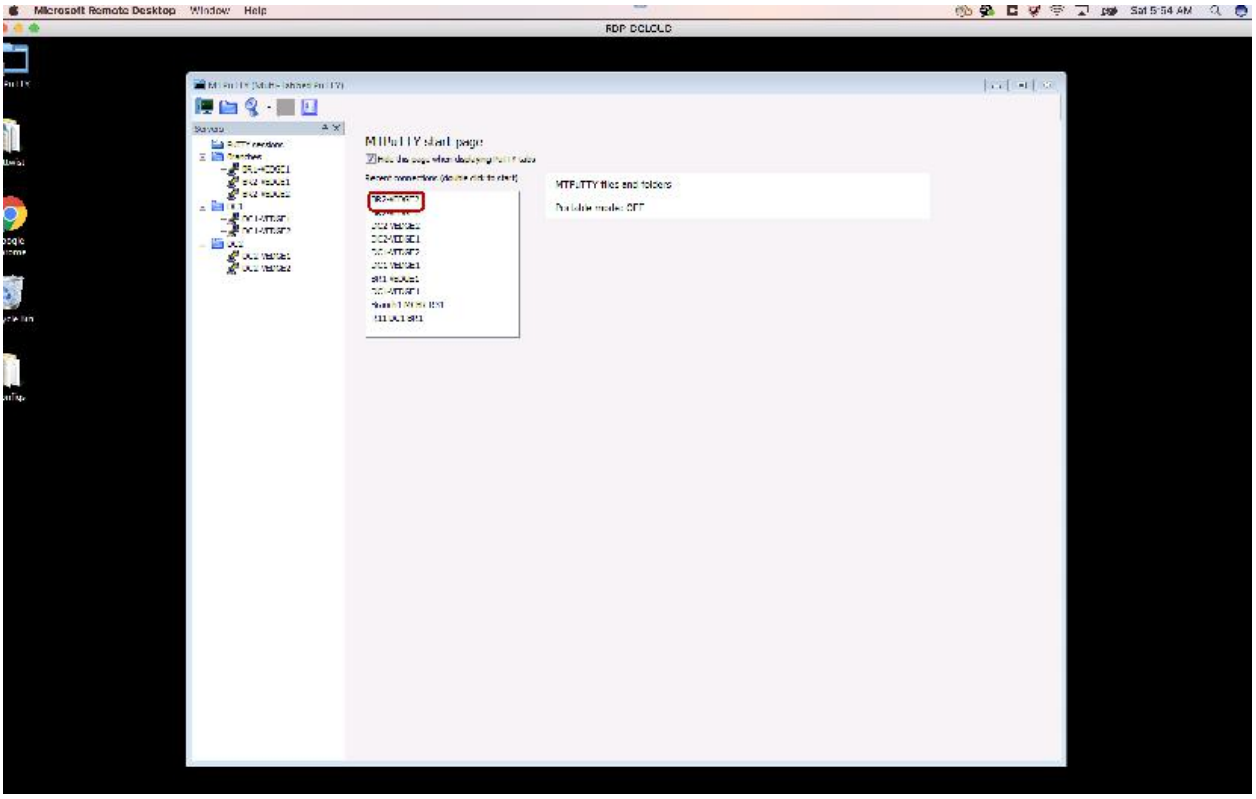
장치 상태가 In Progress 에서 Done - Scheduled 로 바뀔 때까지 몇 초 동안 기다리십시오.



vManage dashboard 아이콘을 클릭하십시오. 대시 보드 아이콘에는 한개의 Branch vEdge 가 아직 네트워크에 연결되지 않았으므로 작동 중지상태임을 나타냅니다.



ZTP 를 통한 장비 연결 시뮬레이션을 위해, 랩 [interface ge0/1]에서 인터넷에 연결된 인터페이스를 "no shut"할 것입니다.
Wkst1 의 바탕 화면에서 MTPutty 를 시작합니다.
BR2-VEDGE1 장치를 더블 클릭하십시오.
자동으로 로그인 됩니다.



BR2-vEdge1 CLI 에 다음 명령을 실행하십시오:

```
show run vpn 0
```

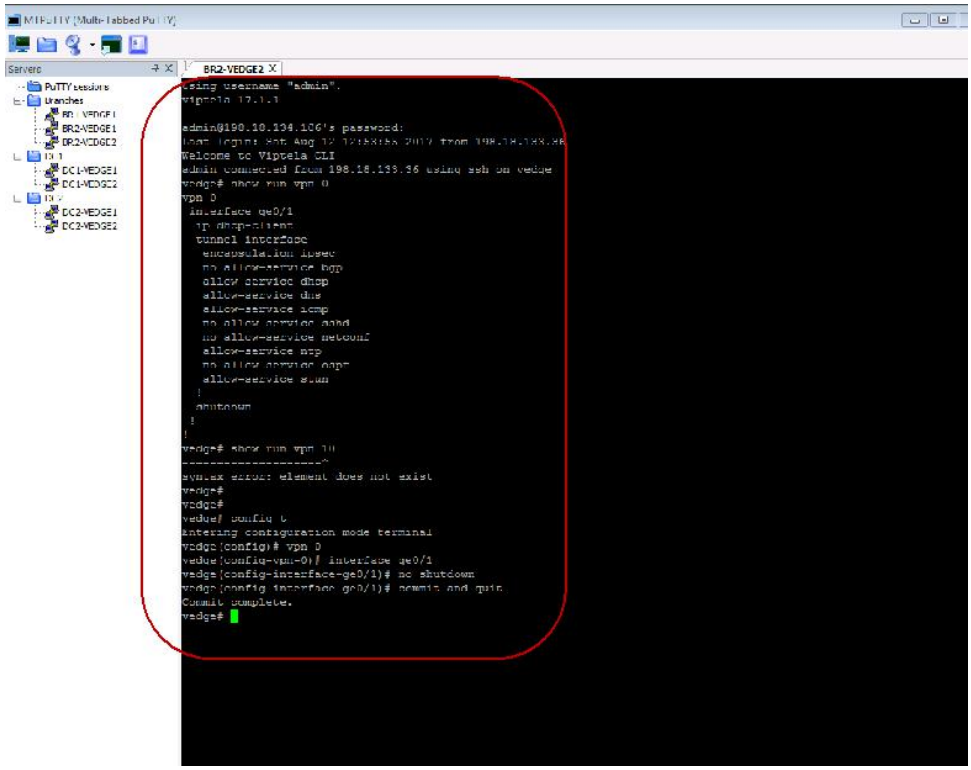
인터페이스가 Shutdown 상태임을 확인하십시오. 이는 라우터가 매니지먼트 및 컨트롤러 통신용으로 사용하는 논리적 인터페이스입니다.

```
show run vpn 10
```

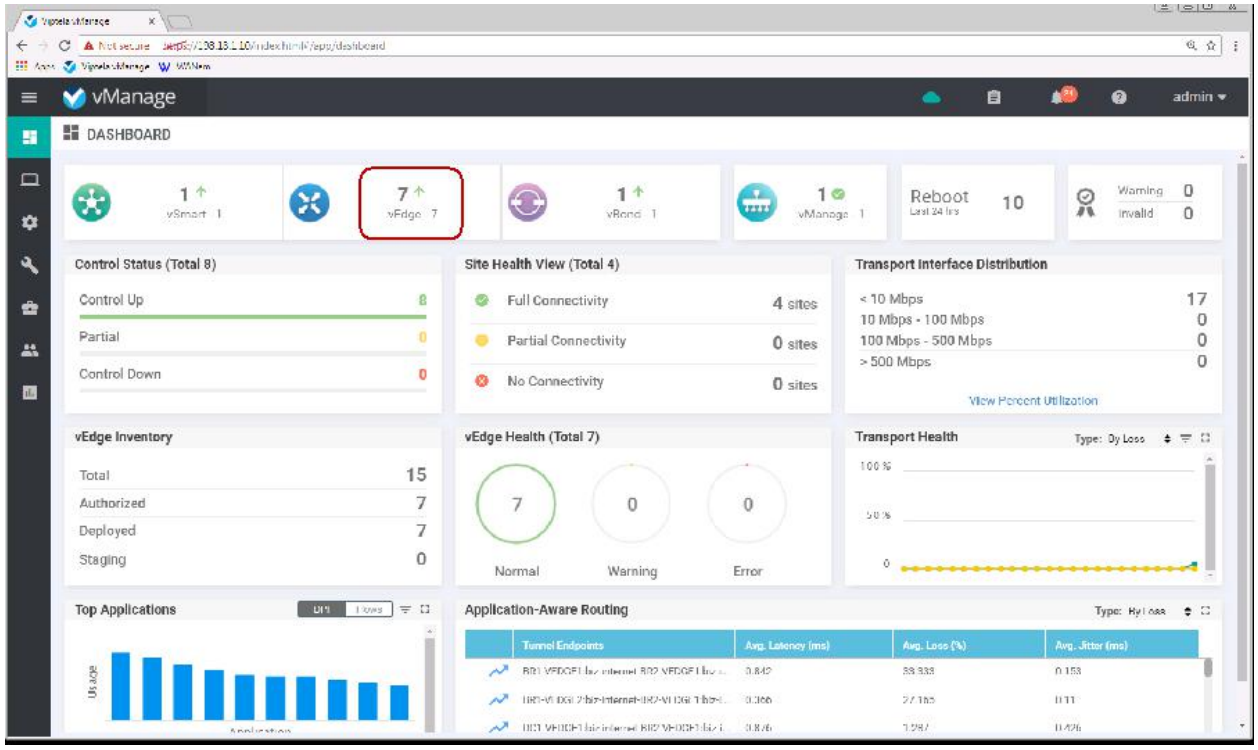
설정 내용이 아직 장치로 다운로드되지 않았으므로 인터페이스를 찾을 수 없습니다. 이제 라우터가 ZTP 를 시뮬레이션을 할 수 있도록 인터페이스를 활성화 할 것입니다.

```
config
vpn 0
interface ge0/1
no shut
commit and-quit
```

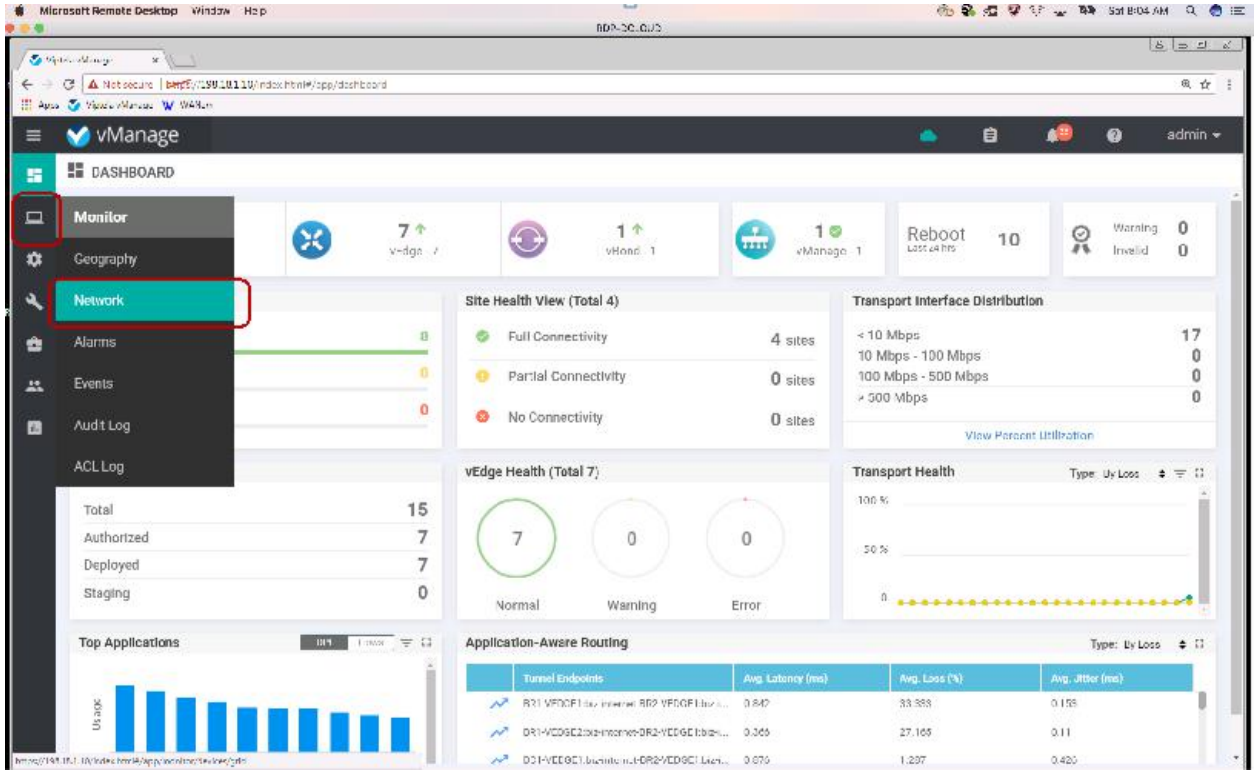
출력 화면에서 transport VPN 0 에 대한 기본 구성이 있고 service/LAN 쪽 VPN 10 구성은 없음을 알 수 있습니다.



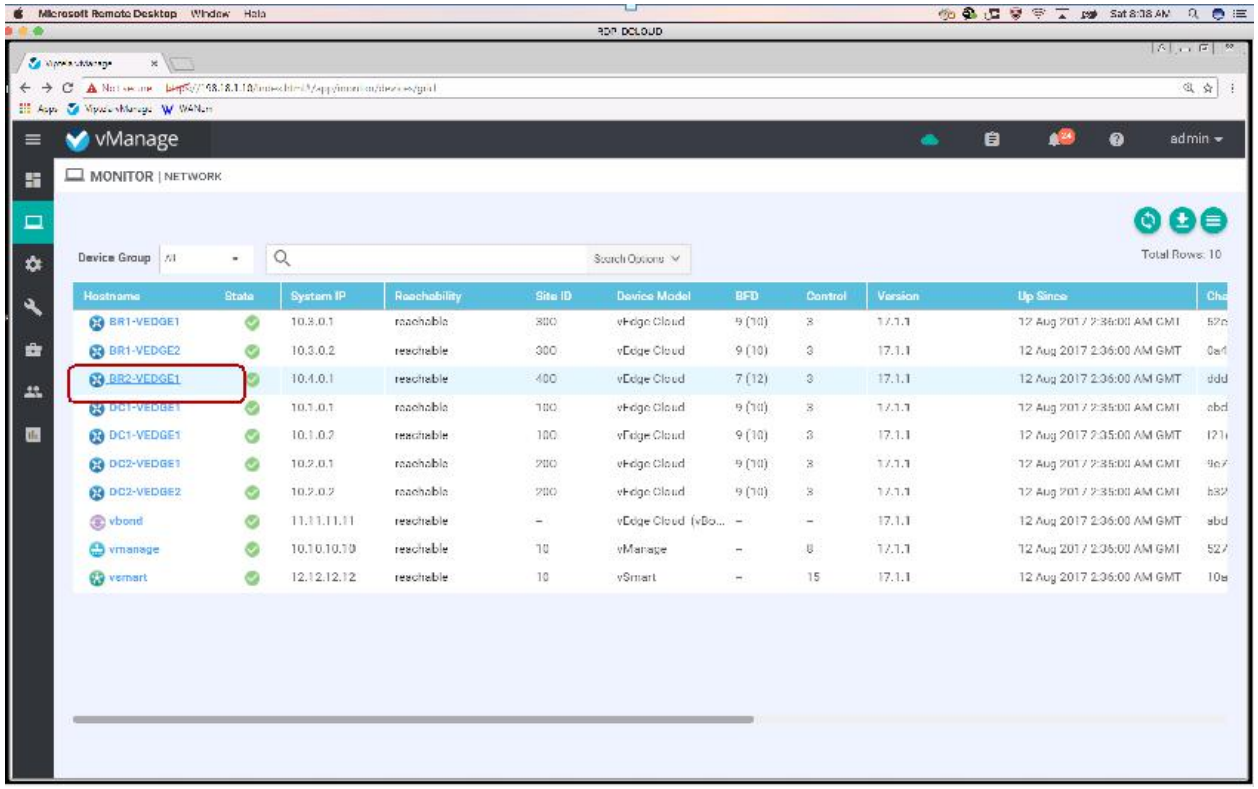
vManage dashboard 에 돌아갑니다. BR2-VEDGE1 이 나타나고 대시보드에 총 7 개의 vEdge 가 동작 중임을 표시합니다.



