클래식 디바이스에 대한 플랫폼 설정

다음 주제에서는 Firepower 플랫폼 설정 및 클래식 디바이스에서 설정하는 방법에 대해 설명합니다.

클래식 디바이스에 대한 플랫폼 설정 관련 정보

매니지드 디바이스용 플랫폼 설정은 정책 기반이며, 따라서 같은 구성을 여러 디바이스에 적용할 수 있습니다. *Firepower* 플랫폼 설정 정책을 클래식 디바이스와 함께 사용:

- 7000/8000 시리즈 디바이스
- ASA FirePOWER 모듈
- NGIPSv

FMC의 경우에는 이러한 설정 중 상당수가 시스템 구성에서 처리됩니다. 시스템 구성 섹션을 참조하십시오.

표 ***1:*** 클래식 디바이스에 대한 ***Firepower*** 플랫폼 설정

플랫폼 설정	설명	확인
액세스 목록	특정 포트에서 시스템에 액세스할 수 있는 컴퓨터를 제어합니다.	클래식 디바이스에 대한 액세스 목록 구성, 3 페이지
감사 로그	감사 로그를 외부 호스트로 보내도록 시스템을 구성합니다.	클래식 디바이스에서의 감사 로그 스트리밍, 4 페이지

플랫폼 설정	설명	확인
외부 인증	외부 RADIUS, LDAP 또는 Microsoft Active Directory 저장소에 의해 인증된 7000/8000 시리즈 디바이스 사용자의 기본 사용자 권한을 설정합니다.	7000/8000 시리즈 디바이스에 대한 외부 인증 활성화, 6 페이지
언어	7000/8000 시리즈 디바이스의 웹 인터페이스에 다른 언어를 지정합니다.	7000/8000 시리즈 웹 인터페이스 언어 설정, 8 페이지
로그인 배너	사용자가 로그인 때 나타나는 사용자 정의 로그인 배너를 만듭니다.	클래식 디바이스에 대한 로그인 배너 맞춤 설정 , 8 페이지
셸 시간 초과	비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 분 단위로 구성합니다.	클래식 디바이스에 대한 세션 시간 초과 구성, 10 페이지
SNMP	SNMP(Simple Network Management Protocol) 폴링을 활성화합니다.	클래식 디바이스에서의 SNMP 폴링 구성, 11 페이지
STIG 컴플라이언스	미 국방부에서 정한 특정 요구 사항 준수 설정을 활성화합니다.	STIG 컴플라이언스
시간 동기화	시스템에 대한 시간 동기화를 관리합니다.	NTP 서버와 클래식 디바이스의 시간 동기화, 9 페이지

클래식 디바이스에 대한 플랫폼 설정 요구 사항

라이선스 요건

없음

모델 요구 사항

모든 클래식 디바이스에 Firepower 플랫폼 설정 정책을 적용할 수 있습니다.

일부 플랫폼 설정은 7000/8000 시리즈 디바이스에만 적용되는데, 외부 인증 설정, 표시 언어, 세션 시간 초과 등의 웹 인터페이스가 있는 디바이스이기 때문입니다. 이 설정을 ASA FirePOWER나 NGIPSv에 적용하면 아무런 효과도 발생하지 않습니다.

7000/8000 시리즈 디바이스의 로컬 웹 인터페이스에 로그인해 비정책 기반 시스템 구성을 이용할 수도 있습니다. 7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성, 12 페이지의 내용을 참조하십시오.

도메인 요구 사항

없음

모든 도메인 레벨에 Firepower 플랫폼 설정 정책을 적용할 수 있습니다.

클래식 디바이스에 대한 플랫폼 설정 구성

매니지드 디바이스용 플랫폼 설정은 정책 기반이며, 따라서 같은 구성을 여러 디바이스에 적용할 수 있습니다. Firepower 플랫폼 설정 정책을 클래식 디바이스와 함께 사용:

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

클래식 디바이스에 대한 플랫폼 설정 관련 정보, 1 페이지 및 플랫폼 설정 정책 생성를 참조하십시오.

단계 **2** **Policy Assignment(**정책 할당**)**를 클릭하여 정책을 구축할 **Available Devices(**사용 가능한 디바이스**)**를 선택합니다.

단계 **3** 정책에 추가를 클릭(또는 끌어서 놓기)하여 선택한 디바이스를 추가합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

클래식 디바이스에 대한 액세스 목록 구성

기본적으로 Firepower 디바이스에 대한 액세스는 제한되지 않습니다. 포트 22(SSH)는 CLI 액세스를 지원합니다. 7000/8000 시리즈 디바이스의 경우, 포트 443(HTTPS)은 웹 인터페이스 액세스도 지원합니다.

더 안전한 환경에서 작동하려면, 특정 IP 주소의 액세스를 추가하는 방법을 고려하십시오. 포트 161을 통해 SNMP 정보를 폴링할 수 있는 액세스 권한을 추가할 수도 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** 액세스 목록을 클릭합니다.

