시스템 설정

다음 주제에서는 시스템 설정 페이지에서 함께 그룹화되어 있는 여러 시스템 설정을 구성하는 방법을 설명합니다. 이러한 설정에는 전반적인 시스템 기능이 포함됩니다.

관리 액세스 구성

관리 액세스는 컨피그레이션 및 모니터링을 위해 threat defense 디바이스에 로그인하는 기능을 의미합니다. 다음과 같은 항목을 구성할 수 있습니다.

- 사용자 액세스 인증에 사용할 ID 소스를 식별할 AAA. 로컬 사용자 데이터베이스 또는 외부 AAA 서버를 사용할 수 있습니다. 관리자 권한 사용자를 관리하는 방법에 대한 자세한 내용은 Device Manager 및 Threat Defense 사용자 액세스 관리의 내용을 참조하십시오.
- 관리 인터페이스 및 데이터 인터페이스에 대한 액세스 제어. 이러한 인터페이스에는 별도의 액세스 목록이 있습니다. HTTPS(device manager에 사용됨) 및 SSH(CLI에 사용됨)에 어떤 IP 주소를 허용할지 결정할 수 있습니다. 관리 액세스 목록 구성, 2 페이지를 참조하십시오.

- 사용자가 Fdevice manager에 연결하기 위해 승인해야 하는 Management Web Server 인증서. 현재 사용 중인 웹 브라우저에서 기존에 인증한 인증서를 업로드하면, 알 수 없는 인증서를 승인하라는 요청이 사용자에게 표시되지 않습니다. Threat Defense 웹 서버 인증서 구성, 5 페이지의 내용을 참조하십시오.

관리 액세스 목록 구성

기본적으로는 모든 IP 주소에서 관리 주소의 디바이스의 device manager 웹 또는 CLI 인터페이스에 연결할 수 있습니다. 시스템 액세스는 사용자/비밀번호를 통해서만 보호됩니다. 그러나 특정 IP 주소 또는 서브넷으로부터의 연결만 허용하도록 액세스 목록을 구성하여 보호 레벨을 추가로 제공할 수 있습니다.

데이터 인터페이스를 열어 device manager 또는 SSH의 CLI 연결을 허용할 수도 있습니다. 그러면 관리 주소를 사용하지 않고도 디바이스를 관리할 수 있습니다. 예를 들어 디바이스를 원격으로 구성하기 위해 외부 인터페이스에 대한 관리 액세스를 허용할 수 있습니다. 사용자 이름/비밀번호를 통해 원치 않는 연결로부터 디바이스를 보호할 수 있습니다. 기본적으로 데이터 인터페이스에 대한 HTTPS 관리 액세스는 내부 인터페이스에서는 활성화되지만 외부 인터페이스에서는 비활성화됩니다. device managerFirepower 1010에서 "내부" 브리지 그룹이 있는 의 경우 브리지 그룹 내에 있는 모든 데이터 인터페이스를 통해 브리지 그룹 IP 주소(기본값: 192.168.95.1)에 대한 Firepower Device Manager 연결을 설정할 수 있습니다. 디바이스에 진입하는 데 사용하는 인터페이스에서만 관리 연결을 열 수 있습니다.

⚠

주의 특정 주소에 대한 액세스를 제한하면 시스템이 잠겨 사용이 차단되기 쉽습니다. 현재 사용 중인 IP 주소에 대한 액세스 권한을 삭제하여 "모든" 주소에 대한 항목이 없으면 정책 배포 시 시스템에 액세스할 수 없게 됩니다. 따라서 액세스 목록을 구성하려는 경우 각별히 주의해야 합니다.

시작하기 전에

동일한 TCP 포트에 대한 동일한 인터페이스에서 device manager 액세스(HTTPS 액세스)와 원격 액세스 SSL VPN을 모두 구성할 수는 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. 동일한 인터페이스에서 두 기능을 모두 구성하는 경우 충돌을 방지하기 위해 이러한 서비스 중 하나 이상에 대해 HTTPS 포트를 변경해야 합니다.

프로시저

단계 **1** 디바이스을(를) 클릭한 다음, **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

이 페이지에서 AAA를 구성하여 외부 AAA 서버에 정의된 사용자에 대해 관리 액세스를 허용할 수도 있습니다. 자세한 내용은 Device Manager 및 Threat Defense 사용자 액세스 관리를 참조해 주십시오.

단계 **2** 관리 주소에 대한 규칙을 생성하려면 다음을 수행합니다.

a) **Management Interface(**관리 인터페이스**)** 탭을 선택합니다.

규칙 목록에 따라 지정된 포트 액세스가 허용되는 주소가 정의됩니다. 이 포트는 device manager의 경우 443(HTTPS 웹 인터페이스)이고 SSH CLI의 경우 22입니다.

규칙은 순서가 지정된 목록이 아닙니다. IP 주소가 요청된 포트에 대한 어떤 규칙에든 일치하는 경우 사용자의 디바이스 로그인 시도는 허용됩니다.

참고 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘()을 클릭합니다. 프로토콜에 대한 모든 규칙을 삭제하는 경우, 아무도 그 프로토콜을 사용하여 해당 인터페이스에 있는 디바이스에 액세스할 수 없습니다.

b) +를 클릭하고 다음 옵션에 내용을 입력합니다.

- 프로토콜 - 규칙이 HTTPS(포트 443)용인지 아니면 SSH(포트 22)용인지를 선택합니다.
- **IP** 주소 - 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **3** 데이터 인터페이스에 대한 규칙을 생성하려면 다음을 수행합니다.

a) **Data Interfaces(**데이터 인터페이스**)** 탭을 선택합니다.

규칙 목록에 따라 인터페이스에서 지정된 포트 액세스가 허용되는 주소가 정의됩니다. 이 포트는 device manager의 경우 443(HTTPS 웹 인터페이스)이고 SSH CLI의 경우 22입니다.

규칙은 순서가 지정된 목록이 아닙니다. IP 주소가 요청된 포트에 대한 어떤 규칙에든 일치하는 경우 사용자의 디바이스 로그인 시도는 허용됩니다.

참고 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘()을 클릭합니다. 프로토콜에 대한 모든 규칙을 삭제하는 경우, 아무도 그 프로토콜을 사용하여 해당 인터페이스에 있는 디바이스에 액세스할 수 없습니다.

b) +를 클릭하고 다음 옵션에 내용을 입력합니다.

- 인터페이스 - 관리 액세스를 허용할 인터페이스를 선택합니다.
- 프로토콜 - 규칙이 HTTPS(포트 443)용인지, SSH(포트 22)용인지 아니면 둘 다에 사용할 수 있는지를 선택합니다. 원격 액세스 VPN 연결 프로파일에 사용되는 외부 인터페이스에 대해서는 HTTPS 규칙을 구성할 수 없습니다.
- 허용된 네트워크 - 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

c) (선택 사항). HTTPS 데이터 포트 번호를 변경하려면 해당 번호를 클릭하고 새 포트를 입력합니다. 데이터 인터페이스에서 관리 액세스에 대한 HTTPS 포트 구성, 4 페이지의 내용을 참조하십시오.

d) **OK(**확인**)**를 클릭합니다.