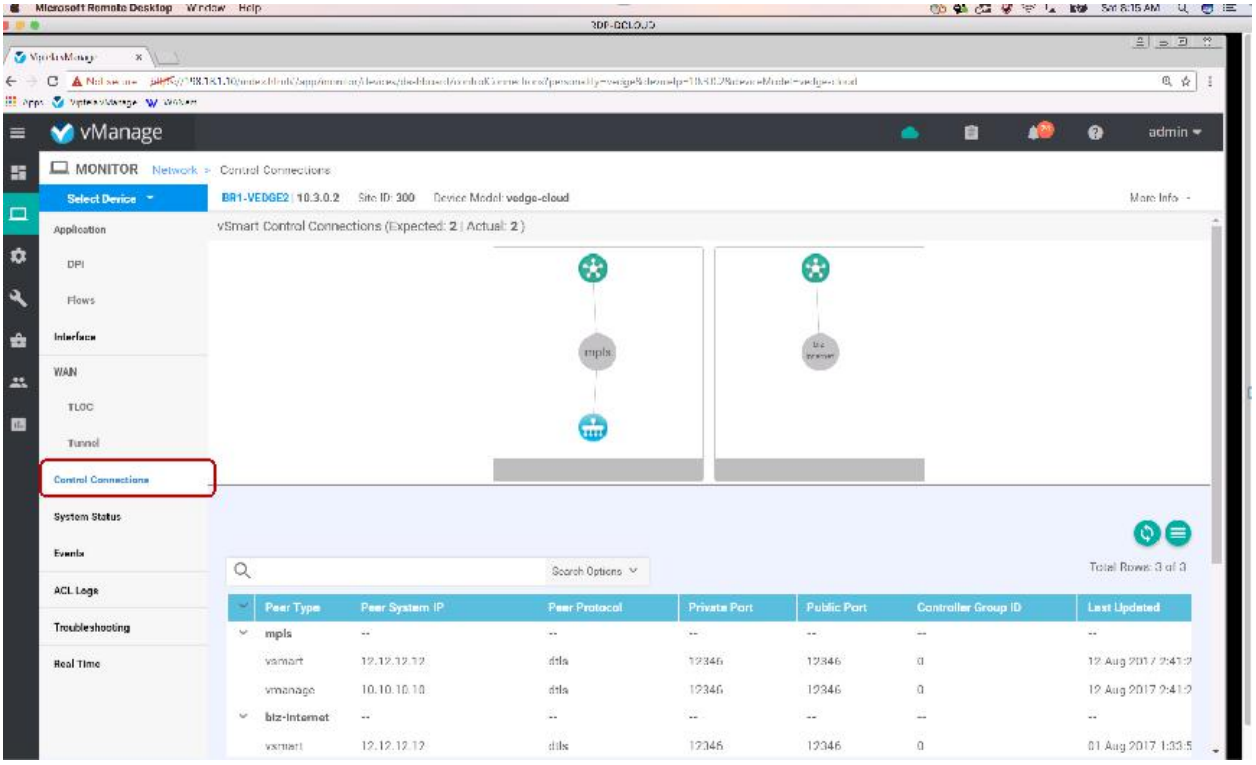
Monitor 아이콘을 클릭 한 다음 Network 를 선택하십시오.



목록에서 BR2-VEDGE1 을 선택하십시오. BR2-VEDGE2 용 대시보드로 이동합니다.

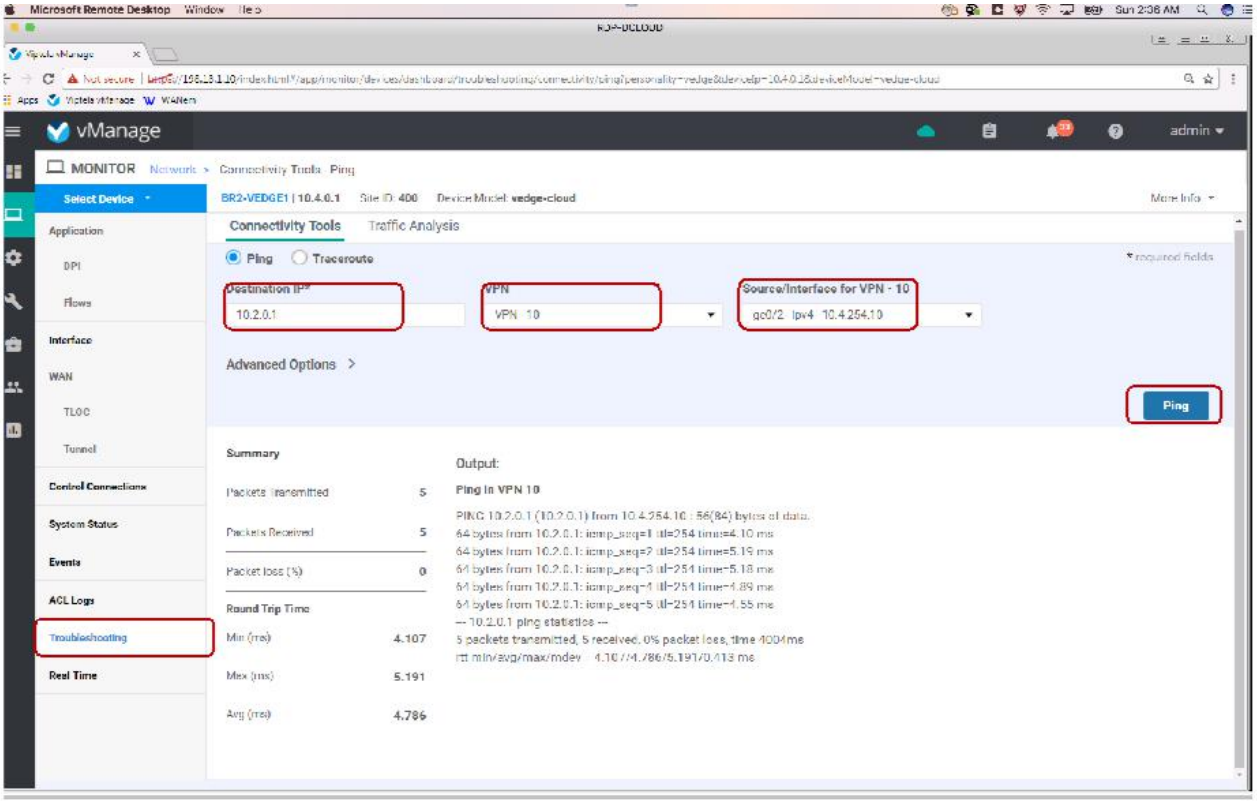


Control Connections 을 클릭하십시오. vSmart 및 vManage 에 컨트롤 세션이 수립됩니다.



IP 연결성을 확인하려면 장치 대시 보드에서 Troubleshooting 을 클릭하십시오..

목적지 IP 로 DC2 는 10.2.0.1, DC2 는 198.18.133.1, Branch 1 은 10.3.0.1 그리고 Branch 2 는 10.4.254.254 를 입력하십시오. 드롭 다운 메뉴에서 VPN 10 (데이터 VPN)과 소스 인터페이스를 선택하십시오. 그 다음 Ping 버튼을 클릭하십시오.

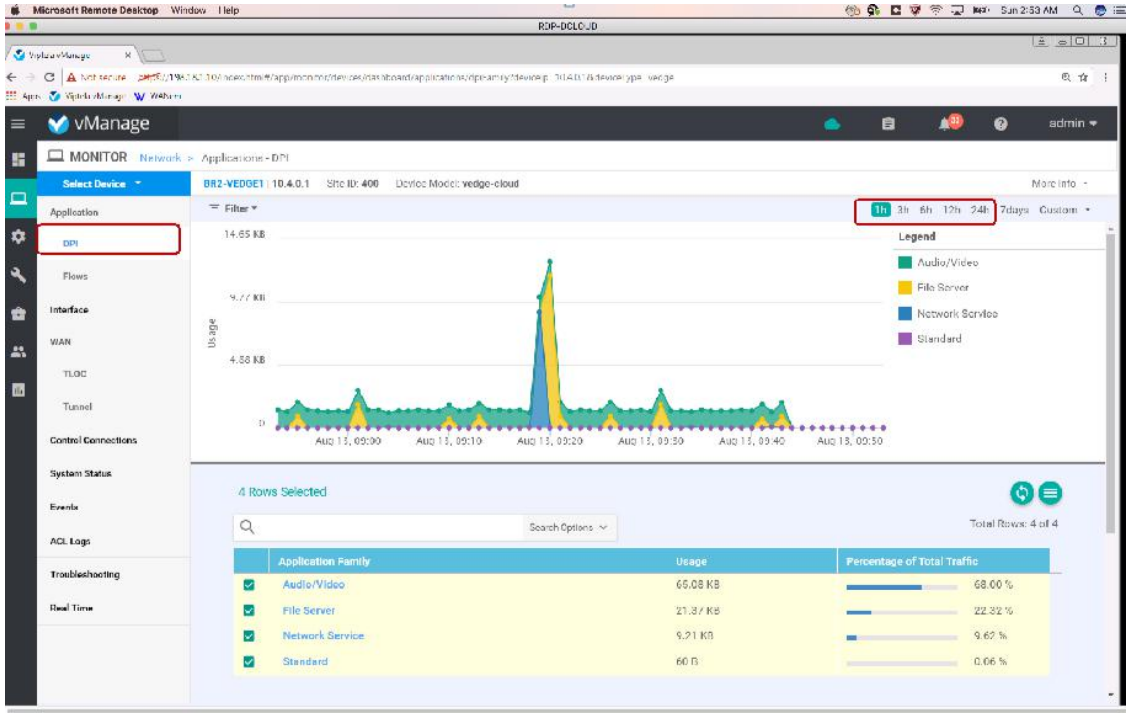


vManage 의 다른 기능을 데모합니다.

Device 대시 보드를 통해 애플리케이션 플로우, IPFIX 플로우 레코드, 인터페이스 통계 그리고 기타 정보를 볼 수 있습니다.

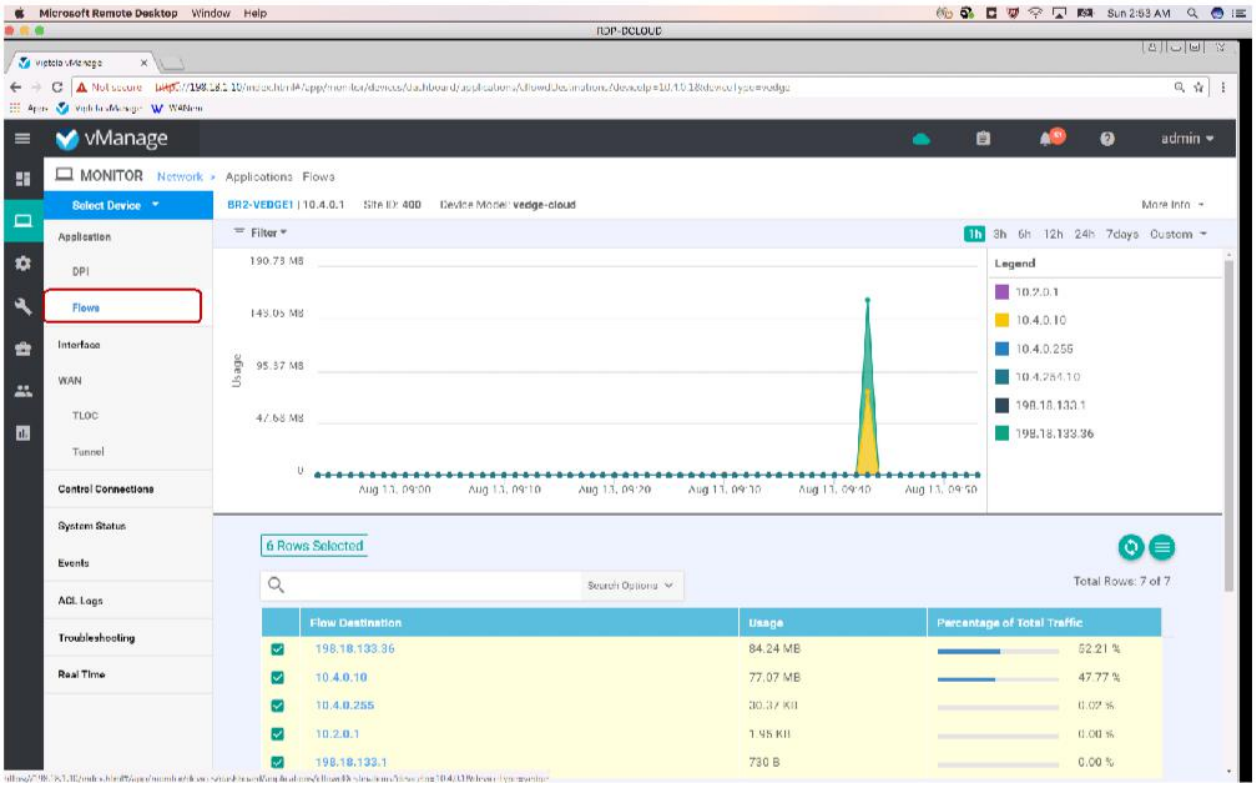
DPI

DPI 를 클릭 한 다음 1 시간 탭[1h]을 클릭하십시오.



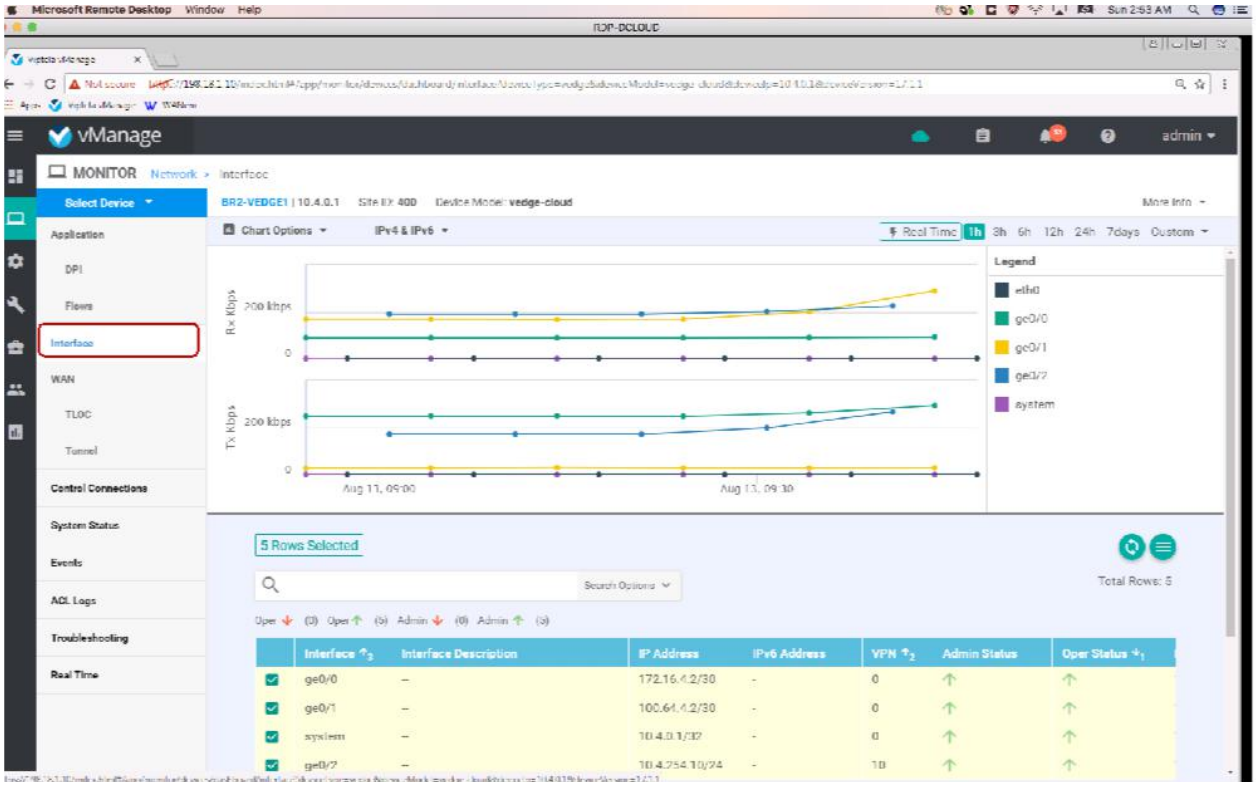
IPFIX 플로우 레코드

Flows 를 클릭 한 다음 1 시간 탭[1h]을 클릭하십시오.

