Microsoft Azure 클라우드에 ASA 가상 구축

Microsoft Azure 클라우드에 ASA 가상를 구축할 수 있습니다.

중요 9.13(1)부터 모든 ASA 가상 라이선스는 지원되는 모든 ASA 가상 vCPU/메모리 구성에서 사용할 수 있습니다. 따라서 ASA 가상 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다. 또한 지원되는 Azure 인스턴스 유형의 수가 증가합니다.

- Microsoft Azure 클라우드에 ASA 가상 구축, 1 페이지
- ASA 가상 및 Azure의 사전 요건과 시스템 요구 사항, 2 페이지
- 지침 및 제한 사항, 3 페이지
- 구축 중에 생성된 리소스, 5 페이지
- Azure 라우팅, 7 페이지
- 가상 네트워크의 VM을 위한 라우팅 컨피그레이션, 7 페이지
- IP 주소, 8 페이지
- DNS, 8 페이지
- Accelerated Networking(AN), 8 페이지
- Microsoft Azure에 ASA 가상 구축, 9 페이지
- 부록 - Azure 리소스 템플릿 예, 18 페이지

Microsoft Azure 클라우드에 ASA 가상 구축

ASA 가상 필요에 맞는 Azure 가상 머신 유형 및 크기를 선택합니다. 모든 ASA 가상 라이선스는 지원되는 ASA 가상 vCPU/메모리 설정에서 사용할 수 있습니다. 이렇게 하면 다양한 Azure 인스턴스 유형에서 ASA 가상을 실행할 수 있습니다.

표 ***1: Azure*** 지원 인스턴스 유형

Instance	특성		인터페이스
	vCPUs	메모리**(GB)**	
D3, D3_v2, DS3, DS3_v2	4	14	4

Instance	특성		인터페이스
	vCPUs	메모리(GB)	
D4, D4_v2, DS4, DS4_v2	8	28	8
D5, D5_v2, DS5, DS5_v2	16	56	8
D8_v3	8	32	4
D16_v3	16	64	4
D8s_v3	8	32	4
D16s_v3	16	64	8
F4, F4s	4	8	4
F8, F8s	8	16	8
F16, F16s	16	32	8
F8s_v2	8	16	4
F16s_v2	16	32	8

Microsoft Azure에 ASA 가상을 구축할 수 있습니다.

- 표준 Azure 퍼블릭 클라우드 및 Azure Government 환경에서 Azure Resource Manager를 사용하여 독립형 방화벽으로 구축합니다.
- Azure Security Center를 사용하여 통합된 파트너 솔루션으로 구축합니다.
- 표준 Azure 퍼블릭 클라우드 환경과 Azure Government 환경에서 Azure Resource Manager를 사용하여 HA(고가용성) 쌍으로 구축합니다.

Azure Resource Manager에서 ASA 가상 구축, 10 페이지의 내용을 참조하십시오. 표준 Azure 퍼블릭 클라우드 및 Azure Government 환경에서 ASA 가상 HA 구성을 구축할 수 있습니다.

ASA 가상 및 Azure의 사전 요건과 시스템 요구 사항

- Azure.com에서 계정을 생성합니다.

  Microsoft Azure에서 계정을 생성한 다음, 로그인하고 Microsoft Azure Marketplace에서 ASA 가상을 선택하여 ASA 가상을 구축합니다.

- ASA 가상에 라이선스를 부여합니다.

  ASA 가상 라이선스를 등록하기 전에는 저성능 모드에서 실행됩니다. 이 모드에서는 100개의 연결 및 100Kbps의 처리량만 허용됩니다. ASA 가상을 위한 Smart Software Licensing을 참조하십시오.

참고 Azure에서 구축될 때 ASA 가상 기본값은 2Gbps 엔타이틀먼트가 됩니다. 100Mbps 및 1Gbps 엔타이틀먼트를 사용할 수 있습니다. 그러나 처리량 수준은 100Mbps 또는 1Gbps 엔타이틀먼트를 사용하도록 명시적으로 구성되어야 합니다.

- 인터페이스 요구 사항:

  4개의 네트워크에서 4개의 인터페이스로 ASA 가상을 구축해야 합니다. 공용 IP 주소를 다른 인터페이스에 할당할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses(퍼블릭 IP 주소)를 참조하십시오.

- 관리 인터페이스:

  Azure에서는 처음 정의되는 인터페이스가 언제나 을 포함하지 않습니다.

- 통신 경로:
  - 관리 인터페이스—SSH 액세스에 그리고 ASDM에 ASA 가상을 연결하는 데 사용합니다.

참고 Azure 가속 네트워킹은 관리 인터페이스에서 지원되지 않습니다.

  - 내부 인터페이스(필수)—ASA 가상를 내부 호스트에 연결하는 데 사용합니다.
  - 외부 인터페이스(필수)—ASA 가상를 공용 네트워크에 연결하는 데 사용합니다.
  - DMZ 인터페이스(선택 사항)—Standard_D3 인터페이스 사용 시 ASA 가상을 DMZ 네트워크에 연결하는 데 사용합니다.

- ASA 가상 하이퍼바이저 및 가상 플랫폼 지원 관련 정보는 Cisco Secure Firewall ASA 호환성을 참조하십시오.

지침 및 제한 사항

지원 기능

- Microsoft Azure 클라우드에서 구축
- Azure Accelerated Networking(AN)
- 선택한 인스턴스 유형에 따라 최대 16개의 vCPU

참고 Azure는 구성 가능한 L2 vSwitch 기능을 제공하지 않습니다.

- 임의의 인터페이스상의 공용 IP 주소

  공용 IP 주소를 다른 인터페이스에 할당할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses(퍼블릭 IP 주소)를 참조하십시오.

- 라우팅 방화벽 모드(기본)

참고 라우팅 방화벽 모드의 ASA 가상는 네트워크의 일반 레이어 3 경계입니다. 이 모드에서는 각 인터페이스에 IP 주소가 필요합니다. Azure에서는 VLAN 태깅 인터페이스를 지원하지 않으므로 태그가 지정되지 않은 비 트렁크 인터페이스에서 IP 주소를 구성해야 합니다.

- IPv6

알려진 문제

유휴 시간 제한

Azure의 ASA 가상에는 VM에서 구성 가능한 유휴 시간 제한이 있습니다. 최소 설정은 4분이고 최대 설정은 30분입니다. 그러나 SSH 세션의 경우 최소 설정은 5분이고 최대 설정은 60분입니다.

참고 ASA 가상의 유휴 시간 제한은 항상 SSH 시간 제한을 재정의하며 세션 연결을 끊는다는 사실에 유의하십시오. 세션이 어느 쪽에서도 시간 초과되지 않도록 VM의 유휴 시간 제한을 SSH 시간 초과와 일치시킬 수도 있습니다.

