보안, 인터넷 액세스 및 통신 포트

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

보안 요건

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

management center 및 관리되는 디바이스가 동일한 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 management center와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 이렇게 하면 management center에서 디바이스를 안전하게 제어할 수 있습니다. 또한 management center에서 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

management center는 다음 기능을 위해 Cisco Cloud의 리소스와 통신합니다.

- **AMP(Advanced Malware Protection)**

  퍼블릭 클라우드는 기본적으로 구성되어 있습니다. 변경하는 방법은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *AMP* 옵션 변경을 참조하십시오.

- **URL** 필터링

자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *URL* 필터링 장을 참조하십시오.

- **Cisco Umbrella** 연결

  자세한 내용은 Cisco Umbrella DNS 정책를 참고하십시오.

인터넷 액세스 요구 사항

기본적으로 시스템은 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 연결하도록 구성됩니다. 어플라이언스가 인터넷에 직접 액세스하지 않도록 하려면 프록시 서버를 구성할 수 있습니다. 대부분의 기능에서 사용자의 위치에 따라 시스템이 액세스하는 리소스가 결정될 수 있습니다.

대부분의 경우, 인터넷에 액세스하는 것은 management center입니다. 고가용성 쌍의 두 management center 모두 인터넷에 액세스할 수 있어야 합니다. 기능에 따라 두 피어가 모두 인터넷에 액세스하는 경우도 있고 활성 피어만 인터넷에 액세스하는 경우도 있습니다.

경우에 따라 매니지드 디바이스도 인터넷에 액세스합니다. 예를 들어 악성코드 방지 구성이 동적 분석을 사용하는 경우, 매니지드 디바이스는 파일을 직접 Secure Malware Analytics 클라우드에 전송합니다. 또는 디바이스를 외부 NTP 서버와 동기화할 수 있습니다.

또한 웹 분석 추적을 비활성화하지 않았다면 브라우저가 Google 웹 분석 서버에 연결하여 개인 식별이 불가능한 사용 데이터를 Cisco에 전송할 수 있습니다.

표 *1:* 인터넷 액세스 요구 사항

기능	이유	**Management Center** 고가용성	리소스
악성코드 대응	악성코드 클라우드 조회.	두 피어 모두 조회를 수행합니다.	적절한 Cisco Secure Endpoint 및 악성코드 분석 작업에 필요한 서버 주소를 참조하십시오.
	파일 사전 분류 및 로컬 악성코드 분석을 위한 서명 업데이트를 다운로드합니다.	활성 피어가 다운로드하고, 대기에 동기화합니다.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	동적 분석을 위해 파일을 제출합니다(매니지드 디바이스). 동적 분석 결과를 쿼리합니다(management center).	두 피어 모두 동적 분석 보고서를 쿼리합니다.	fmc.api.threatgrid.com fmc.api.threatgrid.eu

기능	이유	**Management Center** 고가용성	리소스
AMP for Endpoints 통합	AMP for Endpoints가 탐지한 악성코드 이벤트를 AMP 클라우드에서 수신합니다. 시스템이 탐지한 악성코드 이벤트를 AMP for Endpoints에 표시합니다. AMP for Endpoints에서 생성된 중앙 집중식 파일 차단 및 허용 목록을 사용하여 AMP 클라우드의 속성을 재정의합니다.	두 피어 모두 이벤트를 수신합니다. 또한 두 피어 모두에서 클라우드 연결을 구성해야 합니다(구성이 동기화되지 않음).	적절한 Cisco Secure Endpoint 및 악성코드 분석 작업에 필요한 서버 주소를 참조하십시오.
보안 인텔리전스	보안 인텔리전스 피드를 다운로드합니다.	활성 피어가 다운로드하고, 대기에 동기화합니다.	intelligence.sourcefire.com
URL 필터링	URL 카테고리 및 평판 데이터를 다운로드합니다. 수동으로 URL 카테고리 및 평판 데이터를 쿼리(조회)합니다. 미분류 URL을 쿼리합니다.	활성 피어가 다운로드하고, 대기에 동기화합니다.	URL: • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com IPV4 차단: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 차단: • 2a04: e4c7: ffff::/48 • 2a04: e4c7: fffe::/48
Cisco Smart Licensing	Cisco Smart Software Manager와 통신합니다.	활성 피어가 통신합니다.	tools.cisco.com:443 www.cisco.com
Cisco Success Network	사용 정보 및 통계를 전송합니다.	활성 피어가 통신합니다.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com

기능	이유	**Management Center** 고가용성	리소스
Cisco Support Diagnostics	인증된 요청을 수락하고 사용량 정보 및 통계를 전송합니다.	활성 피어가 통신합니다.	api-sse.cisco.com:8989
시스템 업데이트	Cisco에서 management center로 직접 업데이트를 다운로드합니다. • 시스템 소프트웨어 • 침입 규칙 • VDB(Vulnerability Database) • GeoDB(지리위치 데이터베이스)	활성 피어에서 침입 규칙, VDB, GeoDB를 업데이트한 다음 대기에 동기화합니다. 각 피어에서 독립적으로 시스템 소프트웨어를 업그레이드합니다.	cisco.com sourcefire.com
SecureX threat response 통합	해당 통합 가이드를 참조하십시오.		
시간 동기화	구축에서 시간을 동기화합니다. 프록시 서버에서는 지원되지 않습니다.	외부 NTP 서버를 사용하는 모든 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.	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.	RSS 피드를 표시하는 모든 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.	blog.talosintelligence.com blogs.cisco.com feeds.feedburner.com
Whois	외부 호스트의 whois 정보 요청 프록시 서버에서는 지원되지 않습니다.	whois 정보를 요청하는 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.	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

management center는 포트 8305/tcp의 양방향 SSL 암호화 통신 채널을 사용하여 매니지드 디바이스와 통신합니다. 이 포트는 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:* 통신 포트 요구 사항

포트	프로토콜/기능	플랫폼	방향	세부 사항
53/tcp 53/udp	DNS		아웃바운드	DNS
67/udp 68/udp	DHCP		아웃바운드	DHCP
123/udp	NTP		아웃바운드	시간 동기화
162/udp	SNMP		아웃바운드	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP		아웃바운드	외부 인증을 위해 LDAP 서버와 통신 감지된 LDAP 사용자의 메타데이터 가져오기(Management Center 전용) 구성 가능합니다.
443/tcp	HTTPS	Management Center	인바운드	management center를 온프레미스 Secure Device Connector로 온보딩하는 경우 포트 443에 대한 인바운드 연결을 허용합니다.
443/tcp	HTPS	Management Center	아웃바운드	Cloud Connector를 사용하여 management center를 CDO에 온보딩하는 경우 포트 443에서 아웃바운드 트래픽을 허용합니다.
443/tcp	HTPS	Management Center	아웃바운드	SecureX를 사용하여 management center를 온보딩하는 경우 포트 443에 대한 아웃바운드 연결을 허용합니다.
443/tcp	HTTPS		아웃바운드	인터넷에서 데이터 송수신
514/udp	시스템 로그(알림)		아웃바운드	원격 syslog 서버에 대한 경고 전송
1812/udp 1813/udp	RADIUS		아웃바운드	외부 인증 및 어카운트 관리를 위해 RADIUS 서버와 통신 구성 가능합니다.

포트	프로토콜/기능	플랫폼	방향	세부 사항
8305/tcp	어플라이언스 통신		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.

관련 항목

CDO에 대한 LDAP 외부 인증 개체 추가

CDO에 대한 RADIUS 외부 인증 개체 추가