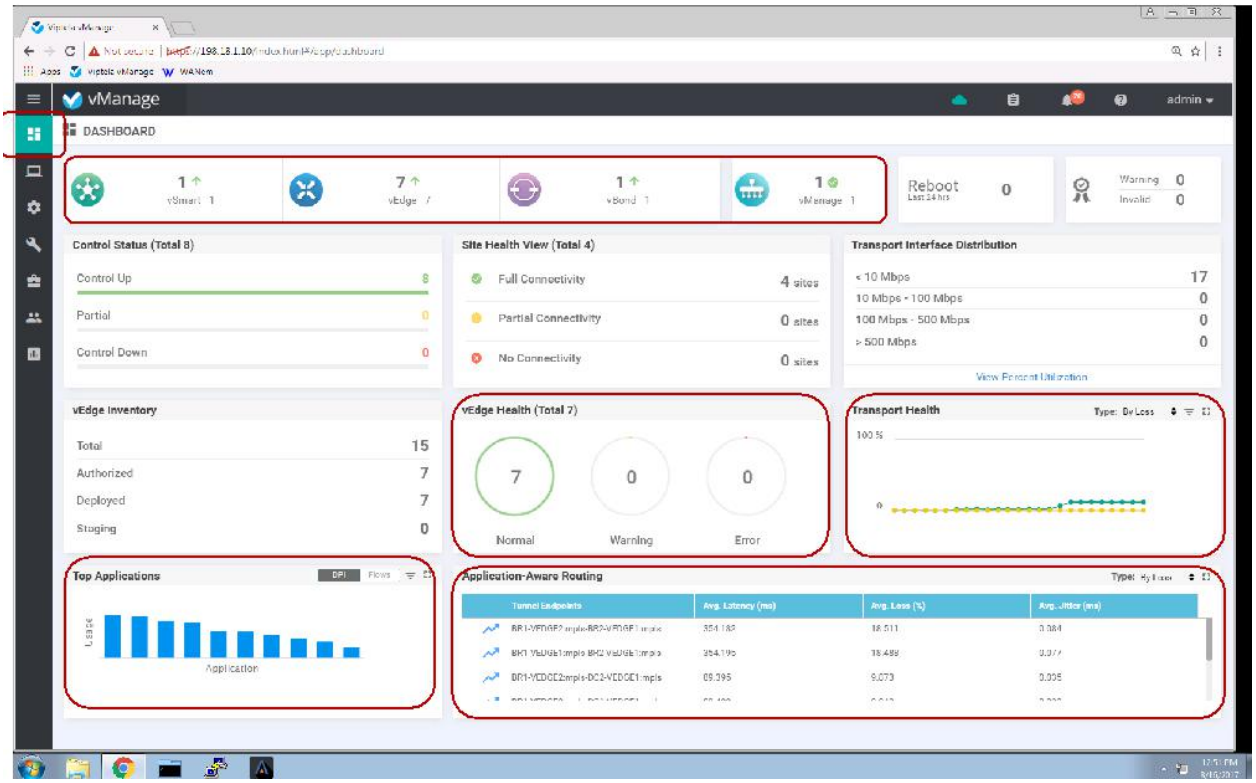


인터페이스 통계

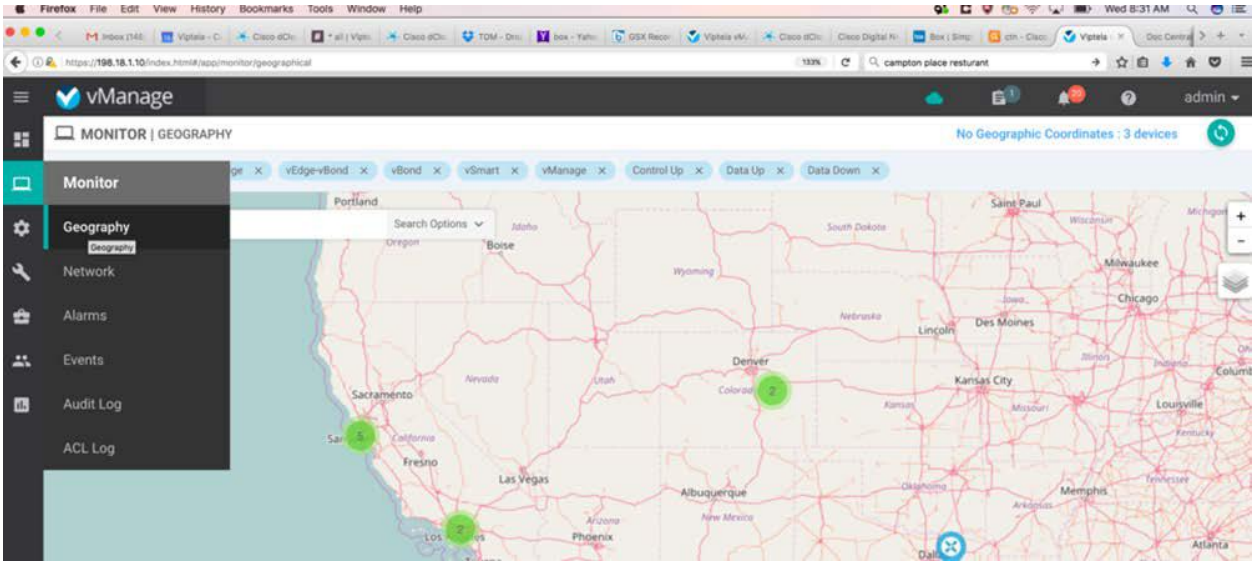
Interfaces 를 클릭 한 다음 1 시간 탭[1h]을 클릭하십시오.



- vManage 대시 보드 아이콘을 클릭하십시오. 아래 기능을 포함한 네트워크 레벨 모니터링 기능에 대해 설명합니다.
  - 모든 Viptela 구성 요소의 Up/Down 상태
  - vEdge 상태
  - 애플리케이션 / 플로우 가시성
  - 전송망 상태 가시성



맵에서 장치 / 사이트를 확인하려면 모니터로 이동하여 Geography 를 선택하십시오..



시나리오 2. Hub-n-Spoke 정책 기반 토폴로지

엔터프라이즈는 일반적으로 Full Mesh 형태의 토폴로지 보다 Hub-n-Spoke 토폴로지를 더욱 선호할 수 있습니다. 이렇게 할 경우 브랜치 사이트에 대한 확장성 및 단순성을 손쉽게 가지고 갈 수 있기 때문입니다. 간단한 정책 기능을 통해 메시 형태의 연결을 순수한 Hub-n-Spoke 형태로 변환시킬 수 있습니다.

과제

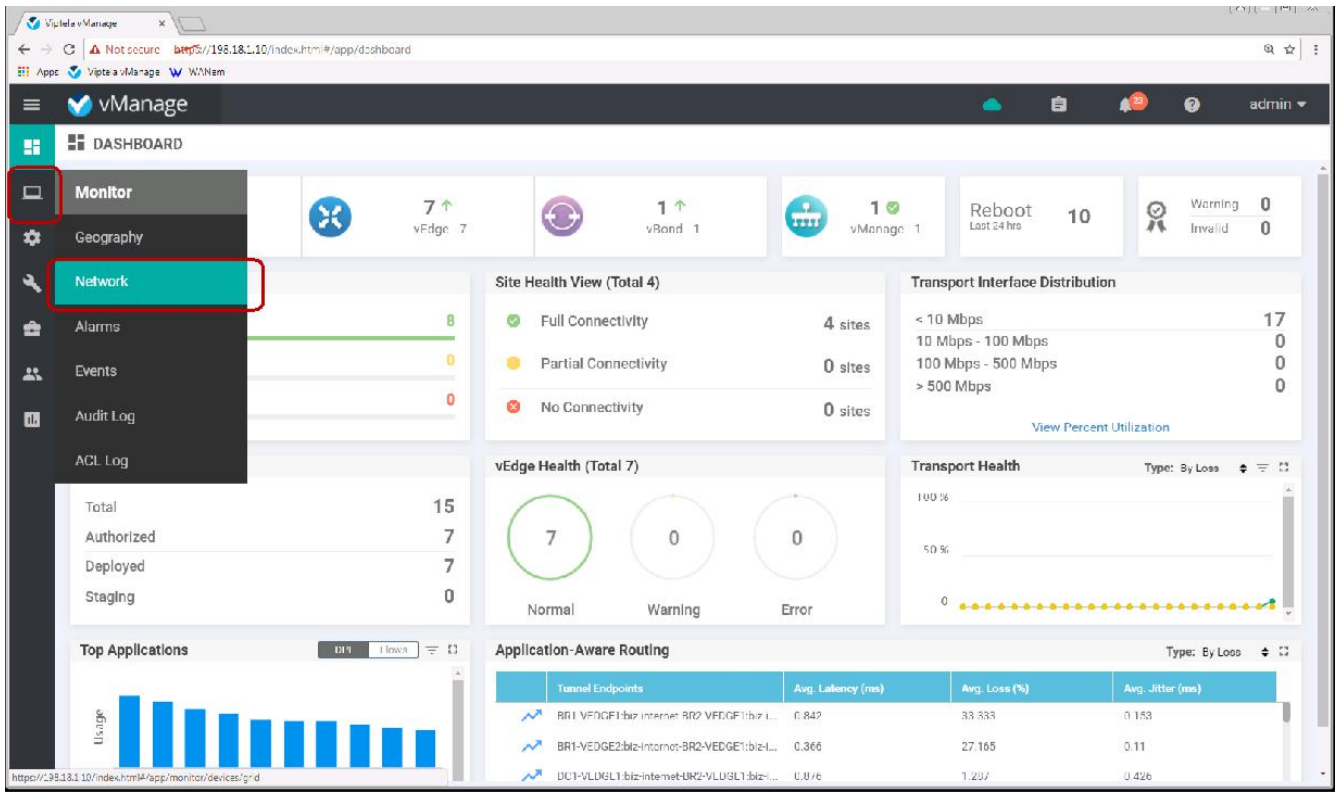
- 불규칙적인 형태의 토폴로지는 운영 측면에서 복잡성을 야기시키고 각각의 브랜치 사이트에 대한 개별 지원이 필요할 수도 있습니다.

효과 – 비용 및 복잡성 감소

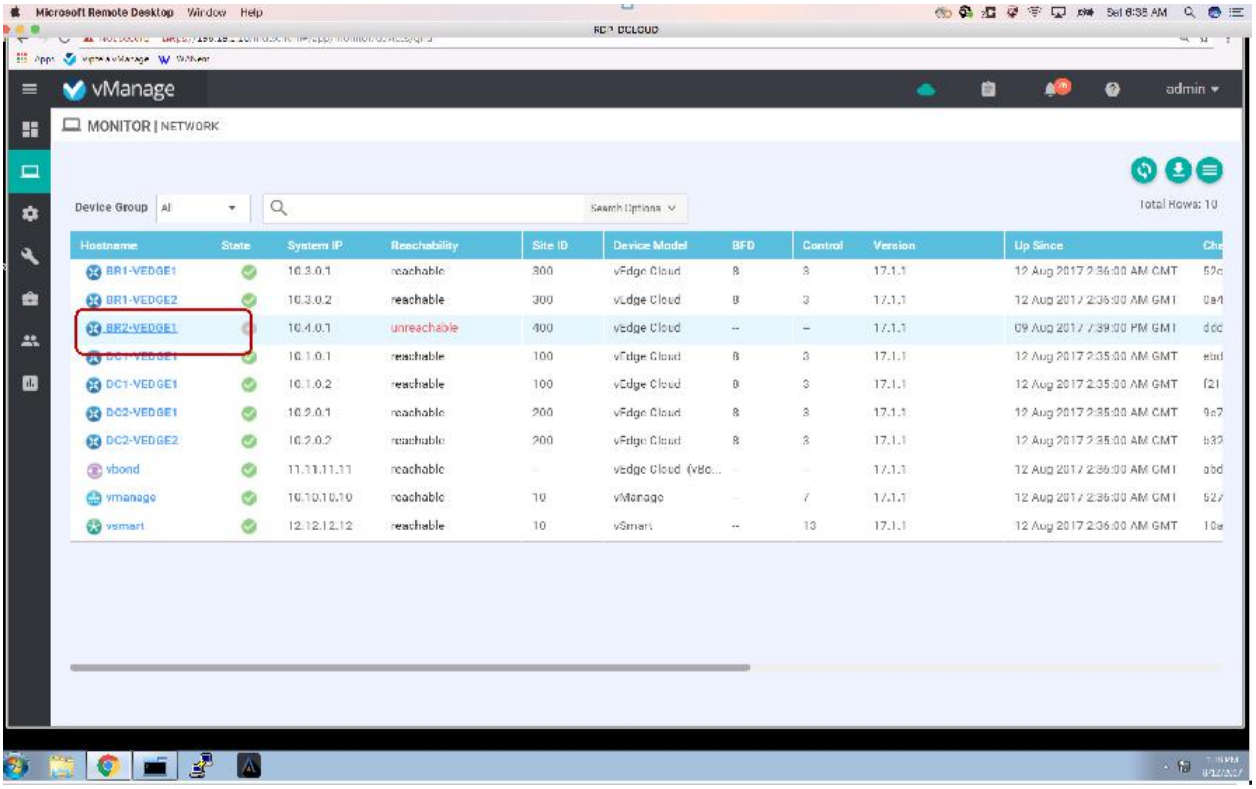
- 센트럴 vManage 통해 손쉽게 정책 활성화. 그에 따른 단순한 운영, 비용 감소 및 작업시간 단축