기본 **ASA** 가상에서 스탠바이 **ASA** 가상로의 장애 조치

Azure 구축의 ASA 가상 HA에서 Azure 업그레이드가 발생하면, 기본 ASA 가상에서 스탠바이 ASA 가상로의 페일오버가 발생할 수 있습니다. Azure를 업그레이드하면 기본 ASA 가상이 일시 중지 상태가 됩니다. 기본 ASA 가상이 일시 중지되면 스탠바이 ASA 가상은 hello 패킷을 수신하지 않습니다. 스탠바이 ASA 가상이 장애 조치 보류 시간이 끝날 때까지 hello 패킷을 받지 못하면, 스탠바이 ASA 가상에 대한 페일오버가 발생합니다.

장애 조치 보류 시간이 초과되지 않았지만 페일오버가 발생할 수도 있습니다. 기본 ASA 가상이 일시 중지 상태로 들어간 후 19초 후에 다시 시작되는 상황을 고려해보십시오. 페일오버 보류 시간은 30초입니다. 그러나 스탠바이 ASA 가상은 시계가 2분마다 동기화되므로 올바른 타임스탬프가 포함된 hello 패킷을 수신하지 못합니다. 따라서 기본 ASA 가상에서 스탠바이 ASA 가상로의 페일오버가 발생합니다.

참고 이 기능은 IPv4만 지원하며, IPv6 구성에서는 ASA Virtual HA가 지원되지 않습니다.

지원되지 않는 기능

- 콘솔 액세스(네트워크 인터페이스를 통해 SSH 또는 ASDM을 사용하여 관리 수행)
- 사용자 인스턴스 인터페이스의 VLAN 태깅
- 점보 프레임
- Azure의 관점에서는 디바이스 소유가 아닌 IP 주소에 대한 프록시 ARP
- 프로미스큐어스 모드(스니핑 또는 투명 모드 방화벽 지원 없음)

참고 Azure 정책에서는 ASA 가상이 투명 방화벽 모드에서 작동할 수 없습니다. 이 모드에서는 인터페이스가 프로미스큐어스 모드에서 작동할 수 없기 때문입니다.

- 멀티컨텍스트 모드
- 클러스터링
- ASA 가상 기본 HA
- VM 가져오기/내보내기
- 기본적으로 FIPS 모드는 Azure 클라우드에서 실행 중인 ASA 가상에 대해 활성화되지 않습니다.

참고 FIPS 모드를 활성화할 경우 **ssh key-exchange group dh-group14-sha1** 명령을 사용하여 Diffie-Helman 키 교환 그룹을 더 강력한 키로 변경해야 합니다. Diffie-Helman 그룹을 변경하지 않으면 ASA 가상에 대한 SSH를 사용할 수 없습니다. 이는 초기에 ASA 가상를 관리할 수 있는 유일한 방법입니다.

- IPv6

Azure DDoS 보호 기능

Microsoft Azure의 Azure DDoS Protection은 ASA 가상의 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.

구축 중에 생성된 리소스

Azure에서 ASA 가상를 구축할 때 다음 리소스가 생성됩니다.

- ASA 가상 머신
- 리소스 그룹(기존 리소스 그룹을 선택하지 않는 한)

  ASA 가상 리소스 그룹은 가상 네트워크 및 스토리지 계정에서 사용하는 것과 동일한 리소스 그룹이어야 합니다.
- 4개의 NIC - vm name-Nic0, vm name-Nic1, vm name-Nic2, vm name-Nic3

  이 NIC는 ASA 가상의 인터페이스인 Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2에 각각 매핑됩니다.

참고 요구 사항에 따라 IPv4 전용 을 사용하여 Vnet을 생성할 수 있습니다.

- vm name-SSH-SecurityGroup이라는 보안 그룹

  보안 그룹이 VM의 Nic0에 매핑되며, 이는 ASA 가상 Management 0/0에 매핑됩니다.

  보안 그룹은 VPN 목적으로 SSH 및 UDP 포트 500, UDP 4500을 허용하는 규칙을 포함합니다. 구축 후에 이 값을 수정할 수 있습니다.
- 공용 IP 주소(구축 중에 선택한 값에 따라 이름이 지정됨)

  공용 IP 주소(IPv4 전용)를 모든 인터페이스에 할당할 수 있습니다.

  공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses(퍼블릭 IP 주소)를 참조하십시오.
- 4개의 서브넷이 있는 가상 네트워크(기존 네트워크를 선택하지 않은 경우)
- 각 서브넷에 대한 라우팅 테이블(이미 있을 경우 업데이트됨)

  이 테이블의 이름은 subnet name-ASAv-RouteTable입니다.

  각 라우팅 테이블에는 다른 3개 서브넷에 대한 경로가 포함되며 ASA 가상 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)

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

Azure 라우팅

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

참고 ASA 가상은 Azure 클라우드 라우팅 특성 때문에 EIGRP나 OSPF 같은 동적 내부 라우팅 프로토콜을 사용할 수 없습니다. 가상 클라이언트에 정적/동적 경로가 구성되었는지에 상관없이, 유효 라우팅 테이블이 따라 다음 홉이 결정됩니다.

현재는 유효 라우팅 테이블과 시스템 라우팅 테이블 중 어느 쪽도 볼 수 없습니다.

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)를 포함합니다. 시스템 라우팅 테이블은 나머지 정의된 서브넷에 대한 경로도 포함하는데, 다음 홉은 Azure의 가상 네트워크 인프라 게이트웨이를 가리킵니다.

ASA 가상 구축 프로세스에서는 ASA 가상을 통과하도록 트래픽을 라우팅하기 위해 각 서브넷에 대한 경로를 다음 홉으로 ASA 가상을 사용 중인 나머지 세 서브넷에 추가합니다. 서브넷의 ASA 가상 인터페이스를 가리키는 기본 경로(0.0.0.0/0)를 추가하려는 경우도 있습니다. 그러면 서브넷의 모든 트래픽이 ASA 가상을 통과합니다. 따라서 이 트래픽 처리를 위해 (아마도 NAT/PAT를 사용하여) 미리 ASA 가상 정책이 구성되어야 할 수도 있습니다.

시스템 라우팅 테이블의 기존 경로 때문에 ASA 가상를 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 ASA 가상를 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 ASA 가상 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.

참고 ASA 가상은 Azure 클라우드 라우팅 특성 때문에 EIGRP나 OSPF 같은 동적 내부 라우팅 프로토콜을 사용할 수 없습니다. 가상 클라이언트에 정적/동적 경로가 구성되었는지에 상관없이, 유효 라우팅 테이블이 따라 다음 홉이 결정됩니다.

IP 주소

다음 정보가 Azure의 IP 네트워크에 적용됩니다.

- DHCP를 사용하여 ASA 가상 인터페이스의 IP 주소를 설정해야 합니다.

  Azure 인프라는 Azure에서 설정된 IP 주소가 ASA 가상 인터페이스에 지정되게 합니다.

- Management 0/0는 연결된 서브넷에서 전용 IP 주소를 받습니다.

