Google 클라우드 교육 및 인증 제품 및 서비스를 최대한 활용하기위한 제안, 업데이트 및 유용한 팁을 보내 주시기 바랍니다. *

예

✓ 회사의 개인 데이터 센터에서 네트워크로 트래픽을 라우팅하는 새로운 VPC 네트워크를 설계하고 있습니다. VPC가 향후 고 가용성을 지원할 수 있도록하려고 합니다. 데이터 센터 팀에서는 데이터 센터에 링크 장애가있는 경우 동적으로 장애 조치 할 수있는 라우팅 프로토콜을 사용해야합니다. 경영진은 기본 클라우드 서비스 만 사용하도록 설계해야합니다. 어떤 라우팅 프로토콜을 사용해야합니까?

- (●) A. BGP ✓
- ( ) B. 립
- ( ) C. OSPF
- ( ) 정적 라우팅

피드백

BGP는 Google Cloud Router에서 지원하는 유일한 라우팅 프로토콜이므로 A는 정확합니다. 클라우드 기본 서비스 만 사용하도록 제한하면 클라우드 라우터를 사용해야합니다.

GCR에서 RIP를 지원하지 않으므로 B가 올바르지 않습니다.

GCR에서 OSPF를 지원하지 않으므로 C가 올바르지 않습니다.

고정 경로가 데이터 센터 팀 요구 사항을 충족하지 않기 때문에 D가 올바르지 않습니다.

https://cloud.google.com/...

✓ 새 프로젝트에는 현재 Google 클라우드 환경에서 회사의 개인 데이터 센터로 5Gbps의 송신 트래픽이 필요하지만 향후 최대 80Gbps의 트래픽으로 확장 될 수 있습니다. 사용할 공개 주소가 없습니다. 귀사는 가장 비용 효율적인 장기 솔루션을 찾고 있습니다. 어떤 유형의 연결을 사용해야합니까?

- A. 캐리어 피어링
- B. 파트너 상호 연결
- C. 전용 인터커넥트 ✓
- D. 단일 VPN (가상 사설망) 터널

피드백

Carrier Peering은 공용 IP 주소 공간을 사용해야하므로 A가 올바르지 않습니다.

Partner Interconnect 총 용량은 각 파트너에 따라 다르며 향후 목표보다 적을 수 있으므로 B는 올바르지 않습니다.

C는 현재 5Gbps 만 필요하지만 향후 용량에는 10Gbps 이상의 단일 연결을 처리 할 수 있어야하므로 C는 정확합니다.

단일 VPN 터널은 최대 3Gbps의 트래픽 만 처리 할 수 있으므로 D는 정확하지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

✓ 회사가 방금 GCP로 이전했습니다. 재무 및 영업 부서에 대해 별도의 VPC 네트워크를 구성했습니다. Finance는 Sales VPC의 일부인 일부 리소스에 액세스해야합니다. 프라이빗 RFC 1918 주소 공간 트래픽이 추가 비용없이 보안 또는 성능 저하없이 영업 및 재무 VPC간에 흐르도록하려고합니다. 어떻게해야합니까?

- A. 두 VPC 사이에 VPN 터널을 만듭니다.
- B. 두 VPC간에 VPC 피어링을 구성하십시오. ✓
- C. 인터넷을 통해 트래픽을 라우팅하려면 두 VPC에 경로를 추가하십시오.
- D. 리소스에 액세스하기위한 상호 연결 연결을 만듭니다.

피드백

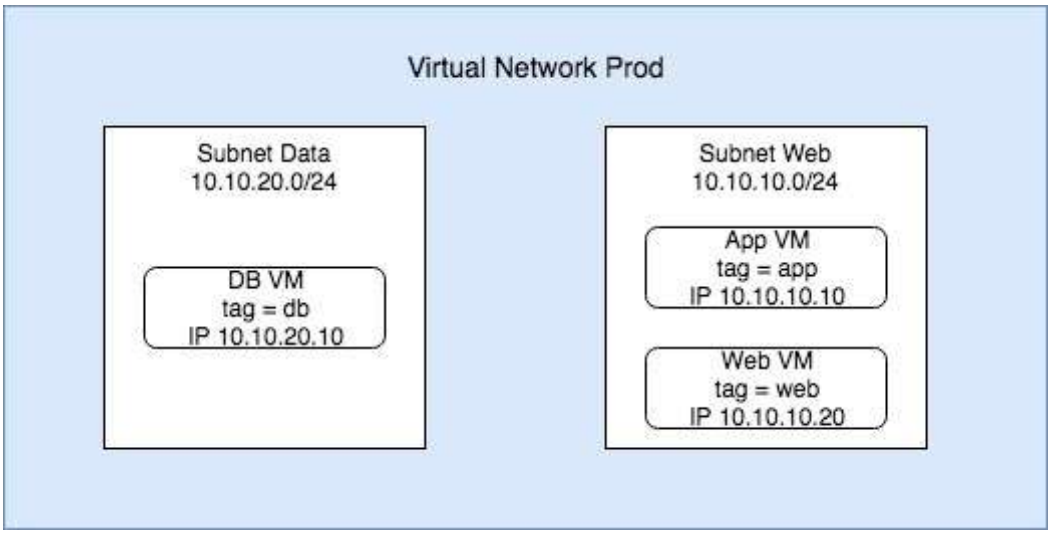
VPN이 성능을 방해하고 추가 비용이 발생하기 때문에A는 올바르지 않습니다.

VPC 네트워크 피어링을 통해 추가 비용없이 보안 또는 성능을 저하시키지 않으면 서 개인 1918 주소 공간을 통해 두vPC간에 트래픽을 전송할 수 있으므로B가 맞습니다.