데이터 인터페이스에서 관리 액세스에 대한 **HTTPS** 포트 구성

기본적으로 device manager 또는 threat defense API 관리를 위해 디바이스에 액세스하면 포트 TCP/443을 통과합니다. 데이터 인터페이스에 대한 관리 액세스 포트를 변경할 수 있습니다.

포트를 변경하는 경우 사용자는 시스템에 액세스하려면 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 데이터 인터페이스가 ftd.example.com이고 포트를 4443으로 변경하는 경우 사용자는 URL을 https://ftd.example.com:4443으로 수정해야 합니다.

모든 데이터 인터페이스는 동일한 포트를 사용합니다. 인터페이스마다 다른 포트를 구성할 수 없습니다.

참고 관리 인터페이스의 관리 액세스 포트는 변경할 수 없습니다. 관리 인터페이스는 항상 포트 443을 사용합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **Data Interfaces(**데이터 인터페이스**)** 탭을 클릭합니다.

단계 **3** **HTTPS Data Port(HTTPS** 데이터 포트**)** 번호를 클릭합니다.

단계 **4** Data Interfaces Setting(데이터 인터페이스 설정) 대화 상자에서 **HTTPS Data Port(HTTPS** 데이터 포트**)**를 사용하려는 포트로 변경합니다.

다음 번호는 지정할 수 없습니다.

- 22. SSH 연결에 사용됩니다.
- 원격 액세스 VPN에 사용되는 포트(관리 액세스도 허용하는 인터페이스에 대해 구성한 경우). 원격 액세스 VPN은 기본적으로 포트 443을 사용하지만 맞춤형 포트를 구성할 수 있습니다.
- ID 정책에서 활성 인증에 사용되는 포트입니다(기본값은 885).

단계 **5** **OK(**확인**)**를 클릭합니다.

Threat Defense 웹 서버 인증서 구성

웹 인터페이스에 로그인할 경우, 시스템은 디지털 인증서를 사용하여 HTTPS를 사용하는 통신을 보호합니다. 기본 인증서는 브라우저에서 신뢰하지 않으므로, Untrusted Authority(신뢰할 수 없는 증명) 경고가 표시되며 해당 인증서를 신뢰할 것인지 묻는 메시지가 표시됩니다. 사용자는 신뢰할 수 있는 루트 인증서 저장소에 인증서를 저장할 수 있지만, 그 대신에 브라우저에서 신뢰하도록 이미 컨피그레이션되었다는 새 인증서를 업로드할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **Management Web Server(**관리 웹 서버**)** 탭을 클릭합니다.

단계 **3** **Web Server Certificate(**웹 서버 인증서**)**에서 device manager에 대한 HTTPS 연결을 보호하는 데 사용할 내부 인증서를 선택합니다.

인증서를 업로드하거나 생성하지 않은 경우, 목록 하단의 **Create New Internal Certificate(**새 내부 인증서 생성**)** 링크를 클릭하여 지금 인증서를 생성합니다.

기본값은 사전 정의된 DefaultWebserverCertificate 개체입니다.

단계 **4** 인증서가 자체 서명되지 않은 경우 완전 신뢰 체인의 모든 중간 및 루트 인증서를 **Trusted Chain(**신뢰할 수 있는 체인**)** 목록에 추가합니다.

체인에서 인증서를 10개까지 추가할 수 있습니다. **+**를 클릭하여 각 중간 인증서를 추가하고 마지막으로 루트 인증서를 추가합니다. **Save(**저장**)**를 클릭한 다음, 웹 서버가 재시작되는 것을 경고하는 대화 상자에서 **Proceed(**계속 진행**)**를 클릭하는 경우, 인증서가 누락되면 누락된 체인에서 다음 인증서의 공통 이름이 포함된 오류 메시지가 표시됩니다. 체인에 없는 인증서를 추가하는 경우에도 오류가 표시됩니다. 이러한 메시지를 신중하게 검사하여 추가하거나 제거해야 하는 인증서를 식별합니다.

+를 클릭한 후에 **Create New Trusted CA Certificate(**신뢰할 수 있는 새 **CA** 인증서 생성**)**을 클릭하여 여기에서 인증서를 업로드할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

변경 사항이 즉시 적용되고, 시스템에서는 웹 서버를 다시 시작합니다. 컨피그레이션을 구축할 필요가 없습니다.

재시작이 완료될 때까지 몇 분간 기다렸다가 브라우저를 새로고침합니다.

시스템 기록 설정 컨피그레이션

threat defense 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. 액세스 제어, 침입 방지, 파일 및 악성코드 기록을 포함한 진단 기록 및 연결 관련 기록에 대해 syslog를 활성화할 수 있습니다.

진단 기록에서는 디바이스 및 시스템 상태, 네트워크 컨피그레이션 관련 이벤트에 대한 syslog 메시지를 제공합니다. 이러한 이벤트는 연결과 관련이 없습니다. 개별 액세스 제어 규칙 내에서 연결 로깅을 구성합니다.

진단 기록에서는 데이터 플레인에서 실행되는 기능, 즉 **show running-config** 명령으로 볼 수 있는 CLI 컨피그레이션에 정의된 기능에 대해 메시지를 생성합니다. 여기에는 라우팅, VPN, 데이터 인터페이스, DHCP 서버, NAT 등과 같은 기능이 포함됩니다.

이 메시지에 대한 정보는 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html의 *Cisco Threat Defense* 시스템 로그 메시지를 참조하십시오.

다음 주제에서는 다양한 출력 위치에 대한 진단 및 파일/악성코드 메시지에 관한 기록을 컨피그레이션하는 방법에 대해 설명합니다.

심각도 레벨

다음 표는 syslog 메시지 심각도 수준을 나열합니다.

표 ***1: Syslog*** 메시지 심각도 레벨

레벨 번호	심각도 레벨	설명
0	**emergencies**(비상)	시스템을 사용할 수 없습니다.
1	**Alert**(긴급 경고)	즉각적인 행동이 필요합니다.
2	**critical**(심각)	심각한 상태입니다.
3	**error**(오류)	오류 상태입니다.
4	**warning**(경고)	경고 상태입니다.
5	**notification**(알림)	일반적이지만 중요한 상태입니다.
6	**informational**(정보)	정보 메시지만 해당됩니다.
7	**debugging**(디버깅)	디버깅 메시지만 해당됩니다. 문제를 디버깅할 때 이 레벨에서 일시적으로만 기록합니다. 이 로그 레벨은 시스템 성능에 영향을 미칠 수 있는 메시지를 너무 많이 생성할 수 있습니다.