단계 **3** 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules(**규칙 추가**)**를 클릭합니다.

단계 **4** **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 모두를 입력하세요.

단계 **5** **SSH**, **HTTPS**, **SNMP** 또는 이 옵션의 조합을 선택하여 이 IP 주소에 활성화할 포트를 지정합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

클래식 디바이스에서의 감사 로그 스트리밍

Firepower 어플라이언스는 사용자 상호작용의 기록(또는 감사 로그)을 생성합니다. 이러한 감사 로그를 시스템 로그나 HTTP 서버에 스트리밍할 수 있습니다. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있음에 유의하십시오.

팁 7000/8000 시리즈 디바이스에서는 디바이스의 웹 인터페이스인 시스템 감사에서 감사 로그를 검토할 수도 있습니다.

감사 로그의 형식은 다음과 같습니다.

```
timestamp host [tag] appliance_name: username@ip_address, subsystem, action
```

예를 들면 다음과 같습니다.

```
Mar 01 14:45:24 localhost [FIREPOWER] MyFirepowerAppliance: admin@10.1.1.2, System >
Configuration, Page View
```

태그는 선택 사항이며 사용자가 구성할 수 있습니다. 또한 시스템 로그 이벤트에는 선택적인 기능 및 심각도가 있습니다..

시작하기 전에

감사 로그를 스트림할 서버 또는 서버 모음과 디바이스가 통신할 수 있는지 확인합니다. 시스템 로그 스트리밍의 경우, 구성을 저장할 때 시스템은 시스템 로그 서버에 연결할 수 있는지를 포트 7/UDP를 사용하여 확인합니다. 그런 다음 시스템은 포트 514/UDP를 사용 하 여 감사 로그를 스트리밍합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Audit Log(**감사 로그**)**를 클릭하여 감사 로그 스트리밍을 구성합니다.

시스템 로그 스트리밍:

a) **Send Audit Log To** 시스템 로그 를 사용으로 설정 합니다.
b) 시스템 로그 서버에 대 한 호스트 정보 (IPv4 주소 또는 정규화된 이름)를 제공 합니다.

c) **Facility(**시설**)**(시스템 로그 알림 시설) 및**Severity(**심각도**)**(Syslog 심각도 레벨)를 선택합니다.

주의 **Send Audit Log to Syslog(**시스템 로그에 감사 로그 보내기**)**를 활성화하고 호스트 정보를 제공할 경우, 시스템 로그 메시지는 감사 로그 외에 설정된 호스트로도 전송됩니다. 감사 로그에서 시스템 로그 필터링, 5 페이지의 내용을 참조하십시오.

HTTP 스트리밍:

a) **Send Audit Log to HTTP Server(**감사 로그를 **HTTP** 서버로 전송**)**를 **Enabled(**활성화**)**로 설정합니다.

b) 감사 로그를 전송할 **URL to Post Audit(**사후 감사를 위한 **URL)**를 입력합니다. HTTPS가 지원됩니다.

URL은 다음과 같은 HTTP POST 변수를 기대하는 리스너 프로그램에 해당해야 합니다. `subsystem`, `actor`, `event_type`, `message`, `action_source_ip`, `action_destination_ip`, `result`, `time`, `tag`(제공되는 경우)

단계 **3** (선택 사항) 각 메시지에 포함할 **Tag(**태그**)**를 입력합니다. 예를 들어 Firepower 감사 로그에 **`FIREPOWER`**라는 태그를 지정할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.
시스템 로그 스트리밍을 구성했다면, 시스템은 시스템 로그 서버에 연결할 수 있는지를 확인합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

- (선택 사항) 시스템 로그 서버로의 감사 로그 스트리밍을 활성화하고 감사 로그에서 시스템 로그 메시지를 필터링하려는 경우: 감사 로그에서 시스템 로그 필터링, 5 페이지.

감사 로그에서 시스템 로그 필터링

Send Audit Log to Syslog(Syslog에 감사 로그 보내기**)**를 활성화하고 호스트 정보를 제공할 경우, 시스템 로그 메시지는 감사 로그 외에 설정된 호스트로도 전송됩니다. 이 동작은 Firepower 플랫폼 설정 정책을 구축할 때 `/etc/syslog-ng.d/syslog-tls.conf`가 생성되어 감사 로그만 전송하는 대신 시스템 로그 메시지가 설정된 호스트로 전달/전송됩니다.

감사 정책에 이러한 시스템 로그 레코드가 필요하지 않은 경우 해당 시스템 로그가 설정된 호스트로 스트리밍되지 않도록 할 수 있습니다. 감사 로그에서 시스템 로그를 필터링하려면 어플라이언스의 **admin** 사용자 계정에 대한 액세스 권한이 있어야 하며, 어플라이언스의 콘솔에 액세스하거나 SSH(Secure Shell)를 열 수 있어야 합니다.