RFC 1918은 개인 주소 공간이므로 공용 인터넷을 통해 라우팅 할 수 없으므로C가 올바르지 않습니다.

Interconnect가 동일한 작업을 수행하는 데 더 많은 비용이 들기 때문에D는 올바르지 않습니다.

✕ 아래와 같이 두 개의 서브넷이있는 사용자 지정 모드에서 Prod라는 VPC를 생성합니다. 1) App VM 만 DB VM 인스턴스에 액세스 할 수 있고 2) Web VM이 App VM에 액세스 할 수 있습니다. 3) VPC 외부의 사용자는 Web VM에만 HTTPS 요청을 보낼 수 있습니다. 어떤 두 가지 방화벽 규칙을 만들어야합니까?



- [ ] A. 소스 태그 "web"의 모든 트래픽을 차단하십시오.
- [ ] B. 소스 태그 "app"에서 포트 80으로의 트래픽 만 허용하십시오.
- [x] C. 소스 태그 "app"에서 대상 태그 "db"로의 모든 트래픽을 허용합니다. ✓
- [ ] D. 대상 태그 "web"에 대해 포트 80 및 443 에서 0.0.0.0/0의 수신 트래픽을 허용 합니다.
- [x] E. 소스 IP 범위 = 10.10.10.0/24 인 소스 필터 = IP 범위를 사용하여 수신 트래픽을 허용하십시오 . ✕

정답

- [x] C. 소스 태그 "app"에서 대상 태그 "db"로의 모든 트래픽을 허용합니다.
- [x] D. 대상 태그 "web"에 대해 포트 80 및 443 에서 0.0.0.0/0의 수신 트래픽을 허용 합니다.

피드백

웹 VM이 여전히 앱 VM과 통신해야하므로 A가 올바르지

않습니다. 요구 사항에 따라 필요하지 않기 때문에 B가 올바르지 않습니다.

이 규칙은 앱 VM에서 db VM으로의 트래픽을 허용하므로 C는 정확합니다.

D는 외부 사용자가 웹 VM에 요청을 보낼 수 있기 때문에 정확합니다.

웹 VM 이 db VM 에 액세스 할 수 있으므로 E 가 올바르지 않습니다.

https://cloud.google.com/...

✓ 동일한 VPC 네트워크에서 Test와 Web이라는 두 개의 서브넷을 생성했습니다. 웹 서브넷에 VPC 흐름 로그를 활성화했습니다. 테스트 서브넷의 인스턴스를 웹 서브넷에서 실행중인 웹 서버에 연결하려고하지만 모든 연결이 실패합니다. Stackdriver 로그에 항목이 표시되지 않습니다. 어떻게해야합니까?

- A. 테스트 서브넷에도 VPC 흐름 로그를 활성화하십시오.
- B. 라우팅 테이블에 유효한 항목이 있는지 확인하십시오.
- C. 테스트 서브넷에서 웹 서브넷으로의 트래픽을 허용하는 방화벽 규칙을 추가하십시오. ✓
- D. 다른 VPC에서 서브넷을 생성하고 웹 서버를 새 서브넷으로 이동하십시오.

피드백

서브넷 'Test' 에서 흐름 로그를 활성화해도 트래픽이 방화벽 규칙에 의해 차단 되어도 데이터를 제공하지 않기 때문에 A 가 올바르지 않습니다.

서브넷이 동일한 VPC 의 일부이므로 라우팅을 구성 할 필요가 없으므로 B 가 올바르지 않습니다. 방화벽 규칙에 의해 트래픽이 차단되고 있습니다.

트래픽이 방화벽 규칙에 의해 차단되고 있으므로 C 가 정확합니다. 구성되면 요청이 VM 에 도달하고 스택 드라이버에 플로우가 기록됩니다.

트래픽이 방화벽 규칙에 의해 차단되고 서브넷이 동일한 VPC 에 있지 않기 때문에 D 가 올바르지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

✕ 기존 고정 경로에 대한 백업으로 고정 경로를 구성해야합니다. 기존 경로를 더 이상 사용할 수없는 경우에만 새 경로를 사용하려고합니다. 어떻게해야합니까?

- A. 새 정적 경로에 대한 백업 값으로 네트워크 태그를 만듭니다.
- B. 기존 고정 경로보다 새로운 고정 경로에 우선 순위를 낮게 설정하십시오. ✕
- C. 기존 고정 경로보다 새로운 고정 경로에 우선 순위를 높게 설정하십시오.
- D. 기존 고정 경로와 동일한 고정 경로에 대해 새 고정 경로에 대한 우선 순위 값을 구성하십시오.

정답

- C. 기존 고정 경로보다 새로운 고정 경로에 우선 순위를 높게 설정하십시오.

피드백

특정 네트워크 태그가있는 경로는 태그 값이있는 인스턴스에만 적용되므로 A가 올바르지 않습니다.

고정 경로 우선 순위가 낮은 값을 사용하여 우선 순위가 높은 것을 나타내므로 B가 올바르지 않습니다.

값이 높을수록 값이 낮은 경로를 사용할 수없는 경우에만 경로가 적용되므로 C가 정확합니다.

동일한 값을 사용하는 경우 GCP가 동일한 비용 다중 경로 라우팅을 사용하고 기존 고정 경로를 계속 사용할 수있을 때 새 경로를 사용하기 때문에 D는 올바르지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

✓ 새로운 Google Cloud HTTPS로드 밸런서를 위해 백엔드 서비스를 구성하고 있습니다. 응용 프로그램에는 고 가용성 및 다중 서브넷이 필요하며 자동으로 확장해야합니다. 어떤 백엔드 구성을 선택해야합니까?