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

- 모든 인터페이스에 공용 IP 주소를 할당할 수 있습니다.
- 동적 공용 IP 주소는 Azure 중지/시작 사이클에 변경될 수 있습니다. 그러나 Azure가 재시작하고 ASA 가상가 다시 로드될 때는 유지됩니다.
- 고정 공용 IP 주소는 Azure에서 변경하지 않는 한 바뀌지 않습니다.

DNS

모든 Azure 가상 네트워크는 내장된 DNS 서버인 168.63.129.16에 액세스할 수 있으며, 이는 다음과 같이 사용 가능합니다.

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

스마트 라이센싱을 구성할 때 자체 DNS 서버가 설정되지 않은 경우 이 컨피그레이션을 사용할 수 있습니다.

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* 매

개 변수를 true로 설정하기만 하면 됩니다. Microsoft 문서 Enable accelerated networking on existing VMs를 참조하십시오. 그런 다음 VM을 다시 시작합니다.

Mellanox 하드웨어 지원

Microsoft Azure 클라우드에는 AN 기능을 지원하는 두 가지 유형의 하드웨어인 Mellanox 4(MLX4)와 Mellanox 5(MLX5)가 있습니다. ASA 가상은 릴리스 9.15부터 다음 인스턴스에 대해 Mellanox 하드웨어용 AN을 지원합니다.

- D3, D3_v2, DS3, DS3_v2
- D4, D4_v2, DS4, DS4_v2
- D5, D5_v2, DS5, DS5_v2
- D8_v3, D8s_v3
- D16_v3, D16s_v3
- F4, F4s
- F8, F8s, F8s_v2
- F16, F16s, F16s_v2

참고 MLX4(Mellanox 4)는 connectx3 = cx3이라고도 하며, MLX5(Mellanox 5)는 connectx4 = cx4라고도 합니다.

VM 구축을 위해 NIC Azure에서 MLX4와 MLX5 중 한쪽을 사용하도록 지정할 수는 없습니다. 가속화된 네트워킹 기능을 사용하려면 ASA 가상을 9.15 이상 버전으로 업그레이드하는 것이 좋습니다.

Microsoft Azure에 ASA 가상 구축

Microsoft Azure에 ASA 가상을 구축할 수 있습니다.

- 표준 Azure 퍼블릭 클라우드 및 Azure Government 환경에서 Azure Resource Manager를 사용하여 ASA 가상을 독립형 방화벽으로 구축합니다. Azure Resource Manager에서 ASA 가상 구축을 참조하십시오.
- Azure Security Center를 사용하여 Azure 내에서 통합된 파트너 솔루션으로 ASA 가상을 구축합니다. 보안에 민감한 고객에게는 Azure 워크로드를 보호하기 위한 방화벽 옵션으로 ASA 가상이 제공됩니다. 보안 및 상태 이벤트는 단일한 통합 대시보드에서 모니터링됩니다. Azure Security Center에서 ASA 가상 구축을 참조하십시오.
- Azure Resource Manager를 사용하여 ASA 가상 고가용성 쌍을 구축합니다. 리던던시를 보장하려면 액티브/백업 고가용성(HA) 구성으로 ASA 가상를 구축하면 됩니다. 퍼블릭 클라우드에서 HA는 액티브 ASA 가상 장애 때문에 백업 ASA 가상로 시스템의 자동 페일오버를 트리거하게 만들

수 있는 스테이트리스 액티브/백업 솔루션을 구현합니다. Azure Resource Manager에서 고가용성을 위한 ASA 가상 구축, 13 페이지의 내용을 참조하십시오.

- VHD(cisco.com에서 사용 가능)의 매니지드 이미지를 사용하여 맞춤형 템플릿과 함께 ASA 가상 또는 ASA 가상 고가용성 쌍을 구축합니다. Cisco에서는 Azure에 업로드하여 ASA 가상 구축 프로세스를 간소화할 수 있는 압축된 VHD(Virtual Hard Disk)를 제공합니다. 매니지드 이미지와 두 개의 JSON 파일(템플릿 파일 및 매개 변수 파일)을 사용하여, 조율된 단일 작업으로 ASA 가상을 위한 모든 리소스를 구축하고 프로비저닝할 수 있습니다. 맞춤형 템플릿을 사용하려면 VHD 및 리소스 템플릿을 사용해서 Azure에서 ASA 가상 구축, 15 페이지를 참조하십시오.

Azure Resource Manager에서 ASA 가상 구축

다음 절차는 ASA 가상에 Microsoft Azure를 설정하는 단계를 간략하게 정리한 것입니다. 자세한 Azure 설정 단계에 대한 자세한 내용은 Azure 시작하기를 참조하십시오.

Azure에서 ASA 가상를 구축할 경우 리소스, 공용 IP 주소, 경로 테이블과 같은 다양한 컨피그레이션이 자동으로 생성됩니다. 구축 후에 이 컨피그레이션을 추가로 관리할 수 있습니다. 이를테면 유휴 시간 초과 값을 낮게 설정된 기본값에서 변경할 수 있습니다.

단계 **1** ARM(Azure Resource Manager) 포털에 로그인합니다.

Azure 포털에서는 데이터 센터 위치와 상관없이 현재 계정 및 서브스크립션의 가상 요소를 보여줍니다.

단계 **2** 마켓플레이스에서 Cisco ASAv를 검색한 다음 구축하려는 ASA 가상을 클릭합니다.

단계 **3** 기본 설정을 구성합니다.

a) 가상 시스템의 이름을 입력합니다. 이 이름은 Azure 서브스크립션 내에서 고유해야 합니다.

중요 이름이 고유하지 않거나 기존 이름을 재사용하면 구축이 실패하게 됩니다.

b) 사용자 이름을 입력합니다.

c) 권한 부여 유형을 비밀번호 또는 **SSH** 공용 키 중 하나로 선택합니다.

비밀번호를 선택할 경우 비밀번호를 입력하고 확인합니다.

d) 서브스크립션 유형을 선택합니다.

e) **Resource group(**리소스 그룹**)**을 선택합니다.

리소스 그룹은 가상 네트워크의 리소스 그룹과 동일해야 합니다.

f) 위치를 선택합니다.

이 위치는 네트워크 및 리소스 그룹과 동일해야 합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **4** ASA 가상 설정을 구성합니다.

a) 가상 머신 크기를 선택합니다.

b) 스토리지 계정을 선택합니다.

기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정의 위치가 네트워크 및 가상 시스템에 대한 위치와 동일해야 합니다.

c) Name(이름) 필드에 IP 주소에 대한 레이블을 입력하여 공용 IP 주소를 요청한 다음 **OK(**확인**)**를 클릭합니다.

Azure는 기본적으로 동적 공용 IP를 생성합니다. 이는 VM이 중지하고 재시작할 때 변경될 수 있습니다. 고정 IP 주소를 선호할 경우 포털에서 public-ip를 열고 동적 주소에서 고정 주소로 변경할 수 있습니다.

d) 필요하다면 DNS 레이블을 추가합니다.

