aws re/start

네트워크 보안 및 문제 해결

학습 내용

강의의 핵심

배울 내용은 다음과 같습니다.

- Virtual Private Cloud(VPC) 내부의 계층화된 네트워크 방어 모델 설명하기
- 일반적인 VPC 네트워크 문제를 해결하는 단계 나열하기
- VPC 구성하기

주제:

- 네트워크 보안
- AWS 기반 네트워크 문제 해결

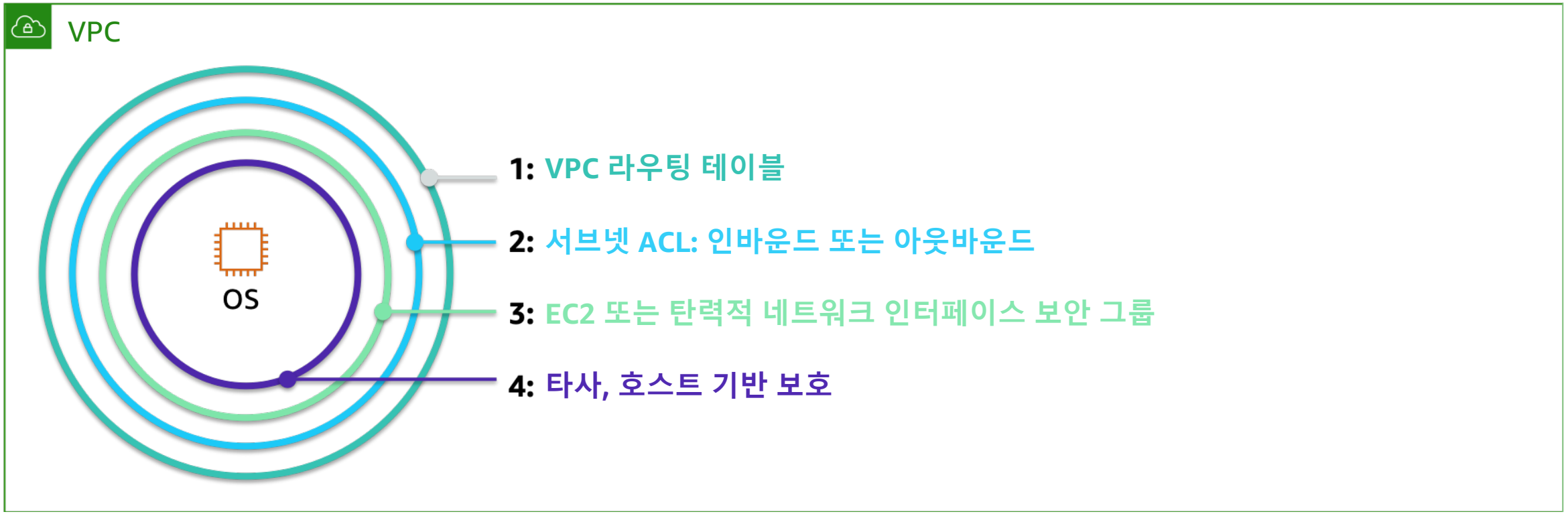
주요 용어

- 네트워크 액세스 제어 목록(네트워크 ACL)
- 보안 그룹
- 배스천 호스트
- Ping 도구

네트워크 보안

계층화된 네트워크

VPC의 계층화된 네트워크 방어



보안 그룹

보안 그룹:

- 탄력적 네트워크 인터페이스 수준에서 트래픽 허용
- 기본적으로 다음과 같이 구성
  - 모든 인바운드 트래픽을 거부
  - 모든 아웃바운드 트래픽 허용
- 스테이트풀 - 규칙에서 트래픽이 한 방향으로 이동하는 것을 허용하면 응답은 자동으로 반대 방향으로 이동할 수 있음
- 일반적으로 애플리케이션 개발자가 관리

아웃바운드 규칙

유형	프로토콜	포트 범위	소스
모든 트래픽	전체	전체	0.0.0.0/0

Mompop 카페 보안 그룹

인바운드 규칙

유형	프로토콜	포트 범위	소스
HTTP	TCP	80	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
MySQL-Aurora	TCP	3306	0.0.0.0/0

네트워크 액세스 제어 목록

네트워크 액세스 제어 목록(네트워크 ACL):