- A. 존 관리 형 인스턴스 그룹
- B. 지역 관리 형 인스턴스 그룹 ✓
- C. 관리되지 않는 인스턴스 그룹
- D. 네트워크 엔드 포인트 그룹

피드백

A는 지역 내에서 단일 영역 만 사용할 수 있기 때문에 올바르지 않습니다.

B는 애플리케이션이 한 지역 내의 여러 영역에 배치 될 수 있기 때문에 정확합니다.

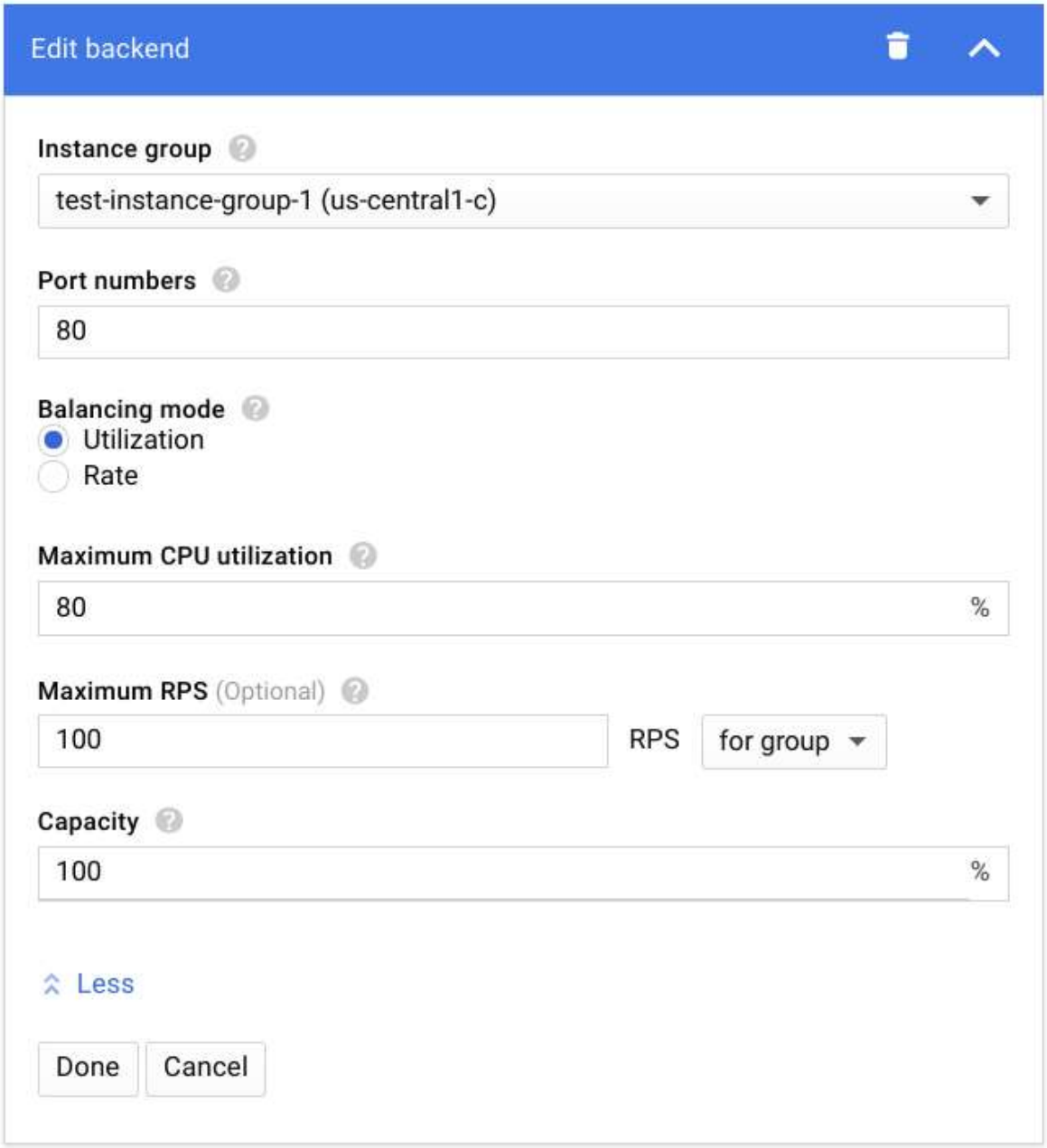
C는 자동 확장을 허용하지 않으므로 올바르지 않습니다.

트래픽이 여러 서브넷에 분산 될 수없고 여러 NEG와 달리 단일 NEG 이므로 D가 올바르지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

https://cloud.google.com/... https://cloud.google.com/...

✕ 아래에 표시된 Google Cloud로드 밸런서 백엔드 구성이 있습니다. 인스턴스 그룹 사용률을 20 % 줄이려고합니다. 어떤 설정을 사용해야합니까?



- A. 최대 CPU 사용률 : 60 및 최대 RPS : 80
- B. 최대 CPU 사용률 : 80 및 용량 : 80
- C. 최대 RPS : 80 및 용량 : 80 ✕
- D. 최대 CPU : 60, 최대 RPS : 80 및 용량 : 80

정답

- B. 최대 CPU 사용률 : 80 및 용량 : 80

피드백

A는 CPU 사용률과 초당 요청을 모두 줄임으로써 20 % 이상 감소하기 때문에 올바르지 않습니다.

