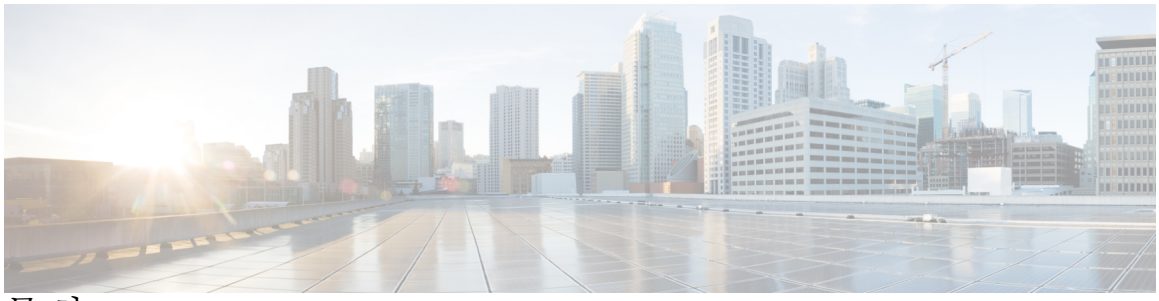
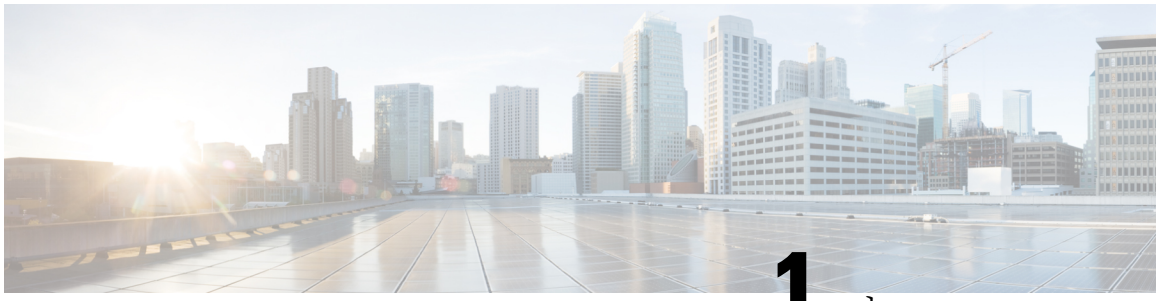
Microsoft Azure Marketplace에서 Cisco Secure Web Appliance 구축

초판: 2022년 7월 11일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

소개

Azure Marketplace 정보

Azure 이미지를 사용하여 Azure에서 가상 머신 인스턴스를 생성할 수 있습니다. Secure Web Appliance용 Azure 이미지는 Azure Marketplace에서 사용할 수 있습니다.

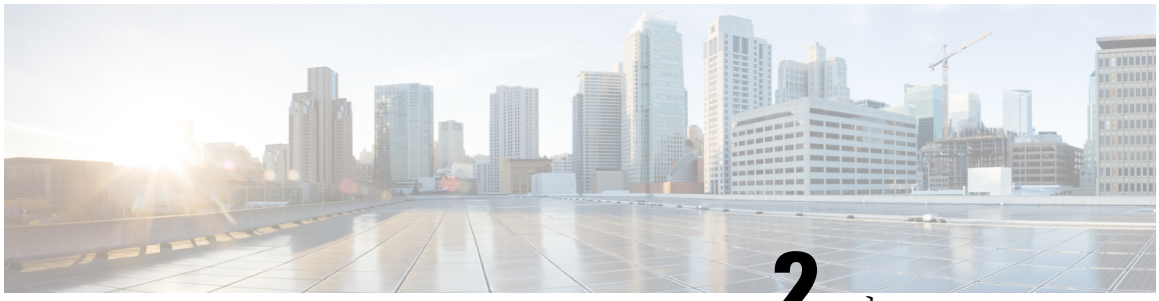
Azure Marketplace는 엔드 투 엔드 솔루션을 제공하기 위해 Azure에서 실행하도록 인증되고 최적화된 모든 소프트웨어 요구 사항을 충족하는 최고의 대상입니다.

보안 웹 어플라이언스 라이선싱

Microsoft Azure에서의 구축에 기존 Secure Web Appliance 라이선스를 사용할 수 있습니다. 인스턴스를 구축하고 시작한 후 라이선스를 설치할 수 있습니다. Azure 인프라 요금만 지불하면 됩니다.