참고 ASA 및 Threat Defense은 심각도 레벨 0(응급)으로 시스템 로그 메시지를 생성하지 않습니다.

원격 **Syslog** 서버에 대한 기록 컨피그레이션

외부 syslog 서버로 syslog 메시지를 전송하도록 시스템을 컨피그레이션할 수 있습니다. 이것은 시스템 기록을 위한 최상의 옵션입니다. 외부 서버를 사용하여 메시지를 보관할 수 있는 공간을 더 많이 제공하고 서버의 기능을 사용하여 메시지를 보고, 분석 및 보관할 수 있습니다.

또한 파일 정책을 액세스 제어 규칙의 트래픽에 적용하는 경우, 파일 액세스나 악성코드 또는 둘 다를 제어하려면 파일 이벤트 메시지를 외부 syslog 서버로 전송하도록 시스템을 컨피그레이션할 수 있습니다. 시스템 로그 서버를 컨피그레이션하지 않는 경우, 이벤트는 device manager 이벤트 뷰어에서만 제공됩니다.

다음 절차에서는 진단 (데이터) 기록 및 파일/악성코드 기록을 위해 syslog를 활성화하는 방법에 대해 설명합니다. 다음 항목에 대해 외부 기록을 컨피그레이션할 수도 있습니다.

- 연결 이벤트: 개별 액세스 제어 규칙, SSL 암호 해독 규칙 또는 보안 인텔리전스 정책 설정에서 syslog 서버 선택
- 침입 이벤트: 침입 정책 설정에서 syslog 서버 선택

시작하기 전에

파일/악성코드 이벤트에 대한 시스템 로그 설정은 IPS 및 악성코드 방어 라이선스 가 필요한 파일 또는 악성코드 정책을 적용하는 경우에만 해당됩니다.

또한 정책을 적용하는 액세스 제어 규칙에서 **File Events(**파일 이벤트**)** > **Log Files(**로그 파일**)** 옵션을 선택해야 합니다. 그러지 않으면 syslog 또는 이벤트 뷰어 이벤트에 대해 이벤트가 전혀 생성되지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Remote Server(**원격 서버**)**에서 **Data Logging(**데이터 기록**)** 슬라이더를 **On(**켜짐**)**으로 밀어 외부 syslog 서버에 대한 진단 데이터 플레인 생성 메시지의 기록을 활성화합니다. 이어서 다음 옵션을 컨피그레이션합니다.

- **Syslog Server(Syslog** 서버**)** - +(을)를 클릭하고 하나 이상의 syslog 서버 개체를 선택한 후 **OK(**확인**)**를 클릭합니다. 개체가 없는 경우, **Add Syslog Server(Syslog** 서버 추가**)** 링크를 클릭하고 지금 바로 개체를 생성합니다. 자세한 내용은 syslog 서버 구성를 참고하십시오.

- **Severity Level for Filtering FXOS Chassis Syslogs(FXOS** 섀시 **syslog** 필터링을 위한 심각도 레벨**)** - FXOS를 사용하는 특정 디바이스 모델의 경우, 기본 FXOS 플랫폼에서 생성한 syslog 메시지의 심각도 레벨. 이 옵션은 디바이스와 관련이 있는 경우에만 표시됩니다. 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 syslog 서버로 전송됩니다.
- **Message Filtering(**메시지 필터링**)** - threat defense 운영 체제에 대해 생성된 메시지를 제어하려면 다음 옵션 중 하나를 선택합니다.
  - **Severity Level for Filtering All Events(**모든 이벤트 필터링을 위한 심각도 레벨**)** - 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 syslog 서버로 전송됩니다.
  - **Custom Logging Filter(**맞춤형 기록 필터**)** - 관심 있는 메시지만 가져올 수 있도록 추가 메시지 필터링을 수행하려는 경우, 생성하려는 메시지를 정의하는 이벤트 목록 필터를 선택합니다. 필터가 아직 없는 경우, **Create New Event List Filter(**새 이벤트 목록 필터 생성**)**를 클릭하여 지금 바로 생성합니다. 자세한 내용은 이벤트 목록 필터 구성, 9 페이지를 참고하십시오.

단계 **3** **File/Malware(**파일/악성코드**)** 슬라이더를 **On(**켜짐**)**으로 밀어 파일 및 악성코드 이벤트용 외부 syslog 서버에 기록을 활성화합니다. 그런 다음, 파일/악성코드 기록에 대해 다음 옵션을 컨피그레이션합니다.

- **Syslog Server(Syslog** 서버**)** - syslog 서버 개체를 선택합니다. 개체가 없는 경우, **Add Syslog Server(Syslog** 서버 추가**)** 링크를 클릭하고 지금 바로 개체를 생성합니다.
- **Log at Severity Level(**심각도 레벨의 로그**)** - 파일/악성코드 이벤트에 할당해야 하는 심각도 레벨을 선택합니다. 모든 파일/악성코드 이벤트는 동일한 심각도에서 생성되므로 필터링이 수행되지 않습니다. 따라서 선택하는 레벨에 관계없이 모든 이벤트가 표시됩니다. 이것은 메시지의 심각도 필드에 표시되는 레벨입니다(즉 FTD-x-<message_ID>의 x). 파일 이벤트는 메시지 ID 430004, 악성코드 이벤트는 430005입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

내부 버퍼에 대한 기록 컨피그레이션

Syslog 메시지를 내부 기록 버퍼에 저장하도록 시스템을 컨피그레이션할 수 있습니다. 버퍼의 내용을 보려면 CLI 또는 CLI 콘솔에서 **show logging** 명령을 사용하십시오.

새 메시지는 버퍼의 끝에 추가됩니다. 버퍼가 가득 차면 시스템에서는 버퍼를 지운 다음, 메시지를 계속 추가합니다. 로그 버퍼가 가득 차면 시스템에서는 가장 오래된 메시지를 삭제하여 새 메시지를 위한 버퍼 공간을 확보합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Internal Buffer(**내부 버퍼**)** 슬라이더를 **On(**켜짐**)**으로 밀어 버퍼를 기록 대상으로 활성화합니다.

단계 **3** 내부 버퍼 기록에 대한 옵션을 다음과 같이 컨피그레이션합니다.