FQDN(fully qualified domain name)은 DNS 레이블 + Azure URL(<*dnslabel*>.<*location*>.*cloupapp.azure.com*)입니다.

e) 기존 가상 네트워크를 선택하거나 새로 만듭니다.

f) ASA 가상 구축 대상이 될 4개의 서브넷을 구성하고 **OK(**확인**)**를 클릭합니다.

중요 각 인터페이스가 고유한 서브넷에 연결되어야 합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **5** 컨피그레이션 요약을 본 다음 **OK(**확인**)**를 클릭합니다.

단계 **6** 이용 약관을 보고 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- SSH를 통해 입력 가능한 CLI 명령을 사용하여 컨피그레이션을 계속하거나 ASDM을 사용합니다. ASDM 액세스에 대한 지침은 ASDM 시작을 참조하십시오.

Azure Security Center에서 ASA 가상 구축

Microsoft Azure Security Center는 고객이 클라우드 구축에 대해 보호를 수행하고 보안 위험을 감지 및 완화하는 데 활용할 수 있게 해주는 Azure용 보안 솔루션입니다. Security Center 대시보드에서 고객은 보안 정책을 설정하고 보안 구성을 모니터링하며 보안 경고를 볼 수 있습니다.

Security Center는 잠재적인 보안 취약점을 식별하기 위해 Azure 리소스의 보안 상태를 분석합니다. 권장 사항 목록은 필요한 제어 기능을 구성하는 프로세스를 고객에게 안내합니다. 이 제어 기능에는 Azure 고객에게 ASA 가상을 방화벽 솔루션으로 배포하는 작업이 포함될 수 있습니다.

Security Center에서 통합 솔루션 역할을 하기 때문에, 몇 번만 클릭하면 ASA 가상을 신속하게 구축한 다음, 단일 대시보드에서 보안 및 상태 이벤트를 모니터링할 수 있습니다. 다음 절차는 Security Center에서 ASA 가상을 구축하는 단계를 간략하게 정리한 것입니다. 자세한 내용은 Azure Security Center를 참조하십시오.

단계 **1** Azure 포털에 로그인합니다.

Azure 포털에서는 데이터 센터 위치와 상관없이 현재 계정 및 서브스크립션의 가상 요소를 보여줍니다.

단계 **2** Microsoft Azure 메뉴에서 **Security Center**를 선택합니다.

처음으로 Security Center에 액세스하는 경우 **Welcome(**시작**)** 블레이드가 열립니다. **Yes! I want to Launch Azure Security Center(**예**, Azure Security Center**를 실행하고 싶습니다**.)**를 선택하여 **Security Center** 블레이드를 열고 데이터 수집을 활성화합니다.

단계 **3** **Security Center** 블레이드에서 **Policy(**정책**)** 타일을 선택합니다.

단계 **4** **Security Center** 블레이드에서 **Prevention policy(**방지 정책**)**를 선택합니다.

단계 **5** **Prevention policy(**방지 정책**)** 블레이드에서 보안 정책의 일부로 보려는 권장 사항을 켭니다.

a) **Next generation firewall(**차세대 방화벽**)**을 **On(**켜기**)**으로 설정합니다. 이렇게 하면 ASA 가상을 Security Center에서 권장 솔루션으로 사용할 수 있습니다.
b) 필요에 따라 다른 권장 사항을 설정합니다.

단계 **6** **Security Center** 블레이드로 돌아가 **Recommendations(**권장 사항**)** 타일로 이동합니다.

Security Center는 Azure 리소스의 보안 상태를 정기적으로 분석합니다. Security Center는 잠재적인 보안 취약점을 식별하고 **Recommendations(**권장 사항**)** 블레이드에서 권장 사항을 표시합니다.

단계 **7** **Recommendations(**권장 사항**)** 블레이드에 있는 **Add a Next Generation Firewall(**차세대 방화벽 추가**)**을 선택하여 자세한 정보를 확인하거나 문제 해결을 위한 조치를 수행합니다.

단계 **8** **Create New(**새로 생성**)** 또는 **Use existing solution(**기존 솔루션 사용**)**을 선택한 다음 구축하려는 ASA 가상을 클릭합니다.

단계 **9** 기본 설정을 구성합니다.

a) 가상 시스템의 이름을 입력합니다. 이 이름은 Azure 서브스크립션 내에서 고유해야 합니다.

중요 이름이 고유하지 않거나 기존 이름을 재사용하면 구축이 실패하게 됩니다.

b) 사용자 이름을 입력합니다.
c) 권한 부여 유형을 비밀번호 또는 SSH 키 중 하나로 선택합니다.

비밀번호를 선택할 경우 비밀번호를 입력하고 커밋합니다.

d) 서브스크립션 유형을 선택합니다.
e) 리소스 그룹을 선택합니다.

리소스 그룹은 가상 네트워크의 리소스 그룹과 동일해야 합니다.

f) 위치를 선택합니다.

이 위치는 네트워크 및 리소스 그룹과 동일해야 합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **10** ASA 가상 설정을 구성합니다.

a) 가상 머신 크기를 선택합니다.

ASA 가상은 Standard D3 및 Standard D3_v2를 지원합니다.

b) 스토리지 계정을 선택합니다.

기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정의 위치가 네트워크 및 가상 시스템에 대한 위치와 동일해야 합니다.

c) Name(이름) 필드에 IP 주소에 대한 레이블을 입력하여 공용 IP 주소를 요청한 다음 **OK(**확인**)**를 클릭합니다.

Azure는 기본적으로 동적 공용 IP를 생성합니다. 이는 VM이 중지하고 재시작할 때 변경될 수 있습니다. 고정 IP 주소를 선호할 경우 포털에서 public-ip를 열고 동적 주소에서 고정 주소로 변경할 수 있습니다.

d) 필요하다면 DNS 레이블을 추가합니다.

FQDN(fully qualified domain name)은 DNS 레이블 + Azure URL(<*dnslabel*>.<*location*>.*cloupapp.azure.com*)입니다.

e) 기존 가상 네트워크를 선택하거나 새로 만듭니다.

f) ASA 가상 구축 대상이 될 4개의 서브넷을 구성하고 **OK(**확인**)**를 클릭합니다.

중요 각 인터페이스가 고유한 서브넷에 연결되어야 합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **11** 컨피그레이션 요약을 본 다음 **OK(**확인**)**를 클릭합니다.

단계 **12** 이용 약관을 보고 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- SSH를 통해 입력 가능한 CLI 명령을 사용하여 컨피그레이션을 계속하거나 ASDM을 사용합니다. ASDM 액세스에 대한 지침은 ASDM 시작을 참조하십시오.
- Security Center 도움말의 권장 사항이 Azure 리소스를 보호하는 데 어떻게 도움이 되는지에 대한 자세한 내용은 Security Center에서 사용 가능한 설명서를 참조하십시오.

Azure Resource Manager에서 고가용성을 위한 ASA 가상 구축

다음 절차는 Microsoft Azure에서 HA(고가용성) ASA 가상 쌍을 설정하는 단계를 간략하게 정리한 것입니다.. 자세한 Azure 설정 단계에 대한 자세한 내용은 Azure 시작하기를 참조하십시오.