신규 고객인 경우 Cisco 파트너에게 문의하여 라이선스를 받으십시오.

기존 고객인 경우 가상 ESA, 가상 WSA 또는 가상 SMA 라이선스에 대한 모범 사례에서 가상 라이선스(VLN) 얻기를 참조하십시오.



2 장

Azure Marketplace에서 Secure Web Appliance 구축

Azure 사용자 인터페이스 및 Azure CLI를 사용하여 Azure Marketplace에 Secure Web Appliance를 구축할 수 있습니다.

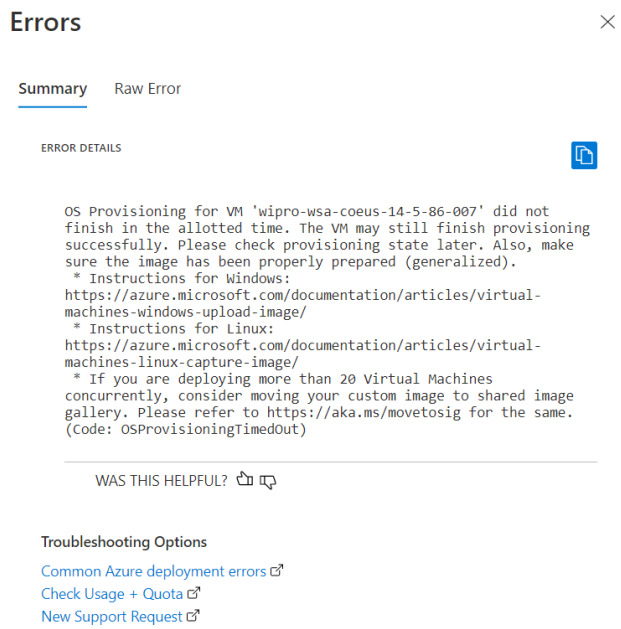
구성 제한 사항

- 다음 구성은 Azure Marketplace에서 Secure Web Appliance를 구축하는 데 지원되지 않습니다.
  - 레이어4 트래픽 모니터
  - 웹 트래픽 탭
- Microsoft Azure CLI만 사용하여 Secure Web Virtual Appliance에서 여러 인터페이스를 생성할 수 있습니다.
- Azure 사용자 인터페이스에서 하나의 인터페이스로만 Secure Web Appliance 인스턴스를 구성할 수 있습니다.

추가 정보

- Secure Web Appliance의 Azure 인스턴스에는 인스턴스의 상태를 Azure 인프라에 보고하는 데 필요한 WAAgent 지원이 없습니다. Azure에서 Secure Web Appliance에 대한 구축 실패(시간 초과)를 보고하지만 인스턴스가 성공적으로 프로비저닝됩니다. 가상 머신의 현재 상태를 확인하려면 **Boot diagnostics(**부팅 진단**)**를 선택합니다.

그림 *1:* 프로비저닝 오류



- 인바운드 규칙은 가상 머신으로 수신되는 특정 트래픽을 허용할지 아니면 거부할지를 지정하는 규칙 집합입니다.

  인바운드 규칙을 변경하려면(Secure Web Appliance에 대한 액세스):

  - Virtual Machines(가상 머신) 아래에서 원하는 VM 인스턴스를 선택합니다.
  - **Networking(**네트워킹**)** 옵션을 선택합니다.

    이제 관리 인터페이스에 대해 나열되는 인바운드 규칙을 볼 수 있습니다.

참고 이미 존재하는 내장된 3개의 보안 규칙을 삭제하지 마십시오.

세 가지 기본 인바운드 규칙은 가상 네트워크, 로드 밸런서 및 허용되는 트래픽을 제외한 모든 인바운드 트래픽을 기본적으로 차단하는 서비스와 같은 Azure 관련 서비스입니다.

- Azure에서 인스턴스를 재부팅하면 동적으로 할당된 공용 IP가 변경될 수 있습니다. https://www.linkedin.com/pulse/how-remote-desktop-centos-virtual-machine-running-azure-cretu의 내용을 참조하십시오.
- Azure 사용자 인터페이스는 단일 인터페이스를 사용하는 보안 웹 어플라이언스 구축을 지원하지만 Azure CLI를 사용하여 여러 인터페이스를 사용하여 인스턴스를 구축할 수 있습니다.

  둘 이상의 인터페이스로 Azure 인스턴스를 구축하는 방법은 CLI를 사용하여 Azure 환경에 Secure Web Appliance 구축, 9 페이지의 내용을 참조하십시오.

