Secure Firewall Threat Defense Virtual 및 Azure 시작하기

Secure Firewall Threat Defense Virtual(이전 Firepower Threat Defense Virtual)는 Cisco의 Firepower NGFW(Next-Generation Firewall) 기능을 가상화된 환경으로 가져와 일관된 보안 정책으로 물리, 가상 및 클라우드 환경 전반 및 클라우드 간 워크로드를 준수하도록 합니다.

이 장에서는 기능 지원, 시스템 요구 사항, 지침, 제한 사항 등 Azure 마켓플레이스 내에서의 threat defense virtual 기능에 대해 설명합니다. 이 장에서는 threat defense virtual을(를) 관리하기 위한 옵션에 대해서도 설명합니다.

구축을 시작하기 전에 관리 옵션을 이해하는 것이 중요합니다. Secure Firewall Management Center(이전 Firepower Management Center) 또는 Secure Firewall device manager(이전 Firepower Device Manager)를 사용하여 threat defense virtual를 관리하고 모니터링할 수 있습니다. 다른 관리 옵션을 사용할 수도 있습니다.

Threat Defense Virtual 및 Microsoft Azure Cloud

Secure Firewall Threat Defense Virtual는 Microsoft Azure 마켓플레이스에 통합되며 다음 인스턴스 유형을 지원합니다.

- Standard D3—4 vCPUs, 14 GB, 4vNICs

- Standard D3_v2—4 vCPUs, 14 GB, 4vNICs
- Standard D4_v2—8 vCPUs, 28 GB, 8vNICs (버전 **6.5**의 신규 유형)
- Standard D5_v2—16 vCPUs, 56 GB, 8vNICs (버전 **6.5**의 신규 유형)
- Standard_D8s_v3—8 vCPU, 32GB, 4vNIC(버전 7.1의 새로운 기능)
- Standard_D16s_v3—16 vCPU, 64GB, 8vNIC(버전 7.1의 새로운 기능)
- Standard_F8s_v2—8 vCPUs, 16 GB, 4vNICs (버전 **7.1**의 새로운 기능)
- Standard_F16s_v2—16 vCPU, 32GB, 4vNIC(버전 7.1의 새로운 기능)

Threat Defense Virtual 및 Azure의 사전 요건과 일반 요건

사전 요건

- Microsoft Azure 계정. https://azure.microsoft.com/en-us/에서 하나를 생성할 수 있습니다.

  Azure에서 계정을 생성한 후에 로그인하여 마켓플레이스에서 Cisco Firepower Threat Defense를 검색하고 Cisco Firepower NGFW Virtual(NGFWv) 제품을 선택할 수 있습니다.

- Cisco Smart Account는 Cisco Software Central에서 생성할 수 있습니다.

  threat defense virtual의 라이선스, Cisco Firepower System 기능 라이선스에서 유용한 링크를 포함해 방화벽 시스템의 기능 라이선스 개요를 확인할 수 있습니다.

- threat defense virtual 및 시스템 호환성에 대해서는 Threat Defense Virtual 호환성을 참조하십시오.

통신 경로

- 관리 인터페이스—threat defense virtual을 보안 방화벽 관리 센터에 연결하는 데 사용합니다.

Note 6.7 이상 버전에서는 선택적으로 관리 인터페이스 대신 management center 관리용 데이터 인터페이스를 구성할 수 있습니다. 관리 인터페이스는 데이터 인터페이스 관리를 위한 전제 조건이므로 초기 설정에서 구성해야합니다. management center 액세스를 위한 데이터 인터페이스 구성에 대한 자세한 내용은 Secure Firewall Threat Defense 명령 참조에서 **configure network management-data-interface** 명령을 참조하십시오.

- 진단 인터페이스—진단 및 보고에 사용되며 통과 트래픽에는 사용할 수 없습니다.
- 내부 인터페이스(필수)—threat defense virtual를 내부 호스트에 연결하는 데 사용합니다.
- 외부 인터페이스(필수)—threat defense virtual를 공용 네트워크에 연결하는 데 사용합니다.