- **Severity Level for Filtering All Events(**모든 이벤트 필터링을 위한 심각도 레벨**)** - 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 내부 버퍼로 전송됩니다.
- **Custom Logging Filter(**맞춤형 기록 필터**)** - (선택 사항) 관심 있는 메시지만 가져올 수 있도록 추가 메시지 필터링을 수행하려는 경우, 생성하려는 메시지를 정의하는 이벤트 목록 필터를 선택합니다. 필터가 아직 없는 경우, **Create New Event List Filter(**새 이벤트 목록 필터 생성**)**를 클릭하여 지금 바로 생성합니다. 자세한 내용은 이벤트 목록 필터 구성, 9 페이지를 참고하십시오.
- **Buffer Size(**버퍼 크기**)** - syslog 메시지가 저장되는 내부 버퍼의 크기. 버퍼는 가득 차면 덮어쓰기 됩니다. 기본값은 4096바이트입니다. 범위는 4096~52428800입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

콘솔에 기록 컨피그레이션

콘솔에 메시지를 전송하도록 시스템을 컨피그레이션할 수 있습니다. 콘솔 포트에서 CLI에 로그인하면 이러한 메시지가 표시됩니다. **show console-output** 명령을 사용하면 다른 인터페이스에 대한 SSH 세션에서도 이러한 로그를 확인할 수 있습니다(관리 주소 포함). 또한 진단 CLI에서 실시간으로 이러한 메시지를 확인할 수 있습니다. 기본 CLI에서 **system support diagnostic-cli**(을)를 입력하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Console Filter(**콘솔 필터**)** 슬라이더를 **On(**켜짐**)**으로 밀어 콘솔을 기록 대상으로 활성화합니다.

단계 **3** 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 콘솔로 전송됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이벤트 목록 필터 구성

이벤트 목록 필터는 어떤 메시지를 대상으로 전송할지 제어하기 위해 기록 대상에 적용할 수 있는 맞춤형 필터입니다. 일반적으로 심각도만을 기준으로 대상에 대한 메시지를 필터링하지만, 이벤트 클래스, 심각도 및 메시지 ID(식별자)의 조합을 기준으로 전송할 메시지를 세부 조정할 수 있습니다.

심각도 레벨에 따라서만 메시지를 제한하는 것으로는 목적을 달성하지 못하는 경우에만 필터를 사용합니다.

다음 절차에서는 **Objects(**개체**)** 페이지에서 필터를 생성하는 방법을 설명합니다. 필터를 사용할 수 있는 기록 대상을 컨피그레이션하는 중에 필터를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**를 선택한 다음, **Event List Filters(**이벤트 목록 필터**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 필터 속성을 다음과 같이 구성합니다.

- **Name(**이름**)** - 필터 개체의 이름입니다.
- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **Severity and Log Class(**심각도 및 로그 클래스**)** - 메시지 클래스를 기준으로 필터링하려는 경우, **+**를 클릭하고 클래스 필터에 대한 심각도 레벨을 선택한 다음, **OK(**확인**)**를 클릭합니다. 그런 다음, 심각도 레벨 내에서 드롭다운 화살표를 클릭하고 해당 심각도 레벨에서 필터링할 클래스를 하나 이상 선택한 후 **OK(**확인**)**를 클릭합니다.

  시스템에서는 지정된 클래스의 메시지가 해당 심각도 레벨 이상인 경우에만 이 메시지에 대해 syslog 메시지를 전송합니다. 각 심각도 레벨에 대해 최대 한 개의 행을 추가할 수 있습니다.

  특정 심각도 레벨에서 모든 클래스를 필터링하려는 경우, 심각도 목록을 빈 상태로 두고 대신에 기록 대상을 활성화할 때 기록 대상에 대한 전역 심각도 레벨을 선택합니다.
- **Syslog Range/Message ID(Syslog** 범위/메시지 **ID)** - syslog 메시지 ID를 기준으로 필터링하려는 경우, 단일 메시지 ID를 입력하거나 메시지를 생성하려는 ID 번호의 범위를 입력합니다. 범위의 시작 및 종료 번호를 하이픈으로 구분합니다(예: 100000-200000). ID는 6자리 숫자입니다. 특정 메시지 ID 및 관련 메시지에 관해서는 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html의 *Cisco Threat Defense* 시스템 로그 메시지를 참조하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 이 개체를 허용하는 기록 대상에 대한 맞춤형 필터링 옵션에서 이 개체를 선택할 수 있습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**로 이동합니다.

DHCP 구성

DHCP 서버는 IP 주소와 같은 네트워크 구성 매개변수를 DHCP 클라이언트에 제공합니다. 연결된 네트워크의 DHCP 클라이언트에 구성 매개변수를 제공하도록 인터페이스에서 DHCP 서버를 구성하거나 인터페이스의 DHCP 릴레이를 활성화하여 네트워크의 다른 디바이스에서 작동 중인 외부 DHCP 서버에 요청을 전달할 수 있습니다.

이러한 기능은 상호 배타적이므로, 둘 중 하나만 구성할 수 있고 두 가지 모두 구성할 수는 없습니다.

DHCP 서버 설정

DHCP 서버는 IP 주소와 같은 네트워크 컨피그레이션 파라미터를 DHCP 클라이언트에 제공합니다. 연결된 네트워크의 DHCP 클라이언트에 컨피그레이션 파라미터를 제공하기 위해 인터페이스에서 DHCP 서버를 구성할 수 있습니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다. DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

참고 이미 DHCP 서버가 작동 중인 네트워크에서는 DHCP 서버를 구성하지 마십시오. 이렇게 하면 두 서버가 충돌하여 예측할 수 없는 결과가 발생합니다.

시작하기 전에

DHCP 클라이언트는 서버가 활성화된 인터페이스와 같은 네트워크에 있어야 합니다. 즉, 서버와 클라이언트 사이에 스위치는 있을 수 있지만 개입하는 라우터가 있어서는 안 됩니다.

여러 네트워크를 지원해야 하고 각 인터페이스에서 DHCP 서버를 구성하지 않으려는 경우, 대신 DHCP 요청을 한 네트워크에서 다른 네트워크에 있는 DHCP 서버로 전달하도록 구성할 수 있습니다. 이 경우 DHCP 서버는 네트워크의 다른 디바이스에 있어야 합니다. 한 디바이스에서 DHCP 서버를 구성하고 동일한 디바이스의 다른 인터페이스에서 DHCP 릴레이를 구성할 수는 없습니다. DHCP 릴레이를 사용하는 경우 DHCP 서버가 관리할 각 네트워크 주소 공간에 대해 주소 풀을 사용하여 DHCP 서버를 설정해야 합니다.

DHCP 릴레이를 구성하려면 DHCP 릴레이 구성, 13 페이지 항목을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DHCP Server / Relay(DHCP** 서버/릴레이**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **DHCP** > **DHCP Server(DHCP** 서버**)**를 클릭하면 됩니다.

이 페이지에는 2개의 탭이 있습니다. 먼저 **Configuration(**컨피그레이션**)** 탭에는 글로벌 파라미터가 표시됩니다.

DHCP Servers(DHCP 서버**)** 탭에는 DHCP 서버를 구성한 인터페이스, 서버 활성화 여부 및 서버의 주소 풀이 표시됩니다.