Azure 사용자 인터페이스를 사용하여 Azure Marketplace에 Secure Web Appliance 구축

참고 가상 머신 구축은 Azure Marketplace에서 제공되는 프로비저닝된 빌드를 사용하여 수행됩니다.

표 *1:* 사용자 인터페이스를 사용하여 ***Azure***에 구축

	수행해야 할 작업	추가 정보
1단계	Azure에서 인스턴스를 설정하기 전에 사전 요구 사항 작업을 완료하고 필요한 정보를 가져와 환경을 준비합니다.	환경 준비, 6 페이지
2단계	Azure Marketplace로 이동하여 원하는 빌드에 대해 프로비저닝된 이미지를 선택합니다. **Create(생성)**를 클릭합니다.	구축을 위해 지원되는 인스턴스 유형, 7 페이지.
3단계	Resource Group(리소스 그룹), VM Name(VM 이름) 및 Size(크기)(RAM 및 CPU가 다른 인스턴스 유형)를 선택합니다. Azure 환경에서 Authentication type(인증 유형)을 password(비밀번호)로, License type(라이선스 유형)을 Other(기타)로 선택합니다.	인스턴스 세부 정보 구성, 7 페이지
4단계	가상 네트워크, 디스크, 서브넷 및 공용 IP 옵션을 구성합니다.	모든 리소스는 구축에 대해 동일한 지역에 있어야 합니다.
5단계	네트워크 보안 그룹을 생성합니다. 기본 인바운드 규칙을 사용하거나 규칙을 추가합니다. 필요한 경우 부팅 진단을 **Yes(예)**로 설정합니다. 게스트 구성은 Day 0을 제공하는 데 사용됩니다.	인스턴스 세부 정보 구성, 7 페이지
6단계	요구 사항에 따라 이름, 그룹, 팀, 모델 및 용도와 같은 태그를 생성합니다.	인스턴스 세부 정보 구성, 7 페이지

	수행해야 할 작업	추가 정보
7단계	변경 사항을 검토하고 Azure 인스턴스를 구축합니다.	Secure Web Appliance의 Azure 인스턴스에는 인스턴스의 상태를 Azure 인프라에 보고하는 데 필요한 WAAgent 지원이 없습니다. Azure에서 Secure Web Appliance에 대한 구축 실패(시간 초과)를 보고하지만 인스턴스가 성공적으로 프로비저닝됩니다.
8단계	인스턴스 **Overview(**개요**)** 페이지로 이동하여 인스턴스의 상태를 확인합니다. 실행 중이어야 합니다. 콘솔 및 브라우저를 통한 로깅에 사용할 수 있는 공용 IP를 할당해야 합니다.	
9단계	• CLI, SSH에서 Azure 인스턴스에 액세스합니다(제공된 경우, 인바운드 규칙이 **Allow(**허용**)**로 설정됨). • **loadlicense** 명령을 사용하고 변경 사항을 커밋합니다.	• 필요한 포트는 환경 준비, 6 페이지의 내용을 참조하십시오. • SSH 액세스 및 웹 액세스에 대해서는 시작된 인스턴스 구성, 8 페이지의 내용을 참조하십시오. .
10단계	Secure Web Appliance의 웹 인터페이스에 연결합니다. 시스템 설정 마법사를 실행하거나, 구성 파일을 업로드하거나, 기능을 구성할 수 있습니다.	Secure Web Appliance 사용자 인터페이스에 연결, 9 페이지.
11단계	Secure Web Appliance에서 라이선스 만료 알림을 구성합니다.	라이선스 만료가 임박했을 때 알림을 보내도록 Secure Web Appliance 구성, 9 페이지.

환경 준비

Secure Web Appliance를 구축하려면 다음이 필요합니다.

- Secure Web Virtual Appliance에 대한 유효한 라이선스.
- Secure Web Appliance의 기본 사용자 이름 및 비밀번호:
  - 사용자 이름—admin
  - 비밀번호 - ironport

  나중에 시스템 설정 마법사 구성에서 기본 자격 증명을 변경할 수 있습니다.
- Azure 구축에 필요한 리소스:

- 인스턴스가 속한 리소스 그룹
- 가상 네트워크 또는 서브넷
- 공용 IP 주소(사용자 인터페이스를 통해 인스턴스를 생성하는 동안 선택됨)
- 네트워크 보안 그룹
- 네트워크 보안 그룹에 추가된 인바운드 및 아웃바운드 규칙
- 개방형 가상 어플라이언스가 통신하려면 다음 포트를 사용합니다.
  - SSH용 SSH TCP 22
  - TCP 8443 UI 및 NGUI
  - TCP 3128
  - TCP 443

구축을 위해 지원되는 인스턴스 유형

Secure Web Appliance 모델에 따라 인스턴스 유형을 선택합니다.