Threat Defense Virtual 및 Azure에 대한 지침과 제한

지원 기능

- 라우팅된 방화벽 모드만 해당
- Azure Accelerated Networking(AN)
- IPv6
- 관리 모드, 두 가지 중 하나:
  - 보안 방화벽 관리 센터를 사용하여 threat defense virtual를 관리할 수 있습니다. FMC를 사용하여 FTDv 관리를 참조하십시오.
  - 통합 Secure Firewall device manager을 사용하여 threat defense virtual를 관리할 수 있습니다. FDM을 사용하여 FTDv 관리를 참조하십시오.
- 공용 IP 주소 지정 - 공용 IP 주소를 Management 0/0 및 GigabitEthernet0/0에 할당합니다.

  필요에 따라 공용 IP 주소를 다른 인터페이스에 할당 할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses를 참조하십시오.
- 인터페이스:
  - threat defense virtual 기본적으로 4개의 vNIC로 구축합니다.
  - 더 큰 인스턴스 지원을 통해 최대 8개의 vNIC로 threat defense virtual를 구축할 수 있습니다.
  - 추가 vNIC를 threat defense virtual 구축에 추가하려면 Microsoft의 Add network interfaces to or remove network interfaces from virtual machines에서 제공하는 지침을 따르십시오.
  - 관리자를 사용하여 threat defense virtual 인터페이스를 구성합니다. 인터페이스 지원 및 구성에 대한 자세한 내용은 관리 플랫폼, 즉 management center 또는 device manager에 대한 구성 지침서를 참조하십시오.

라이선싱

- Cisco Smart License 계정을 사용하는 BYOL(Bring Your Own License)
- PAYG(Pay As You Go) 라이선싱 - Cisco Smart Licensing을 구매하지 않고도 고객이 threat defense virtual을 실행할 수 있는 사용 기반 청구 모델입니다. 모든 라이선스 기능(악성 코드 / 위협 / URL 필터링 / VPN 등)은 등록된 PAYG threat defense virtual 디바이스에 대해 활성화됩니다. 라이선스가 있는 기능은 management center에서 수정하거나 변경할 수 없습니다. (버전 6.5 이상)

Note PAYG 라이선싱은 device manager 모드로 구축된 threat defense virtual 디바이스에서 지원되지 않습니다.

threat defense virtual 디바이스 라이선싱에 대한 지침은 보안 방화벽 관리 센터 관리 가이드의 "라이선싱" 장을 참조하십시오.

Threat Defense Virtual 스마트 라이선싱의 성능 계층

threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.

Table 1: 자격 기준 ***Threat Defense Virtual*** 라이선스 기능 제한

성능 계층	디바이스 사양 **(Core/RAM)**	속도 제한	**RA VPN** 세션 제한
FTDv5, 100Mbps	4 코어/8GB	100Mbps	50
FTDv10, 1Gbps	4 코어/8GB	1Gbps	250
FTDv20, 3Gbps	4 코어/8GB	3Gbps	250
FTDv30, 5Gbps	8 코어/16GB	5Gbps	250
FTDv50, 10Gbps	12 코어/24GB	10Gbps	750
FTDv100, 16Gbps	16 코어 / 34GB	16Gbps	10,000

성능 최적화

threat defense virtual에서 최상의 성능을 얻으려면 VM과 호스트를 모두 조정할 수 있습니다. 자세한 내용은 Azure에서의 가상화 조정 및 최적화를 참조하십시오.

Receive Side Scaling — threat defense virtual는 RSS(Receive Side Scaling)를 지원합니다. RSS는 네트워크 수신 트래픽을 여러 프로세서 코어로 분산하기 위해 네트워크 어댑터에서 활용하는 기술입니다. 버전 7.0 이상에서 지원됩니다. 자세한 내용은 RSS(Receive Side Scaling)를 위한 다중 RX 대기열을 참조하십시오.