- 서브넷과 주고받는 트래픽 허용 또는 거부
- 기본 네트워크 ACL:
  - 모든 인바운드 및 아웃바운드 트래픽 허용
- 스테이트리스
  - 규칙에서 트래픽이 한 방향으로 흐르도록 허용하는 경우에도, 응답이 반대 방향으로 흐르도록 명시적으로 허용해야 함
- 서브넷 수준에서 2차 방어 계층으로 보안 강화

네트워크 액세스 제어 목록

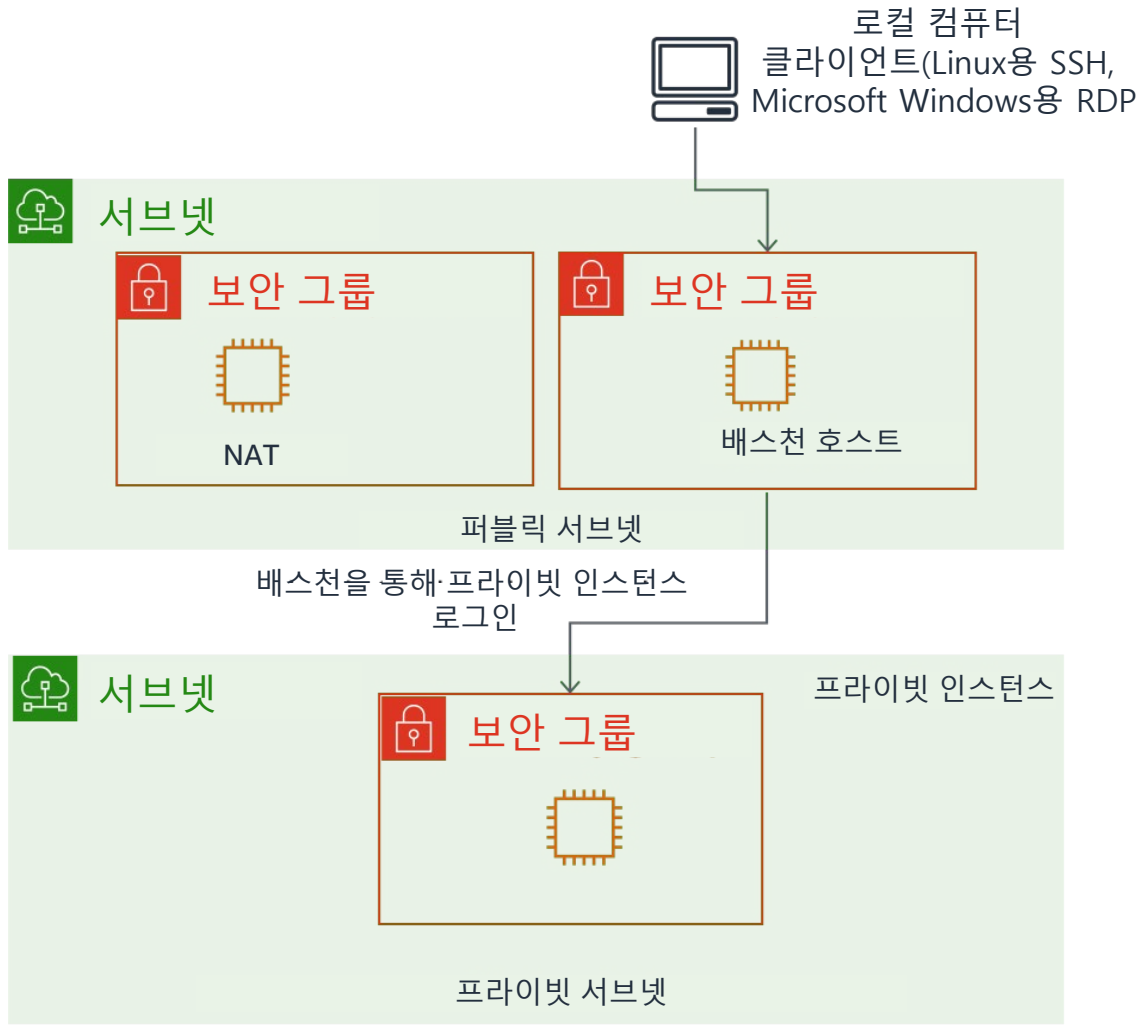
기본 네트워크 ACL의 인바운드 규칙

규칙 #	유형	프로토콜	포트 범위	소스	허용 또는 거부
100	모든 트래픽	전체	80	0.0.0.0/0	허용
*	SSH	TCP	22	0.0.0.0/0	거부

