# Firepower Device Manager를 이용한 Firepower Threat Defense Virtual 관리

이 장에서는 FDM로 관리되는 독립형 FTDv 디바이스를 구축하는 방법을 설명합니다. 고가용성 쌍을 구축하려면 FDM 설정 가이드를 참조하십시오.



# Firepower Device Manager를 이용하는 Firepower Threat Defense Virtual 관련 정보

Firepower Threat Defense Virtual(FTDv)은(는) Cisco NGFW 솔루션의 가상화된 구성 요소입니다. FTDv은 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, AMP(Advanced Malware Protection)와 같은 차세대 방화벽 서비스를 제공합니다.

일부 Firepower Threat Defense 모델이 포함된 웹 기반 디바이스 설정 마법사인 Firepower Device Manager(FDM)을(를) 사용해 FTDv을(를) 관리할 수 있습니다. FDM은(는) 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성하도록 합니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 Firepower Threat Defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

다수의 디바이스를 관리하거나 Firepower Threat Defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 Firepower Device Manager 대신 Firepower Management Center을(를) 사용하여 디바이스를 구성하십시오. 자세한 내용은 Firepower Management Center로 Firepower Threat Defense Virtual 관리를 참조하십시오.

문제 해결을 위해 관리 인터페이스에서 SSH를 사용해 FTD CLI에 액세스하거나, Firepower CLI에서 FTD에 연결할 수 있습니다.

# 기본 구성

FTDv 기본 컨피그레이션에서는 관리 인터페이스와 내부 인터페이스를 동일한 서브넷에 배치합니다. 스마트 라이선싱을 사용하고 시스템 데이터베이스로 업데이트를 가져오려면 관리 인터페이스에서 인터넷에 연결할 수 있어야 합니다.

따라서 기본 컨피그레이션은 가상 스위치의 동일한 네트워크에 Management0-0 및 GigabitEthernet0-1(내부)을 둘 다 연결할 수 있도록 설계되어 있습니다. 기본 관리 주소는 내부 IP 주소를 게이트웨이로 사용합니다. 그러므로 관리 인터페이스는 인터넷에 연결하기 위해 내부 인터페이스와 외부 인터페이스를 차례로 통과하여 라우팅합니다.

인터넷에 액세스할 수 있는 네트워크를 사용한다면 내부 인터페이스에 사용하는 것과는 다른 서브넷에 Management0-0을 연결할 수도 있습니다. 이 경우 네트워크용으로 관리 인터페이스 IP 주소 및 게이트웨이를 적절하게 구성해야 합니다.

FTDv은(는) 전원이 공급되는 첫 부팅 시 최소 4개의 인터페이스를 사용해야 합니다.

- 가상 머신의 첫 번째 인터페이스는 관리 인터페이스(Management0-0)입니다.
- 가상 머신의 두 번째 인터페이스는 진단 인터페이스(Diagnostic0-0)입니다.
- 가상 머신의 세 번째 인터페이스(GigabitEthernet0-0)는 외부 인터페이스입니다.
- 가상 머신의 네 번째 인터페이스(GigabitEthernet0-1)는 내부 인터페이스입니다.

데이터 트래픽의 경우 최대 6개 이상의 인터페이스를 추가하여 총 8개의 데이터 인터페이스를 사용할 수 있습니다. 추가 데이터 인터페이스의 경우 소스 네트워크가 올바른 대상 네트워크에 매핑되는지, 또한 각 데이터 인터페이스가 고유한 서브넷 또는 VLAN에 매핑되는지 확인합니다. VMware 인터페이스 구성을 참조하십시오.

# 초기 구성

네트워크에 보안 어플라이언스를 삽입하고 인터넷 또는 기타 업스트림 라우터에 연결하는 데 필요한 주소 구성을 포함한 FTDv 기능이 네트워크에서 올바르게 작동하는 초기 구성을 완료해야 합니다. 다음 두 가지 방법 중 하나로 시스템의 초기 구성을 수행할 수 있습니다.

- FDM 웹 인터페이스(권장)를 사용합니다. FDM는 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.
- CLI(명령줄 인터페이스) 설정 마법사를 사용합니다(선택). 초기 구성에 FDM 대신 CLI 설정 마법사를 사용할 수 있으며, 문제 해결에도 CLI를 사용할 수 있습니다. FDM을(를) 사용해 여전히 시스템을 구성, 관리, 모니터링할 수 있습니다. (선택 사항) Firepower Threat Defense CLI 마법사 시작을 참조하십시오.

다음 주제에서는 이런 인터페이스를 사용해 시스템의 초기 구성을 수행하는 방법을 설명합니다.