단계 **2** **Configuration(**컨피그레이션**)** 탭에서 자동 컨피그레이션 및 글로벌 설정을 구성합니다.

DHCP 자동 컨피그레이션은 DHCP 서버가 지정된 인터페이스에서 실행 중인 어떤 DHCP 클라이언트로부터 얻은 DNS 서버, 도메인 이름, WINS 서버 정보를 DHCP 클라이언트에 제공할 수 있게 합니다. 일반적으로는 외부 인터페이스의 DHCP를 사용하여 주소를 가져오는 경우 자동 컨피그레이션을 사용하지만, DHCP를 통해 주소를 가져오는 모든 인터페이스를 선택할 수 있습니다. 자동 컨피그레이션을 사용할 수 없는 경우에는 필요한 옵션을 수동으로 정의할 수 있습니다.

a) 자동 컨피그레이션을 사용하려면 **Enable Auto Configuration(**자동 컨피그레이션 활성화**)** > **On(**켜기**)**을 클릭(슬라이더가 오른쪽에 있어야 함)한 다음 인터페이스에서에서 DHCP를 통해 주소를 가져오는 인터페이스를 선택합니다.

가상 라우터를 구성하는 경우 전역 가상 라우터의 인터페이스에서만 DHCP 서버 자동 컨피그레이션을 사용할 수 있습니다. 자동 컨피그레이션은 사용자 정의 가상 라우터에 할당된 인터페이스에 대해 지원되지 않습니다.

b) 자동 컨피그레이션을 활성화하지 않거나 자동으로 구성된 설정을 재정의하려는 경우 다음의 글로벌 옵션을 구성합니다. 이러한 설정은 DHCP 서버를 호스팅하는 모든 인터페이스의 DHCP 클라이언트에 전송됩니다.

- **1**차 **WINS IP** 주소, **2**차 **WINS IP** 주소 - 클라이언트가 NetBIOS 이름 확인에 사용해야 하는 WINS(Windows 인터넷 이름 서비스) 서버의 주소입니다.
- **Primary DNS IP Address(**기본 **DNS IP** 주소**)**, **Secondary DNS IP Address(**보조 **DNS IP** 주소**)** - 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS(Domain Name System) 서버의 주소입니다. OpenDNS 공개 DNS 서버를 구성하려면 **Use OpenDNS(OpenDNS** 사용**)**를 클릭합니다. 버튼을 클릭하면 필드에 적절한 IP 주소가 로드됩니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **3** **DHCP Servers(DHCP** 서버**)** 탭을 클릭하고 서버를 구성합니다.

a) 다음 중 하나를 수행합니다.

- 이미 나열되어 있지 않은 인터페이스에 대해 DHCP 서버를 구성하려면 **+**를 클릭합니다.
- 기존 DHCP 서버를 수정하려면 해당 서버의 수정 아이콘()을 클릭합니다.

서버를 삭제하려면 해당 서버의 휴지통 아이콘()을 클릭합니다.

b) 서버 속성을 구성합니다.

- **DHCP** 서버 활성화 - 서버를 활성화할지를 선택합니다. 서버를 구성하되 사용할 준비가 될 때까지 비활성화해 둘 수 있습니다.
- 인터페이스 - 클라이언트에 DHCP 주소를 제공할 인터페이스를 선택합니다. 이 인터페이스에는 고정 IP 주소가 있어야 합니다. 인터페이스에서 DHCP 서버를 실행하려는 경우 DHCP

를 사용하여 인터페이스 주소를 가져올 수는 없습니다. 브리지 그룹의 경우 멤버 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에서 DHCP 서버를 구성합니다. 그러면 서버가 모든 멤버 인터페이스에서 작동합니다.

진단 인터페이스에서는 DHCP 서버를 설정할 수 없습니다. 대신 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 페이지를 통해 관리 인터페이스에서 DHCP 서버를 설정합니다.

- 주소 풀 - 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 10.100.10.12-10.100.10.250과 같이 지정합니다.

  이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다.

  주소 풀의 크기는 threat defense 디바이스에 있는 풀당 최대 256개 주소로 제한됩니다. 주소 풀의 범위가 253개 주소보다 클 경우, threat defense 인터페이스의 넷마스크는 클래스 C 주소(예: 255.255.255.0)가 될 수 없으며 그보다 더 커야 합니다(예: 255.255.254.0).

c) **OK(**확인**)**를 클릭합니다.

DHCP 릴레이 구성

인터페이스에서 수신한 DHCP 요청을 하나 이상의 DHCP 서버에 전달하도록 DHCP 릴레이 에이전트를 구성할 수 있습니다.

DHCP 클라이언트는 최초 DHCPDISCOVER 메시지를 보내는 데 UDP 브로드캐스트를 사용합니다. 연결된 네트워크에 대한 정보가 없기 때문입니다. 클라이언트가 연결된 세그먼트에 서버가 없을 경우, threat defense 디바이스는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다. DHCP 릴레이 에이전트를 사용하면 DHCP 요청을 다른 인터페이스를 통해 DHCP 서버로 전송하는 브로드캐스트를 수신하는 threat defense 디바이스의 인터페이스를 구성할 수 있습니다.

따라서 DHCP 서버를 호스팅하지 않는 서브넷의 클라이언트는 다른 서브넷에 있는 DHCP 서버에서 IP 주소 리스를 계속 가져올 수 있습니다.

시작하기 전에

- 추가할 각 서브넷에 대해 주소 풀을 사용하여 DHCP 서버를 구성합니다. 예를 들어, 192.168.1.1/24 주소의 인터페이스에서 DHCP 릴레이 클라이언트를 활성화한 경우, 192.168.1.0/24 네트워크의 클라이언트를 지원하려면 DHCP 서버가 192.168.1.0/24 서브넷의 IP 주소를 제공할 수 있어야 합니다(예: 192.168.1.2-192.168.1.254).
- 각 DHCP 서버에 대한 호스트 네트워크 개체를 생성하고, 서버의 IP 주소를 지정합니다.
- **DHCP** > **DHCP Servers(DHCP** 서버**)** 페이지에서 모든 서버를 제거 또는 비활성화해야 합니다. 인터페이스에서 DHCP 릴레이가 활성화된 상태에서는 서로 다른 인터페이스인 경우에도 DHCP 서버를 호스팅할 수 없습니다.