전체 인스턴스 그룹 사용률을 20 % 변경하기 때문에 B가 맞습니다.

C는 초당 요청을 20 % 이상 줄이므로 올바르지 않습니다.

D는 최대 CPU와 RPS를 모두 줄여서 20 % 이상이되기 때문에 정확하지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

✓ 조직에 하이브리드 클라우드 토폴로지를 구성하고 있습니다. Cloud VPN 및 Cloud Router를 사용하여 온-프레미스 환경에 연결합니다. 온 프레미스에서 Cloud Storage 버킷 및 BigQuery로 데이터를 전송해야합니다. 조직에는 클라우드와의 통신에 VPN을 사용해야하는 엄격한 보안 정책이 있습니다. Google 권장 사례를 따르고 싶습니다. 어떻게해야합니까?

A. 프라이빗 Google 액세스가 활성화 된 VPC에서 인스턴스를 생성합니다. VPN 연결을 사용하여 VPC의 인스턴스로 데이터를 전송하십시오. 인스턴스에서 "gsutil cp 파일 gs : // bucketname"및 "bq --location = [LOCATION] load --source_format = [FORMAT] [DATASET]. [TABLE] [PATH_TO_SOURCE] [SCHEMA]"을 사용하여 클라우드 스토리지 및 BigQuery.

B.“nslookup -q = TXT _ spf.google.com ”을 사용하여 Google의 넷 블록에서 Cloud Storage 및 BigQuery에 사용되는 API IP 엔드 포인트를 얻습니다. 유연한 라우팅 광고를 사용하여 이러한 넷 블록을 온-프레미스 라우터에 알리도록 Cloud Router를 구성하십시오. "gsutil cp 파일 gs : // bucketname"및 "bq --location = [LOCATION] load --source_format = [FORMAT] [DATASET]. [TABLE] [PATH_TO_SOURCE] [SCHEMA]"를 사용하여 데이터를 클라우드 스토리지 및 BigQuery.

C. 유연한 라우팅 광고를 사용하여 199.36.153.4/30 을 온-프레미스 라우터에 알리도록 Cloud Router를 구성 하십시오. 온-프레미스 DNS 서버 CNAME 항목을 *에서 수정하십시오. googleapis.com 에 restricted.googleapis.com . "gsutil cp 파일 gs : // bucketname 및 bq --location = [LOCATION] load --source_format = [FORMAT] [DATASET]. [TABLE] [PATH_TO_SOURCE] [SCHEMA]"온 프레미스를 사용하여 데이터를 Cloud Storage로 전송 그리고 BigQuery. ✓

D.“gsutil cp 파일 gs : // bucketname”및“bq --location = [LOCATION] load --source_format = [FORMAT] [DATASET]. [TABLE] [PATH_TO_SOURCE] [SCHEMA] "온-프레미스를 사용하여 전송 Cloud Storage 및 BigQuery로 데이터를 전송합니다.

피드백

A 운영상의 복잡성을 추가하고 데이터를 전송하기위한 단일 장애 지점 (인스턴스) 을 도입하기 때문에 올바르지 않습니다. 온 프레미스 개인 API 액세스를위한 Google 권장 사례는 아닙니다.

B 이러한 넷 블록이 변경 될 수 있고 이러한 API 가 다른 넷 블록으로 이동하지 않을 것이라는 보장이 없기 때문에 정확하지 않습니다.

C On-Prem Private API 액세스를 활성화하여 VPN 및 Interconnect 고객이 기본적으로 상호 연결 / VPN 연결을 통해 bigquery 및 클라우드 스토리지와 같은 API 에 도달 할 수 있기 때문에 정확합니다.

D 사용 가능한 인터넷 링크를 사용하여 데이터를 전송하기 때문에 정확하지 않습니다 (있는 경우). 클라우드에 대한 VPN 연결 사용의 보안 요구 사항을 충족하지 않습니다.

https://cloud.google.com/...

✓ GCP로 이전하는 대학에서 근무합니다. 중앙 네트워킹 관리 팀의 일원입니다. 클라우드에 대한 대기 시간이 10Gbps이고 지연 시간이 짧은 온 프레미스 연결이 필요합니다. 하드 코딩 된 IP 주소를 사용하여 여러 응용 프로그램을 해제하고 이동해야합니다. 공용 인터넷 링크를 통해 온-프레미스 BGP 가능 VPN 게이트웨이를 사용하여 여러 CIDR 범위를 가진 소규모 원격 캠퍼스 위치를 클라우드에 연결하려고합니다. 온-프레미스 게이트웨이는 IKEv1 만 지원하며 최대 3Gbps의 처리량 요구 사항이 있습니다. Google 권장 사례를 따르고 싶습니다. 어떻게해야합니까?

A. 1 개의 Cloud VPN 인스턴스를 만듭니다. 경로 기반 VPN을 사용하여 VPN 게이트웨이를 향한 1 개의 터널을 만듭니다. 트래픽 선택기를 0.0.0.0/0으로 설정하십시오 . 온-프레미스 원격 캠퍼스 CIDR 범위를 가리 키도록 경로를 구성하십시오.

B. 1 개의 Cloud VPN 인스턴스를 만듭니다. 정책 기반 VPN을 사용하여 VPN 게이트웨이를 향한 1 개의 터널을 만듭니다. 로컬 트래픽 선택기를 GCP 범위로 설정하고 원격 트래픽 선택기를 온-프레미스 범위로 설정하십시오.