스텝

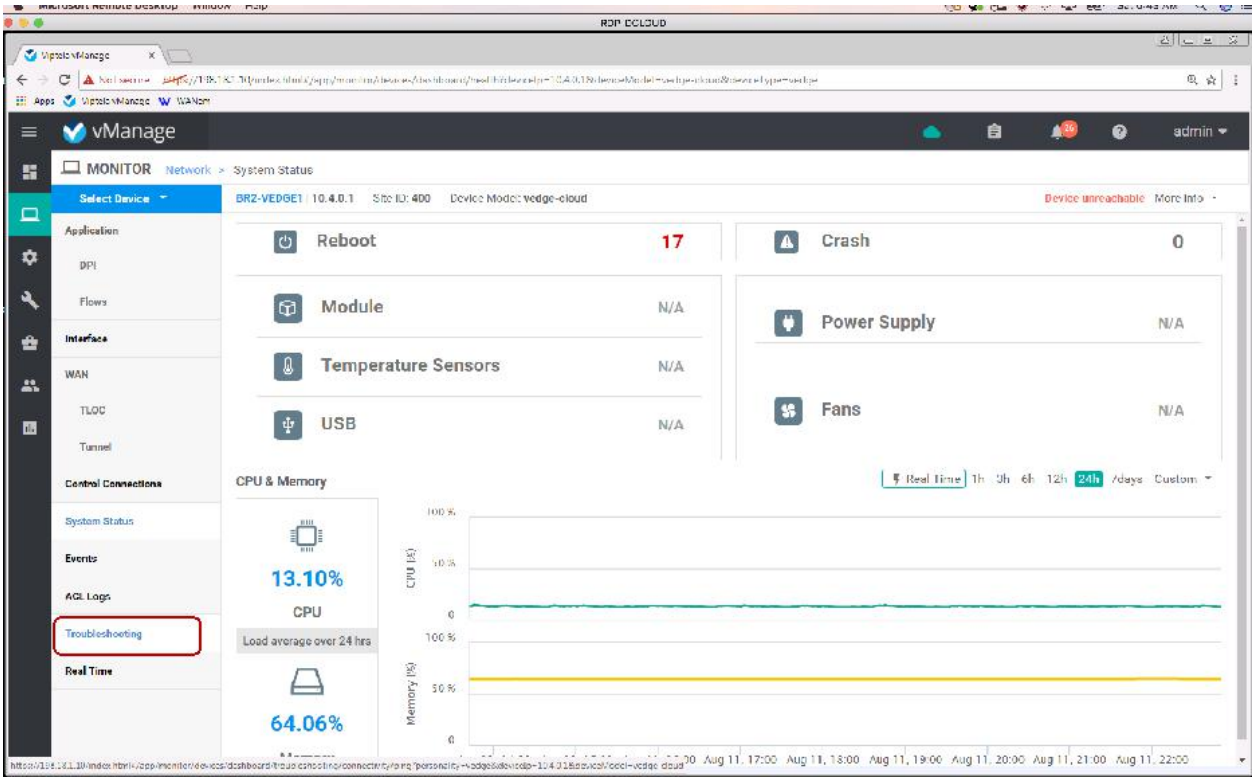
vManage 대시 보드로 이동하십시오. 모니터 아이콘을 클릭하고 드롭 다운에서 Network 를 클릭하십시오.



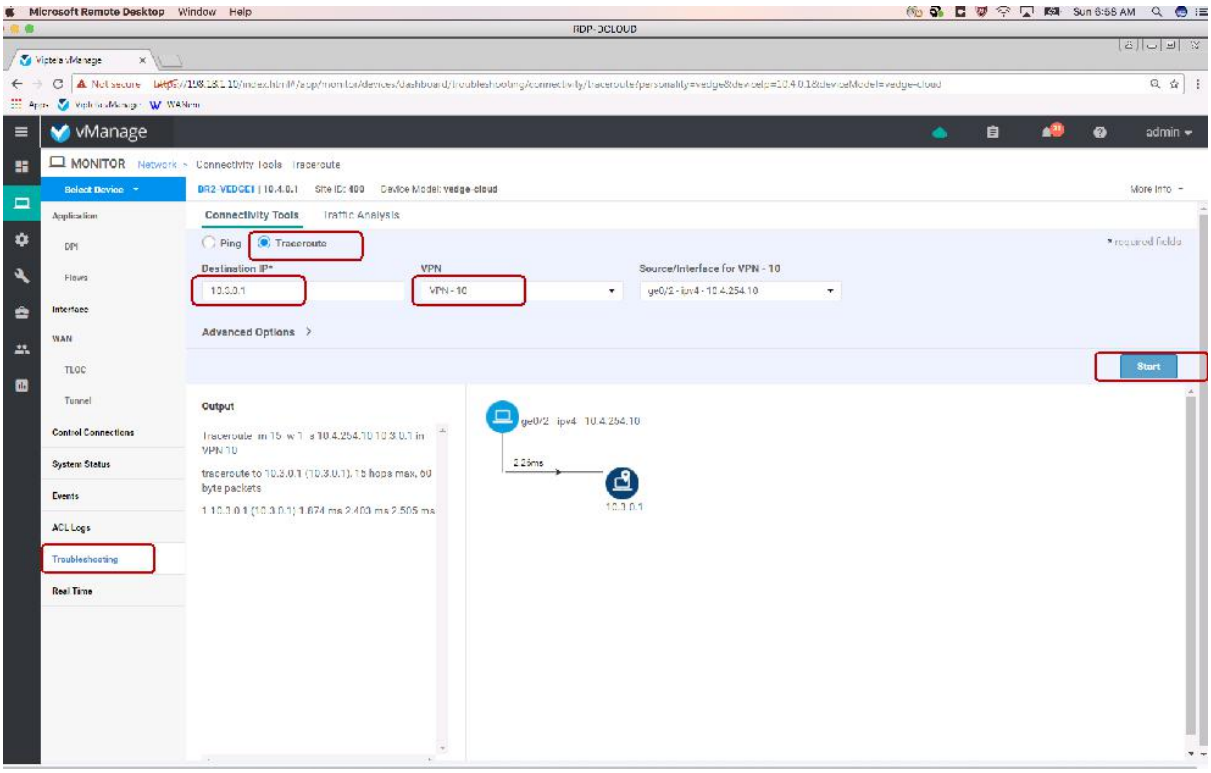
BR2-VEDGE1 을 찾아 해당 장비를 클릭하십시오.



왼쪽에서 Troubleshooting 을 선택하십시오..



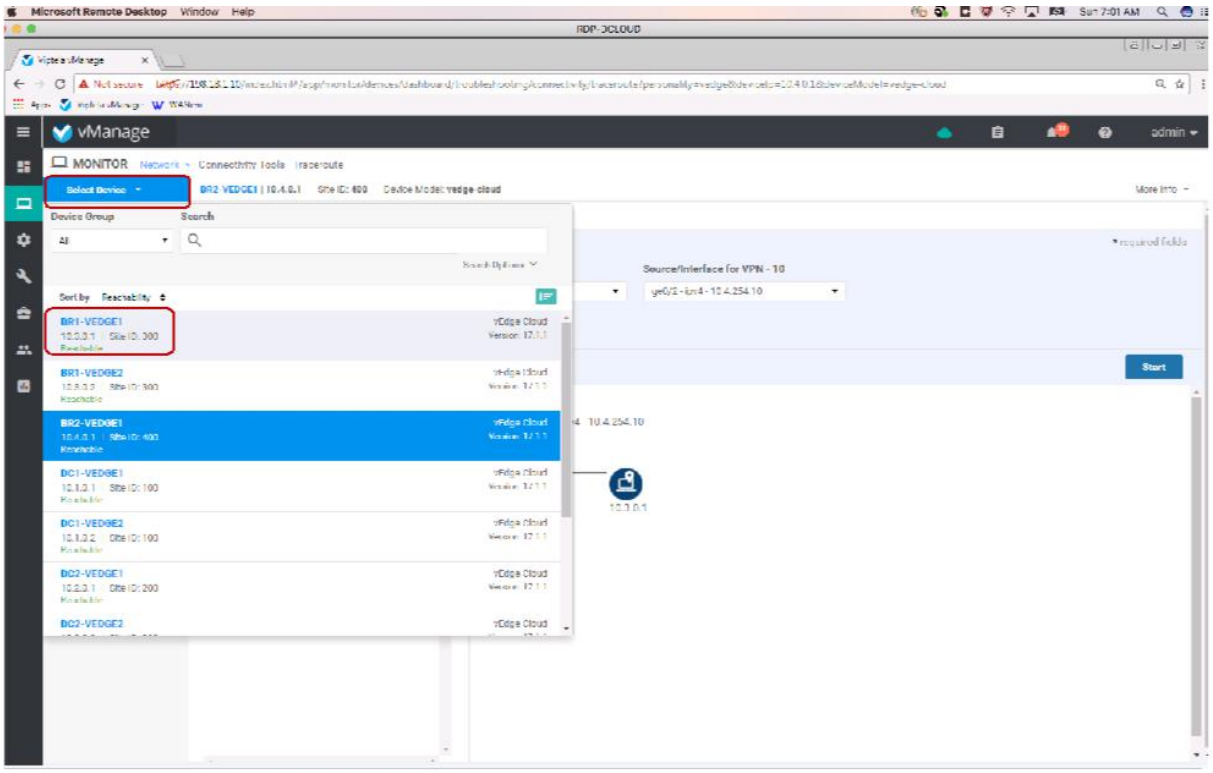
Traceroute 를 선택하십시오. Branch1 의 목적지 IP 로 10.3.0.2 를 입력하십시오. 드롭 다운 메뉴에서 VPN 10 및 소스 인터페이스를 선택합니다. Start 버튼을 클릭.



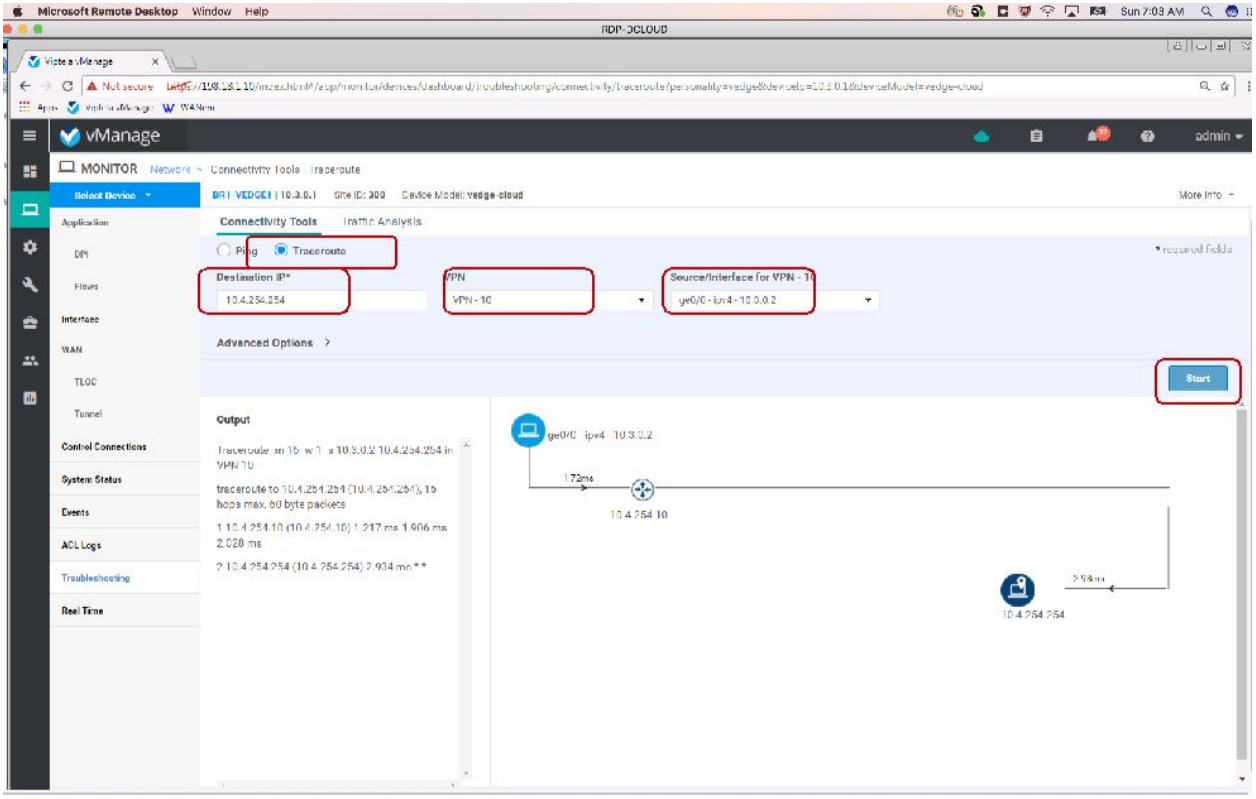
.

브랜치 1 (10.3.0.1)과 브랜치 2 (10.4.254.254) 사이의 직접 연결을 보여줍니다.

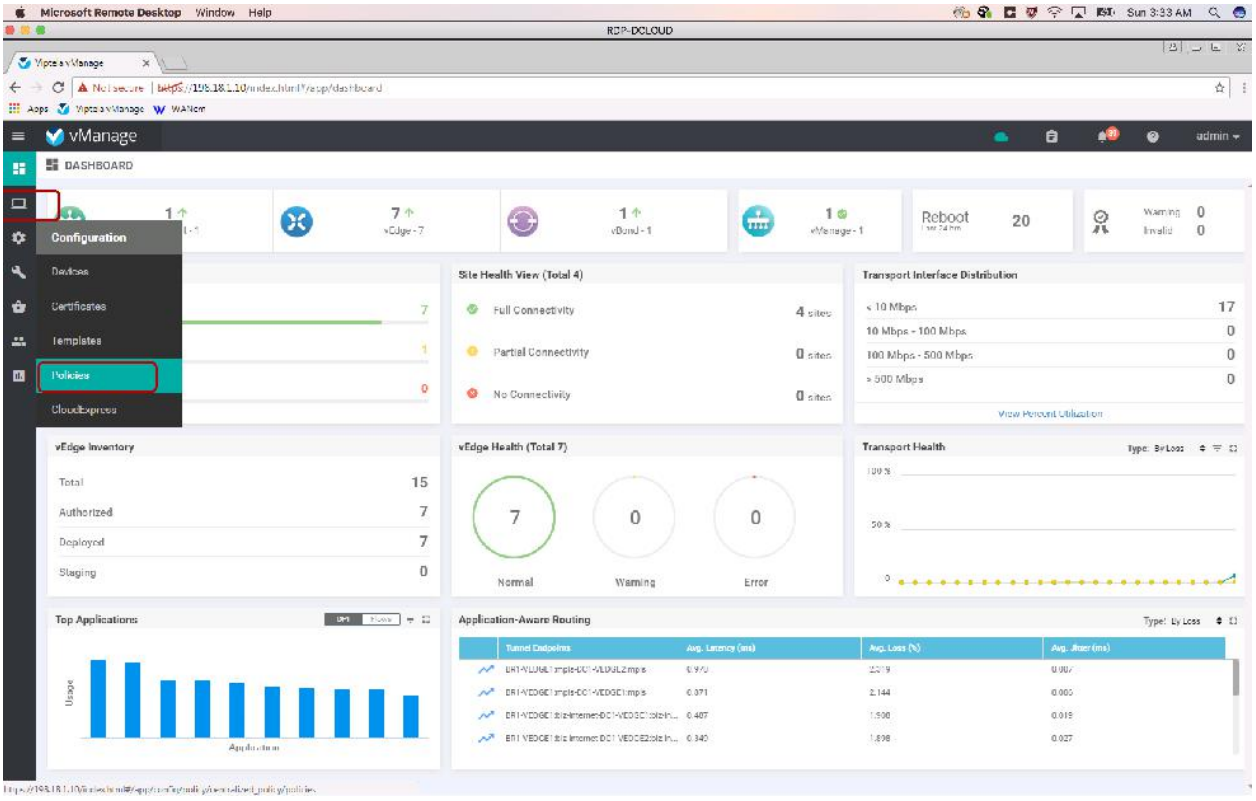
브랜치 1 에서 선택하여 똑같이 하십시오. Select Device 를 클릭하고 BR1-VEDGE1 을 선택하십시오.