Azure에서의 ASA 가상 HA는 ASA 가상 2개를 가용성 모음에 구축하며, 리소스와 퍼블릭 IP 조수 및 라우트 테이블 같은 다양한 구성을 자동으로 생성합니다. 구축 후에 이 컨피그레이션을 추가로 관리할 수 있습니다.

단계 **1** Azure 포털에 로그인합니다.

Azure 포털에서는 데이터 센터 위치와 상관없이 현재 계정 및 서브스크립션의 가상 요소를 보여줍니다.

단계 **2** Marketplace에서 **Cisco ASAv**를 검색한 다음 **ASAv 4 NIC HA**를 클릭하여 페일오버 ASA 가상 구성을 구축합니다.

단계 **3** **Basics(**기본**)** 설정을 구성합니다.

a) ASA 가상 머신 이름의 접두사를 입력합니다. ASA 가상 이름은 'prefix'-A 및 'prefix'-B입니다.

중요 기존 접두사를 사용하면 구축이 실패하므로 주의해야 합니다.

b) 사용자 이름을 입력합니다.

두 가상 머신 모두의 관리 사용자 이름이 됩니다.

중요 사용자 이름 **admin**은 Azure에서 허용되지 않습니다.

c) 두 가상 머신의 권한 부여 유형을 비밀번호 또는 **SSH** 공개 키 중 하나로 선택합니다.

비밀번호를 선택할 경우 비밀번호를 입력하고 확인합니다.

d) 서브스크립션 유형을 선택합니다.

e) **Resource group(**리소스 그룹**)**을 선택합니다.

Create new(새로 만들기**)**를 선택하여 새 리소스 그룹을 생성하거나 **Use existing(**기존 리소스 그룹 사용**)**을 선택하여 기존 리소스 그룹을 선택합니다. 기존 리소스 그룹을 사용한다면 비어 있어야 합니다. 비어 있지 않다면 새 리소스 그룹을 생성해야 합니다.

f) 위치를 선택합니다.

이 위치는 네트워크 및 리소스 그룹과 동일해야 합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **4** **Cisco ASAv settings(Cisco ASAv** 설정**)**를 구성합니다.

a) 가상 머신 크기를 선택합니다.

b) **Managed(**관리형**)** 또는 **Unmanaged OS disk(**언매니지드 **OS** 디스크**)** 스토리지를 선택합니다.

중요 ASA HA 모드는 항상 **Managed(**관리형**)**를 사용합니다.

단계 **5** **ASAv-A** 설정을 구성합니다.

a) (선택 사항) **Create new(**새로 만들기**)**를 선택하고 Name(이름) 필드에 IP 주소에 대한 레이블을 입력하여 공용 IP 주소를 요청하고, **OK(**확인**)**를 클릭합니다. 공용 IP 주소를 사용하지 않으려면 **None(**없음**)**을 선택합니다.

참고 Azure는 기본적으로 동적 공용 IP를 생성합니다. 이는 VM이 중지하고 재시작할 때 변경될 수 있습니다. 고정 IP 주소를 선호할 경우 포털에서 public-ip를 열고 동적 주소에서 고정 주소로 변경할 수 있습니다.

b) 필요하다면 DNS 레이블을 추가합니다.

FQDN(fully qualified domain name)은 DNS 레이블 + Azure URL(<*dnslabel*>.<*location*>.*cloupapp.azure.com*)입니다.

c) ASAv-A 부팅 진단을 위한 스토리지 계정에 필요한 설정을 구성합니다.

단계 **6** **ASAv-B** 설정에 대해 이전 단계를 반복합니다.

단계 **7** 기존 가상 네트워크를 선택하거나 새로 만듭니다.

a) ASA 가상 구축 대상이 될 4개의 서브넷을 구성하고 **OK(**확인**)**를 클릭합니다.

중요 각 인터페이스가 고유한 서브넷에 연결되어야 합니다.

b) **OK(**확인**)**를 클릭합니다.

단계 **8** 컨피그레이션 **Summary(**요약**)**을 본 다음 **OK(**확인**)**를 클릭합니다.

단계 **9** 이용 약관을 보고 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- SSH를 통해 입력 가능한 CLI 명령을 사용하여 컨피그레이션을 계속하거나 ASDM을 사용합니다. ASDM 액세스에 대한 지침은 ASDM 시작을 참조하십시오.
- Azure에서 ASA 가상 HA 컨피그레이션에 대한 자세한 내용은 ASA 컨피그레이션 가이드의 "퍼블릭 클라우드의 고가용성을 위한 페일오버" 장을 참조하십시오.

VHD 및 리소스 템플릿을 사용해서 Azure에서 ASA 가상 구축

이제 Cisco에서 사용 가능한 압축된 VHD 이미지를 사용하여 Azure에서 고유한 맞춤형 ASA 가상 이미지를 생성할 수 있습니다. VHD 이미지를 사용하여 구축하려면 Azure 스토리지 계정에 VHD 이미지를 업로드합니다. 그런 다음, 업로드된 디스크 이미지 및 Azure Resource Manager 템플릿을 사용하여 매니지드 이미지를 생성할 수 있습니다. Azure 템플릿은 리소스 설명 및 파라미터 정의를 포함하는 JSON 파일입니다.

시작하기 전에

- ASA 가상 템플릿 구축을 위한 JSON 템플릿 및 해당 JSON 매개변수 파일이 필요합니다. 다음 GitHub 리포지토리에서 템플릿 파일을 다운로드할 수 있습니다.

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- 템플릿 및 매개변수 파일을 작성하는 방법은 부록 - Azure 리소스 템플릿 예, 18 페이지를 참조하십시오.
- 이 절차를 수행하려면 Azure의 기존 Linux VM이 필요합니다. 압축된 VHD 이미지를 Azure에 업로드하려면 임시 Linux VM(예: Ubuntu 16.04)을 사용하는 것이 좋습니다. 이 이미지는 압축을 풀 때 약 50G의 스토리지가 필요합니다. 또한 Azure의 Linux VM에서 Azure 스토리지로의 업로드 시간이 더 빨라집니다.

  VM을 생성해야 하는 경우 다음 방법 중 하나를 사용합니다.

  - Azure CLI를 사용하여 Linux 가상 시스템 생성
  - Azure Portal에서 Linux 가상 머신 생성

- Azure 구독에서 ASA 가상를 구축하려는 위치에서 사용 가능한 스토리지 계정이 있어야 합니다.

단계 **1** https://software.cisco.com/download/home페이지에서 ASA 가상 압축 VHD 이미지를 다운로드합니다.

a) **Products(**제품**)** > **Security(**보안**)** > **Firewalls(**방화벽**)** > **ASA(Adaptive Security Appliances)** > **Adaptive Security Appliance (ASA) Software(ASA[Adaptive Security Appliance]** 소프트웨어**)**로 이동합니다.

b) **ASAv(Adaptive Security Virtual Appliance)**를 클릭합니다.