AsyncOS 14.5 이상에서 각 모델을 구축하기 위한 권장 사항은 다음과 같습니다.

표 ***2:*** 구축을 위해 지원되는 인스턴스 유형

모델	최대 인터페이스	**Azure**
S100V 3 코어, 8GB RAM, 디스크 200GB	2	Standard_F4s_v2 Standard F4s v2에는 4개의 vCPU, 8GiB RAM이 있습니다.
S300V 5 코어, 12GB RAM, 디스크 500GB	4	Standard_F8s_v2 Standard F8s v2에는 8개의 vCPU, 16GiB RAM이 있습니다.
S600V 12 코어, 24GB RAM, 디스크 750GB	4	Standard_F16s_v2 Standard F16s v2에는 16개의 vCPU, 32GiB RAM이 있습니다.

인스턴스 세부 정보 구성

단계 **1** 리소스 그룹을 선택합니다.

단계 **2** VM 이름을 입력합니다

Azure 리소스 이름에는 특수 문자 \/""[]:|<>+=;,?*@&, 공백을 포함하거나 '_'로 시작하거나 '-'로 끝날 수 없습니다.

단계 **3** 지역을 선택합니다.

이는 리소스 그룹을 기준으로 자동으로 검색됩니다.

단계 **4** Azure Marketplace에서 이미지를 선택합니다.

단계 **5** 구축할 모델에 따라 크기를 선택합니다.

예를 들어, 인스턴스 유형 F8_S_V2는 S300V 모델 구축에 권장됩니다.

단계 **6** 비밀번호로 인증 유형을 선택합니다.

사용자 이름 및 비밀번호에 대한 문자열을 입력합니다.

참고 사용자 이름은 예약어를 포함할 수 없습니다.

그러나 구축 후에는 기본 자격 증명을 사용하여 **SSH**에 액세스할 수 있습니다.

- 사용자 이름—admin
- 비밀번호 - ironport

단계 **7** 인바운드 포트는 SSH, HTTPS 등이 될 수 있습니다.

네트워크 보안 그룹에서 동일하게 변경할 수 있습니다.

단계 **8** License type(라이선스 유형)을 **other(**기타**)**로 선택합니다.

단계 **9** SSD 또는 HDD일 수 있는 디스크를 선택합니다.

단계 **10** 가상 네트워크 및 가상 네트워크에서 구성된 서브넷을 선택합니다.

단계 **11** 맞춤형 스토리지 계정을 사용하여 관리 구성을 활성화합니다.

단계 **12** 태그를 추가한 다음 VM 인스턴스를 검토하고 생성합니다.

시작된 인스턴스 구성

단계 **1** 검색 창에서 가상 머신을 필터링합니다.

단계 **2** 가상 머신을 선택하고 VM 이름을 검색합니다.

가상 머신은 검색된 공용 IP 주소로 실행되어야 합니다.

단계 **3** 맞춤형 DNS 이름을 구성합니다.

단계 **4** 필수 포트에 대한 보안을 위해 필요한 IP 주소를 인바운드 규칙에 추가합니다.

단계 **5** SSH를 사용하여 다음 자격 증명을 사용하여 인스턴스에 연결합니다.

- 사용자 이름—admin
- 비밀번호 - ironport

단계 **6** 필요한 경우 기능 키를 추가합니다.

단계 **7** CLI를 통해 라이선스를 붙여넣거나 파일에서 로드하려면 **loadlicense** 명령을 사용합니다.

단계 **8** 인터페이스 구성을 수행하고 Azure VM DNS 이름을 사용하여 사용자 인터페이스를 사용하도록 포트 8443을 활성화합니다.

단계 **9** **Commit(**커밋**)**을 클릭합니다.

Secure Web Appliance 사용자 인터페이스에 연결

사용자 인터페이스를 사용하여 어플라이언스 소프트웨어를 구성합니다.