⚠

주의 권한이 있는 사용자만 어플라이언스 및 **admin** 계정에 액세스할 수 있습니다.

프로시저

단계 1 `/etc/syslog-ng.conf` 파일에서 `@include "/etc/syslog-ng.d/*.conf"` 줄을 주석 처리합니다.

예제:

```
#@include "/etc/syslog-ng.d/*.conf"
```

단계 2 시스템 로그 설정 파일을 다시 로드합니다. `syslog-ng-ctl reload` 명령을 사용하여 애플리케이션을 재시작하지 않고 설정 파일을 다시 로드합니다.

예제:

```
syslog-ng-ctl reload
```

7000/8000 시리즈 디바이스에 대한 외부 인증 활성화

디바이스 플랫폼 설정을 사용하여 7000/8000 시리즈 디바이스 사용자가 로컬 데이터베이스를 사용하는 대신 LDAP 또는 RADIUS 서버에 인증하게 합니다.

시작하기 전에

외부 인증 개체를 구성합니다. 외부 인증의 내용을 참조하십시오.

프로시저

단계 1 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 2 **External Authentication(**외부 인증**)**을 클릭합니다.

단계 3 **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 4 외부에서 인증된 사용자에게 허용할 기본 권한을 정의하기 위한 사용자 역할을 **Default User Role(**기본 사용자 역할**)** 드롭다운 목록에서 선택합니다.

단계 5 외부 서버를 사용하여 CLI 또는 셸 액세스 계정도 인증하려면 **Shell Authentication(**셸 인증**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 6 CAC 인증 및 권한 부여를 활성화하려면 **CAC Authentication(CAC** 인증**)** 드롭다운 목록에서 사용 가능한 CAC 인증 개체를 선택합니다.

자세한 내용은 CAC 인증을 참고하십시오.

단계 7 사용할 각 외부 인증 개체 옆의 확인란을 선택합니다. 객체를 1개 이상 활성화하는 경우, 사용자가 지정된 순서대로 서버에 대해 확인됩니다. 다음 단계를 참조하고 서버를 재정렬합니다.

셸 인증을 활성화 하는 경우에 셸 액세스 필터를 포함 하는 외부 인증 개체를 활성화 해야 합니다. CLI/셸 액세스 사용자는 인증 객체가 목록에서 순위가 가장 높은 서버에 대해 인증할 수 있습니다.

CLI 및 CAC 인증이 모두 필요한 경우 각 용도별로 별도의 인증 개체를 사용해야 합니다.

단계 **8** (선택 사항) 위쪽 및 아래쪽 화살표를 사용해 인증 요청이 발생할 때 인증 서버에 액세스하는 순서를 변경합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

7000/8000 시리즈 디바이스에 대한 외부 인증 관련 정보

외부 인증 서버를 참조하는 인증 객체를 생성하는 경우, 매니지드 디바이스에 로그인한 사용자가 해당 서버에 대해 인증을 받도록(로컬 데이터베이스를 사용하는 대신) 외부 인증서를 활성화할 수 있습니다.

외부 인증을 활성화하면 시스템이 LDAP 또는 RADIUS 서버의 사용자에 대해 사용자 자격 증명을 확인합니다. 또한 사용자의 로컬 내부 인증이 활성화되었는데 내부 데이터베이스에 사용자 자격 증명이 없으면, 시스템은 일치하는 자격 증명 집합을 외부 서버에서 확인합니다. 여러 시스템에서 사용자의 사용자 이름이 동일하면 모든 서버에서 모든 비밀번호가 작동합니다. 그러나 사용 가능한 외부 인증 서버에서 인증이 실패하면 시스템은 로컬 데이터베이스를 다시 확인하지 않습니다.

외부 인증을 활성화하는 경우, 외부에서 계정이 인증되는 사용자에 대해 기본 사용자 역할을 설정할 수 있습니다. 역할을 결합할 수 있는 한 여러 역할을 선택할 수 있습니다. 예를 들어 회사의 Network Security 그룹의 사용자만 검색하는 외부 인증을 활성화하는 경우, Security Analyst 역할을 포함하도록 기본 사용자 역할을 설정할 수 있습니다. 그러면 추가 사용자 구성 없이도 사용자가 수집된 이벤트 데이터에 액세스할 수 있습니다. 그러나 외부 인증에서 보안 그룹 외에 다른 직원의 레코드를 검색하는 경우에는 기본 역할을 선택하지 않은 상태로 둘 수 있습니다.

액세스 역할을 선택하지 않으면 사용자는 로그인할 수 있지만 어떤 기능에도 액세스할 수 없습니다. 사용자가 로그인을 시도하면 해당 계정이 User Management 페이지**(System(**시스템**)** > **Users(**사용자**))**에 나열됩니다. 여기에서 추가 권한을 허용하도록 계정 설정을 수정할 수 있습니다.