C. 2 개의 Cloud VPN 인스턴스를 만듭니다. 클라우드 라우터를 만듭니다. VPN 게이트웨이를 향한 인스턴스 당 동적 VPN 터널을 만듭니다. 온-프레미스 원격 캠퍼스와 GCP간에 교환 할 경로를 구성하십시오. ✓

D. 2 개의 Cloud VPN 인스턴스를 만듭니다. 정책 기반 VPN을 사용하여 VPN 게이트웨이를 향해 2 개의 터널을 만듭니다. 로컬 트래픽 선택기를 GCP 범위로 설정하고 원격 트래픽 선택기를 두 터널의 온-프레미스 범위로 설정하십시오.

피드백

1 개의 VPN 터널이 충분한 용량을 지원하지 않기 때문에 A 가 올바르지 않습니다.

1 개의 VPN 터널이 충분한 용량을 지원하지 않고 IKEv1 이 여러 로컬 트래픽 및 원격 트래픽 선택기를 지원하지 않기 때문에 B 가 올바르지 않습니다.

동적 경로를 사용하여 Cloud VPN 을 사용하면 여러 CIDR 블록으로 IKEv1 을 지원할 수 있으므로 C 가 정확합니다. 또한 2 개의 VPN 게이트웨이는 3Gbps 를 지원하기에 충분합니다.

D IKEv1 은 여러 로컬 트래픽 및 원격 트래픽 선택기를 지원하지 않기 때문에 올바르지 않습니다.

https://cloud.google.com/...

✕ Dedicated Interconnect를 통해 단일 클라우드 라우터를 사용하여 VPC와 온프레미스 네트워크 간 경로를 교환하고 있습니다. 한 지역의 모든 클라우드 라우터가 다운 되더라도 트래픽을 계속 전달할 수 있도록하려고합니다. 어떻게해야합니까?

- A. Cloud Router의 백업으로 고정 경로를 사용하십시오.
- B. 온-프레미스 라우터에서 정상적으로 다시 시작합니다.
- C. VPC에서 글로벌 라우팅을 켜고 다른 지역에 다른 클라우드 라우터를 만듭니다.
- D. 동일한 리전에서 두 번째 온-프레미스 장치에 대한 BGP (Border Gateway Protocol) 세션을 사용하여 두 번째 클라우드 라우터를 만듭니다. ✕

정답

- C. VPC에서 글로벌 라우팅을 켜고 다른 지역에 다른 클라우드 라우터를 만듭니다.

피드백

고정 경로가 Dedicated Interconnect 에서 작동하지 않기 때문에 A 가 올바르지 않습니다.

정상적인 재시작은 클라우드 라우터 가용성에 영향을 미치지 않으므로 B 는 올바르지 않습니다.

글로벌 라우팅을 통해 다른 지역의 Cloud Router 가 다른 지역의 경로를 알 수 있기 때문에 C 가 정확합니다.

두 번째 온-프레미스 장치는 클라우드 라우터 가용성에 영향을 미치지 않기 때문에 D 가 올바르지 않습니다.

https://cloud.google.com/...

✓ GCP로 이전하는 다국적 기업의 중앙 네트워크 관리 팀에서 근무합니다. 귀사에는 미국 오레곤 주와 뉴욕에 위치한 온 프레미스 데이터 센터가 있으며 클라우드 지역 us-west1 및 us-east4에 대한 전용 상호 연결이 있습니다. 유럽 및 APAC에 여러 지역 사무소가 있고 europe-west1 및 australia-southeast1에 지역 데이터 처리가 있습니다. 런던의 지역 사무소에있는 Compute Engine 인스턴스에서 미국 데이터 센터의 데이터를 처리 할 수 있도록 Cloud Router를 구성하려고합니다. 영국과 시드니, 호주. 토폴로지를 어떻게 구성해야합니까?

- ○ A. europe-west1 및 australia-southeast1 지역의 지역 라우팅을 사용하여 클라우드 라우터를 만듭니다. europe-west1 및 australia-southeast1에서 클라우드 라우터를 가리키는 상호 연결에서 VLAN 첨부 파일을 작성하십시오. europe-west1 및 australia-southeast1 지역에서 온-프레미스 환경으로의 적절한 경로를 광고하십시오.
- ○ B. europe-west1 및 australia-southeast1 지역에서 글로벌 라우팅을 사용하여 클라우드 라우터를 만듭니다. europe-west1 및 australia-southeast1에서 클라우드 라우터를 가리키는 상호 연결에서 VLAN 첨부 파일을 작성하십시오. europe-west1 및 australia-southeast1 지역에서 온-프레미스 환경으로의 적절한 경로를 광고하십시오.
- ◉ C. us-west1 및 us-east4 리전에서 글로벌 라우팅을 사용하여 클라우드 라우터를 만듭니다. us-west1 및 us-east4에서 클라우드 라우터를 가리키는 상호 연결에서 VLAN 연결을 작성하십시오. europe-west1 및 australia-southeast1 지역에서 온-프레미스 환경으로의 적절한 경로를 광고하십시오. ✓
- ○ D. us-west1 및 us-east4 리전에서 지역 라우팅을 사용하여 클라우드 라우터를 만듭니다. us-west1 및 us-east4에서 클라우드 라우터를 가리키는 상호 연결에서 VLAN 연결을 작성하십시오. europe-west1 및 australia-southeast1 지역에서 온-프레미스 환경으로의 적절한 경로를 광고하십시오.

피드백

VLAN / 인터커넥트 연결 장치에 지역 위치가 있으므로 A가 올바르지 않습니다. 상호 연결이 아닌 다른 대륙 지역에서는 VLAN 연결을 연결할 수 없습니다.