- 인터페이스 제한 - 인터페이스에는 서버 또는 에이전트에 사용할 이름이 있어야 합니다. 그 외에도,
  - 인터페이스는 라우팅 ECMP 트래픽 영역의 멤버일 수 없습니다.
  - 인터페이스는 DHCP를 사용하여 주소를 가져올 수 없습니다.
  - 물리적 인터페이스, 하위 인터페이스, VLAN 인터페이스 및 EtherChannel(멤버 제외)에서 DHCP 서버와 DHCP 릴레이를 모두 구성할 수 있습니다.
  - VTI(Virtual Tunnel Interface)에서 DHCP 릴레이 서버를 구성할 수도 있습니다.
  - 어떤 서비스도 관리 인터페이스 또는 브리지 그룹과 멤버를 지원하지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DHCP Server / Relay(DHCP** 서버/릴레이**)** 링크를 클릭하고, 목차에서 **DHCP** > **DHCP Relay(DHCP** 릴레이**)**를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **DHCP** > **DHCP Relay(DHCP** 릴레이**)**를 클릭하면 됩니다.

단계 **2** (선택 사항). 필요에 따라 **IPv4 Relay Timeout(IPv4** 릴레이 시간 초과**)** 및 **IPv6 Relay Timeout(IPv6** 릴레이 시간 초과**)** 설정을 조정합니다.

이러한 시간 제한은 지정된 IP 버전에 대한 DHCP 릴레이 주소 협상에 허용되는 시간(초)을 설정합니다. 기본값은 60초(1분)이지만 1~3600초에서 시간 제한을 설정할 수 있습니다. 서브넷과 DHCP 서버 간에 상당한 지연이 있는 경우 더 긴 시간 초과가 적절할 수 있습니다.

단계 **3** **DHCP** 릴레이 서버를 구성합니다.

DHCP 릴레이 서버는 DHCP 릴레이 요청을 처리해야 하는 네트워크의 DHCP 서버입니다. 이러한 DHCP 서버는 네트워크에서 구성 중인 디바이스와 다른 디바이스에 있습니다.

a) +를 클릭하고 DHCP 서버의 IP 주소가 있는 호스트 네트워크 개체를 선택한 다음 **OK(**확인**)**를 클릭합니다.

개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다. 추가한 DHCP 서버를 더 이상 사용하지 않으려면 서버 항목의 오른쪽에 있는 **X**를 클릭하여 삭제합니다.

b) 추가한 DHCP 서버 항목을 클릭하고, DHCP 서버에 연결할 수 있는 인터페이스를 선택합니다.

단계 **4** DHCP 릴레이 에이전트를 구성합니다.

DHCP 릴레이 에이전트는 인터페이스에서 실행됩니다. 네트워크 세그먼트의 클라이언트에서 DHCP 서버로 DHCP 요청을 전달한 다음 응답을 클라이언트로 반환합니다.

a) +를 클릭하고 DHCP 릴레이 에이전트를 실행해야 하는 인터페이스를 선택한 다음 **OK(**확인**)**를 클릭합니다.

더 이상 인터페이스에서 DHCP 릴레이 에이전트를 실행하지 않으려면 서버 항목의 오른쪽에 있는 **X**를 클릭하여 삭제합니다. 선택적으로 테이블에서 인터페이스를 제거하지 않고 모든 DHCP 릴레이 서비스를 비활성화할 수 있습니다.

b) 추가한 인터페이스 항목을 클릭하고 에이전트에서 제공할 DHCP 서비스를 선택한 다음 **OK(**확인**)**를 클릭합니다.

- **Enable IPv4(IPv4** 활성화**)** - DHCP 서버에 대한 IPv4 주소 요청을 전달합니다. 이 옵션을 선택하지 않으면 모든 IPv4 주소 요청이 무시되고 클라이언트가 IPv4 주소를 가져올 수 없습니다.
- **Set Route(**경로 설정**)**(IPv4만 해당) - DHCP 서버에서 전송된 패킷의 첫 번째 기본 라우터 주소를 DHCP 릴레이 에이전트를 실행 중인 threat defense 디바이스 인터페이스의 주소로 변경합니다. 이 작업을 수행하면 클라이언트는 DHCP 서버가 다른 라우터를 지정하더라도 threat defense 디바이스를 가리키는 기본 경로를 설정할 수 있습니다. 패킷에 기본 라우터 옵션이 없는 경우 DHCP 릴레이 에이전트는 인터페이스 주소를 포함하는 옵션을 추가합니다.
- **Enable IPv6(IPv6** 활성화**)** - DHCP 서버에 대한 IPv6 주소 요청을 전달합니다. 이 옵션을 선택하지 않으면 모든 IPv6 주소 요청이 무시되고 클라이언트가 IPv6 주소를 가져올 수 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

동적 **DNS** 구성

DDNS(Dynamic Domain Name System) 변경 사항을 동적 DNS 서비스에 전송하기 위해 웹 업데이트 방법을 사용하도록 시스템을 설정할 수 있습니다. 이러한 서비스는 FQDN(Fully Qualified Domain Name)과 연결된 새 IP 주소를 사용하도록 DNS 서버를 업데이트합니다. 따라서 사용자가 호스트 이름을 사용하여 시스템에 액세스하려고 하면 DNS가 올바른 IP 주소로 이름을 확인합니다.

DDNS를 사용하면 시스템의 인터페이스에 대해 정의된 FQDN이 항상 올바른 IP 주소로 확인되도록 할 수 있습니다. 이는 DHCP를 사용하여 주소를 가져오도록 인터페이스를 설정하는 경우 특히 중요합니다. 하지만 DNS 서버가 올바른 주소를 갖도록 하고 정적 주소를 변경하는 경우 쉽게 업데이트될 수 있도록 할 수 있다는 점에서 정적 IP 주소에 사용하는 것이 좋습니다.

선택한 DDNS 서비스 제공자 그룹을 사용하도록 DDNS를 설정하거나, 맞춤형 옵션을 사용하여 웹 업데이트를 지원하는 다른 DDNS 제공자로 업데이트를 전달할 수 있습니다. 인터페이스에 대해 지정하는 FQDN은 이러한 서비스 제공자에 등록되어야 합니다.

참고 device manager을 사용하여 웹 업데이트 DDNS만 설정할 수 있습니다. IETF RFC 2136에 정의된 방법에 대해 DDNS를 설정할 수 없습니다.

시작하기 전에

시스템에 제공자의 인증서를 검증할 신뢰할 수 있는 CA 인증서가 있어야 합니다. 그러지 않으면 DDNS 연결에 실패합니다. 서비스 제공자 사이트에서 인증서를 다운로드할 수 있습니다. 적절한 인

증서가 업로드 및 구축되었는지 확인하십시오. 또한 **SSL** 서버를 포함하도록 업로드된 인증서의 검증 사용을 설정해야 합니다. 신뢰할 수 있는 CA 인증서 업로드의 내용을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **DDNS Service(DDNS** 서비스**)**를 클릭하면 됩니다.