팁 하나의 사용자 역할을 사용하도록 시스템을 구성하고 적용한 다음 나중에 다른 기본 사용자 역할을 사용하도록 구성을 수정하면, 계정을 수정하거나 삭제하고 다시 생성하기 전에는 수정 전에 생성된 사용자 계정에 첫 번째 사용자 역할이 그대로 유지됩니다.

CLI 액세스 또는 CAC 인증 및 권한 부여를 위해 LDAP 서버에 대해 인증할 수 있는 사용자 집합을 지정하려면 각각에 대해 별도의 인증 개체를 생성하여 개체를 개별적으로 활성화해야 합니다.

내부에서 인증되는 사용자가 로그인을 시도하면 시스템은 해당 사용자가 로컬 사용자 데이터베이스에 있는지를 우선 확인합니다. 사용자가 있으면 시스템은 로컬 데이터베이스에서 사용자 이름과 비밀번호를 확인합니다. 일치가 확인되면 로그인이 성공합니다. 그러나 로그인이 실패하고 외부 인증이 활성화되면 시스템은 구성에 명시된 인증 순서에 따라 각 외부 인증 서버에서 사용자를 확인합니다. 사용자 이름 및 비밀번호가 외부 서버의 결과와 일치하면 시스템은 사용자를 해당 인증 객체에 대한 기본 권한이 있는 외부 사용자로 변경합니다.

외부 사용자가 로그인을 시도하면 시스템은 외부 인증 서버에 대해 사용자 이름과 비밀번호를 확인합니다. 일치가 확인되면 로그인이 성공합니다. 로그인이 실패하면 사용자 로그인 시도가 거절됩니다. 외부 사용자는 로컬 데이터베이스의 사용자 목록을 기준으로 인증할 수 없습니다. 사용자가 새로운 외부 사용자이면 외부 인증 객체로부터의 기본 권한과 함께 로컬 데이터베이스에 외부 사용자 계정이 생성됩니다.

7000/8000 시리즈 웹 인터페이스 언어 설정

여기서 지정하는 언어는 로그인하는 모든 사용자에 대한 웹 인터페이스에 사용됩니다. 다음 언어를 선택할 수 있습니다.

- 영어
- 일본어

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Language**를 클릭합니다.

단계 **3** 사용하려는 언어를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

클래식 디바이스에 대한 로그인 배너 맞춤 설정

클래식 디바이스의 CLI 로그인 배너를 사용자 지정할 수 있습니다. 7000/8000 시리즈 디바이스의 경우 로그인 배너는 웹 인터페이스에도 표시됩니다. 로그인 배너가 너무 크거나 오류가 발생하면, 시스템에서 배너를 표시하려고 시도할 때 CLI 세션이 실패할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Login Banner(**로그인 배너**)**를 선택합니다.

단계 **3** **Custom Login Banner(**사용자 정의 로그인 배너_ 필드에서 사용하려는 로그인 배너 텍스트를 입력합니다.

시스템은 탭 간격을 유지하지 않습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

NTP 서버와 클래식 디바이스의 시간 동기화

Firepower Management Center 및 매니지드 디바이스에서 시스템 시간을 동기화하는 작업은 성공적인 작업을 위해 반드시 필요합니다.구축에 FTD 디바이스가 포함된다면 Threat Defense를 위한 NTP 시간 동기화 구성의 내용을 참조하십시오.

디바이스는 NTPv4를 지원합니다.

⚠

주의 시간이 FMC 및 매니지드 디바이스 간에 동기화되지 않으면 의도하지 않은 결과가 발생할 수 있습니다.

구축이 끝나면, 매니지드 디바이스를 구성된 NTP 서버와 동기화하는 데 몇 분 정도 걸릴 수 있습니다.

시작하기 전에

사용하려는 NTP 서버 또는 서버 모음과 통신할 수 있는지 확인합니다. 다음 중 하나를 수행할 수 있습니다.

- (권장) FMC와 동일한 NTP 서버인 FMC의 시간을 NTP 서버와 동기화을(를) 사용합니다.

  FMC와 NTP 서버 간의 보안 연결을 구성하더라도(인증된 **NTP** 서버만 사용), 해당 서버에 대한 디바이스 연결은 인증을 사용하지 않습니다.

  이 옵션을 선택하면 디바이스가 설정된 NTP 서버에서 직접 시간을 가져옵니다. 어떤 이유로든 디바이스의 설정된 NTP 서버에 연결할 수 없는 경우, 시간을 FMC와 동기화합니다.

- 디바이스가 NTP 서버에 연결할 수 없거나 조직에 NTP 서버가 없는 경우에는 다음 절차에 설명된 대로 **Via NTP from Management Center(**관리 센터에서 **NTP**를 통해**)** 옵션을 사용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Time Synchronization(**시간 동기화**)**을 클릭합니다.

단계 **3** 시간이 동기화되는 방법을 지정합니다.