인스턴스를 선택하면 **Overview(**개요**)** 페이지에 공용 IP 주소가 표시됩니다. 기본 자격 증명은 다음과 같습니다.

- 사용자 이름—admin
- 비밀번호 - ironport

단계 **1** 웹 액세스 형식 `https://<hostname>:8443`.

단계 **2** **System Setup Wizard(**시스템 설정 마법사**)**를 실행합니다.

단계 **3** 컨피그레이션 파일을 업로드합니다.

단계 **4** 기능을 수동으로 구성합니다.

필요한 정보 수집을 포함하여 어플라이언스를 액세스하고 구성하는 방법은 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오. 관련 정보, 13 페이지의 내용을 참조하십시오.

라이선스 만료가 임박했을 때 알림을 보내도록 Secure Web Appliance 구성

자세한 내용은 AsyncOS 사용 설명서의 알림 관리 항목을 참조하십시오.

CLI를 사용하여 Azure 환경에 Secure Web Appliance 구축

CLI를 사용하여 Azure 환경에서 Secure Web Appliance를 구축할 수 있습니다.

다른 운영 체제에서 Azure CLI를 설치하는 단계는 여기에서 확인할 수 있습니다.https://docs.microsoft.com/en-us/cli/azure/install-azure-cli

또는 Azure 사용자 인터페이스에서 검색 창 옆에 있는 클라우드 쉘을 찾을 수 있습니다. 클라우드 쉘을 사용하여 Azure 사용자 인터페이스에서 Azure CLI 명령을 실행할 수 있습니다.

.

단계 **1** Azure 계정에 로그인하려면 Azure 콘솔에서 다음 명령을 실행합니다.

az login -u <username> -p <password>

az account set --subscription <subscription_id>

subscription_id는 스토리지 계정에서 가져올 수 있습니다.

단계 **2** 관리 인터페이스에 대한 NIC를 생성하려면 다음 명령을 실행합니다.

az network nic create --resource-group <Resource_group_name> --name <M1_interface_name> --vnet-name <Virtual_network>--subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

단계 **3** P1 인터페이스에 대한 NIC를 생성하려면 다음 명령을 실행합니다.

az network nic create --resource-group <Resource_group_name> --name <P1_interface_name > --vnet-name <Virtual_network> --subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

단계 **4** 관리 인터페이스에 대한 공용 IP를 생성하려면 다음 명령을 실행합니다.

az network public-ip create --resource-group <Resource_group_name> --name <M1-IP>

단계 **5** 데이터 인터페이스에 대한 공용 IP를 생성하려면 다음 명령을 실행합니다.

az network public-ip create --resource-group <Resource_group_name> --name <P1-IP>

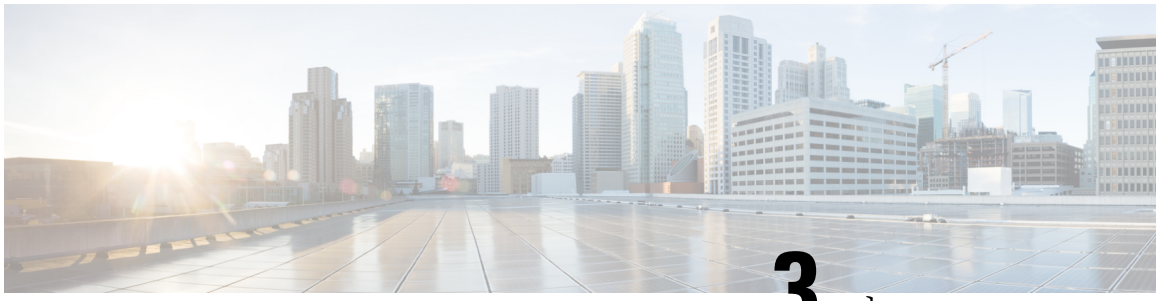
단계 **6** 생성된 공용 IP를 해당 인터페이스에 할당하려면 다음 명령을 실행합니다.

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <M1_interface_name> --name ipconfig1 --public-ip <M1-IP>

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <P1_interface_name> --name ipconfig1 --public-ip <P1-IP>

단계 **7** 관리 및 데이터 인터페이스를 사용하여 VM을 생성하려면 다음 명령을 실행합니다.

az vm create --resource-group <Resource_group_name> --name <VM_Name> --image <Image_name> --size <instance_type> --admin-username rtestuser --admin-password ironport_123 --nics <M1_interface_name > <P1_interface_name >



3 장

가상 어플라이언스 관리

가상 어플라이언스의 CLI 명령

다음은 가상 어플라이언스에 대한 CLI 명령 변경 사항입니다.