이 페이지에는 서비스 제공자, 인터페이스, 인터페이스의 FQDN(Fully Qualified Domain Name)을 비롯한 DDNS 업데이트 방법 목록과 FQDN의 IP 주소 변경을 위해 DNS 서버가 업데이트되는 빈도가 표시됩니다. 항목의 **Show Status(**상태 표시**)** 링크를 클릭하여 항목이 올바르게 작동하는지 확인할 수 있습니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새로운 동적 DNS 업데이트 방법을 생성하려면 **+** 또는 **Create DDNS Service(DDNS** 서비스 생성**)** 버튼을 클릭합니다.
- 기존 동적 DNS 업데이트 방법을 편집하려면 해당 방법의 편집 아이콘( )을 클릭합니다.

방법을 삭제하려면 해당 방법의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 동적 DNS 서비스 속성 설정:

- **Name(**이름**)** - 서비스의 이름입니다.
- **Web Type Update(**웹 유형 업데이트**)** - DDNS 서비스 제공자가 지원하는 주소를 기반으로 하여 업데이트할 주소 유형을 선택합니다. 기본값은 IPv4와 IPv6, **All Addresses(**모든 주소**)** 업데이트입니다. **IPv4 Address(IPv4** 주소**)**, **IPv4 and One IPv6 Address(IPv4**와 **1**개의 **IPv6** 주소**)**, **One IPv6 Address(1**개의 **IPv6** 주소**)**, **All IPv6 Addresses(**모든 **IPv6** 주소**)** 업데이트 옵션을 선택할 수 있습니다.

  IPv6 주소의 경우 다음에 유의하십시오.

  - 전역 주소만 업데이트됩니다. 링크 로컬 주소는 업데이트되지 않습니다.
  - device manager에서는 인터페이스당 단일 IPv6 주소를 설정할 수 있으므로 실제로는 1개의 IPv6 주소만 업데이트됩니다.

- **Service Provider(**서비스 제공자**)** - 동적 DNS 업데이트를 수신 및 처리하는 서비스 제공자를 선택합니다. 다음 서비스 제공자를 사용할 수 있습니다.
  - **No-IP** - No-IP DDNS 서비스 제공자(https://www.noip.com/).
  - **Dynamic DNS** - Oracle Dynamic DNS 서비스 제공자(https://account.dyn.com/).
  - **Google** - Google Domains 서비스 제공자(https://domains.google.com).

- **Custom URL(맞춤형 URL)** - 다른 모든 DDNS 서비스 제공자. 사용자 이름 및 암호를 포함하여 선택한 제공자가 요구하는 URL을 **Web URL(웹 URL)** 필드에 입력해야 합니다. DDNS 서비스는 https://help.dyn.com/remote-access-api/에서 설명하는 표준을 준수해야 합니다.

- **Username(사용자 이름)**, **Password(암호)**(맞춤형이 아닌 URL 방법) - 동적 DNS 업데이트를 전송할 때 서비스 제공자의 플랫폼에서 정의한 사용자 이름 및 암호를 사용합니다.

  참고:

  - 사용자 이름에는 공백이나 @ 및 : 기호가 포함될 수 없습니다. 구분 기호 역할을 하기 때문입니다.
  - 암호에는 공백이나 @ 문자가 포함될 수 없습니다. 구분 기호 역할을 하기 때문입니다. 첫 번째 : 기호 뒤와 @ 앞에 사용되는 모든 : 기호는 암호의 일부로 간주됩니다.

- **Web URL(웹 URL)**(맞춤형 URL 방법) - 서비스 제공자로 맞춤형 URL을 선택한 경우 동적 DNS 서비스에 대한 URL을 입력해야 합니다. URL은 511자로 제한되는 다음 형식이어야 합니다.

  http(s)://username:password@provider-domain/xyz?hostname=<h>&myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- **Interfaces and Fully-Qualified Domain Name(인터페이스 및 FQDN)** - 이 서비스 제공자에 업데이트하고자 하는 DNS 레코드의 인터페이스를 선택한 다음 각 인터페이스에 대한 FQDN(Fully Qualified Domain Name)을 입력합니다. interface.example.com을 예로 들 수 있습니다. 인터페이스는 다음과 같이 제한됩니다.

  - 이름이 지정된 물리적 인터페이스와 하위 인터페이스만 선택할 수 있습니다.
  - 관리, BVI/EtherChannel 또는 해당 구성원, VLAN, VTI(Virtual Tunnel Interface) 유형의 인터페이스는 선택할 수 없습니다.
  - 지정된 인터페이스는 하나의 DDNS 업데이트 방법으로만 선택할 수 있습니다. 동일한 DDNS 업데이트 개체에서 서비스 제공자를 사용해야 하는 모든 인터페이스를 선택할 수 있습니다.

- **Update Interval(업데이트 간격)** - 동적 DNS 업데이트를 보내는 빈도입니다. 기본값은 **On Change(변경 시)**로, 인터페이스의 IP 주소가 변경될 때마다 업데이트를 보냅니다. 또는 **Hourly(매시간)**, **Daily(매일)** 또는 **Monthly(매월)**를 선택할 수 있습니다. 매일 또는 매월의 경우 업데이트를 보낼 시간을 설정하고, 매월의 경우 업데이트를 보낼 날짜를 설정합니다.

단계 **4** **OK(확인)**를 클릭합니다.

DNS 구성

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 초기 시스템 설정 중에 DNS 서버를 구성하면 이러한 서버가 데이터 및 관리 인터페이스에 적용됩니다. 설정 후에

이러한 서버를 변경할 수 있으며 데이터 및 관리 인터페이스에 별도의 서버 집합을 사용할 수 있습니다.

최소한 관리 인터페이스용 DNS를 구성해야 합니다. FQDN 기반 액세스 제어 규칙을 사용하려는 경우 또는 **ping** 등의 CLI 명령에서 호스트네임을 사용하려는 경우에는 데이터 인터페이스용 DNS도 컨피그레이션해야 합니다.

DNS 구성은 2단계 프로세스입니다. 즉, DNS 그룹을 구성한 다음 이러한 인터페이스용 DNS를 구성합니다.

다음 주제에서는 이 프로세스에 대해 자세히 설명합니다.

DNS 그룹 구성

DNS 그룹은 DNS 서버 및 일부 관련 특성의 목록을 정의합니다. 관리 및 데이터 인터페이스에서 DNS를 각기 별도로 구성할 수 있습니다. www.example.com과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다.

디바이스 설정 마법사를 완료하고 나면 다음의 시스템 정의 DNS 그룹 중 하나 또는 두 그룹이 모두 생성됩니다.