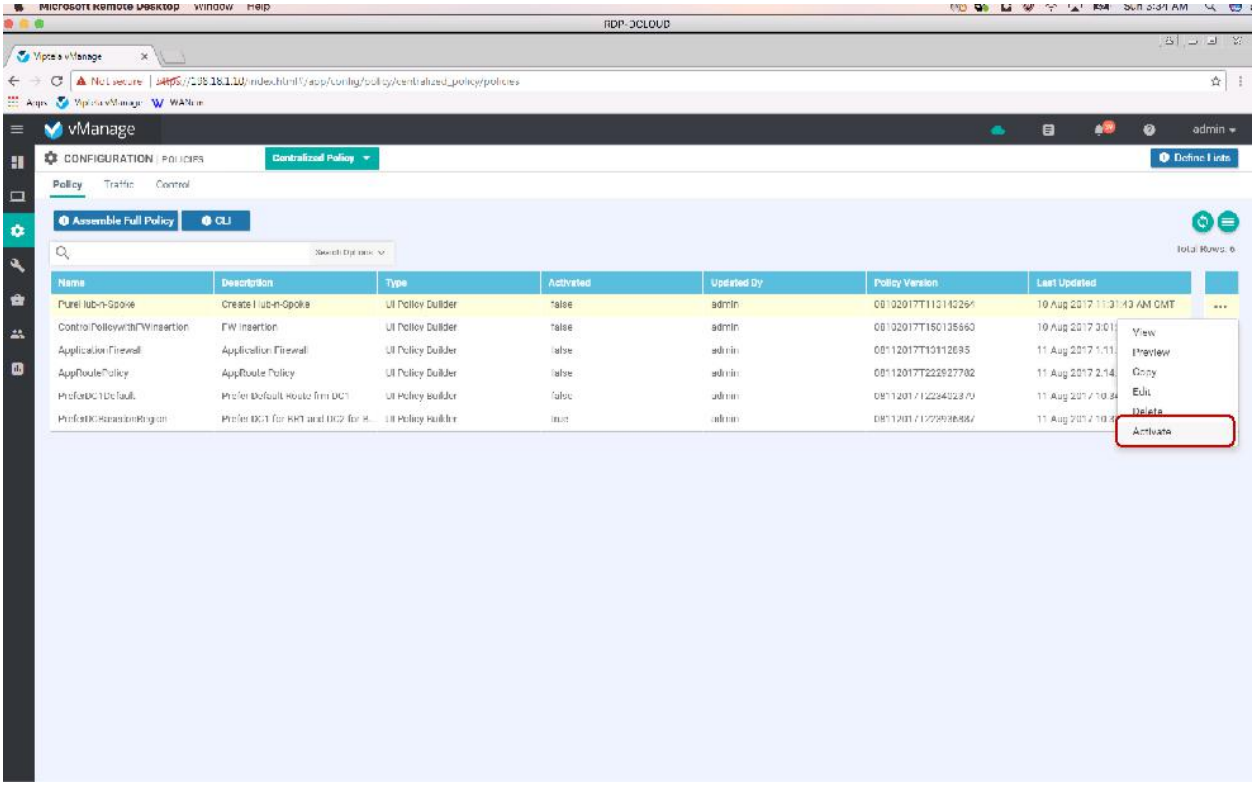
Traceroute 를 선택하여 목적지 IP 로 10.4.254.254 를 입력하고 VPN 10 을 선택한 다음 소스 인터페이스를 선택하십시오. 그 다음 Start 버튼을 클릭하십시오.



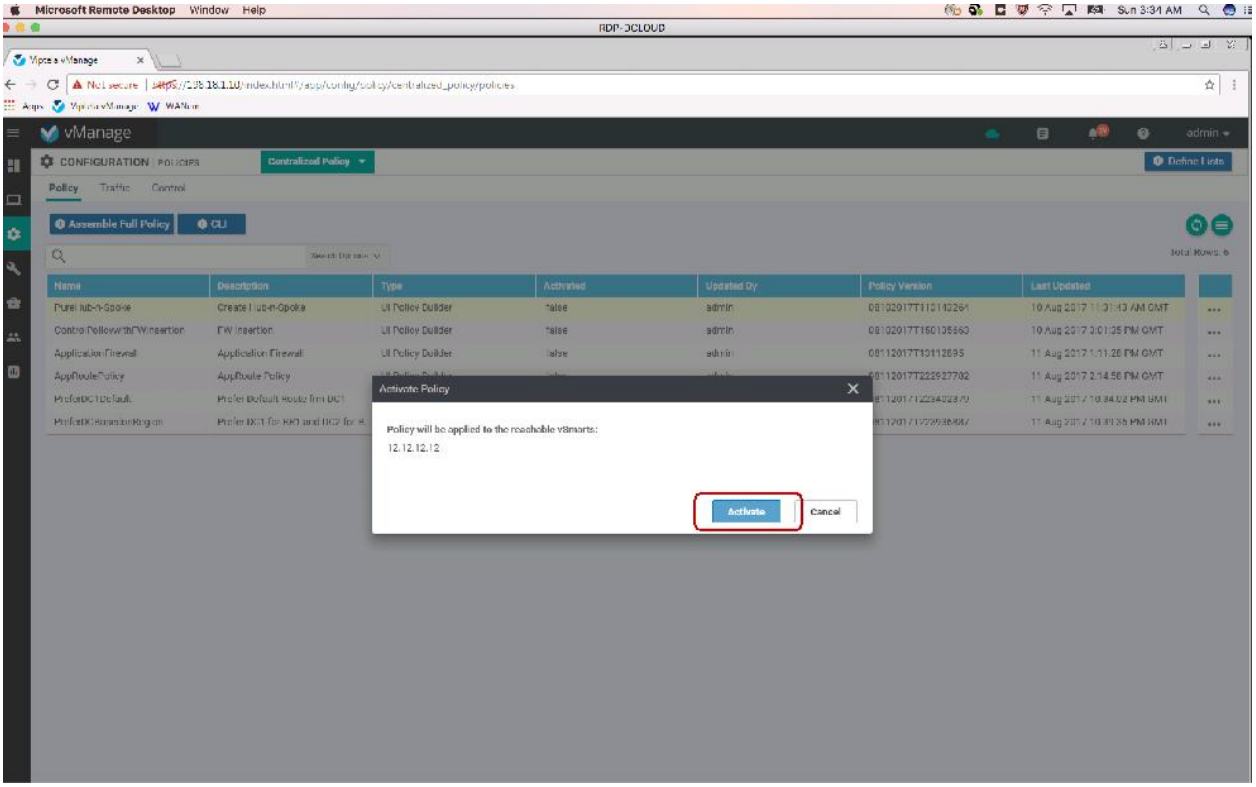
vManage 대시 보드로 이동하여 Configuration 으로 이동한 다음 Policies 를 선택하십시오.



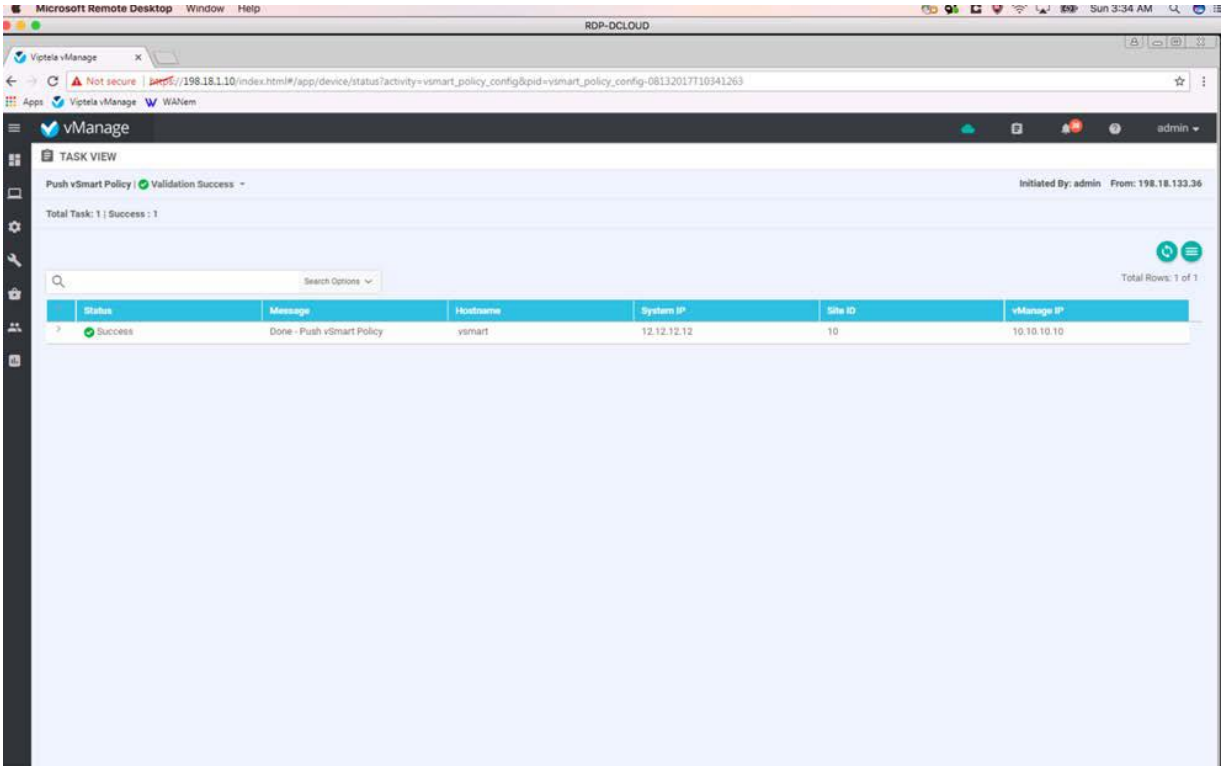
PureHub-n-Spoke 라는 정책의 가장 오른쪽 열을 클릭하십시오. 풀다운 메뉴에서 Activate 를 클릭하십시오.



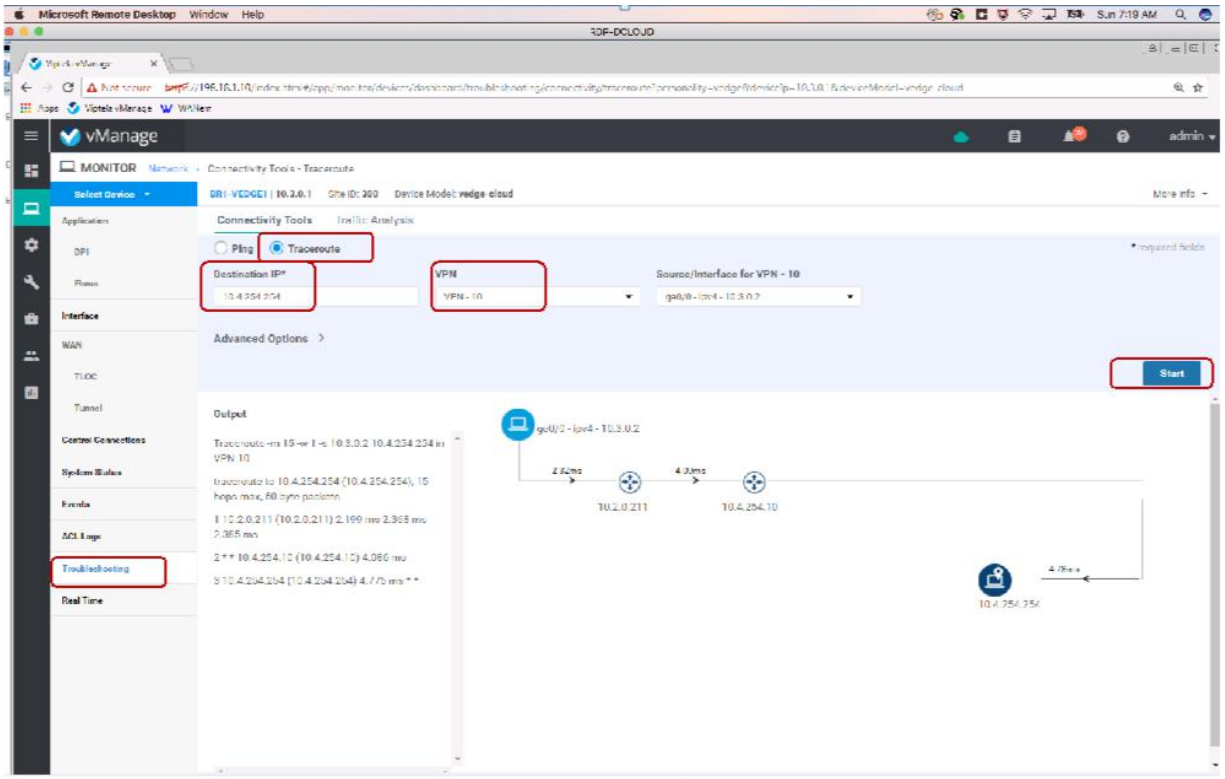
팝업에서 Activate 버튼을 클릭하십시오.



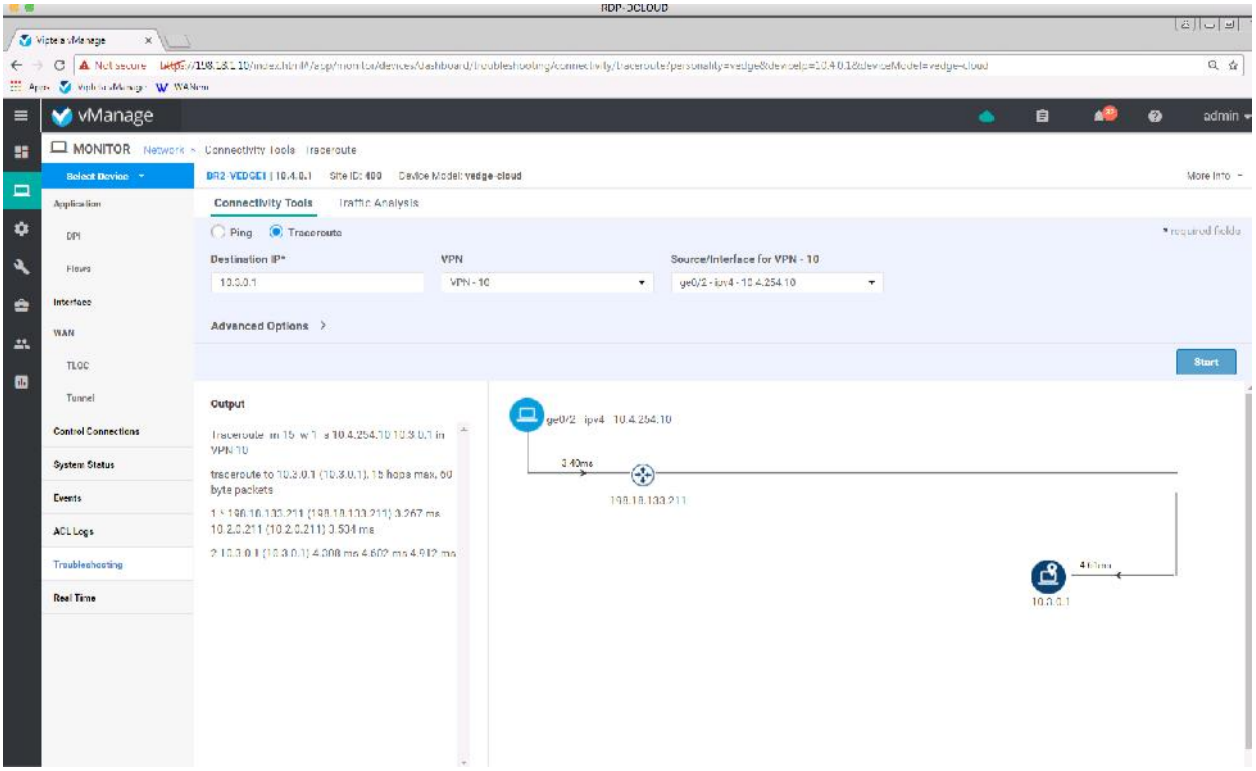
정책의 활성화 상태가 성공으로 바뀔 때까지 기다리십시오. 그러면 정책이 vSmart 에 적용됩니다.
vSmart 는 정책 컨트롤러이며 적절한 vEdge 박스로 정책을 내려보냅니다.