# Firepower Device Manager 실행

Firepower Device Manager(FDM)을(를) 사용하여 시스템을 구성, 관리 및 모니터링합니다. 브라우저를 통해 구성할 수 있는 기능은 CLI(Command Line Interface)를 통해서는 구성할 수 없습니다. 즉, 반드시 웹 인터페이스를 사용하여 보안 정책을 구현해야 합니다.

아래 브라우저의 최신 버전인 Firefox, Chrome, Safari, Edge를 사용하십시오.

참고 초기 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않는 한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

잘못된 비밀번호를 입력하고 3회 연속하여 로그인 시도에 실패할 경우, 5분 동안 어카운트가 잠깁니다. 따라서 다시 로그인을 시도하기 전에 잠시 기다려야 합니다.

프로시저

단계 **1** 브라우저를 사용하여 FDM에 로그인합니다. CLI에서 초기 컨피그레이션을 수행하지 않았다고 가정하겠습니다. **https:***ip-address*에서 Firepower Device Manager를 엽니다. 여기서 주소는 다음 중 하나입니다.

- 관리 주소. 기본적으로 대부분의 플랫폼에서 관리 인터페이스는 DHCP 클라이언트이므로 IP 주소는 DHCP 서버에 따라 달라집니다.
- FTDv가 Microsoft Azure 또는 Amazon Web Services와 같은 공용 클라우드 환경에 구축된 경우 공용 주소 풀에서 FTDv 인스턴스에 주소가 지정된 공용 IP가 자동으로 할당됩니다. 클라우드 대시보드에서 공용 IP 주소를 찾습니다.

단계 **2** 사용자 이름 **admin** 및 기본 비밀번호로 로그인합니다.

버전 7.0 이상에서 초기 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않는 한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

이전 릴리스에서 기본 관리자 비밀번호는 **Admin123**입니다.

단계 **3** 시스템에 처음으로 로그인하며 CLI 설정 마법사를 사용하지 않은 경우에는 엔드 유저 라이선스 계약을 확인 및 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다. 계속하려면 이러한 단계를 완료해야 합니다.

단계 **4** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

참고 **Next(**다음**)**를 클릭하면 설정이 디바이스에 구축됩니다. 인터페이스는 이름이 "외부"로 지정되어 "outside_zone" 보안 영역에 추가됩니다. 설정이 올바른지 확인합니다.

a) **Outside Interface(**외부 인터페이스**)** - 게이트웨이 모드 또는 라우터에 연결한 데이터 포트입니다. 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다.

**IPv4** 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다.

**IPv6** 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

b) 관리 인터페이스

**DNS** 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공개 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS(OpenDNS** 사용**)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다.

방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

참고 디바이스 설정 마법사를 사용해 Firepower Threat Defense 디바이스를 구성할 때 시스템은 아웃바운드 및 인바운드 트래픽에 대해 두 가지 기본 액세스 규칙을 제공합니다. 초기 설정 후에 다시 돌아가 이 액세스 규칙을 편집할 수 있습니다.

단계 **5** 시스템 시간 설정을 구성하고 **Next(**다음**)**를 클릭합니다.

a) 표준 시간대 - 시스템의 표준 시간대를 선택합니다.

b) **NTP** 시간 서버 - 기본 NTP 서버를 사용할지 아니면 NTP 서버의 주소를 수동으로 입력할지를 선택합니다. 백업을 제공하기 위해 여러 서버를 추가할 수 있습니다.

단계 **6** 시스템에 대한 스마트 라이선스를 구성합니다.

시스템에 필요한 라이선스를 가져오고 적용하려면 스마트 라이선스 어카운트가 있어야 합니다. 처음에는 90일 평가 라이선스를 사용하고 나중에 스마트 라이선싱을 설정할 수 있습니다.

디바이스를 바로 등록하려면 링크를 클릭하여 Smart Software Manager 어카운트에 로그인한 다음 새 토큰을 생성해 수정 상자에 복사합니다.

평가 라이선스를 사용하려면 등록 없이 **90**일 평가 기간 시작을 선택합니다. 나중에 디바이스를 등록하고 스마트 라이선스를 가져오려면 메뉴의 디바이스 이름을 클릭한 다음 **Device Dashboard(**디바이스 대시보드**)**로 이동해 **Smart Licenses(**스마트 라이선스**)** 그룹에서 링크를 클릭합니다.

단계 **7** **Finish(**마침**)**를 클릭합니다.

---

다음에 수행할 작업

- Firepower Device Manager에서 디바이스를 구성하려면 Firepower Device Manager에서 디바이스를 구성하는 방법, 4 페이지을 참조하십시오.