표 *3:* 가상 어플라이언스의 *CLI* 명령

명령	가상 **Secure Web Appliance**에서 지원되는지 여부	정보
loadlicense	예	가상 어플라이언스에 대한 라이선스를 설치할 수 있습니다. 라이선스를 설치하지 않으면 가상 어플라이언스에서 시스템 설정 마법사를 실행할 수 없습니다.
etherconfig	예	가상 어플라이언스에는 페어링 옵션이 포함되지 않습니다.
version	예	UDI, RAID 및 BMC 정보를 제외하고 가상 어플라이언스에 대한 모든 정보를 반환합니다.
resetconfig	예	어플라이언스에서 가상 어플라이언스 라이선스 및 기능 키를 유지합니다.
revert	예	어플라이언스에서 가상 어플라이언스 라이선스 및 기능 키를 유지합니다.
reload	예	어플라이언스에서 가상 어플라이언스 라이선스 및 기능 키를 제거합니다. 참고 이 명령은 Secure Web Appliance에만 사용할 수 있습니다.

명령	가상 **Secure Web Appliance**에서 지원되는지 여부	정보

diagnostic	예	다음의 **diagnostic** > **raid** 하위 메뉴 옵션은 정보를 반환하지 않습니다.
		`1. Run disk verify`
		`2. Monitor tasks in progress`
		`3. Display disk verify verdict`
		참고 이 명령은 Secure Web Appliance에만 사용할 수 있습니다.

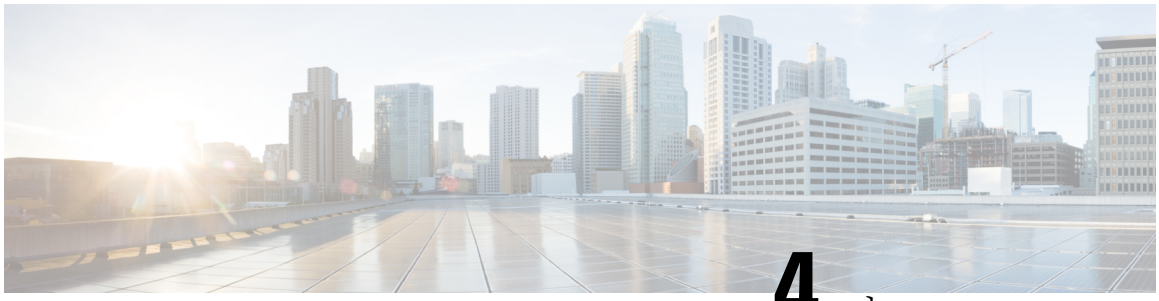
showlicense	예	라이센스 세부 정보를 봅니다. 가상 Cisco Secure Web Appliance의 경우, **featurekey** 명령을 통해 추가 정보가 제공됩니다.

Azure 모니터링

이 항목에서는 Secure Web Appliance에 대한 Microsoft Azure 모니터링에 대한 지원을 제공합니다.

표 ***4: Azure*** 모니터링

모니터링 유형	**Secure Web Appliance**에 대한 지원	코멘트
애플리케이션 인사이트	아니요	Secure Web Appliance에 대해 **Azure** 에이전트 업데이트를 사용할 수 없으므로 Application Insights를 활성화할 수 없습니다.
알림	예	맞춤형 알림과 기본 알림을 모두 사용할 수 있습니다.
로그	아니요	Secure Web Appliance에 대해 **Azure** 에이전트 업데이트를 사용할 수 없으므로 Application Insights를 활성화할 수 없습니다.
메트릭	예	—
진단 설정	아니요	보안 웹 어플라이언스에 대한 진단 설정을 활성화할 수 없습니다.



4 장

관련 정보

관련 정보

지원 옵션에 대한 정보를 비롯한 자세한 내용은 AsyncOS 릴리스 관련 설명서를 참조하십시오.

- Secure Web Appliance 사용 설명서
- Secure Web Appliance 릴리스 노트
- Secure Email 및 Web Manager 사용 설명서
- Secure Email 및 Web Manager 릴리스 노트
- Secure Email Gateway 사용 설명서
- Secure Email Gateway 릴리스 노트

Cisco TAC

추가 지원이 필요한 경우 Cisco TAC에 문의하십시오.

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html