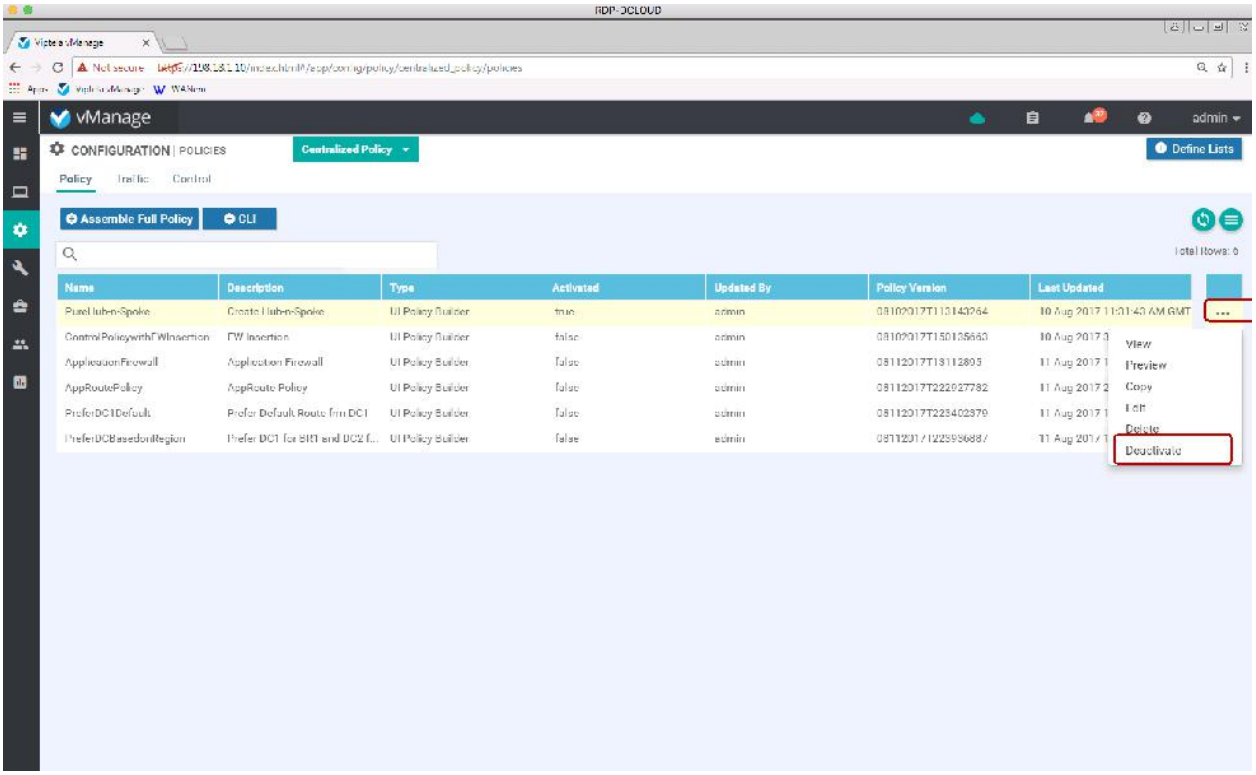
장치의 대시 보드로 이동하여 Hub-n-Spoke 토폴로지를 확인하십시오. BR1 에서 BR2 로 Traceroute 합니다. 추가적인 DC Hop (198.18.x.x 또는 10.2.x.x)을 볼 수 있습니다.



BR2 에서 BR1 로 Traceroute 합니다. 목적지 IP 는 10.3.0.1 을 사용하십시오.



정책을 비활성화합니다. 메인 대시 보드에서 Configuration, Policies 를 차례로 선택한 다음 PureHub-n-Spoke 정책을 선택 후 Deactivate 를 선택하여 클릭합니다.



시나리오 3. 서비스 체이닝 FW (M&A)

기업의 인수 합병으로 인해 새로운 브랜치가 추가되면 기업은 초기에 브랜치들 간의 통신이 특정 데이터센터의 FW 을 통과하길 원할 수도 있습니다.

과제

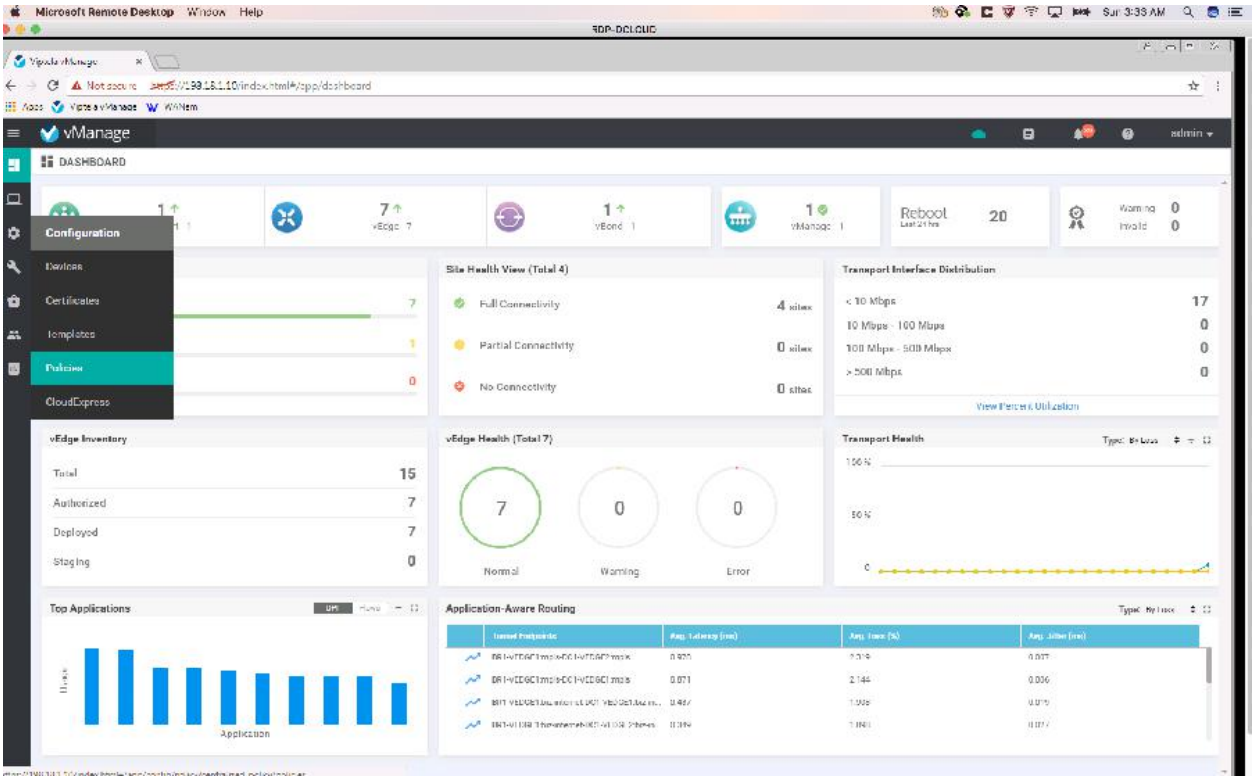
- 불규칙적인 토폴로지의 구성 및 관리는 복잡한 작업이며 브랜치 관리를 목적으로 경우에 따라 회선 사업자와 연계해야 하는 경우도 있습니다. FW 과 다른 서비스간의 경로 연결에 있어서 FW 은 기업의 위치와 상관없이 제공될 수 있습니다.

효과 – 비용 및 복잡성의 감소

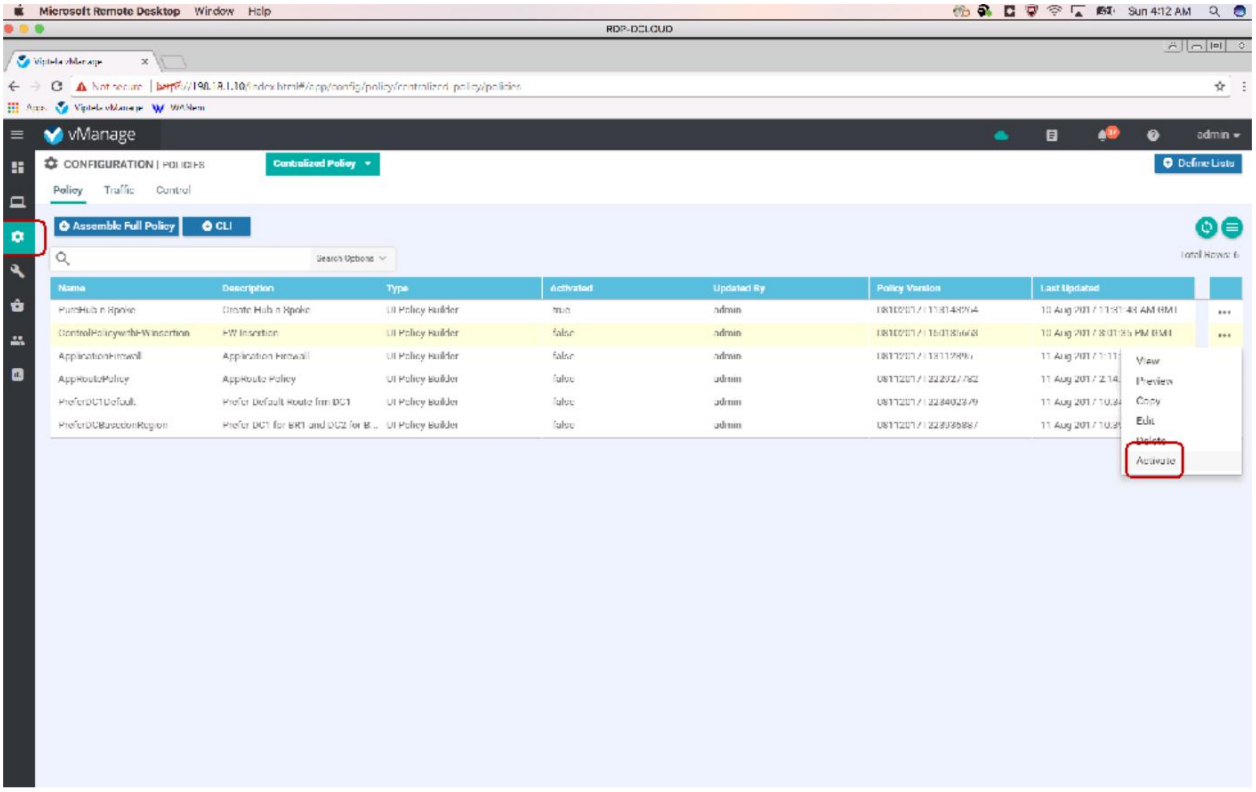
- 센트럴 vManage 를 통해 손쉽게 정책 활성화. 그에 따른 단순한 운영, 비용 감소 및 작업시간 단축

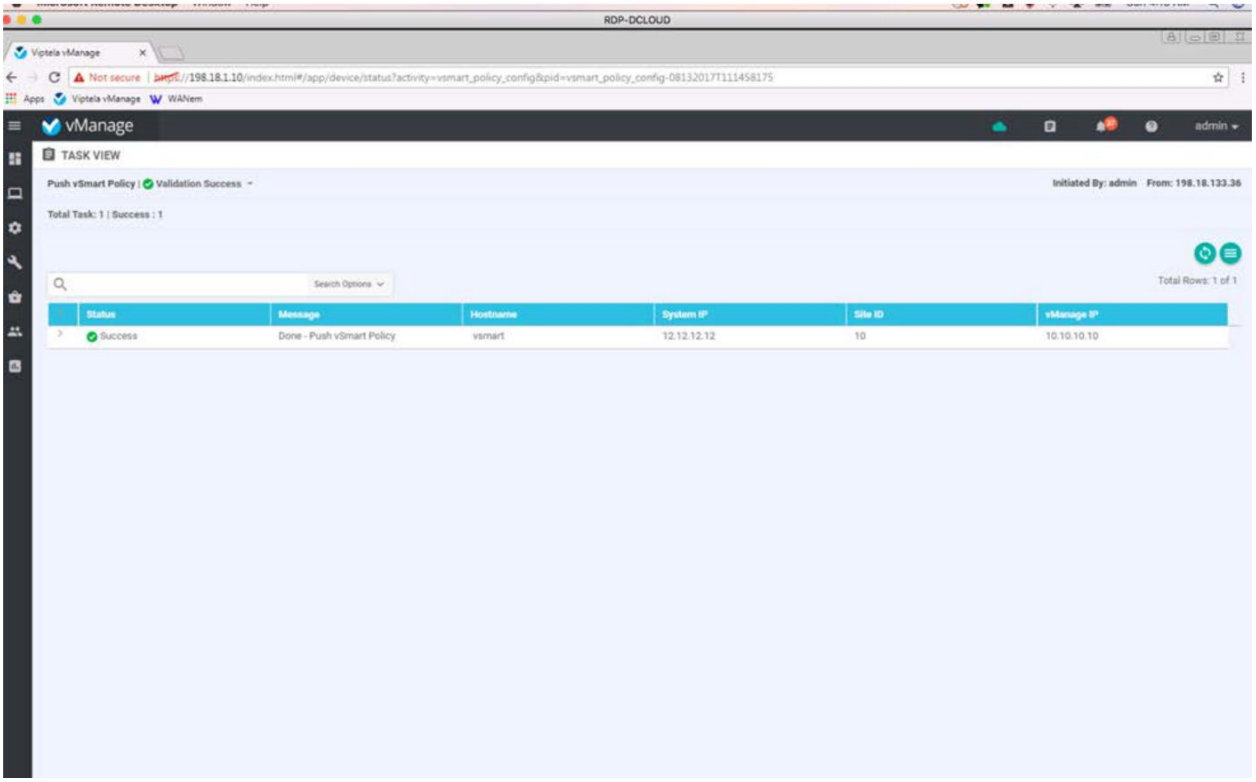
스텝

vManage 대시 보드로 이동하여 Configuration 으로 이동한 다음 Policies 를 선택하십시오.