지침에 따라 다운로드합니다.

예: asav9-14-1.vhd.bz2

단계 **2** 압축된 VHD 이미지를 Azure의 Linux VM에 복사합니다.

파일을 Azure로 또는 Azure에서 아래로 이동하는 데 사용할 수 있는 여러 옵션이 있습니다. 이 예에서는 SCP 또는 보안 복사본을 보여줍니다.

```
# scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```

단계 **3** Azure에서 Linux VM에 로그인하고 압축된 VHD 이미지를 복사한 디렉터리로 이동합니다.

단계 **4** ASA 가상 VHD 이미지의 압축을 풉니다.

파일의 압축을 풀거나 압축을 풀 때 사용할 수 있는 여러 옵션이 있습니다. 이 예에서는 Bzip2 유틸리티를 보여 주지만, 작동하는 Windows 기반 유틸리티도 있습니다.

```
# bunzip2 asav9-14-1.vhd.bz2
```

단계 **5** Azure 스토리지 계정의 컨테이너에 VHD를 업로드합니다. 기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정 이름은 소문자와 숫자만 포함할 수 있습니다.

스토리지 계정에 VHD를 업로드하는 데 사용할 수 있는 여러 옵션(AzCopy, Azure Storage Copy Blob API, Azure Storage Explorer, Azure CLI 또는 Azure Portal)이 있습니다. ASA 가상만큼 큰 파일에는 Azure Portal을 사용하지 않는 것이 좋습니다.

다음 예에서는 Azure CLI를 사용하는 구문을 보여줍니다.

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

단계 **6** VHD에서 관리되는 이미지 생성:

a) Azure Portal에서 **Images(**이미지**)**를 선택합니다.

b) **Add(**추가**)**를 클릭하여 새 엔트리를 만듭니다.

c) 다음 정보를 제공합니다.

- **Name(**이름**)**-관리되는 이미지의 사용자 정의 이름을 입력합니다.
- **Subscription(**구독**)**-드롭 다운 목록에서 구독을 선택합니다.
- **Resource group(**리소스 그룹**)**-기존 리소스 그룹을 선택하거나 새 리소스 그룹을 생성합니다.
- **OS disk(OS** 디스크**)**-OS 유형으로 Linux를 선택합니다.
- **Storage blob(**스토리지 블롭**)**-스토리지 계정을 찾아 업로드된 VHD를 선택합니다.
- **Account type(**계정 유형**)**-드롭 다운 목록에서 표준(HDD)을 선택합니다.
- **Host caching(**호스트 캐싱**)**-드롭 다운 목록에서 Read/write(읽기/쓰기)를 선택합니다.
- **Data Disk(**데이터 디스크**)**-기본값을 그대로 둡니다. 데이터 디스크를 추가하지 마십시오.

d) **Create(**생성**)**를 클릭합니다.

Notifications(알림**)** 탭 아래에서 정상적으로 생성된 이미지 메시지를 기다립니다.

참고 관리되는 이미지가 생성되면 업로드된 VHD 및 업로드 스토리지 계정을 제거할 수 있습니다.

단계 **7** 새로 생성한 관리 이미지의 리소스 ID를 가져옵니다.

내부적으로 Azure는 모든 리소스를 리소스 ID와 연결합니다. 이 관리되는 이미지에서 새 ASA 가상 방화벽을 구축할 때는 리소스 ID가 필요합니다.

a) Azure Portal에서 **Images(**이미지**)**를 선택합니다.
b) 이전 단계에서 생성한 관리 이미지를 선택합니다.
c) 이미지 속성을 보려면 **Overview(**개요**)**를 클릭합니다.
d) 리소스 **ID**를 클립 보드에 복사합니다.

리소스 **ID**의 형식은 다음과 같습니다.

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup> /providers/Microsoft.Compute/<container>/<vhdname>

단계 **8** 관리되는 이미지 및 리소스 템플릿을 사용하여 ASA 가상 방화벽을 구축합니다.

a) **New(**새로 만들기**)**를 선택하고 옵션에서 선택할 수 있을 때까지 **Template Deployment(**템플릿 구축**)**를 검색합니다.
b) **Create(**생성**)**을 선택합니다.
c) **Build your own template in the editor(**편집기에서 자체 템플릿 구축**)**를 선택합니다.

맞춤화할 수 있는 빈 템플릿이 있습니다. 템플릿을 생성하는 방법의 예는 리소스 템플릿 생성, 19 페이지를 참조하십시오.

d) 맞춤화된 JSON 템플릿 코드를 창에 붙여넣은 다음 **Save(**저장**)**를 클릭합니다.
e) 드롭 다운 목록에서 **Subscription(**구독**)**을 선택합니다.
f) 기존 **Resource group(**리소스 그룹**)**을 선택하거나 새 리소스 그룹을 생성합니다.
g) 드롭다운 목록에서 **Location(**위치**)**를 선택합니다.
h) 이전 단계의 관리 이미지 리소스 **ID**를 **Vm** 관리 이미지 **ID** 필드에 붙여 넣습니다.

단계 **9** **Custom deployment(**맞춤형 구축**)** 페이지 상단에서 **Edit parameters(**매개 변수 수정**)**를 클릭합니다. 맞춤화할 수 있는 매개변수 템플릿이 있습니다.

a) **Load file(**파일 로드**)**을 클릭하고 사용자 맞춤화된 ASA 가상 매개변수 파일을 찾습니다. 매개변수 템플릿을 생성하는 방법의 예는 매개변수 파일 생성, 28 페이지를 참조하십시오.
b) 사용자 맞춤화된 JSON 매개변수 코드를 창에 붙여 넣은 다음 **Save(**저장**)**를 클릭합니다.

단계 **10** 맞춤형 구축 세부 정보를 검토합니다. **Basics(**기본**)** 및 **Settings(**설정**)**의 정보가 리소스 **ID**를 포함하여 예상되는 구축 컨피그레이션과 일치하는지 확인합니다.

단계 **11** 약관을 검토하고 위에 명시된 약관에 동의합니다 확인란을 선택합니다.

단계 **12** 관리 이미지 및 맞춤형 템플릿을 사용하여 ASA 가상 방화벽을 구축하려면 **Purchase(**구매**)**를 클릭합니다.

템플릿 및 매개변수 파일에 충돌이 없는 경우 구축이 성공적으로 이루어지게 됩니다.

Managed Image(관리 이미지)는 동일한 구독 및 지역 내의 여러 구축에 사용할 수 있습니다.

다음에 수행할 작업

- SSH를 통해 입력 가능한 CLI 명령을 사용하여 컨피그레이션을 계속하거나 ASDM을 사용합니다. ASDM 액세스에 대한 지침은 ASDM 시작, 87페이지를 참조하십시오.

부록 - Azure 리소스 템플릿 예

이 섹션에서는 ASA 가상 구축에 사용할 수 있는 Azure Resource Manager 템플릿의 구조에 대해 설명합니다. Azure 리소스 템플릿은 JSON 파일입니다. 필요한 모든 리소스의 구축을 간소화하기 위해 이 예에는 JSON 파일 두 개가 포함되어 있습니다.

- **Template File(**템플릿 파일**)** - 리소스 그룹 내의 모든 구성 요소를 구축하는 기본 리소스 파일입니다.
- **Parameter File(**매개변수 파일**)** - 이 파일에는 ASA 가상을 성공적으로 구축하는 데 필요한 매개변수가 포함되어 있습니다. 여기에는 서브넷 정보, 가상 머신 계층 및 크기, ASA 가상의 사용자 이름 및 비밀번호, 스토리지 컨테이너의 이름 등의 세부 정보가 포함됩니다. Azure Stack Hub 구축 환경에 맞게 이 파일을 사용자 지정할 수 있습니다.

템플릿 파일 형식

이 섹션에서는 Azure Resource Manager 템플릿 파일 구조에 대해 설명합니다. 다음 예에서는 템플릿 파일의 축소 보기와 템플릿의 다양한 섹션을 확인할 수 있습니다.

Azure Resource Manager JSON 템플릿 파일