VLAN / 인터커넥트 연결 장치에 지역 위치가 있으므로 B가 올바르지 않습니다. 상호 연결이 아닌 다른 대륙 지역에서는 VLAN 연결을 연결할 수 없습니다.

C는 정확합니다. Global Routing을 사용하여 미국의 상호 연결을 활용하고 Global Backbone을 사용하여 원격 EU / APAC 지역으로 트래픽을 라우팅하십시오.

D 지역 라우팅을 사용하기 때문에 올바르지 않습니다. 해당 원격 지역은 사내 광고로 다시 광고되지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

✓ 관리자가 Identity Access Management 내에서 일반 가용성 단계가있는 모든 사용자 지정 역할 목록을 요청했습니다. 어떻게해야합니까?

- ○ A. GCloud 명령 행에서 "gcloud iam list-testable-permissions"를 실행하십시오.
- ◉ B. GCloud 명령 행에서 "gcloud iam 역할 목록 --project vpcuser09project"를 실행하십시오. ✓
- ○ C. IAM 콘솔을 열고 사용자 지정 역할을 정렬합니다. 상태 필드에서 필요한 정보를 수집하십시오.
- ○ D. IAM 콘솔을 열고 사용자 지정 역할을 정렬합니다. 권한 필드에서 필요한 정보를 수집하십시오.

피드백

역할 단계가 사용자 정의 그룹과 관련이없고 적합한 관리 권한의 정적 목록을 리턴하므로 A가 올바르지 않습니다.

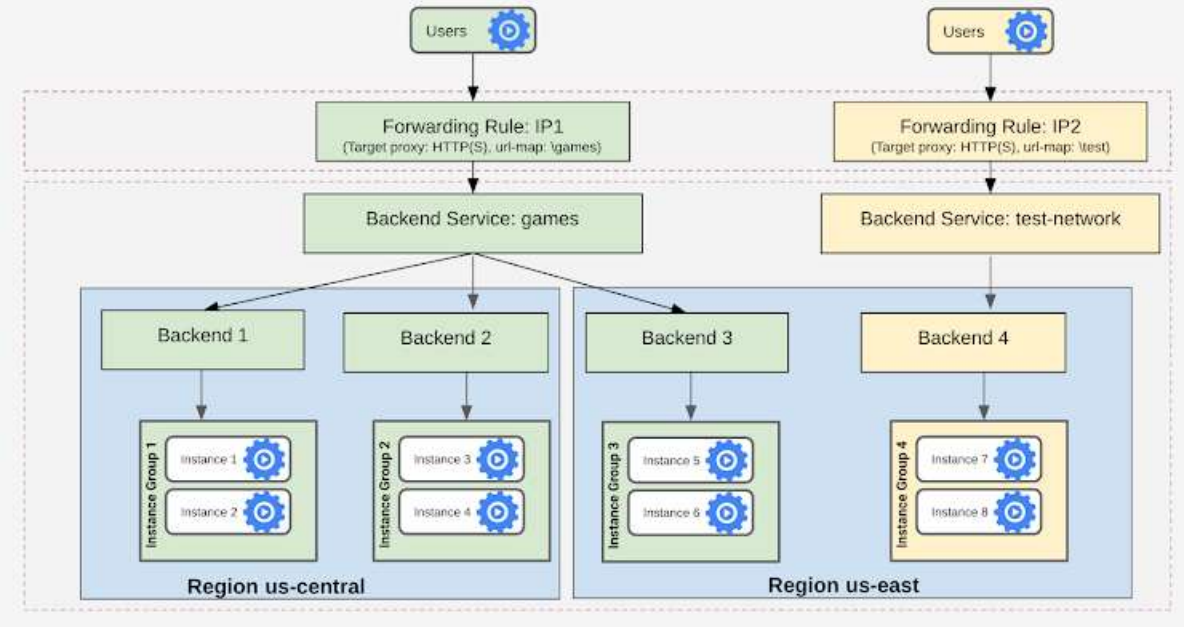
이 명령은 스테이지 필드에 값을 반환하므로 B는 맞습니다.

GUI에 Role Launch Stage가 표시되지 않아 C가 올바르지 않습니다.

GUI에 Role Launch Stage가 표시되지 않아 D가 올바르지 않습니다.

https://cloud.google.com/...

✓ 귀사는 인기있는 게임 서비스를 제공합니다. 서비스 아키텍처는 아래 다이어그램에 나와 있습니다. 인스턴스는 프라이빗 IP 주소로 배포되며 글로벌 액세스 밸런서를 통해 외부 액세스가 허용됩니다. 응용 프로그램 팀은 조직 외부의 사용자를 선택하기 위해 테스트 환경을 공개하려고합니다. 테스트 환경을 기존 배포에 통합하여 관리 오버 헤드를 줄이고 선택한 사용자 만 액세스를 제한하려고 합니다. 어떻게해야합니까?



- A. 새로드 밸런서를 생성하고 테스트 클라이언트를 허용하도록 VPC 방화벽 규칙을 업데이트하십시오.
- B. 새로드 밸런서를 생성하고 VPC 서비스 제어 경계를 업데이트하여 테스트 클라이언트를 허용합니다.
- C. 기존로드 밸런서에 백엔드 서비스를 추가하고 기존 Cloud Armor 정책을 수정하십시오.
- D. 기존로드 밸런서에 백엔드 서비스를 추가하고 새로운 Cloud Armor 정책 및 대상 테스트 네트워크를 추가하십시오. ✓

피드백

HTTPS로드 밸런서가 프록시 역할을하며 올바른 클라이언트 IP 주소를 제공하지 않기 때문에 A가 올바르지 않습니다.