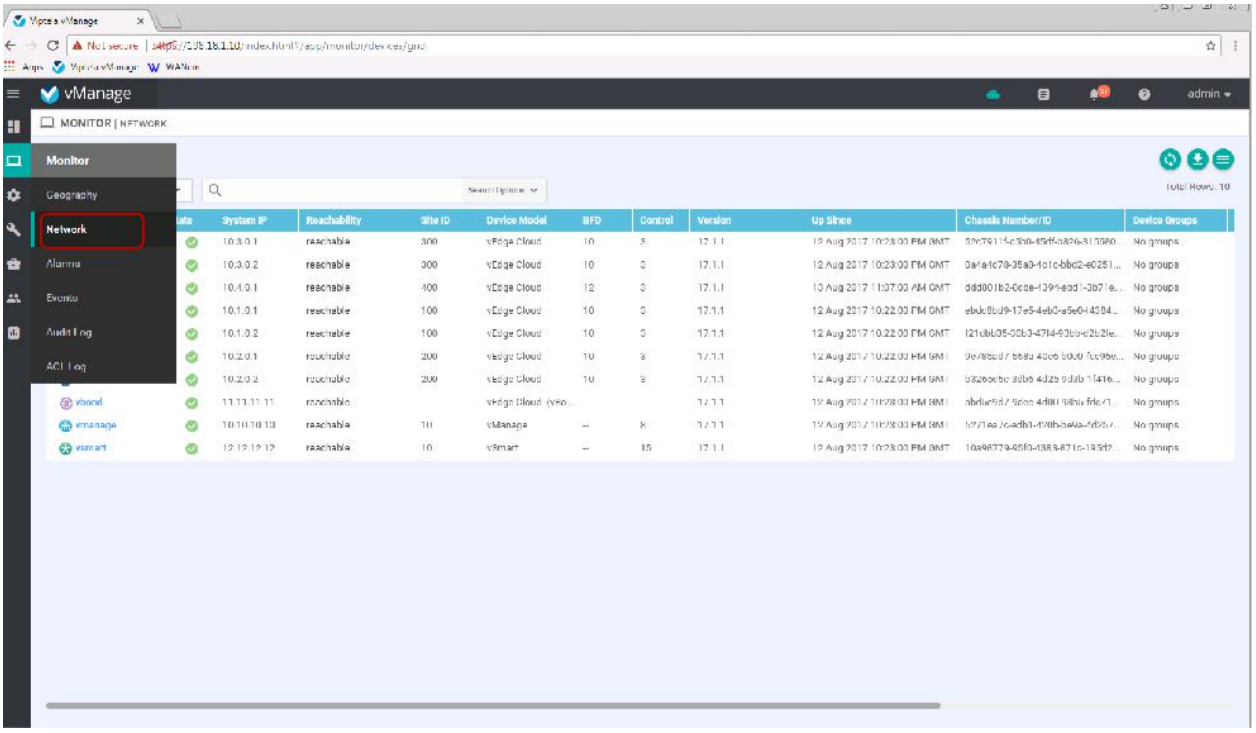


ControlPolicywithFWInsertion 라는 정책을 활성화합니다.

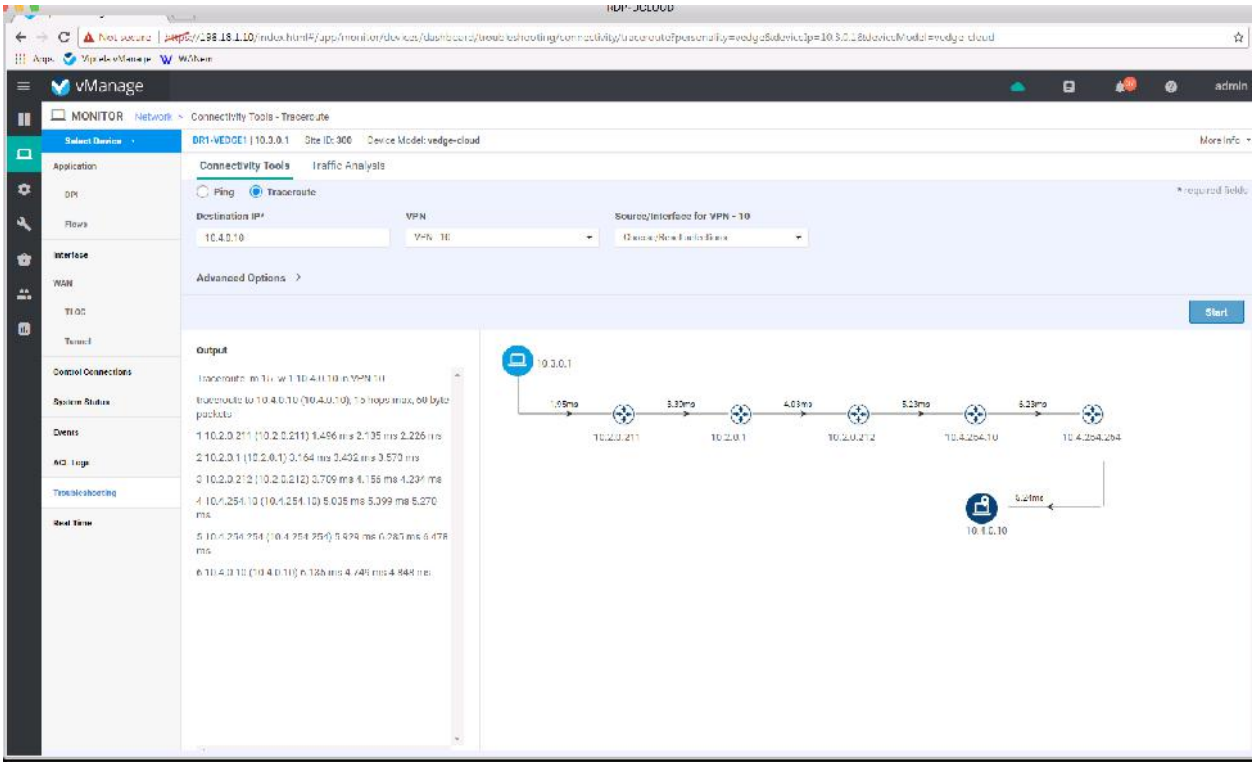




BR1-VEDGE1 의 Device Dashboard 로 이동하십시오. Monitor 에서 Network 를 선택합니다. BR1-VEDGE1 을 클릭하십시오.



Troubleshooting 로 이동 한 다음 10.4.254.254 로 traceroute 를 수행하십시오. DC2 에 위치한 FW(10.2.0.1)을 통과하는 트래픽을 확인할 수 있습니다.



BR2-VEDGE1 에서도 동일 과정을 반복합니다. 10.3.0.1 의 목적지 IP 로 traceroute 를 수행하십시오.

ControlPolicywithFWInsertion 의 정책을 비활성화합니다.

시나리오 4. 중앙 정책을 이용한 애플리케이션 방화벽 기능

기업은 예외적인 네트워크 사항에 대해 온디맨드(On-demand) 방식으로 보안 정책을 구현하고자 하는 경우가 있습니다. 방화벽 정책을 적용한 후에는 브랜치 1 (10.3.0.1)과 브랜치 2 (10.4.254.254)간의 애플리케이션 커뮤니케이션을 막을 수 있습니다. 출발지 포트가 선택된 일부 애플리케이션은 브랜치 1 과 DC 간에 통신할 수 없습니다.

과제

- 불규칙적인 토폴로지의 구성 및 관리는 복잡한 작업이며 브랜치 관리를 목적으로 경우에 따라 회선 사업자와 연계해야 하는 경우도 있습니다.

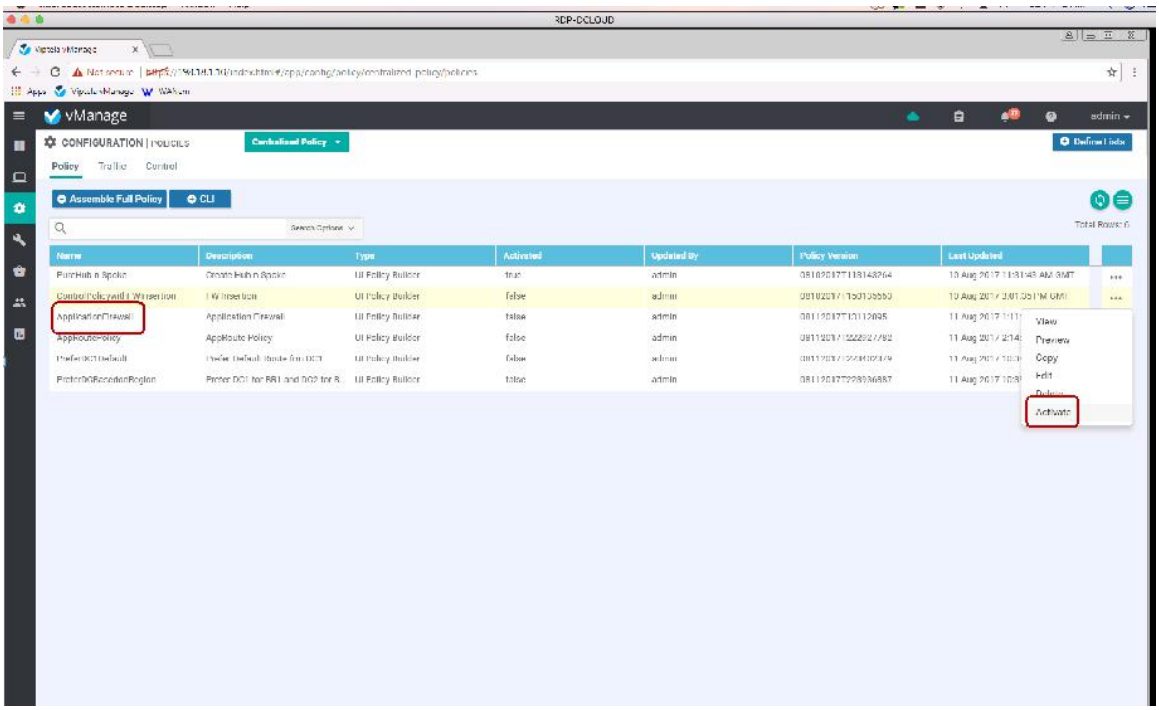
효과 – 비용 및 복잡성 감소

- Central vManage 에서 정책을 간단하게 활성화합니다. 결과적으로 운영이 단순 해지고 비용이 절감되며 시간 / 노력이 줄어듭니다.

스텝

Policy 을 활성화하기 전에 미리보기(preview)를 클릭하여 정책 전송 전, 보내려는 내용을 확인하십시오.

ApplicationFirewall 이라는 Policy 을 활성화하십시오.



vManage 메인 대시 보드에서 장치 대시 보드로 이동하십시오. Monitor 로 이동 한 다음 Device 를 선택하십시오.

브랜치 1 에서 브랜치 2 로 ping 테스트를 수행하십시오.

브랜치 2 에서 브랜치 1 로 ping 테스트를 수행하십시오.

테스트가 모두 실패할 겁니다.

정책을 비활성화하면 통신이 다시 시작됩니다.

시나리오 5. 애플리케이션 인식 라우팅

다양한 형태의 토폴로지에 대해 빠른 구축 및 모든 유형의 서킷을 지원하며, 이는 곧 다양한 유형의 링크를 통한 서로 다른 유형의 트래픽을 전달할 수 있는 기능을 제공합니다. 비디오는 인터넷을 통해 전달되고 업무상 중요한 애플리케이션은 MPLS 를 사용할 수 있습니다. 그리고 LTE 는 최후의 수단이 될 수 있습니다. 이는 경로 다양성 및 고가용성을 제공합니다.

애플리케이션 퍼포먼스를 기반으로 트래픽을 전달할 수 있는 기능을 갖춘 새로운 방식의 애플리케이션 전달 모델의 중요성에 대해 고객과 이야기하십시오.

이 데모에서 일부 애플리케이션의 SLA 가 사전에 정의되어 있고 MPLS (BR2-VEDGE1 의 인터페이스 ge0 / 0)에 연결되어 있습니다. 그리고 일부 다른 애플리케이션은 인터넷 전송 (BR2-VEDGE1 의 ge0 / 1 인터페이스)에 맞춰져 있습니다.

이 정책은 모든 사이트에 적용되어 있기 때문에 BR2-VEDGE1 에서 송수신된 모든 트래픽에 대해 영향을 미칩니다. BR2-VEDGE1 는 송신한 트래픽보다 수신한 트래픽이 많습니다. BR2-VEDGE1 의 mpls 인터페이스 (ge0 / 0) 및 인터넷 인터페이스 (ge0 / 1)에서 수신된 트래픽을 확인해 보십시오.

MPLS 에서 지연(latency) 장애가 발생한 후 mpls 인터페이스에서 인터넷 인터페이스로 트래픽이 전환되는 것을 확인할 수 있습니다.

과제

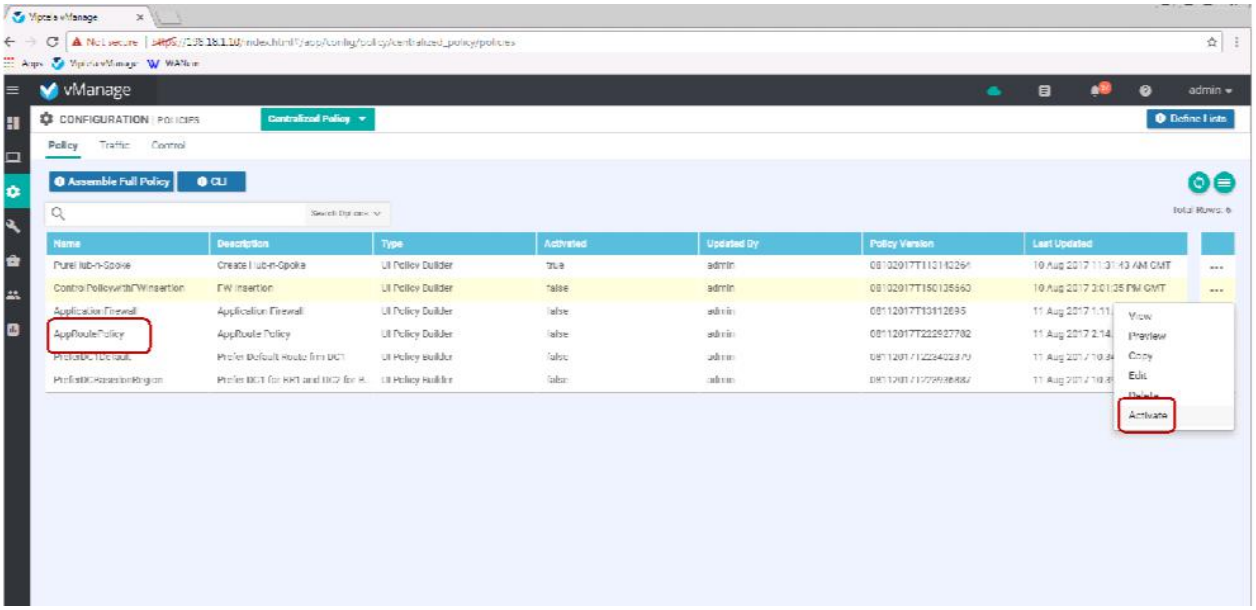
- 전송 성능 기반의 동적 경로 선택은 구축이 복잡하고 온디맨드(On-demand) 형태로 정책을 배포하기 어렵습니다.

효과 – 비용 및 복잡성 감소

- Central vManage 에서 정책을 간단하게 활성화합니다. 결과적으로 운영이 단순 해지고 비용이 절감되며 시간 / 노력이 줄어 듭니다.