배스천 호스트

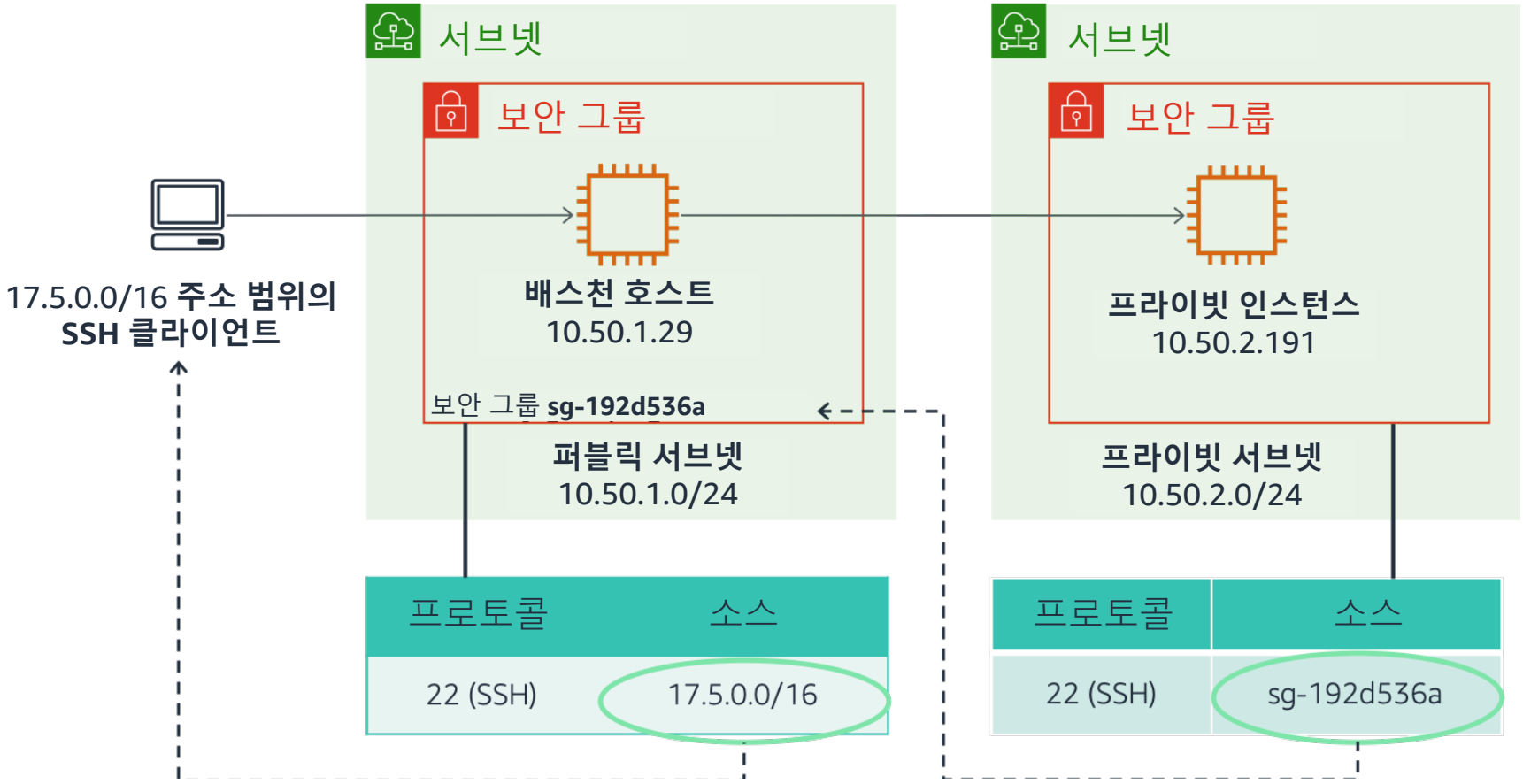
배스천 호스트:

- 퍼블릭 서브넷과 프라이빗 서브넷 간의 액세스를 제공합니다.
  - 프라이빗 서브넷에 액세스하기 위한 점프 지점
- 배스천에 프라이빗 키를 저장하지 마십시오.
  - Linux 인스턴스의 경우 Secure Shell(SSH) 클라이언트의 에이전트 전달 기능을 사용하여 키를 지정합니다.
  - Microsoft Windows 인스턴스의 경우 Amazon Elastic Compute Cloud(Amazon EC2) 콘솔에서 키를 사용하여 암호를 해독한 뒤 도메인으로 인스턴스를 복사합니다.