지원되지 않는 기능

- 라이선싱:
  - PLR(영구 라이선스 예약)
  - PAYG(Pay As You Go)(버전 6.4 이하)
- 네트워킹(이러한 제한의 많은 수는 Microsoft Azure 제한임):

- 점보 프레임
- 802.1Q VLAN
- 투명 모드 및 기타 레이어 2 기능, 브로드 캐스트도 없고 멀티 캐스트도 없습니다.
- Azure의 관점에서는 디바이스 소유가 아닌 IP 주소에 대한 프록시 ARP(일부 NAT 기능에 영향을 미침)
- 프로미스큐어스 모드(서브넷 트래픽 캡처 없음)
- 인라인 설정 모드, 패시브 모드

Note Azure 정책에서는 threat defense virtual가 투명 방화벽 모드에서 작동할 수 없습니다. 이 모드에서는 인터페이스가 프로미스큐어스 모드에서 작동할 수 없기 때문입니다.

- ERSPAN(Azure에서 전달되지 않는 GRE 사용)

- 관리:
  - 콘솔 액세스; 관리는 management center를 사용하여 네트워크를 통해 수행됩니다(일부 설정 및 유지 보수 활동에 SSH 사용 가능).
  - Azure Portal "비밀번호 재설정" 기능
  - 콘솔 기반 비밀번호 복구: 사용자는 콘솔에 실시간으로 액세스할 수 없으므로 비밀번호를 복구할 수 없습니다. 비밀번호 복구 이미지는 부팅할 수 없습니다. 유일한 방법은 새 threat defense virtual VM을 구축하는 것입니다.
- 고가용성(활성-대기)
- 클러스터링
- VM 가져오기/내보내기
- Device Manager 사용자 인터페이스(버전 6.4 이하)

Azure DDoS 보호 기능

Microsoft Azure의 Azure DDoS Protection은 threat defense virtual의 최전선에서 구현되는 추가 기능입니다. 가상 네트워크에서 이 기능을 활성화하면 네트워크 예상 트래픽의 초당 패킷 수에 따라 일반적인 네트워크 레이어 공격으로부터 애플리케이션을 방어할 수 있습니다. 네트워크 트래픽 패턴에 따라 이 기능을 맞춤화할 수 있습니다.

Azure DDoS Protection 기능에 대한 자세한 내용은 Azure DDoS Protection 표준 개요를 참고하십시오.

Snort

- Snort를 종료하는 데 시간이 오래 걸리거나, VM이 일반적으로 느려지거나, 특정 프로세스가 실행되는 등의 비정상적인 동작이 관찰되는 경우 threat defense virtual 및 VM 호스트에서 로그를 수집합니다. 전체 CPU 사용량, 메모리, I/O 사용량 및 읽기/쓰기 속도 로그를 수집하면 문제를 해결하는 데 도움이 됩니다.
- Snort가 종료될 때 높은 CPU 및 I/O 사용량이 관찰됩니다. 메모리가 충분하지 않고 전용 CPU가 없는 단일 호스트에서 여러 threat defense virtual 인스턴스가 생성된 경우 Snort가 종료되는 데 시간이 오래 걸리므로 Snort 코어가 생성됩니다.

Secure Firewall Threat Defense Virtual 디바이스 관리 방법

두 가지 옵션을 통해 Secure Firewall Threat Defense Virtual 디바이스를 관리할 수 있습니다.

보안 방화벽 관리 센터

다수의 디바이스를 관리하거나 threat defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 device manager 대신 management center를 사용하여 디바이스를 구성하십시오.

중요 device manager와 management center를 모두 사용하여 threat defense 디바이스를 관리할 수는 없습니다. device manager 통합 관리가 활성화되면 로컬 관리를 사용하지 않도록 설정하고 management center를 사용하도록 재구성하기 전에는 management center를 사용해 threat defense 디바이스를 관리할 수 없습니다. 반면 management center에 threat defense 디바이스를 등록하면 device manager 온보드 관리 서비스가 비활성화됩니다.

주의 현재 Cisco에서는 device manager 구성을 management center로, 또는 그 반대로 마이그레이션 할 수 있는 옵션이 없습니다. threat defense 디바이스를 구성할 때는 이를 고려해 관리 유형을 선택해야 합니다.