스텝

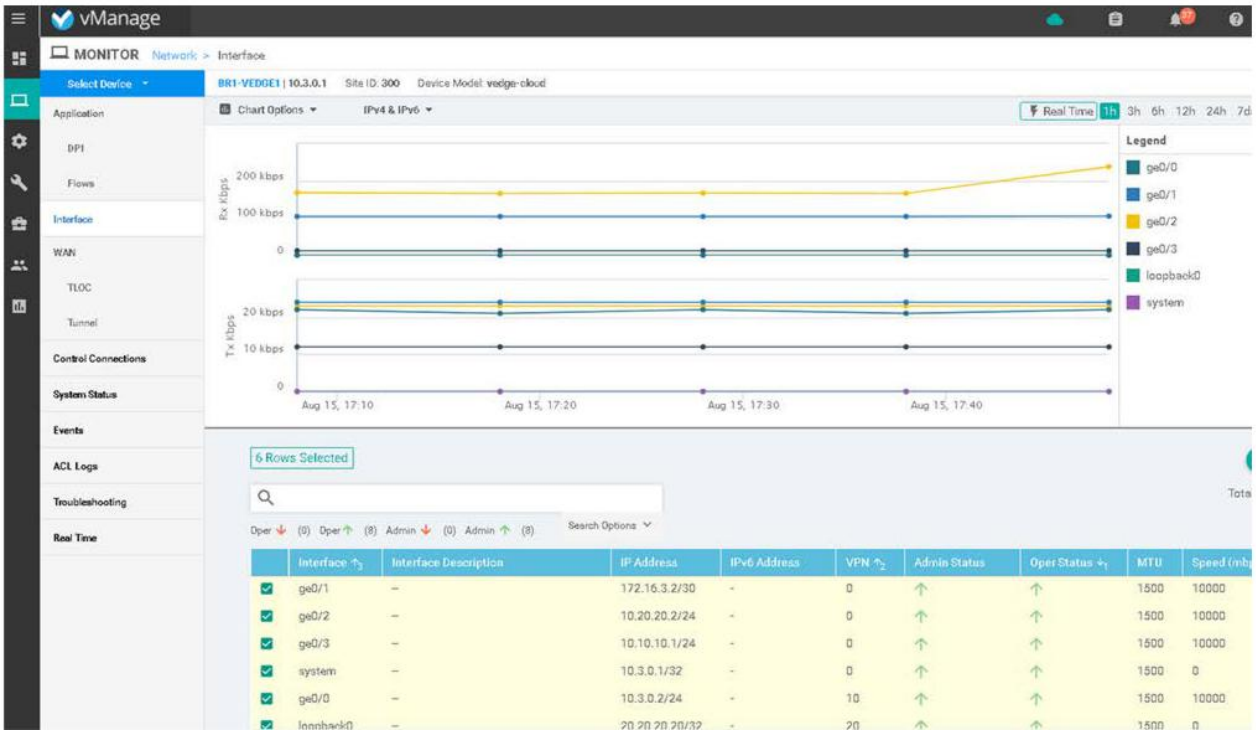
정책 구성 페이지로 이동하여 AppRoutePolicy 라는 이름의 애플리케이션 인식 라우팅(Application Aware Routing) 정책을 활성화하십시오.
이 정책은 MPLS 기본 경로에서 음성 / 영상 애플리케이션에 대해 최대 5 %의 패킷 손실 및 50msec 의 지연 시간에 대한 SLA 가 정의돼 있습니다.



BR1-VEDGE1 의 장치 대시 보드로 이동하십시오. Interface 를 클릭하고 BW(대역폭) 차트를 보십시오.

대부분의 트래픽은 MPLS 경로 (ge0 / 1)로 전달됩니다.

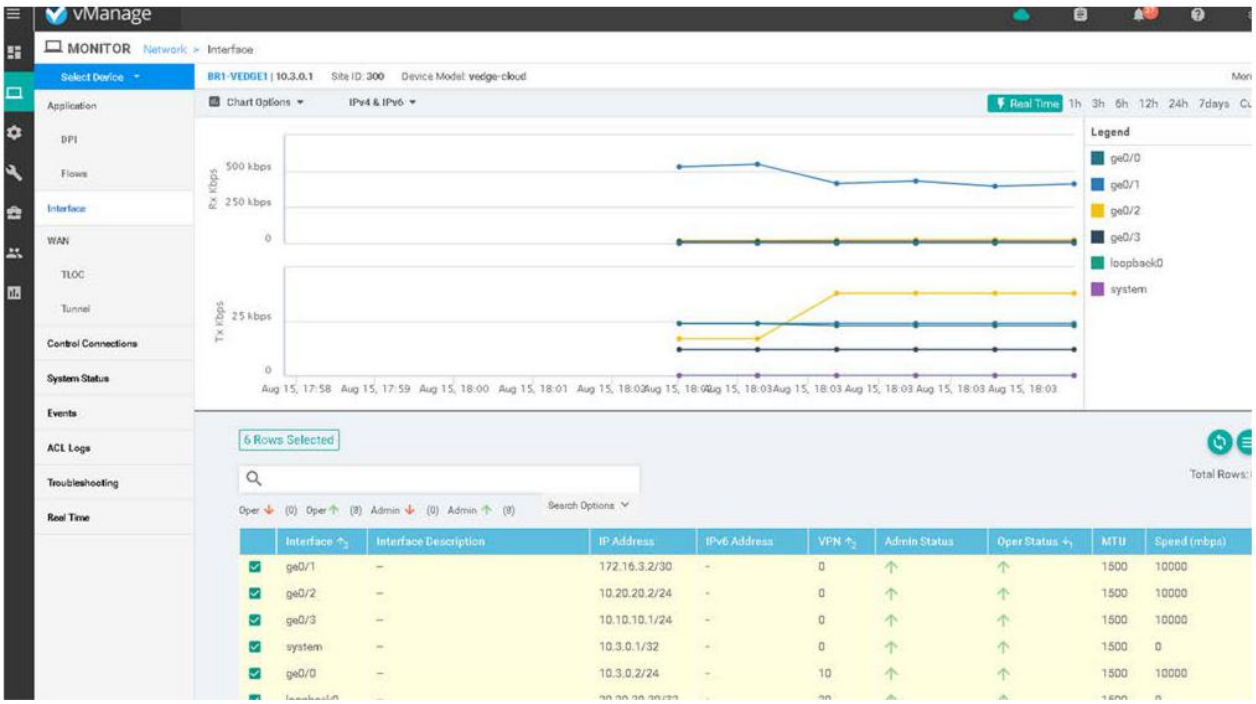
노트: 디스플레이 기본값이 24 시간이면 1 시간 또는 실시간으로 변경하십시오.



RDP 데스크탑에서 WAN EM URL 탭을 마우스 오른쪽 단추로 클릭하여 WAN 에뮬레이터를 엽니다.

MPLS 회선에 100msec 지연을 추가하고 적용하십시오.

BR1-VEDGE1 의 장치 대시 보드로 돌아가 Interface 탭을 클릭하십시오. 그리고 오른쪽 상단의 Real Time 버튼을 클릭하십시오. 트래픽이 MPLS (ge0 / 1)에서 인터넷 전송 (ge0 / 2)으로 전환된 것을 볼 수 있습니다.



WAN 에뮬레이션 툴에서 대기 시간을 제거하십시오.

vManage GUI 에서 app-route 정책을 비활성화하십시오.

시나리오 6. 브랜치 사이트별 각기 다른 인터넷 게이트웨이(DC1, DC2) 설정.

경우에 따라, 기업은 동일 오버레이 환경에서 브랜치 사이트별로 서로 다른 인터넷 게이트웨이 설정을 원할 수 있습니다.

DC1 을 브랜치 1 의 게이트웨이로, DC2 를 브랜치 2 의 게이트웨이라고 가정 해 봅시다.

과제

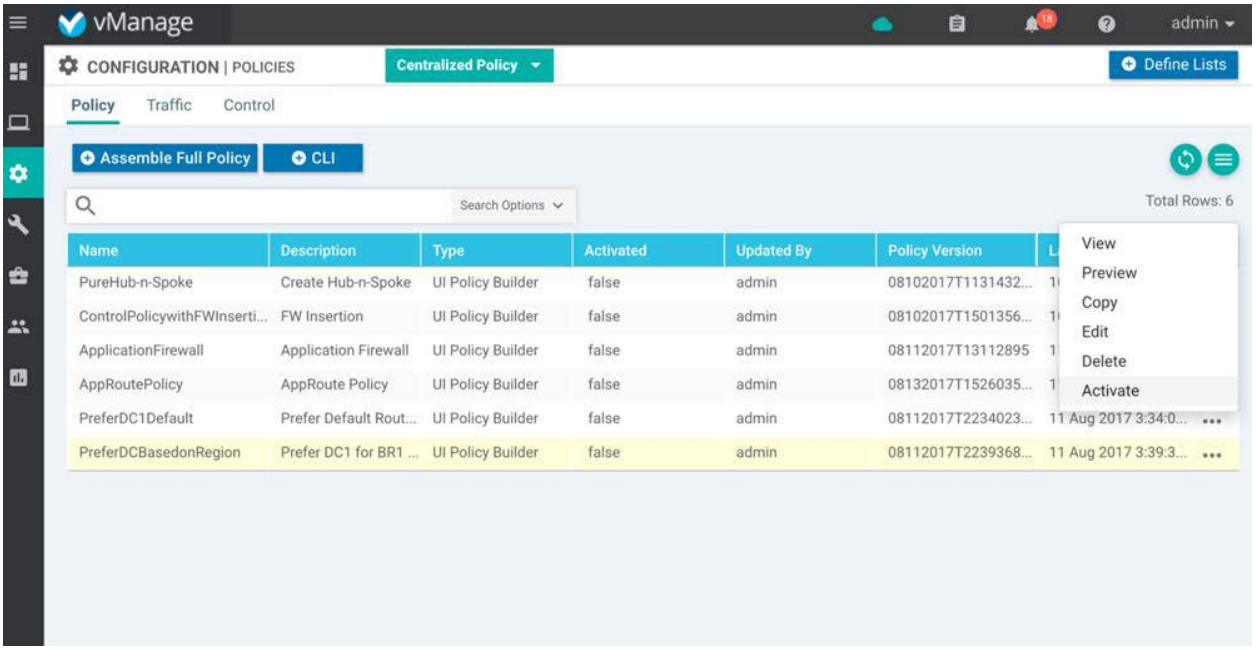
- 서로 다른 브랜치 지점에 각기 다른 게이트웨이를 갖게 하는 것은 복잡한 문제입니다.

효과 – 비용 및 복잡성 감소

- Central vManage 에서 정책을 간단하게 활성화합니다. 결과적으로 운영이 단순 해지고 비용이 절감되며 시간 / 노력이 줄어듭니다.

스텝

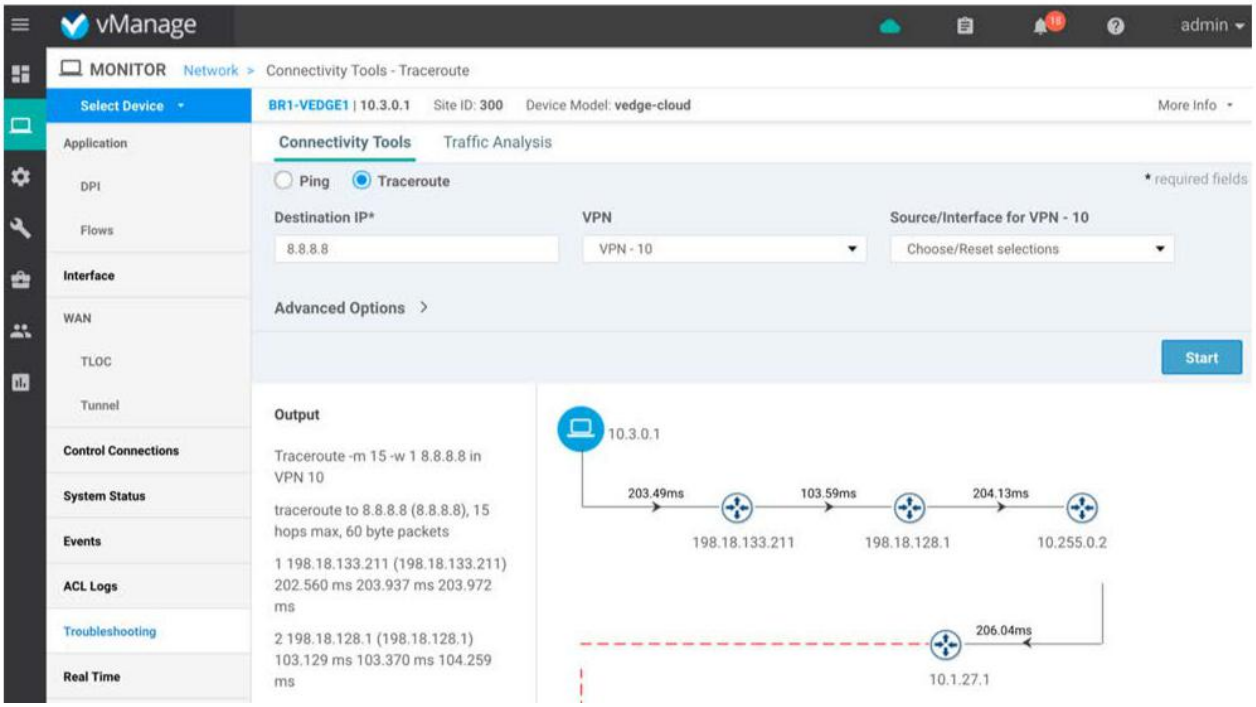
PreferDCBasedonRegion 이라는 정책을 활성화하십시오.



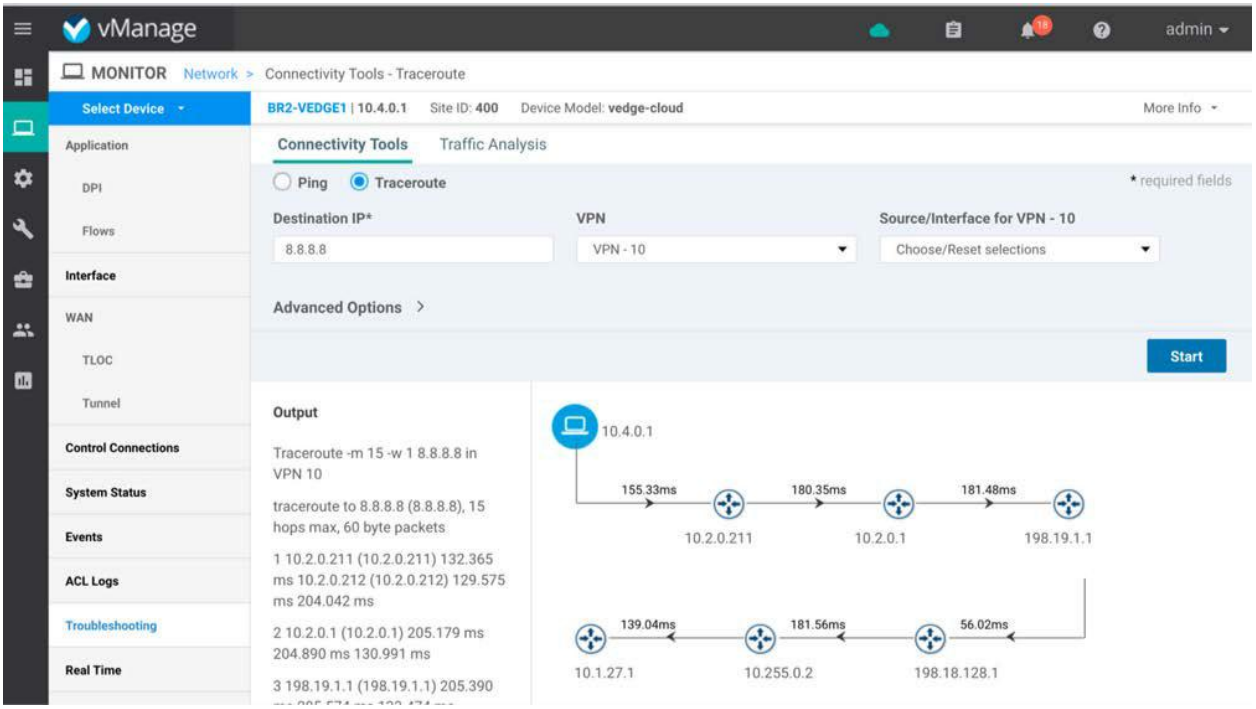
이 데모에서는 ping / traceroute 을 위한 인터넷 액세스는 차단되어 있습니다. 따라서 traceroute 는 실패하겠지만 (인터넷 마지막 연결 부분에서 타임아웃), 어떤 DC 가 게이트웨이로 사용되는지는 보여줍니다.

브랜치 1 은 DC1 을 사용하고 브랜치 2 는 DC2 를 통해 인터넷에 연결합니다.

BR1-VEDGE1 의 디바이스 대시 보드로 이동해 VPN10 의 목적지 경로를 8.8.8.8 로 하여 traceroute 합니다. DC1 (198.18.x.x)로 전송됩니다.



BR2-VEDGE1 도 마찬가지로 DC2 로 향할 것입니다.



Policy 을 비활성화하십시오.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**