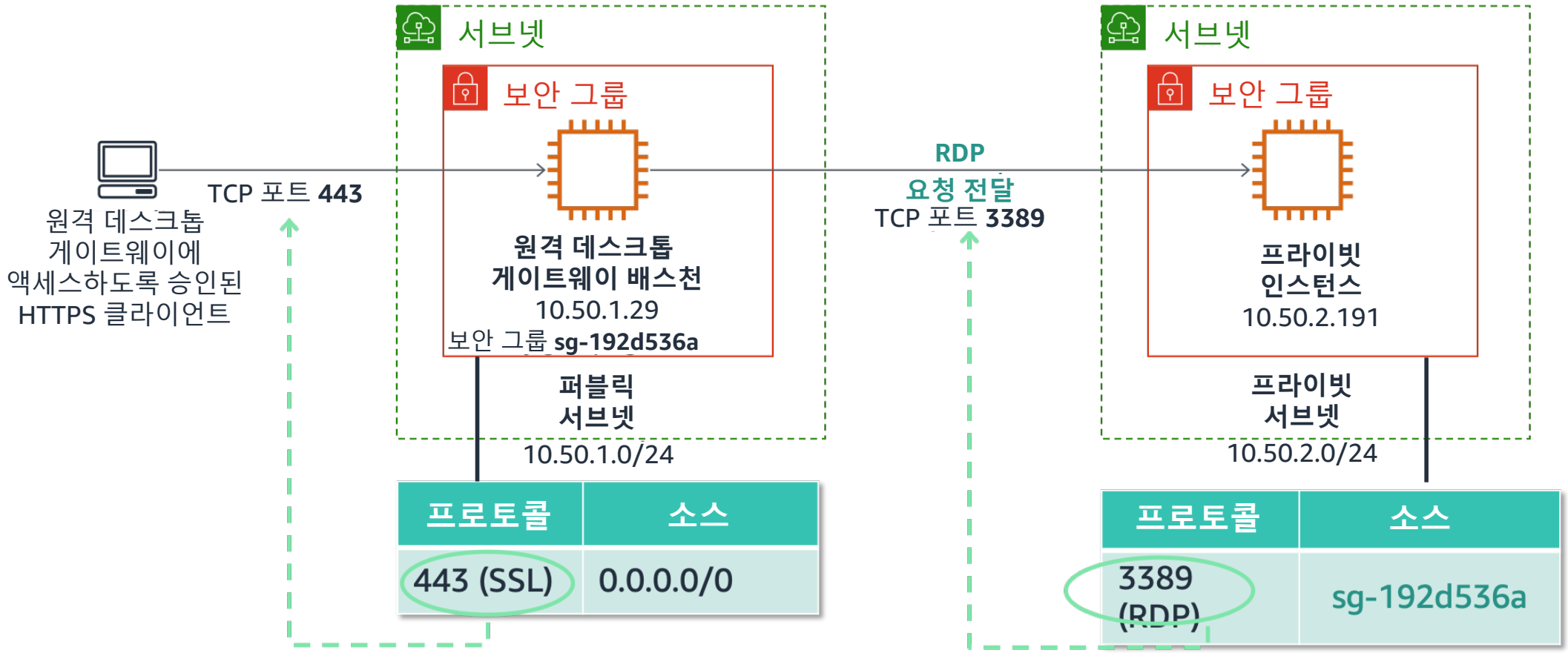
aws re/start

Linux 배스천 호스트 보안 그룹



aws re/start

Windows 배스천 호스트로서의 원격 데스크톱 게이트웨이



aws re/start

AWS 기반 네트워크 문제 해결

일반적인 문제 해결 태스크

1. 해당 인스턴스가 시작 및 실행되고 있는지 확인합니다.
   - **시스템 상태** 및 **인스턴스 상태** 검사를 모두 통과했는지 확인합니다.
2. 인스턴스와 연결된 보안 그룹이 필요한 프로토콜 및 포트에 대한 연결을 허용하는지 확인합니다.
3. 서브넷과 연결된 네트워크 ACL이 필요한 포트 및 프로토콜의 트래픽을 허용하는지 확인합니다.
4. 서브넷과 연결된 라우팅 테이블에 적절한 대상을 가리키는 대상 규칙이 있는지 확인합니다.