VPC 서비스 컨트롤이 Google 관리 서비스를 보호하기 때문에 B가 올바르지 않습니다.

이 변경으로 모든 사람이 테스트 서비스에 액세스 할 수 있으므로 C는 올바르지 않습니다.

D는 여러 백엔드 서비스를 통합하고 지원하기 때문에 정확합니다.

https://cloud.google.com/...

✓ 회사는 온-프레미스 데이터 센터에서 물리적 보안 어플라이언스를 사용하여 침입을 탐지합니다. 회사는 GCP 환경을 온-프레미스 데이터 센터와 연결하는 VPN을 사용하여 원격 측정 데이터를 수집하려고합니다. GCP 환경을 통합하고 가능한 신속하고 효과적으로 온-프레미스 물리적 보안 어플라이언스로 원격 분석 데이터를 전송하는 솔루션을 구현하려고합니다. 어떻게해야합니까?

- A. GCP의 모든 Compute Engine 인스턴스에서 iptables를 설정하여 연결 세션을 추적하십시오.
- B. GCP로 다시 전달하기 전에 GCP 환경의 모든 트래픽을 검사를 위해 온-프레미스로 라우팅합니다.
- C. Stackdriver 및 GCP 네트워크 로깅 정보를 사용하여 침입 탐지를위한 모니터링 데이터를 수집 및 분석하는 스크립트를 작성하십시오.
- D. 다중 공급 업체 인스턴스가있는 동일한 공급 업체의 GCP Marketplace 가상 보안 어플라이언스를 배포하고 필요에 따라 보안 팀에 인스턴스를 구성 할 수있는 권한을 부여하십시오. ✓

피드백

연결을 추적하기 위해 iptables를 설정하는 것이 침입을 탐지 할 수있는 것과 같지 않기 때문에 A가 올바르지 않습니다.

VPN은 원격 측정 데이터 만 수집하고 VPN을 통해 트래픽을 라우팅하고 검사 목적으로 만 되돌아가는 것이 적합하지 않기 때문에 B가 올바르지 않습니다.

C는 노동 집약적이기 때문에 정확하지 않으며 산업 표준 솔루션을 개발하기에 충분한 보안 경험이 없습니다.

D는 이와 같은 특정 요구 사항을 배포하는 가장 좋고 권장되는 방법이므로 정확합니다.

✓ 두 개의 10Gbps 링크가있는 전용 상호 연결이 있습니다. 두 링크 중 하나가 다운되면이를 알려주는 Stackdriver 경고 정책을 생성하려고합니다. 정책에 어떤 경고를 추가해야합니까?

- (●) A. 두 회로 중 하나에 대한 회로 작동 상태 메트릭 임계 값이 1 미만인 경우에 대한 경고입니다. ✓
- ( ) B. 상호 연결에 대한 상호 연결 작동 상태 메트릭 임계 값이 1 미만인 경우에 대한 경고.
- ( ) C. 상호 연결에 대한 상호 연결 네트워크 용량 메트릭 임계 값이 20 미만인 경우에 대한 경고입니다.
- ( ) D. 상호 연결에 대한 Interconnect Dropped Packets 메트릭 임계 값이 0을 초과하는 경우에 대한 경고.

피드백

회로 작동 상태가 두 회로 모두를 추적하기 때문에 A 가 정확합니다.

Interconnect Operational Status 메트릭은 두 링크가 모두 다운 된 경우에만 경고하므로 B 가 올바르지 않습니다.

Interconnect Network Capacity 메트릭은 가동 / 정지 상태가 아닌 사용률을 추적하므로 C 가 올바르지 않습니다.

Dropped Packets 메트릭은 업 / 다운 상태가 아닌 패킷 손실을 추적하므로 D 가 올바르지 않습니다. 패킷 손실은 용량 감소를 나타낼 수 있지만 다른 이유로 인해 발생할 수도 있습니다.

https://cloud.google.com/...

✓ 외부 주소에서 "webservers"태그가있는 서버에 포트 80 및 443을 통한 액세스를 허용하려고합니다. 현재 모든 포트와 프로토콜의 외부 주소에서 들어오는 모든 트래픽을 거부하는 우선 순위가 1000 인 방화벽 규칙이 있습니다. 기존 규칙을 삭제하지 않고 원하는 트래픽을 허용하려고합니다. 어떻게해야합니까?

- A. 거부 설명 전에 규칙의 외부 주소에서 포트 80 및 443을 통한 트래픽을 허용하는 수신 규칙을 추가하십시오.
- B. 외부 주소에서 포트 80 및 443을 통한 트래픽을 우선 순위 값이 500 인 대상 네트워크 태그 "webservers"로 허용하는 수신 규칙을 추가하십시오. ✓
- C. 거부 설명 전에 규칙의 외부 주소에서 포트 80 및 443을 통한 트래픽을 허용하는 송신 규칙을 추가하십시오.
- D. 외부 주소에서 포트 80 및 443을 통한 트래픽을 우선 순위 값 1500으로 대상 네트워크 태그 "webservers"로 허용하는 송신 규칙을 추가하십시오.

피드백

규칙 순서에 관계없이 허용과 거부가 모두 동일한 우선 순위를 갖는 경우 방화벽이 트래픽을 거부하기 때문에 A가 올바르지 않습니다.

방화벽이 우선 순위 1000보다 낮은 우선 순위를 가진 적절한 허용 수신 규칙으로 트래픽을 전달할 수 있기 때문에 B는 정확합니다.