```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "",
    "parameters": { },
    "variables": { },
    "resources": [ ],
    "outputs": { }
}
```

템플릿은 ASA 가상 구축을 위한 값을 구성하는 데 사용할 수 있는 JSON 및 식으로 구성됩니다. 가장 간단한 구조에서 템플릿에는 다음 요소가 포함됩니다.

표 *2: Azure Resource Manager JSON* 템플릿 파일 요소 정의됨

요소	필수	**Description**
$schema	예	템플릿 언어의 버전을 설명하는 JSON 스키마 파일의 위치입니다. 위의 그림에 표시된 URL을 사용합니다.

요소	필수	**Description**
contentVersion	예	템플릿의 버전(예: 1.0.0.0)입니다. 이 요소에 임의의 값을 입력할 수 있습니다. 템플릿을 사용하여 리소스를 구축할 때 이 값을 사용하여 올바른 템플릿이 사용되고 있는지 확인할 수 있습니다.
parameters	아니요	리소스 구축을 사용자 지정하기 위해 구축을 실행할 때 제공되는 값입니다. 매개변수를 사용하면 구축할 때 값을 입력할 수 있습니다. 반드시 필요하지만 않지만, 이 값이 없으면 JSON 템플릿은 매번 동일한 매개변수를 사용하여 리소스를 구축합니다.
변수	아니요	템플릿 언어 식을 간소화하기 위해 템플릿에서 JSON 프래그먼트로 사용하는 값입니다.
리소스	예	리소스 그룹에서 구축되거나 업데이트된 리소스 유형입니다.
출력	아니요	구축 후 반환되는 값입니다.

JSON 템플릿을 사용하면 구축할 리소스 유형뿐만 아니라 관련 구성 매개변수도 선언할 수 있습니다. 다음 예에서는 새 ASA 가상을 구축하는 템플릿을 확인할 수 있습니다.

리소스 템플릿 생성

아래 예를 참고하여 텍스트 편집기를 이용해 자체 구축 템플릿을 생성할 수 있습니다.

단계 **1** 다음 예의 텍스트를 복사합니다.

예제**:**

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "defaultValue": "ngfw",
            "metadata": {
                "description": "Name of the NGFW VM"
            }
        },
        "vmManagedImageId": {
            "type": "string",
            "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",

            "metadata": {
                "description": "The ID of the managed image used for deployment.
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"
```

```
            }
        },
        "adminUsername": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
               "description": "Username for the Virtual Machine. admin, Administrator among other values
 are disallowed - see Azure docs"
            }
        },
        "adminPassword": {
            "type": "securestring",
            "defaultValue" : "",
            "metadata": {
                "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars and
have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
            }
        },
        "vmStorageAccount": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "A storage account name (boot diags require a storage account). Between
3 and 24 characters. Lowercase letters and numbers only"
            }
        },
        "virtualNetworkResourceGroup": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network's Resource Group"
            }
        },
        "virtualNetworkName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network"
            }
        },
        "mgmtSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv management interface will attach to this subnet"
            }
        },
        "mgmtSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
            }
        },
        "diagSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
            }
        },
        "diagSubnetIP": {
            "type": "string",
            "defaultValue": "",
```

```
            "metadata": {
                "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
            }
        },
        "gig00SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
            }
        },
        "gig00SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
            }
        },
        "gig01SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
            }
        },
        "gig01SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
            }
        },
        "VmSize": {
            "type": "string",
            "defaultValue": "Standard_D3_v2",
            "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
            "metadata": {
                "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
            }
        }
    },
    "variables": {

        "virtualNetworkID":
"[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",

        "vmNic0Name":"[concat(parameters('vmName'),'-nic0')]",
        "vmNic1Name":"[concat(parameters('vmName'),'-nic1')]",
        "vmNic2Name":"[concat(parameters('vmName'),'-nic2')]",
        "vmNic3Name":"[concat(parameters('vmName'),'-nic3')]",

        "vmNic0NsgName":"[concat(variables('vmNic0Name'),'-NSG')]",

        "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
        "vmMgmtPublicIPAddressType": "Static",
        "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
    },
    "resources": [
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/publicIPAddresses",
            "name": "[variables('vmMgmtPublicIPAddressName')]",
            "location": "[resourceGroup().location]",
```

```
    "properties": {
      "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
      "dnsSettings": {
        "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
      }
    }
},
{
    "apiVersion": "2015-06-15",
    "type": "Microsoft.Network/networkSecurityGroups",
    "name": "[variables('vmNic0NsgName')]",
    "location": "[resourceGroup().location]",
    "properties": {
        "securityRules": [
            {
                "name": "SSH-Rule",
                "properties": {
                    "description": "Allow SSH",
                    "protocol": "Tcp",
                    "sourcePortRange": "*",
                    "destinationPortRange": "22",
                    "sourceAddressPrefix": "Internet",
                    "destinationAddressPrefix": "*",
                    "access": "Allow",
                    "priority": 100,
                    "direction": "Inbound"
                }
            },
            {
                "name": "SFtunnel-Rule",
                "properties": {
                    "description": "Allow tcp 8305",
                    "protocol": "Tcp",
                    "sourcePortRange": "*",
                    "destinationPortRange": "8305",
                    "sourceAddressPrefix": "Internet",
                    "destinationAddressPrefix": "*",
                    "access": "Allow",
                    "priority": 101,
                    "direction": "Inbound"
                }
            }
        ]
    }
},
{
    "apiVersion": "2017-03-01",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('vmNic0Name')]",
    "location": "[resourceGroup().location]",
    "dependsOn": [
        "[concat('Microsoft.Network/networkSecurityGroups/',variables('vmNic0NsgName'))]",
      "[concat('Microsoft.Network/publicIPAddresses/', variables('vmMgmtPublicIPAddressName'))]"

    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Static",
                    "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
                    "subnet": {
                        "id": "[concat(variables('virtualNetworkID'),'/subnets/',
```

```
parameters('mgmtSubnetName'))]"
                            },
                            "publicIPAddress":{
                                "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
                            }
                        }
                    }
                ],
                "networkSecurityGroup": {
                    "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
                },
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic1Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('diagSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('diagSubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic2Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig00SubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
```

```
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic3Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig01SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig01SubnetName'))]"

                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[concat(parameters('vmStorageAccount'))]",
            "apiVersion": "2015-06-15",
            "location": "[resourceGroup().location]",
            "properties": {
              "accountType": "Standard_LRS"
            }
        },
        {
            "apiVersion": "2017-12-01",
            "type": "Microsoft.Compute/virtualMachines",
            "name": "[parameters('vmName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic0Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic1Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic2Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic3Name'))]"
            ],
            "properties": {
                "hardwareProfile": {
                    "vmSize": "[parameters('vmSize')]"
                },
                "osProfile": {
                    "computername": "[parameters('vmName')]",
                    "adminUsername": "[parameters('AdminUsername')]",
                    "adminPassword": "[parameters('AdminPassword')]"
                },
                "storageProfile": {
                    "imageReference": {
                        "id": "[parameters('vmManagedImageId')]"
                    },
                    "osDisk": {
                        "osType": "Linux",
                        "caching": "ReadWrite",
                        "createOption": "FromImage"
                    }
                },
                "networkProfile": {
                    "networkInterfaces": [
```

```
                        {
                            "properties": {
                                "primary": true
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
                        }
                    ]
                },
                "diagnosticsProfile": {
                    "bootDiagnostics": {
                        "enabled": true,
                        "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
                    }
                }
            }
        }
    ],
    "outputs": {  }
}
```