- **Via NTP from(NTP**를 통해**)** - Firepower Management Center가 네트워크에서 NTP 서버를 사용 중인 경우, 이 옵션을 선택하고 정규화된 DNS 이름(예: ntp.example.com) 또는 FMC의 **System(**시스템**) > Configuration(**구성**) > Time Synchronization(**시간 동기화**)**에서 지정한 동일한 NTP 서버의 IPv4 또는 IPv6 주소를 입력합니다. NTP 서버에 연결할 수 없는 경우, Firepower Management Center는 NTP 서버로 작동합니다.
- **Via NTP from Management Center(**관리 센터에서 **NTP**를 통해**)**: (기본값) 매니지드 디바이스는 Firepower Management Center에 대해 설정한 NTP 서버에서 시간을 가져오고 (인증된 NTP 서버 제외) 시간을 해당 서버와 직접 동기화합니다. 그러나 다음 중 하나라도 해당하는 경우, 매니지드 디바이스는 Firepower Management Center에서 시간을 동기화합니다.
  - 디바이스에서 Firepower Management Center의 NTP 서버에 연결할 수 없습니다.
  - Firepower Management Center에 인증되지 않은 서버가 없습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

클래식 디바이스에 대한 세션 시간 초과 구성

무인 로그인 세션은 보안 위험이 될 수 있습니다. 비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 구성할 수 있습니다. 최대값은 24시간 또는 1440분입니다.

프로시저

단계 **1** **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Shell Timeout(**셸 시간 초과**)**를 클릭합니다.

단계 **3** 셸 시간 제한**(**분**)**을 입력합니다.

단계 **4** 세션 시간 제한 구성

- 웹 인터페이스(7000/8000 시리즈에만 해당): 브라우저 세션 시간 제한**(**분**)**을 입력합니다.

  시스템을 오랫동안 패시브 방식으로 안전하게 모니터링하려는 상황이라면, 특정 웹 인터페이스 사용자를 시간 제한에서 제외할 수 있습니다. 자세한 내용은 사용자 어카운트 로그인 옵션를 참고하십시오.

- CLI: 셸 시간 제한**(**분**)**을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

클래식 디바이스에서의 SNMP 폴링 구성

단순 네트워크 관리 프로토콜(SNMP) 폴링을 이용하면 연락처, 관리, 위치, 서비스 정보, IP 주소 지정 및 라우팅 정보, 전송 프로토콜 사용 통계 등의 시스템 세부 사항을 포함하는, Firepower 디바이스의 표준 MIB(management information base)에 액세스할 수 있습니다. 7000/8000 시리즈 디바이스에 대한 추가 MIB는 물리적 인터페이스, 논리적 인터페이스, 가상 인터페이스, ARP, NDP, 가상 브리지, 가상 라우터 등을 통과하는 트래픽에 대한 통계를 포함합니다. SNMP 폴링을 활성화한다고 해서 시스템에서 SNMP 트랩을 전송하지는 않습니다. MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐입니다.

시스템은 SNMPv1, v2 및 v3을 지원합니다. SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3은 읽기 전용 사용자만 지원합니다. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

시작하기 전에

시스템 폴링에 사용할 각 컴퓨터에 대해 SNMP 액세스를 추가합니다. 클래식 디바이스에 대한 액세스 목록 구성, 3 페이지의 내용을 참조하십시오.

참고 SNMP MIB에는 구축을 공격하는 데 사용할 수 있는 정보가 있습니다. Cisco에서는 MIB를 폴링하는 데 사용하는 특정 호스트에 대한 SNMP 액세스용 액세스 목록을 제한할 것을 권장합니다. 또한 SNMPv3을 사용하고 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것도 권장합니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 2 **SNMP**를 클릭합니다.

단계 3 **SNMP Version(SNMP** 버전**)** 드롭다운 목록에서, 사용할 SNMP 버전을 선택합니다.

- **Version(**버전**) 1** 또는 **Version(**버전**) 2**: 커뮤니티 문자열 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- **Version 3(**버전 **3)**: **Add User(**사용자 추가**)**를 클릭하여 사용자 정의 페이지를 표시합니다. SNMPv3는 읽기 전용 사용자 및 AES128 암호화만 지원합니다.

단계 4 사용자 이름을 입력합니다.

단계 5 **Authentication Protocol(**인증 프로토콜**)** 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

단계 **6** **Authentication Password(**인증 비밀번호**)** 필드에 SNMP 서버와 함께 인증에 필요한 비밀번호를 입력합니다.

단계 **7** **Verify Password(**비밀번호 확인**)** 필드에 인증 비밀번호를 다시 입력합니다.

단계 **8** 사용할 비공개 프로토콜을 **Privacy Protocol** 목록에서 선택하거나, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택합니다.

단계 **9** **Privacy Password(**프라이버시 비밀번호**)** 필드에 SNMP 서버에 필요한 SNMP 프라이버시 키를 입력합니다.