설명 된 시나리오가 EGRESS 트래픽에 적용되지 않으므로 C는 올바르지 않습니다. 설계 상 방화벽은 상태 저장 상태이며 터널이 있으면 트래픽이 전달됩니다.

설명 된 시나리오가 EGRESS 트래픽에 적용되지 않기 때문에 D가 올바르지 않습니다. 설계 상 방화벽은 상태 저장 상태이며 터널이 있으면 트래픽이 전달되고 우선 순위 값이 기본 값보다 높게 설정되어 규칙이 고려되지 않습니다.

https://cloud.google.com/...

✓ GCP 프로젝트의 보안 웹 응용 프로그램 중 하나는 현재 북미 지역 사용자에게만 서비스를 제공합니다. 모든 애플리케이션 리소스는 현재 단일 GCP 리전에서 호스팅됩니다. 애플리케이션은 Cloud Storage 버킷의 대규모 그래픽 자산 카탈로그를 사용합니다. 이제 애플리케이션이 추가 GCP 리전 또는 Compute Engine 인스턴스를 추가하지 않고도 글로벌 클라이언트에 서비스를 제공해야 한다는 알림을받습니다. 어떻게해야합니까?

- (●) A. Cloud CDN을 구성하십시오. ✓
- ( ) B. TCP 프록시를 구성하십시오.
- ( ) C. 네트워크로드 밸런서를 구성합니다.
- ( ) D. 응용 프로그램을 호스팅하는 서브넷에 대한 동적 라우팅을 구성합니다.

피드백

Cloud CDN이 Cloud Storage 버킷을 향하고 그래픽 리소스를 사용자에게 가장 가까운 위치로 이동하기 때문에 A가 맞습니다.

Cloud CDN에 HTTPS 프록시가 필요하므로 B가 올바르지 않습니다.

Cloud CDN에 HTTPS 프록시가 필요하므로 C가 올바르지 않습니다.

동적 라우팅은 추가 웹 클라이언트를 지원하는 데 도움이되지 않으므로 D가 올바르지 않습니다.

https://cloud.google.com/... https://cloud.google.com/...

✓ Compute Engine 가상 머신 인스턴스간에 요청의 균형을 맞추기 위해 HTTP (S) 로드 밸런서를 구현했습니다. 사용량이 많은 시간 동안 백엔드 인스턴스는 초당 요청 수를 처리 할 수 없으므로 일부 요청이 삭제됩니다. Google 권장 사례에 따라 향후이 시나리오를 피하기 위해 인스턴스를 효율적으로 확장하려고합니다. 어떻게해야합니까?

- A. 관리되지 않는 인스턴스 그룹을 사용하고 인스턴스 머신 유형을 업그레이드하여 고성능 CPU를 사용하십시오.
- B. 관리되지 않는 인스턴스 그룹을 사용하고 사용량이 적은 시간에 필요한 인스턴스 수를 두 배로 늘리십시오.
- C. 관리 형 인스턴스 그룹을 사용하고 인스턴스의 평균 CPU 사용률에 따라 자동 확장을 설정합니다.
- D. 관리 형 인스턴스 그룹을 사용하고 HTTP (S)로드 밸런싱 사용량에 대한 자동 확장을 설정하고 대상로드 밸런싱 사용량을 서빙 비율의 백분율로 설정하십시오. ✓

피드백

명시된 제한이 CPU가 아니기 때문에 A가 올바르지 않으며이 방법은 비효율적입니다.

인스턴스 수를 두 배로 늘리는 것은 비효율적이므로 B가 올바르지 않습니다.

명시된 제한이 CPU가 아닌 초당 요청 수이므로 C가 올바르지 않습니다.

자동 확장 방법은로드 밸런서를 활용하고 인스턴스를 효율적으로 확장하기 때문에 D는 정확합니다.

https://cloud.google.com/...

✕ 애플리케이션 개발 팀이 Dedicated Interconnect를 통해 새로운 애플리케이션을 베타 테스트하고 있습니다. 이 애플리케이션은 단일 TCP 소켓을 사용하며 최적의 성능을 위해 7Gbps 대역폭이 필요합니다. 개발 팀은 애플리케이션의 연결 속도가 Dedicated Interconnect를 통해 3Gbps로 제한되어 있음을 알았습니다. 이 문제를 해결하려고합니다. 어떻게해야합니까?

- (◉) A. 대역폭을 늘리려면 새 인터커넥트를 주문하십시오. ✕
- ( ) B. 인터커넥트 외에 클라우드 VPN과 ECMP 트래픽을 생성합니다.
- ( ) C. 개발 팀에게 응용 프로그램 트래픽을 여러 TCP 흐름 세션에 분산 시키도록 지시합니다.
- ( ) D. 개발 팀에게 응용 프로그램 TCP 혼잡 창, 수신 창 및 기타 모든 tcp 버퍼를 조정하도록 지시하십시오.

정답

- (◉) C. 개발 팀에게 응용 프로그램 트래픽을 여러 TCP 흐름 세션에 분산 시키도록 지시합니다.

피드백

A는 대역폭 제한 문제를 해결하지 못하므로 단일 스레드 흐름에서 추가 상호 연결을 사용할 수 없으므로 A가 올바르지 않습니다.

B가 올바르지 않습니다 (위의 A와 동일).

여러 흐름에 걸쳐 트래픽을 스트라이핑하면 애플리케이션에서 사용하는 대역폭의 양이 증가하므로 C는 정확합니다.

TCP 매개 변수를 조정해도 아무런 차이가 없으므로 D는 정확하지 않습니다. 흐름은 이미 TCP 흐름 당 지원하는 것의 정점에 도달했습니다.

https://cloud.google.com/...