보안, 인터넷 액세스 및 통신 포트

다음 항목에서는 시스템 보안, 인터넷 액세스 및 통신 포트에 대한 정보를 제공합니다.

보안 요건

Firepower Management Center를 보호하려면 보호된 내부 네트워크에 설치해야 합니다. 필요한 서비스와 사용 가능한 포트만 사용하도록 FMC를 구성한 경우에도 방화벽 외부의 공격이 방어 센터(또는 매니지드 디바이스)에 도달할 수 없는지 확인해야 합니다.

FMC 및 관리되는 디바이스가 동일한 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 FMC와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 이렇게 하면 FMC에서 디바이스를 안전하게 제어할 수 있습니다. 또한 FMC에서 다른 네트워크에 있는 디바이스의 트래픽을 관리 및 격리할 수도 있도록 복수 관리 인터페이스를 구성할 수도 있습니다.

어플라이언스를 구축하는 방식과 상관없이 어플라이언스 간 통신은 암호화됩니다. 하지만 DDoS(Distributed Denial of Service) 또는 중간자 공격(man-in-the-middle attack)등으로 어플라이언스 간 통신이 중단, 차단 또는 변조될 수 없도록 방지하는 단계를 수행해야 합니다.

Cisco Cloud

FMC는 다음 기능을 위해 Cisco Cloud의 리소스와 통신합니다.

- **AMP(Advanced Malware Protection)**

  퍼블릭 클라우드는 기본적으로 구성되어 있습니다. 변경하는 방법은 AMP 옵션 변경의 내용을 참조하십시오.

- **URL** 필터링

  자세한 내용은 다음을 참조해 주십시오.

- URL 필터링 옵션
- 범주 및 평판을 사용한 URL 필터링 활성화

- **SecureX** 및 **Cisco SecureX Threat Response**의 통합

  자세한 내용은 다음에서 연결된 통합 문서를 참조하십시오.

  - Cisco SecureX와의 통합
  - 다음을 이용한 이벤트 분석 Cisco SecureX Threat Response

- 사전 지원 기능

  자세한 내용은 Cisco 지원 진단를 참조하십시오.

- **Cisco Success Network**

  자세한 내용은 Cisco Success Network를 참고하십시오.

인터넷 액세스 요구 사항

기본적으로 Firepower 어플라이언스는 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성됩니다. 어플라이언스가 인터넷에 직접 액세스하지 않도록 하려면 프록시 서버를 구성할 수 있습니다.

대부분의 경우, 인터넷에 액세스하는 것은 Firepower Management Center입니다. 하지만 때로는 매니지드 디바이스도 인터넷에 액세스합니다. 예를 들어 악성코드 방지 구성이 동적 분석을 사용하는 경우, 매니지드 디바이스는 파일을 직접 Cisco Threat Grid 클라우드에 전송합니다. 또는 디바이스를 외부 NTP 서버와 동기화할 수 있습니다.

팁 AMP for Networks 또는 AMP for Endpoints를 사용하는 경우, FMC가 액세스하는 AMP 클라우드 리소스는 위치에 따라 결정될 수 있습니다. Required Server Addresses for Proper AMP Operations Troubleshooting TechNote에는 Firepower 어플라이언스뿐 아니라 커넥터와 프라이빗 클라우드 어플라이언스 같은 Cisco AMP 구성 요소에 필요한 인터넷 리소스(고정 IP 주소 포함)가 나열되어 있습니다.

보안, 인터넷 액세스 및 통신 포트

표 ***1: Firepower*** 인터넷 액세스 요구 사항

기능	이유	리소스
AMP for Networks	악성코드 클라우드 조회.	cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.sourcefire.com cloud-sa.apjc.amp.sourcefire.com cloud-sa-589592150.us-east-1. elb.amazonaws.com
	파일 사전 분류 및 로컬 악성코드 분석을 위한 서명 업데이트를 다운로드합니다.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	동적 분석을 위해 파일을 제출합니다(매니지드 디바이스). 동적 분석 결과를 쿼리합니다(FMC).	panacea.threatgrid.com
AMP for Endpoints 통합	AMP for Endpoints가 탐지한 악성코드 이벤트를 AMP 클라우드에서 수신합니다.	api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com export.amp.sourcefire.com export.eu.amp.sourcefire.com export.apjc.amp.sourcefire.com
보안 인텔리전스	보안 인텔리전스 피드를 다운로드합니다.	intelligence.sourcefire.com
URL 필터링	URL 카테고리 및 평판 데이터를 다운로드합니다. 수동으로 URL 카테고리 및 평판 데이터를 쿼리합니다. 미분류 URL을 쿼리합니다.	database.brightcloud.com service.brightcloud.com
Cisco Smart Licensing	Cisco Smart Software Manager와 통신합니다.	tools.cisco.com
시스템 업데이트	Cisco에서 어플라이언스로 직접 업데이트를 다운로드합니다. • 시스템 소프트웨어 • 침입 규칙 • VDB(Vulnerability Database) • GeoDB(지리위치 데이터베이스)	cisco.com sourcefire.com

기능	이유	리소스
시간 동기화	구축에서 시간을 동기화합니다. 프록시 서버에서는 지원되지 않습니다.	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS 피드	대시보드에 Cisco Threat Research 블로그를 표시합니다.	blogs.cisco.com/talos cloud.google.com
Whois	외부 호스트의 whois 정보 요청 프록시 서버에서는 지원되지 않습니다.	whois 클라이언트는 쿼리할 적절한 서버를 추측하려 시도합니다. 추측할 수 없는 경우, 다음을 사용합니다. • NIC 핸들: whois.networksolutions.com • IPv4 주소 및 네트워크 이름: whois.arin.net

통신 포트 요구 사항

Firepower 어플라이언스는 포트 8305/tcp를 사용하는 양방향 SSL-암호화 통신을 사용하여 통신합니다. 이 포트는 플랫폼 내 기본 통신을 위해 반드시 열려 있어야 합니다.