# Firepower Device Manager에서 디바이스를 구성하는 방법

설치 마법사를 완료하고 나면 작동 중인 디바이스에 몇 가지 기본 정책이 갖추어져 있어야 합니다.

- 내부 및 외부 인터페이스용 보안 영역
- 내부에서 외부로 이동하는 모든 트래픽을 신뢰하는 액세스 규칙
- 내부에서 외부로 이동하는 모든 트래픽을 외부 인터페이스의 IP 주소에 있는 고유한 포트로 변환하는 인터페이스 NAT 규칙입니다.
- 내부 인터페이스 또는 브리지 그룹에서 실행 중인 DHCP 서버

다음 단계에서는 구성하려는 추가적인 기능에 대한 개요가 제공됩니다. 각 단계에 대한 자세한 내용을 보려면 페이지에서 도움말 버튼(**?**)을 클릭하십시오.

프로시저

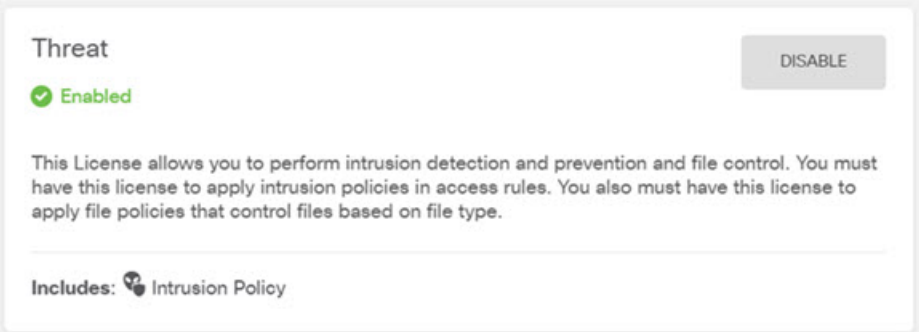
단계 **1** **Device(**디바이스**)**를 선택한 다음 **Smart License(**스마트 라이선스**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**를 클릭합니다.

사용할 각 라이선스 옵션(Threat(위협), Malware(악성코드), URL)에 대해 **Enable(**활성화**)**을 클릭합니다. 설치 시 디바이스를 등록한 경우, 원하는 RA VPN 라이선스를 활성화할 수도 있습니다. 필요 여부가 확실하지 않은 경우 각 라이선스에 대한 설명을 읽어보십시오.

등록하지 않은 경우에는 이 페이지에서 등록할 수 있습니다. **Request Register(**등록 요청**)**를 클릭하고 지침을 따릅니다. 평가 라이선스가 만료되기 전에 등록하십시오.

예를 들어, 활성화된 위협 라이선스는 다음과 같이 표시됩니다.

그림 ***1:*** 활성화된 위협 라이선스

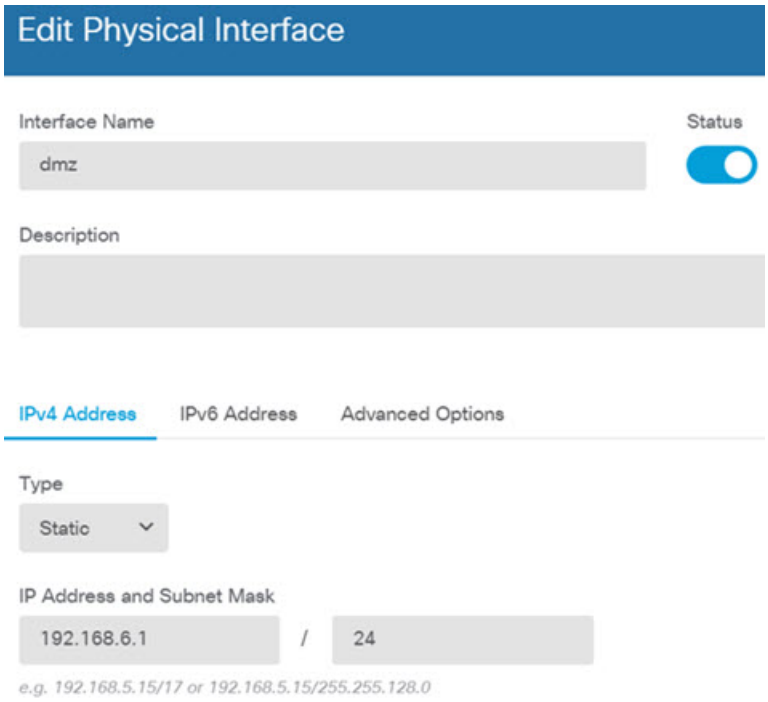



단계 **2** 다른 인터페이스를 구성한 경우 **Device(**디바이스**)**를 선택하고 **Interfaces(**인터페이스**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**를 클릭한 뒤 각 인터페이스를 구성합니다.