단계 **2** 파일을 JSON 파일로 로컬에 저장합니다(예: **azureDeploy.json**).

단계 **3** 파일을 편집하여 구축 파라미터에 맞게 템플릿을 생성합니다.

단계 **4** 이 템플릿을 사용하여 VHD 및 리소스 템플릿을 사용해서 Azure에서 ASA 가상 구축, 15 페이지에 설명된 대로 ASA 가상을 구축합니다.

매개변수 파일 형식

새 구축을 시작하면 리소스 템플릿에 매개변수가 정의됩니다. 구축을 시작하려면 매개변수를 입력해야 합니다. 리소스 템플릿에 정의한 매개변수를 수동으로 입력하거나, 템플릿 매개변수 JSON 파일에 매개변수를 추가할 수 있습니다.

매개변수 파일에는 매개변수 파일 생성, 28 페이지의 매개변수 예에 나와 있는 각 매개변수에 대한 값이 포함되어 있습니다. 이러한 값은 구축 중에 자동으로 템플릿에 전달됩니다. 다양한 구축 시나리오를 위한 여러 매개변수 파일을 생성할 수 있습니다.

이 예에 나오는 ASA 가상 템플릿의 경우 매개변수 파일에 다음 매개변수가 정의되어 있어야 합니다.

표 ***3: ASA*** 가상 매개변수 정의

필드	**Description**	예
vmName	ASA 가상 머신의 Azure에서 의 이름입니다.	cisco-asav
vmManagedImageId	구축에 사용하는 관리형 이미지의 ID입니다. 내부적으로 Azure는 모든 리소스를 리소스 ID와 연결합니다.	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv910-Managed-I mage
adminUsername	ASA 가상에 로그인하기 위한 사용자 이름입니다. 예약된 이름인 'admin'은 사용할 수 없습니다.	jdoe
adminPassword	관리자 비밀번호입니다. 길이는 12~72자여야 하며 소문자 1개, 대문자 1개, 숫자 1개, 특수 문자 1개 중에서 3개를 포함해야 합니다.	Pw0987654321
vmStorageAccount	Azure 스토리지 계정입니다. 기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정 이름은 3~24자이고 소문자와 숫자만 포함할 수 있습니다.	ciscoasavstorage
virtualNetworkResourceGroup	가상 네트워크 리소스 그룹의 이름입니다. ASA 가상는 항상 새 리소스 그룹에 구축됩니다.	ew-west8-rg
virtualNetworkName	가상 네트워크의 이름입니다.	ew-west8-vnet
mgmtSubnetName	관리 인터페이스가 이 서브넷에 연결됩니다. 첫 번째 서브넷인 Nic0에 매핑됩니다. 기존 네트워크에 조인하는 경우 기존 서브넷 이름과 일치해야 합니다.	mgmt
mgmtSubnetIP	관리 인터페이스 IP 주소입니다.	10.8.0.55

필드	**Description**	예
gig00SubnetName	GigabitEthernet 0/0 인터페이스가 이 서브넷에 연결됩니다. 두 번째 서브넷인 Nic1에 매핑됩니다. 기존 네트워크에 조인하는 경우 기존 서브넷 이름과 일치해야 합니다.	내부
gig00SubnetIP	GigabitEthernet 0/0 인터페이스 IP 주소입니다. ASA 가상의 첫 번째 데이터 인터페이스에 사용합니다.	10.8.2.55
gig01SubnetName	GigabitEthernet 0/1 인터페이스가 이 서브넷에 연결됩니다. 세 번째 서브넷인 Nic2에 매핑됩니다. 기존 네트워크에 조인하는 경우 기존 서브넷 이름과 일치해야 합니다.	외부
gig01SubnetIP	GigabitEthernet 0/1 인터페이스 IP 주소입니다. ASA 가상의 두 번째 데이터 인터페이스에 사용합니다.	10.8.3.55
gig02SubnetName	GigabitEthernet 0/2 인터페이스가 이 서브넷에 연결됩니다. 네 번째 서브넷인 Nic3에 매핑됩니다. 기존 네트워크에 조인하는 경우 기존 서브넷 이름과 일치해야 합니다.	dmz
gig02SubnetIP	GigabitEthernet 0/2 인터페이스 IP 주소입니다. ASA 가상의 세 번째 데이터 인터페이스에 사용합니다.	10.8.4.55
vmSize	ASA 가상 VM에 사용할 VM 크기입니다. Standard_D3_V2 및 Standard_D3가 지원됩니다. Standard_D3_V2가 기본값입니다.	Standard_D3_V2 또는 Standard_D3

매개변수 파일 생성

아래 예를 참고하여 텍스트 편집기를 사용하여 자체 매개변수 파일을 생성할 수 있습니다.

참고 다음 예는 IPV4에만 해당됩니다.

단계 **1** 다음 예의 텍스트를 복사합니다.

예제:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"

    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
```

```
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

단계 **2** 파일을 JSON 파일로 로컬에 저장합니다(예: **azureParameters.json**).

단계 **3** 파일을 편집하여 구축 파라미터에 맞게 템플릿을 생성합니다.

단계 **4** 이 매개변수 템플릿을 사용하여 VHD 및 리소스 템플릿을 사용해서 Azure에서 ASA 가상 구축, 15 페이지에 설명된 대로 ASA 가상을 구축합니다.