다른 포트는 특정 기능에 필요한 외부 리소스에 대한 액세스뿐만 아니라 보안 관리도 허용합니다. 일반적으로 기능과 관련된 포트는 관련 기능을 활성화 또는 구성할 때까지 닫은 상태를 유지해야 합니다. 개방된 포트를 닫음으로써 구축에 어떤 영향을 미칠지 이해하기 전까지 개방된 포트를 변경하거나 닫지 마십시오.

표 ***2: Firepower*** 통신 포트 요구 사항

Port(포트)	프로토콜/기능	플랫폼	방향	세부 사항
7/UDP	UDP/감사 로깅	FMC, 클래식	아웃바운드	감사 로깅을 구성할 때 시스템 로그 서버와의 연결을 확인합니다.
22/tcp	SSH	FMC 모든 디바이스	인바운드	어플라이언스에 대한 보안 원격 연결
25/tcp	SMTP	FMC	아웃바운드	이메일 알림 및 경고 전송
53/tcp 53/udp	DNS	FMC 모든 디바이스	아웃바운드	DNS
67/udp 68/udp	DHCP	FMC 모든 디바이스	아웃바운드	DHCP

보안, 인터넷 액세스 및 통신 포트

Port(포트)	프로토콜/기능	플랫폼	방향	세부 사항
80/tcp	HTTP	FMC 7000/8000 시리즈	아웃바운드	대시보드에 RSS 피드 표시
80/tcp	HTTP	FMC	아웃바운드	URL 카테고리 및 평판 데이터 다운로드 또는 쿼리(포트 443도 필요)
80/tcp	HTTP	FMC	아웃바운드	HTTP를 통해 사용자 정의 보안 인텔리전스 다운로드
123/udp	NTP	FMC 모든 디바이스	아웃바운드	시간 동기화
161/udp	SNMP	FMC 모든 디바이스	인바운드	SNMP 폴링을 통해 MIB에 대한 액세스 허용
162/udp	SNMP	FMC 모든 디바이스	아웃바운드	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP	FMC 7000/8000 시리즈	아웃바운드	외부 인증을 위해 LDAP 서버와 통신 감지된 LDAP 사용자의 메타데이터 가져오기(FMC 전용) 구성 가능합니다.
443/tcp	HTTPS	FMC 7000/8000 시리즈	인바운드	웹 인터페이스 액세스
443/tcp	Remote Access VPN(SSL/IPSec)	FTD	인바운드	원격 사용자로부터 네트워크에 보안 VPN 연결 허용
500/udp 4500/udp	Remote Access VPN(IKEv2)	FTD	인바운드	원격 사용자로부터 네트워크에 보안 VPN 연결 허용
443/tcp	HTTPS	FMC 모든 디바이스	아웃바운드	인터넷에서 데이터 송수신 자세한 내용은 인터넷 액세스 요구 사항, 2 페이지을 참조해 주십시오.
443	HTTPS	FMC	아웃바운드	AMP 클라우드와 통신(퍼블릭 또는 프라이빗) 포트 32137에 대한 정보를 참조하십시오.
443	HTTPS	FMC	인바운드 및 아웃바운드	AMP for Networks와의 통합

보안, 인터넷 액세스 및 통신 포트

Port(포트)	프로토콜/기능	플랫폼	방향	세부 사항
514/udp	시스템 로그(알림)	FMC 모든 디바이스	아웃바운드	원격 syslog 서버에 대한 경고 전송
623/udp	SOL/LOM	FMC 7000/8000 시리즈	인바운드	SOL(Serial Over LAN) 연결을 사용하여 Lights-Out Management(LOM) 수행
885/tcp	캡티브 포털	모든 디바이스	인바운드	캡티브 포털 ID 소스와 통신
1500/tcp 2000/tcp	데이터베이스 액세스	FMC	인바운드	서드파티 클라이언트의 이벤트 데이터베이스에 대한 읽기 전용 액세스 허용
1812/udp 1813/udp	RADIUS	FMC 7000/8000 시리즈	아웃바운드	외부 인증 및 어카운트 관리를 위해 RADIUS 서버와 통신 구성 가능합니다.
5222/tcp	ISE	FMC	아웃바운드	ISE ID 소스와 통신
8302/tcp	eStreamer	FMC 7000/8000 시리즈	인바운드	eStreamer 클라이언트와 통신
8305/tcp	어플라이언스 통신	FMC 모든 디바이스	Both(모두)	구축 어플라이언스 간 보안 통신. 구성 가능합니다. 이 포트를 변경하는 경우 구축의 모든 어플라이언스에 대해 이 포트를 변경해야 합니다. 기본값을 유지하는 것이 좋습니다.
8307/tcp	호스트 입력 클라이언트	FMC	인바운드	호스트 입력 클라이언트와 통신
8989/tcp	Cisco 지원 진단	FMC FTD	Both(모두)	인증된 요청을 수락하고 사용량 정보 및 통계를 전송합니다.
32137/tcp	AMP for Networks	FMC	아웃바운드	Cisco AMP 클라우드와 통신 이 구성은 레거시 구성입니다. 기본값(443)을 사용하는 것이 좋습니다.

관련 항목

- LDAP 인증 서버 식별
- FMC에 대한 LDAP 외부 인증 개체 추가
- RADIUS 연결 설정 구성
- FMC에 대한 RADIUS 외부 인증 개체 추가