단계 **10** **Verify Password(**비밀번호 확인**)** 필드에 프라이버시 비밀번호를 다시 입력합니다.

단계 **11** **Add(**추가**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성

7000/8000 시리즈 디바이스의 로컬 웹 인터페이스에 로그인해 비정책 기반 시스템 구성을 이용할 수 있습니다. 이러한 구성은 대부분 병렬 FMC 시스템 구성으로, FMC 시스템 구성 장인 시스템 구성에서 설명합니다.

표 ***2: 7000/8000*** 시리즈 디바이스에 대한 로컬 시스템 구성

시스템 구성	설명	확인
검증 번경	지난 24시간 동안의 시스템 변경 사항에 대한 상세한 보고서를 전송합니다.	검증 번경
콘솔 구성	VGA 또는 시리얼 포트나 LOM(Lights-Out Management)을 통한 콘솔 액세스를 구성합니다.	원격 콘솔 액세스 관리
HTTPS 인증서	필요하다면 신뢰된 권한 및 업로드 인증서에서 시스템에 HTTPS 서버 인증서를 요청합니다.	HTTPS 인증서
정보	어플라이언스에 대한 현재 정보를 보고 표시 이름을 편집합니다.	어플라이언스 정보
Management Interfaces(관리 인터페이스)	어플라이언스의 IP 주소, 호스트 이름 및 프록시 설정과 같은 옵션을 변경합니다.	7000/8000 시리즈 디바이스의 관리 인터페이스 구성, 13 페이지
프로세스	Firepower 프로세스를 종료, 리부팅 또는 다시 시작합니다.	7000/8000 시리즈 디바이스 종료 또는 재시작, 17 페이지

시스템 구성	설명	확인
패킷 전송 금지	낮은 대역폭 구축에서 7000/8000 시리즈 디바이스의 패킷 데이터를 FMC로 전송하지 않도록 설정합니다.	FMC로의 패킷 전송 금지, 13 페이지
시간	현재 시간 설정을 봅니다.	7000/8000 시리즈 디바이스의 시스템 시간 보기, 18 페이지

FMC로의 패킷 전송 금지

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
해당 없음	Any(모든)	7000 및 8000 Series	해당 없음	Admin(관리자)

침입 정책 위반을 유발한 패킷의 특정 콘텐츠를 염려하지 않는다면, 저대역폭 구축에서는 7000 또는 8000 Series 디바이스에서 Firepower Management Center(으)로의 패킷 데이터 전송을 해제하는 것이 좋습니다.

프로시저

단계 **1** 7000 또는 8000 Series 디바이스의 로컬 웹 인터페이스에서 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Information(**정보**)**을 클릭합니다.

단계 **3** **Prohibit Packet Transfer to the Management Center(Management Center**에 대한 패킷 전송 금지**)**를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

7000/8000 시리즈 디바이스의 관리 인터페이스 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
해당 없음	Any(모든)	7000 및 8000 Series	전역만 해당	Admin(관리자)

웹 인터페이스를 사용하여 매니지드 디바이스의 관리 인터페이스 설정을 수정합니다. 모델에서 지원하는 경우 이벤트 인터페이스를 선택적으로 활성화할 수 있습니다. 관리 인터페이스에 대한 자세한 내용은 디바이스 관리 인터페이스 섹션을 참조하십시오.

⚠

주의 관리 인터페이스를 변경할 때는 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 디바이스 콘솔 포트에 액세스하여 CLI에서 설정을 재구성해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을 선택한 다음 **Management Interface(**관리 인터페이스**)**를 선택합니다.

단계 **2** **Interfaces(**인터페이스**)** 영역에서 구성하려는 인터페이스 옆에 있는 **Edit(**편집**)**를 클릭합니다.

이 섹션에는 사용 가능한 모든 인터페이스가 나열되어 있습니다. 다른 인터페이스를 추가할 수 없습니다.

각 관리 인터페이스에서 다음 옵션을 구성할 수 있습니다.

- **Enabled(**활성화됨**)** - 관리 인터페이스를 활성화합니다. 기본 eth0 관리 인터페이스를 비활성화하지 마십시오. 일부 프로세스에는 eth0 인터페이스가 필요합니다.
- **Channels(**채널**)** - (8000 Series에만 해당) 이벤트 전용 인터페이스를 구성합니다. 8000 Series의 eth1 관리 인터페이스를 이벤트 인터페이스로 사용하도록 활성화할 수 있습니다. 이렇게 하려면 **Management Traffic(**관리 트래픽**)** 확인란을 선택 취소하고 **Event Traffic(**이벤트 트래픽**)** 확인란을 선택한 상태로 유지합니다. eth0 관리 인터페이스의 경우 두 확인란을 모두 선택 상태로 둡니다.

  Firepower Management Center 이벤트 전용 인터페이스는 관리 채널 트래픽을 허용할 수 없으므로 디바이스 이벤트 인터페이스에서 관리 채널을 비활성화해야 합니다.