Secure Firewall device manager

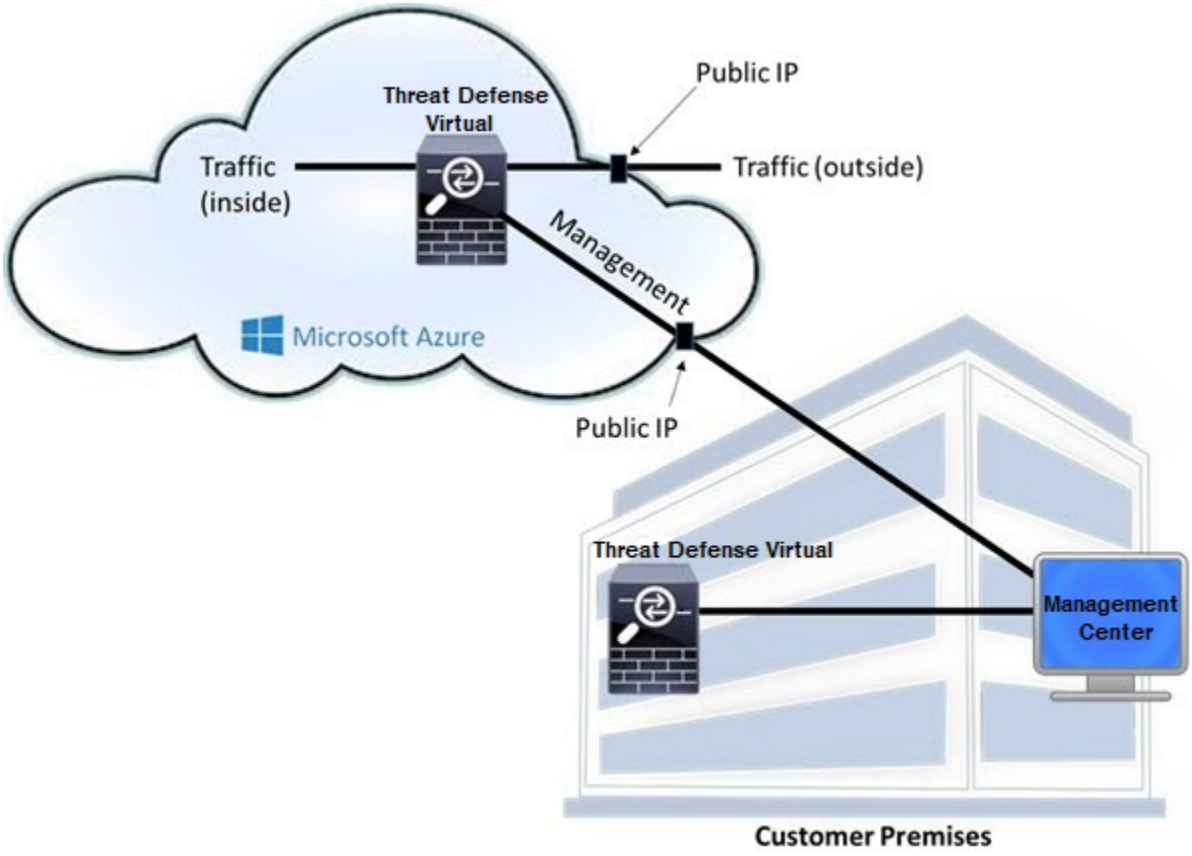
device manager은 온보드 통합 관리자입니다.

device manager는 일부 threat defense 디바이스에 포함된 웹 기반 구성 인터페이스입니다. device manager 사용을 통해 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성할 수 있습니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 threat defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

참고 device manager을 지원하는 threat defense 디바이스 목록은 Cisco Secure Firewall Device Manager 구성 가이드을 참조하십시오.

Azure에서 Threat Defense Virtual를 위한 네트워크 토폴로지 샘플

다음 그림에는 Azure 내 라우팅 방화벽 모드의 threat defense virtual에 대한 일반적인 토폴로지가 나와 있습니다. 첫 번째로 정의된 인터페이스는 항상 관리 인터페이스이며 Management 0/0 및 GigabitEthernet0 / 0에만 공용 IP 주소가 할당됩니다.