인스턴스 용량 문제 해결

일반적인 문제 해결 태스크

- 인스턴스가 실행되고 있는지 확인합니다.
- 보안 그룹 규칙을 확인합니다.
- 네트워크 ACL 규칙을 확인합니다.
- 라우팅 테이블 규칙을 확인합니다.

인터넷을 통해 인스턴스에 연결할 수 없는 경우:

- 사용 중인 공용 IP 주소 또는 도메인 이름 시스템(DNS) 이름이 올바른지 확인합니다.
- 인스턴스에 공인 IP 주소 또는 탄력적 IP 주소가 있는지 확인합니다.
- 인터넷 게이트웨이가 인스턴스의 VPC에 연결되어 있는지 확인합니다.
- 인스턴스 서브넷의 라우팅 테이블에 인터넷 게이트웨이를 통한 대상 0.0.0.0/0에 대한 라우팅 규칙이 있는지 확인합니다.

SSH 연결 문제 해결

일반적인 문제 해결 태스크

- 인스턴스가 실행되고 있는지 확인합니다.
- 보안 그룹 규칙을 확인합니다.
- 네트워크 ACL 규칙을 확인합니다.
- 라우팅 테이블 규칙을 확인합니다.

SSH를 통해 인스턴스에 연결할 수 없는 경우:

- 다음 인스턴스 연결 보안 인증 정보를 확인합니다.
  - 사용자 이름
  - 인스턴스 프라이빗 키

NAT 문제 해결

일반적인 문제 해결 태스크

- 인스턴스가 실행되고 있는지 확인합니다.
- 보안 그룹 규칙을 확인합니다.
- 네트워크 ACL 규칙을 확인합니다.
- 라우팅 테이블 규칙을 확인합니다.

NAT 구성이 작동하지 않는 경우:

NAT 게이트웨이 또는 NAT 인스턴스:

- 라우팅 테이블에 NAT 인스턴스 또는 NAT 게이트웨이에 대한 경로가 있는지 확인합니다.

NAT 인스턴스:

- **원본/대상 확인**이 비활성화되어 있는지 확인합니다.
- NAT 인스턴스를 다시 시작합니다.
- 인바운드 보안 그룹 규칙을 확인합니다.

VPC 피어링 문제 해결

일반적인 문제 해결 태스크

- 인스턴스가 실행되고 있는지 확인합니다.
- 보안 그룹 규칙을 확인합니다.
- 네트워크 ACL 규칙을 확인합니다.
- 라우팅 테이블 규칙을 확인합니다.

피어링된 네트워크에 있는 리소스에 도달할 수 없는 경우:

- 피어링 요청이 승인되었는지 확인합니다.
- **보안 그룹 규칙 확인** – VPC A의 Classless Inter-Domain Routing(CIDR) 차단 범위를 사용하여 VPC B에서 액세스를 허용하거나 VPC A의 보안 그룹 ID를 사용해야 합니다.
- **네트워크 ACL 확인** – 네트워크 ACL이 모든 외부 트래픽을 거부하는지 확인합니다.

핵심 사항

- 계층화된 설계로 네트워크를 보호합니다. 계층 네트워크는 다음을 활용할 수 있습니다.
  - 트래픽 흐름을 제어하기 위한 **라우팅 테이블**
  - 네트워크로 들어오고 나가는 트래픽을 제어하기 위한 **네트워크 액세스 제어 목록**(NACL)
  - 호스트 및 서비스에 대한 트래픽을 제어하는 **보안 그룹**(SG)

- 다음을 사용하여 관리에 대한 액세스를 보호합니다.
  - Linux 기반 호스트에 대한 액세스의 경우 **배스천 호스트**
  - Windows의 경우 **원격 데스크톱(RDP)용 배스천 호스트**

- 문제 해결 시 다음을 수행합니다.
  - 리소스를 사용할 수 있는지 확인합니다.
  - 차단하는 NACL 또는 SG가 있는지 확인합니다.
  - 호스트 또는 서비스에 대한 라우팅이 올바른지 확인합니다.

aws re/start