  관리 인터페이스에 대한 **Event Traffic(**이벤트 트래픽**)**을 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다.

  인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.
- **Mode(**모드**)** - 연결 모드를 지정합니다. GigabitEthernet 인터페이스의 경우 자동 협상에 대한 변경 사항은 무시됩니다.
- **MTU** - 최대 전송 단위(MTU)를 설정합니다. 기본값은 1500입니다. MTU 설정 가능 범위는 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

  시스템은 구성된 MTU 값에서 자동으로 18바이트를 잘라내므로 1298 아래의 값은 최소 IPv6 MTU 설정인 1280을 준수하지 못하며 594 아래의 값은 최소 IPv4 MTU 설정인 576을 준수하지 못합니다. 예를 들면 시스템은 구성된 값 576을 자동으로 558로 자릅니다.
- **MDI/MDIX** - **Auto-MDIX**를 설정합니다.
- **IPv4 Configuration(IPv4** 구성**)** - IPv4 IP 주소를 설정합니다. 선택:
  - **Static(**정적**)** - 수동으로 **IPv4 Management IP(IPv4** 관리 **IP)** 주소 및 **IPv4 Netmask(IPv4** 넷마스크**)**를 입력합니다.
  - **DHCP** - DHCP를 사용하도록 인터페이스를 설정합니다(eth0 전용).
  - **Disabled(**비활성화됨**)** - IPv4를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
- **IPv6 Configuration(IPv6** 구성**)** - IPv6 IP 주소를 설정합니다. 선택:

- **Static(**정적**)** - 수동으로 **IPv6 Management IP(IPv6** 관리 **IP)** 주소 및 **IPv6 Prefix Length(IPv6** 프리픽스 길이**)**를 입력합니다.
- **DHCP** - DHCPv6를 사용하도록 인터페이스를 설정합니다(eth0 전용).
- **Router Assigned(**라우터 할당**)** - 상태 비저장 자동 구성을 활성화합니다.
- **Disabled(**비활성화됨**)** - IPv6를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
- **IPv6 DAD** - IPv6을 활성화할 때 DAD(Duplicate Address Detection)를 활성화 또는 비활성화합니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다.

단계 **3** **Routes(**경로**)** 영역에서 수정( )을 클릭하여 정적 경로를 편집하거나 추가( )를 클릭하여 경로를 추가합니다. 보기 ( )를 클릭하여 경로 통계를 봅니다.

참고 Firepower Management Center가 원격 네트워크에 있는 경우 이벤트 전용 인터페이스에 정적 경로를 추가해야 합니다. 그렇지 않으면 모든 트래픽이 관리 인터페이스를 통해 기본 경로와 일치하게 됩니다. 기본 경로의 경우 게이트웨이 IP 주소만 변경할 수 있습니다. 기본 경로는 항상 eth0 인터페이스를 사용합니다. 라우팅에 대한 내용은 디바이스 관리 인터페이스의 네트워크 라우트 섹션을 참조하십시오.

정적 경로에 대해 다음 설정을 구성할 수 있습니다.

- **Destination(**대상**)** - 경로를 생성할 네트워크의 대상 주소를 설정합니다.
- **Netmask(**넷마스크**)** 또는 **Prefix Length(**프리픽스 길이**)** - 네트워크의 넷마스크(IPv4) 또는 프리픽스 길이(IPv6)를 설정합니다.
- **Interface(**인터페이스**)** - 이그레스 관리 인터페이스를 설정합니다.
- **Gateway(**게이트웨이**)** - 게이트웨이 IP 주소를 설정합니다.

단계 **4** **Shared Settings(**공유 설정**)** 영역의 모든 인터페이스에서 공유하는 네트워크 파라미터를 설정합니다.

참고 eth0 인터페이스에 **DHCP**를 선택한 경우 DHCP 서버에서 파생된 일부 공유 설정을 수동으로 지정할 수 없습니다.

다음 공유 설정을 구성할 수 있습니다.

- **Hostname(**호스트네임**)** - 디바이스 호스트네임을 설정합니다. 호스트네임을 변경하는 경우 새 호스트네임을 시스템 로그 메시지에 반영하려면 디바이스를 리부팅합니다. 시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.
- **Domains(**도메인**)** - 디바이스에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.

- **Primary DNS Server(**기본 **DNS** 서버**)**, **Secondary DNS Server(**보조 **DNS** 서버**)Tertiary DNS Server(3**차 **DNS** 서버**)** - 환경설정 순서대로 사용할 DNS 서버를 설정합니다.
- **Remote Management Port(**원격 관리 포트**)** - FMC와의 통신을 위한 원격 관리 포트를 설정합니다. FMC 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

  참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

단계 **5** **ICMPv6** 영역에서 ICMPv6 설정을 구성합니다.