구축 중에 생성된 리소스

Azure에서 Secure Firewall Threat Defense Virtual를 구축할 때 다음 리소스가 생성됩니다.

- threat defense virtual 머신(VM)

- 리소스 그룹
  - threat defense virtual는 항상 새 리소스 그룹에 구축됩니다. 그러나 다른 리소스 그룹의 기존 가상 네트워크에 연결할 수 있습니다.

- 4개의 NIC - *vm name*-Nic0, *vm name*-Nic1, *vm name*-Nic2, *vm name*-Nic3

Note 요구 사항에 따라 IPv4 전용 또는 듀얼 스택 (IPv4 및 IPv6 활성화)을 사용하여 VNet을 생성할 수 있습니다.

이러한 NIC는 threat defense virtual interfaces Management, 진단 0/0, GigabitEthernet 0/0 및 GigabitEthernet 0/1에 각각 매핑됩니다.

- *vm name* -mgmt-SecurityGroup으로 명명된 보안 그룹

  보안 그룹이 VM의 Nic0에 매핑되며 이는 threat defense virtual 관리 인터페이스에 매핑됩니다.

  보안 그룹에는 SSH (TCP 포트 22) 및 management center인터페이스 (TCP 포트 8305)의 관리 트래픽을 허용하는 규칙이 포함되어 있습니다. 구축 후에 이 값을 수정할 수 있습니다.

- 공용 IP 주소(구축 중에 선택한 값에 따라 이름이 지정됩니다)

  공용 IP 주소를 다른 인터페이스에 할당할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses를 참조하십시오.

- New Network(새 네트워크) 옵션을 선택하면 서브넷이 4개인 가상 네트워크가 생성됩니다.
- 각 서브넷에 대한 라우팅 테이블(이미 있을 경우 업데이트됨)

  이 테이블의 이름은 "*subnet name* "-FTDv-RouteTable입니다.

  각 라우팅 테이블에는 다른 3개 서브넷에 대한 경로가 포함되며 threat defense virtual IP 주소가 다음 홉입니다. 트래픽이 다른 서브넷 또는 인터넷에 도달해야 하는 경우 기본 경로 추가를 선택할 수 있습니다.

- 선택된 스토리지 계정의 부팅 진단 파일

  부팅 진단 파일은 Blob(binary large object)에 포함됩니다.

- Blob과 컨테이너 VHD인 *vm name*-disk.vhd 및 *vm name*-<uuid>.status에 속한 선택된 스토리지 계정의 파일 2개
- 스토리지 계정(기존 스토리지 계정을 선택하지 않은 경우)

Note VM을 삭제할 경우 이 리소스에서 유지할 것을 제외하고 각각을 개별적으로 삭제해야 합니다.

Accelerated Networking(AN)

Azure의 AN(Accelerated Networking) 기능은 VM에 대한 SR-IOV(Single Root I / O Virtualization)를 활성화합니다. 그러면 VM NIC가 하이퍼바이저를 우회하여 PCIe 카드로 바로 이동할 수 있습니다. AN은 VM의 처리량 성능을 크게 향상시키며 추가 코어(예: 더 큰 VM)로 확장됩니다.

기본적으로 비활성화되어 있습니다. Azure는 사전 프로비저닝된 가상 머신에서 AN 활성화를 지원합니다. Azure에서 VM을 중지하고 네트워크 카드 속성을 업데이트하여 *enableAcceleratedNetworking* 매개 변수를 true로 설정하기만 하면 됩니다. Microsoft 문서 Enable accelerated networking on existing VMs를 참조하십시오. 그런 다음 VM을 다시 시작합니다.

Azure 라우팅

Azure 가상 네트워크 서브넷의 라우팅은 해당 서브넷의 유효 라우팅 테이블에 따라 결정됩니다. 유효 라우팅 테이블은 기존 시스템 라우팅 테이블과 사용자 정의 라우팅 테이블의 조합입니다.

Note VM NIC 속성 아래에서 유효 라우팅 테이블을 볼 수 있습니다.