다른 인터페이스용 브리지 그룹을 생성하거나, 별도의 네트워크를 구성하거나 이 두 방법을 조합해 사용할 수 있습니다. 각 인터페이스의 편집 아이콘( )을 클릭하여 IP 주소 및 기타 설정을 정의합니다.

다음 예에서는 인터페이스를 웹 서버와 같이 공개적으로 액세스할 수 있는 자산을 배치하는 DMZ("Demilitarized Zone(비무장지대)")로 사용되도록 구성합니다. 완료되면 **Save(**저장**)**를 클릭합니다.

그림 *2:* 인터페이스 수정




단계 **3** 새로운 인터페이스를 구성한 경우 목차에서 **Objects(**개체**)**를 선택한 다음 **Security Zones(**보안 영역**)**를 선택합니다.

새로운 영역을 적절히 편집하거나 생성합니다. 정책은 인터페이스가 아니라 보안 영역을 기반으로 구성하기 때문에 각 인터페이스는 하나의 영역에 속해 있어야 합니다. 인터페이스를 구성할 때는 영역에 인터페이스를 배치할 수 없으므로 새 인터페이스를 생성하거나 기존 인터페이스의 용도를 변경한 후에는 항상 영역 개체를 편집해야 합니다.

다음 예에는 dmz 인터페이스에서 새 dmz-zone을 생성하는 방법이 나와 있습니다.

그림 *3:* 보안 영역 개체


단계 **4** 내부 클라이언트가 DHCP를 사용해 디바이스에서 IP 주소를 가져오도록 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**을 선택하고 **DHCP Servers(DHCP** 서버**)** 탭을 선택합니다.

내부 인터페이스에 이미 DHCP 서버가 구성되어 있지만 주소 풀을 편집하거나 삭제할 수도 있습니다. 다른 내부 인터페이스를 구성한 경우, 이러한 인터페이스에서 DHCP 서버를 설정하는 것은 매우 일반적입니다. +를 클릭하여 각 내부 인터페이스에 서버 및 주소 풀을 구성합니다.

또한 **Configuration(**컨피그레이션**)** 탭에서 클라이언트에게 제공된 WINS 및 DNS 목록을 조정할 수 있습니다. 다음 예에는 주소 풀이 192.168.4.50-192.168.4.240인 inside2 인터페이스에서 DHCP 서버를 설정하는 방법이 나와 있습니다.

그림 *4: DHCP* 서버


단계 **5** **Device(**디바이스**)**를 선택한 후 **Routing(**라우팅**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**(또는 **Create First Static Route(**첫 번째 정적 경로 생성**)**)을 클릭하고 기본 경로를 컨피그레이션합니다.

기본 경로는 일반적으로 외부 인터페이스 외에 있는 업스트림 또는 ISP 라우터를 가리킵니다. 기본 IPv4 경로는 any-ipv4(0.0.0.0/0)용인 반면, 기본 IPv6 경로는 any-ipv6(::0/0)용입니다. 사용하는 각 IP 버전에 대해 경로를 생성합니다. DHCP를 사용하여 외부 인터페이스에 대한 주소를 얻으려는 경우, 필요한 기본 경로가 이미 있을 수도 있습니다.

참고 이 페이지에서 정의하는 경로는 데이터 인터페이스 전용입니다. 이러한 경로는 관리 인터페이스에 영향을 주지 않습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 관리 게이트웨이를 설정합니다.

다음 예에는 IPv4의 기본 경로가 나와 있습니다. 이 예에서 isp-gateway는 ISP 게이트웨이의 IP 주소(ISP에서 주소를 획득해야 함)를 식별하는 네트워크 개체입니다. 이 개체는 **Gateway(**게이트웨이**)** 드롭다운 목록의 아래쪽에서 **Create New Network(**새 네트워크 생성**)**를 클릭하여 생성할 수 있습니다.

그림 *5:* 기본 라우터


단계 **6** **Policies(**정책**)**를 선택하고 네트워크의 보안 정책을 구성합니다.

디바이스 설치 마법사를 사용하면 외부 인터페이스로 이동할 때 모든 인터페이스에 대한 inside-zone, outside-zone 및 인터페이스 NAT 간의 트래픽 플로우가 가능합니다. 새 인터페이스를 구성하는 경우에도 inside-zone 개체에 이러한 인터페이스를 추가하면 이러한 인터페이스에 액세스 제어 규칙이 자동으로 적용됩니다.