- **Allow Sending Echo Reply Packets(**에코 응답 패킷 전송 허용**)** - 에코 응답 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.
- **Allow Sending Destination Unreachable Packets(**대상에 연결할 수 없는 패킷 전송 허용**)** - 대상에 연결할 수 없는 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다.

단계 **6** **LCD Panel(LCD** 패널**)** 영역에서 **Allow reconfiguration of network settings(**네트워크 설정의 재구성 허용**)** 확인란을 선택하여 디바이스의 LCD 패널을 통해 네트워크 설정 변경을 활성화합니다.

디바이스에 대한 IP 주소를 편집하려면 LCD 패널을 사용할 수 있습니다. 변경 사항이 관리되는 Firepower Management Center에 반영되었는지 확인합니다. 경우에 따라 Firepower Management Center에서 수동으로 데이터를 업데이트해야 할 수도 있습니다.

주의 LCD 패널을 사용한 재구성을 허용할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 사용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다. 이 옵션을 활성화하면 보안 문제가 발생할 수 있다는 경고 메시지가 표시됩니다.

단계 **7** **Proxy(**프록시**)** 영역에서 HTTP 프록시 설정을 구성합니다.

디바이스는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다.

참고 NTLM(NT LAN Manager) 인증을 사용하는 프록시는 지원되지 않습니다.

a) **Enable(**활성화**)** 확인란을 선택합니다.
b) 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 **HTTP Proxy(HTTP** 프록시**)** 필드에 입력합니다.
c) **Port(**포트**)** 필드에서 포트 번호를 입력합니다.
d) **Use Proxy Authentication(**프록시 인증 사용**)**을 선택하여 인증 자격 증명을 제공하고 **User Name(**사용자 이름**)** 및 **Password(**비밀번호**)**를 제공합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** 관리 IP 주소를 변경하는 경우 FMC 및 매니지드 디바이스 간의 통신에 영향을 미칠 수 있습니다.

IP 주소를 변경해도 현재 연결에는 영향을 주지 않습니다. 하지만 디바이스 또는 FMC가 다시 로드되면 연결을 다시 설정해야 합니다. 피어의 올바른 IP 주소를 사용하려면 적어도 하나의 디바이스(FMC 또는 매니지드 디바이스)가 필요합니다. 예를 들어 디바이스 설정 중 IP 주소 대신 FMC에 대한 NAT ID를 지정했고 디바이스에 추가할 때 FMC에 정의한 디바이스 IP 주소가 잘못되는 경우 FMC가 통신을 다시 설정할 수 없게 됩니다 . 이 경우 FMC에서 디바이스의 관리 IP 주소를 변경해야 합니다. FMC에서 호스트 이름 또는 IP 주소 업데이트 섹션을 참조하십시오.

7000/8000 시리즈 디바이스 종료 또는 재시작

프로시저

단계 **1** 디바이스의 웹 인터페이스에서 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Process(**프로세스**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

종료	**Shutdown Appliance(**어플라이언스 종료**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 주의 전원 버튼을 사용하여 Firepower 어플라이언스를 종료하지 마십시오. 데이터가 손실될 수 있습니다. 웹 인터페이스(또는 CLI)를 사용하여 구성 데이터 손실 없이 시스템의 전원을 안전하게 끄고 재시작할 수 있도록 준비합니다.
재부팅	**Reboot Appliance(**어플라이언스 리부팅**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 참고 리부팅하면 로그아웃되며, 완료하는 데 최대 1시간이 소요될 수 있는 데이터베이스 검사가 실행됩니다.
콘솔 재시작	**Restart Appliance Console(**어플라이언스 콘솔 재시작**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다.
Snort 프로세스 다시 시작	**Restart Snort(Snort** 다시 시작**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 주의 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 디바이스의 구성 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작를 참조하십시오.

7000/8000 시리즈 디바이스의 시스템 시간 보기

시간 설정이 대부분의 페이지에서 로컬 시간으로 표시됩니다. 여기서 사용되는 시간대는 User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 페이지에서 설정하며, UTC 시간을 사용해 어플라이언스에 저장합니다. 또한 현재 시간은 Time Synchronization(시간 동기화) 페이지 상단에 UTC로 표시됩니다(로컬 시간은 활성화한 경우 Manual(수동) 시계 설정 옵션으로 표시됨).

제한

Time Zone(표준 시간대) 기능(User Preferences(사용자 환경 설정))에서는 기본 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 이 설정은 변경하지 마십시오**.** 시스템 시간을 UTC 이외로 변경하는 것은 지원되지 않으며, 디바이스를 이미지로 다시 설치해야 합니다.

7000 및 8000 Series 디바이스의 시스템 시간 정보를 확인하려면 이 절차를 사용합니다.

프로시저

단계 **1** 디바이스의 웹 인터페이스에 로그인하고 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Time(**시간**)**을 클릭합니다.

NTP를 사용한다면 NTP 서버 상태 섹션을 참조하십시오.