Azure Virtual WAN에 대한 가상 네트워크 연결 구성

Virtual WAN 개요

Azure 클라우드 서비스를 사용하는 경우 VWAN(Virtual WAN)을 생성하여 온프레미스 네트워크, 브랜치 오피스 및 원격 사용자 간의 네트워크 연결성을 오케스트레이션하고 간소화할 수 있습니다. 서비스 VNet과 가상 허브(vHub) 간에 가상 네트워크 연결 및 경로 전파를 조정함으로써 Azure VWAN과 Multicloud Defense 기능을 통합할 수 있습니다.

일반적으로 vHub 내에서 Multicloud Defense는 NVA(Network Virtual Appliance)로 지원되지 않습니다. 대신 VWAN 경로 오케스트레이션을 사용하여 이 문제를 해결할 수 있습니다. Multicloud Defense를 사용하여 Azure에서 애플리케이션을 보호하려면 서비스 VNet에서 VWAN 내부의 vHub로의 가상 네트워크 연결 생성을 오케스트레이션할 수 있습니다. vHub와 Multicloud Defense 간에 경로를 전파할 수 있습니다. Multicloud Defense는 이그레스 모드에 대해서만 VWAN을 지원합니다. Azure VWAN은 Multicloud Defense 게이트웨이에 대해서만 지원됩니다. Azure는 보안 허브 간의 트래픽 라우팅 문제로 인해 VWAN에 대한 동-서 트래픽을 지원하지 않습니다.

Azure vHub에 대한 Virtual WAN 연결을 위한 지침

사전 요건

- VWAN 및 vHub를 사용하여 Azure 구독을 구성해야 합니다.
- 서비스 VNet 및 스포크 VNet은 Azure에서 설정해야 합니다.
- Multicloud Defense 게이트웨이는 서비스 VNet에 구축해야 합니다.

- Azure에서 가상 네트워크 연결 및 경로 테이블을 생성하고 관리할 수 있는 권한을 사용할 수 있어야 합니다.
- vHub 연결을 활성화 및 비활성화할 수 있는 권한이 있어야 합니다.

제한 사항

- Multicloud Defense는 vHub 내에서 NVA로 지원되지 않습니다.
- CIDR(Classless Inter Domain Routing) 선택은 편집 단계에서만 사용할 수 있으며 VNet 생성 중에는 사용할 수 없습니다.
- 경로 전파는 이그레스 또는 인그레스 게이트웨이의 구성에 따라 달라집니다.

가상 WAN 첨부 파일이 있는 서비스 VPC 생성

어카운트를 보호할 때 쉬운 설정 마법사를 사용하여 VWAN 첨부 파일 있는 서비스 VPC를 생성할 수 있습니다. 자세한 내용은 중앙 집중식 모델: VPC 또는 VNet 추가을 참조하십시오.

다음 절차를 사용하여 서비스 VPC를 생성하고 VWAN을 연결합니다.

프로시저

단계 1 Multicloud Defense 컨트롤러에서 **Infrastructure(**인프라**)** > **Gateways(**게이트웨이**)** > **VPCs/VNets**로 이동합니다.

단계 2 **Create Service VPC/VNet(**서비스 **VPC/VNet** 생성**)**을 클릭하여 서비스 VPC를 생성합니다.

단계 3 **Name(**이름**)**을 입력합니다.

단계 4 **Region(**지역**)** 드롭다운 목록에서 지역을 선택합니다.

단계 5 **CSP Account(CSP** 어카운트**)** 드롭다운 목록에서 어카운트를 선택합니다.

단계 6 **CIDR Block(CIDR** 차단**)**에 대한 세부 정보를 입력합니다.

단계 7 **Availability Zones(**가용성 영역**)** 드롭다운 목록에서 영역을 선택합니다.

단계 8 **Resource Group(**리소스 그룹**)** 드롭다운 목록에서 리소스 그룹을 선택합니다.

단계 9 NAT 게이트웨이를 통해 트래픽을 포워딩하려면 **Use NAT Gateway(NAT** 게이트웨이 사용**)** 체크 박스를 선택합니다.

단계 10 **vWAN Attachment(vWAN** 연결**)** 섹션에서 토글을 **Enabled(**활성화됨**)**로 설정합니다.

단계 11 **vHub** 드롭다운 목록에서 허브를 선택합니다.

단계 12 **Associate Route Table(**경로 테이블 연결**)** 드롭다운 목록에서 경로 테이블을 선택합니다.

단계 13 **Propagate Route Tables(**경로 테이블 전파**)** 드롭다운 목록에서 전파할 경로 테이블을 선택합니다.

단계 14 **Save(**저장**)**를 클릭합니다.

Azure VWAN에 대한 vHub 연결을 사용하여 서비스 VPC가 생성됩니다. Azure 어카운트에서 구성 변경 사항을 볼 수도 있습니다.

참고
Multicloud Defense에서 서비스 VPC를 삭제하면 VWAN과 Azure 서비스 VPC 간의 vHub 연결도 삭제됩니다.

가상 WAN 첨부 파일을 사용하여 서비스 VPC 수정

프로시저

단계 1 Multicloud Defense 컨트롤러에서 **Infrastructure(**인프라**)** > **Gateways(**게이트웨이**)** > **VPCs/VNets**로 이동합니다.
단계 2 목록에서 편집할 서비스 VPC를 선택합니다.
단계 3 **Edit(**편집**)**를 클릭합니다.
단계 4 **vWAN Attachment(vWAN** 연결**)** 섹션에서 토글을 **Enabled(**활성화됨**)**로 설정합니다.
단계 5 **vHub** 드롭다운 목록에서 허브를 선택합니다.
단계 6 **Associated Route Table(**경로 테이블 연결**)** 드롭다운 목록에서 연결할 경로 테이블을 선택합니다.
단계 7 **Propagate Route Tables(**경로 테이블 전파**)** 드롭다운 목록에서 전파할 경로 테이블을 선택합니다.
단계 8 모든 스포크 CIDR을 vHub에 전파하려면 토글을 **Always(**항상**)**로 설정합니다.

참고
여러 스포크 VPC를 경로 테이블에 추가하려면 목록 작성기를 사용하여 스포크 VPC를 **Available(**사용 가능**)** 섹션에서 **Selected(**선택됨**)** 섹션으로 이동합니다. VPC를 **Selected(**선택됨**)** 섹션으로 이동하면 VPC가 추가됩니다.

단계 9 **Save(**저장**)**를 클릭합니다.

서비스 VPC가 Azure의 vHub 및 스포크 VPC를 포함하는 VWAN에 연결됩니다. 경로 테이블에 대한 변경 사항은 Azure에서도 업데이트됩니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.