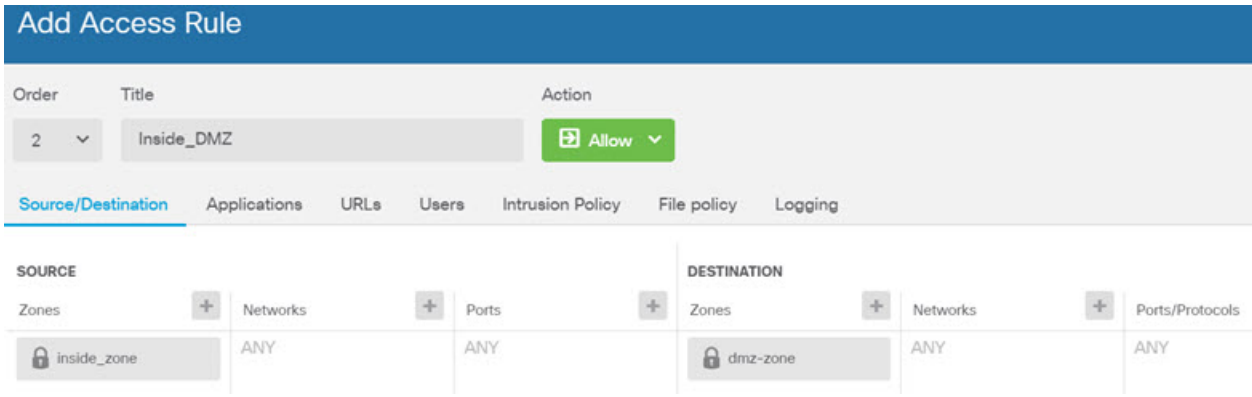
그러나 내부 인터페이스가 여러 개 있는 경우, inside-zone 간의 트래픽 플로우를 허용하기 위해 액세스 제어 규칙이 필요합니다. 다른 보안 영역을 추가하는 경우, 이러한 영역을 오고 가는 트래픽을 허용하는 규칙이 필요합니다. 이렇게 해야 변경 사항이 가장 적습니다.

또한, 다른 정책을 구성하여 추가 서비스를 제공할 수 있으며 NAT 및 액세스 규칙을 조정하여 조직에 필요한 결과를 얻을 수 있습니다. 다음과 같은 정책을 구성할 수 있습니다.

- **SSL Decryption(SSL** 암호 해독**)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.
- **Security Intelligence(**보안 인텔리전스**)** — 보안 인텔리전스 정책을 사용하여 블랙리스트에 추가된 IP 주소 또는 URL를 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 블랙리스트에 추가함으로써 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 블랙리스트가 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 블랙리스트에서 항목을 추가하거나 제거하기 위해 정책을 편집할 필요가 없습니다.
- **NAT(Network Address Translation)** - NAT 정책을 사용하여 내부 IP 주소를 외부에서 라우팅 가능한 주소로 변환합니다.
- **Access Control(**액세스 제어**)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, IP 주소, 프로토콜, 포트, 애플리케이션, URL, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 URL 필터링을 구현할 수 있습니다.
- **Intrusion(**침입**)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다.

다음 예에는 액세스 제어 정책에서 inside-zone 및 dmz-zone 간의 트래픽을 허용하는 방법이 나와 있습니다. 이 예에서는 **Logging(**로깅**)(At End of Connection(**연결 종료 시**)**이 선택된 경우)을 제외하고는 다른 어떤 탭에도 옵션이 설정되어 있지 않습니다.

그림 ***6:*** 액세스 제어 정책




단계 **7** **Device(**디바이스**)**를 선택한 다음 **Updates(**업데이트**)** 그룹에서 **View Configuration(**구성 보기**)**를 클릭하고 시스템 데이터베이스에 대한 업데이트 일정을 구성합니다.

침입 정책을 사용하는 경우 규칙 및 VDB 데이터베이스에 대한 정기 업데이트를 설정합니다. 보안 인텔리전스 피드를 사용하는 경우 피드의 업데이트 일정을 설정합니다. 모든 보안 정책의 일치 기준으로 지리적 위치를 사용하는 경우 해당 데이터베이스에 대한 업데이트 일정을 설정합니다.

단계 **8** 메뉴에서 **Deploy(구축)** 버튼을 클릭한 다음 지금 구축 버튼( )을 클릭하여 디바이스에 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다.

---

다음에 수행할 작업

Firepower Device Manager로 Firepower Threat Defense Virtual을 관리하는 방법에 대한 자세한 내용은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드 또는 Firepower Device Manager 온라인 도움말을 참조하십시오.