사용자 정의 라우팅 테이블은 보고 수정할 수 있습니다. 시스템 테이블과 사용자 정의 테이블의 조합으로 유효 라우팅 테이블이 구성될 경우 가장 구체적인 경로가 선택되며 동등할 때는 사용자 정의 라우팅 테이블이 적용됩니다. 시스템 라우팅 테이블은 Azure의 가상 네트워크 인터넷 게이트웨이를 가리키는 기본 경로(0.0.0.0/0) IPv4 또는 [::/0] IPv6를 포함합니다. 시스템 라우팅 테이블은 나머지 정의된 서브넷에 대한 경로도 포함하는데, 다음 홉은 Azure의 가상 네트워크 인프라 게이트웨이를 가리킵니다.

Azure 라우팅 threat defense virtual을 통해 트래픽을 라우팅하려면 각 데이터 서브넷과 연결된 사용자 정의 라우팅 테이블에서 경로를 추가/업데이트해야 합니다. 관심 트래픽은 해당 서브넷의 threat defense virtual IP 주소를 다음 홉으로 사용하여 라우팅해야 합니다. 또한 필요한 경우 threat defense virtual IP의 다음 홉과 함께 0.0.0.0/0 IPv4 또는 [::/0] IPv6의 기본 경로를 추가할 수 있습니다.

시스템 라우팅 테이블의 기존 경로 때문에 threat defense virtual를 다음 홉으로 가리키는 경로를 사용자 정의 라우팅 테이블에 추가해야 합니다. 그렇지 않으면 사용자 정의 테이블의 기본 경로가 시스템 라우팅 테이블의 더 구체적인 경로에 밀려 트래픽이 threat defense virtual를 우회하게 됩니다.

가상 네트워크의 VM을 위한 라우팅 컨피그레이션

Azure 가상 네트워크의 라우팅은 클라이언트의 특정 게이트웨이 설정이 아니라 유효 라우팅 테이블에 따라 달라집니다. 가상 네트워크에서 실행 중인 클라이언트는 DHCP에서 경로를 지정할 수도 있습니다. 이는 해당 서브넷의 1번 주소입니다. 이는 자리 표시자이며 가상 네트워크의 인프라 가상 게이트웨이에 패킷을 보내는 기능만 할 뿐입니다. 패킷이 VM을 떠나면 유효 라우팅 테이블에 따라 (사용자 정의 테이블에서 수정한 대로) 라우팅됩니다. 클라이언트가 .1 또는 threat defense virtual 주소로 구성된 경우에도 유효 라우팅 테이블에 따라 다음 홉이 결정됩니다.

Azure VM ARP 테이블에서는 모든 확인된 호스트에 대해 동일한 MAC 주소(1234.5678.9abc)를 표시합니다. 그러면 Azure VM을 떠나는 모든 패킷이 Azure 게이트웨이에 도달하며, 여기서 유효 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

IP 주소

다음 정보가 Azure의 IP 네트워크에 적용됩니다.

- threat defense virtual의 첫 NIC(Management에 매핑됨)는 연결된 서브넷에서 전용 IP 주소를 받습니다.

  공용 IP 주소를 이 전용 IP 주소와 연결할 수 있으며 Azure Internet 게이트웨이에서 NAT 변환을 처리합니다.

  threat defense virtual이 구축된 후 공용 IP 주소를 데이터 인터페이스(예: GigabitEthernet0/0)와 연결할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 공용 IP와 관련된 Azure 지침은 Public IP addresses를 참조하십시오.

- 공용 IP 주소(IPv4 및 IPv6)는 동적이며 Azure 중지/시작 사이클 중 변경될 수 있습니다. 그러나 Azure가 재시작하고 threat defense virtual가 다시 로드될 때는 유지됩니다. IPv6 공용 IP 주소 표준을 참조하십시오.

- 고정 상태의 공용 IP 주소는 Azure에서 변경하지 않는 한 바뀌지 않습니다.

- Threat Defense Virtual 인터페이스에서 IP 주소 설정에 DHCP를 사용할 수 있습니다. Azure 인프라는 Azure에서 설정된 IP 주소가 threat defense virtual 인터페이스에 지정되게 합니다.