- CiscoUmbrellaDNSServerGroup - 이 그룹에는 Cisco Umbrella에서 사용할 수 있는 DNS 서버의 IP 주소가 포함되어 있습니다. 초기 설정 중에 이러한 서버를 선택한 경우 시스템 정의 그룹은 이 그룹뿐입니다. 이 그룹의 이름 또는 서버 목록을 변경할 수는 없지만 기타 속성을 수정할 수는 있습니다.
- CustomDNSServerGroup - 디바이스 설정 중에 Umbrella 서버를 선택하지 않는 경우 시스템에서 서버 목록이 포함된 이 그룹을 생성합니다. 이 그룹의 모든 속성을 수정할 수 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **DNS Groups(DNS** 그룹**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 그룹을 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다.
- 그룹을 수정하려면 해당 그룹의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - DNS 서버 그룹의 이름입니다. DefaultDNS는 예약된 이름이므로 사용할 수 없습니다.
- **DNS IP Addresses(DNS IP** 주소**)** — DNS 서버의 IP 주소를 입력합니다. 두 개 이상의 서버를 구성하려면 **Add Another DNS IP Address(**다른 **DNS IP** 주소 추가**)**를 클릭합니다. 서버 주소를 제거하려는 경우 해당 주소의 삭제 아이콘( )을 클릭합니다.

목록은 우선순위에 따라 나열됩니다. 목록의 첫 번째 서버가 항상 사용되며, 그다음 서버는 위에 있는 서버에서 응답이 수신되지 않는 경우에만 사용됩니다. 서버는 6개까지 구성할 수 있습니다. 그러나 6개의 서버는 데이터 인터페이스에서만 지원됩니다. 관리 인터페이스에서는 처음 3개 서버만 사용됩니다.

- **Domail Search Name(**도메인 검색 이름**)** - example.com과 같은 네트워크의 도메인 이름을 입력합니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다. 그룹을 데이터 인터페이스에 사용하려면 이름이 63자 미만이어야 합니다.
- **Retries(**재시도 횟수**)** — 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수(0~10회)입니다. 기본값은 2입니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.
- **Timeout(**시간 초과**)** — 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

데이터 및 관리 트래픽용 **DNS** 설정

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 서로 다른 트래픽 유형에 적용되는 두 가지 DNS 서버 설정(데이터 및 특수 관리 트래픽)이 있습니다. 데이터 트래픽에는 액세스 제어 규칙 및 원격 액세스 VPN과 같이 DNS 조회가 필요한 FQDN을 사용하는 모든 서비스가 포함됩니다. 특수 관리 트래픽에는 스마트 라이선싱 및 데이터베이스 업데이트와 같은 관리 인터페이스에서 발생하는 트래픽이 포함됩니다.

CLI 설정 마법사를 사용하는 경우 초기 시스템 컨피그레이션 중에 관리 DNS 서버를 구성합니다. device manager 설정 마법사에서 데이터 및 관리 DNS 서버를 설정할 수도 있습니다. 다음 절차를 사용하여 DNS 서버 기본값을 변경할 수 있습니다.

configure network dns servers 및 **configure network dns searchdomains** 명령을 사용하여 CLI에서 관리 DNS 컨피그레이션을 변경할 수도 있습니다. 데이터 및 관리 인터페이스가 같은 DNS 그룹을 사용 중이라면 해당 그룹이 업데이트되며 다음 구축 시 데이터 인터페이스에도 변경 사항이 적용됩니다.

DNS 서버 통신에 대한 올바른 인터페이스를 결정하기 위해 threat defense는 라우팅 조회를 사용하지만, 사용되는 라우팅 테이블은 DNS를 활성화하는 인터페이스에 따라 다릅니다. 자세한 내용은 아래 인터페이스 설정을 참조하십시오.

DNS 확인에 문제가 있는 경우 다음 주제를 참조하십시오.

- 일반 DNS 문제 문제 해결, 21 페이지
- 관리 인터페이스용 DNS 문제 해결

시작하기 전에

- DNS 서버 그룹을 만들었는지 확인합니다. 자세한 내용은 DNS 그룹 구성, 18 페이지 섹션을 참조해 주십시오.
- threat defense 디바이스에 DNS 서버에 액세스하기 위한 적절한 정적 또는 동적 경로가 있는지 확인합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **DNS Server(DNS** 서버**)**를 클릭합니다.

단계 **2** 데이터 인터페이스용 DNS를 설정합니다.

a) 모든 인터페이스 또는 특정 인터페이스에서 DNS 조회를 활성화합니다. 이러한 선택은 사용되는 라우팅 테이블에도 영향을 미칩니다.

인터페이스에서 DNS 조회를 활성화하는 것은 조회를 위해 소스 인터페이스를 지정하는 것과 다릅니다. 디바이스는 항상 경로 조회를 사용하여 소스 인터페이스를 결정합니다.

- **ANY**(인터페이스를 선택하지 않음) - 관리 및 관리 전용 인터페이스를 포함하여 모든 인터페이스에서 DNS 조회를 활성화합니다. 디바이스는 데이터 라우팅 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 인터페이스 미선택, 진단 인터페이스 또는 관리 전용 인터페이스 - 지정된 인터페이스에 DNS 조회를 활성화합니다. 디바이스는 데이터 라우팅 테이블만 확인합니다.
- 인터페이스 선택, 진단 인터페이스 또는 관리 전용 인터페이스 - 지정된 인터페이스에 DNS 조회를 활성화합니다. 디바이스는 데이터 라우팅 테이블을 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 진단 인터페이스 또는 관리 전용 인터페이스만 선택 - 진단 또는 관리 전용 인터페이스에서 DNS 조회를 활성화합니다. 디바이스는 관리 전용 라우팅 테이블만 확인합니다.

b) 데이터 인터페이스에서 사용할 서버를 정의하는 **DNS Group(DNS** 그룹**)**을 선택합니다. 그룹이 아직 없으면 **Create New DNS Group(**새 **DNS** 그룹 생성**)**을 클릭하여 바로 생성합니다. 데이터 인터페이스에서 조회를 금지하려는 경우 **None(**없음**)**을 선택합니다.

c) (선택 사항). 액세스 제어 규칙에서 FQDN 네트워크 개체를 사용하려면 **FQDN DNS Settings(FQDN DNS** 설정**)**를 구성합니다.

이러한 옵션은 FQDN 개체를 확인할 때만 사용되며 기타 모든 유형의 DNS 확인에서는 무시됩니다.

- **Poll Time(**폴링 시간**)** - FQDN 네트워크 개체를 IP 주소로 확인하는 데 사용되는 폴링 주기의 시간(분)입니다. FQDN 개체는 액세스 제어 정책에서 사용되는 경우에만 확인됩니다. 타이머는 최대 확인 주기를 결정합니다. IP 주소 확인을 업데이트할 시기를 결정할 때는 DNS 항

목의 TTL(Time to Live) 값도 사용되므로, 개별 FQDN은 폴링 주기보다 더 자주 확인될 수 있습니다. 기본값은 240분(4시간)입니다. 범위는 1~65535분입니다.

- **Expiry(**만료**)** - DNS 항목이 만료(즉, DNS 서버에서 가져온 TTL이 경과함)될 때까지의 시간(분)입니다. 이 시간이 지나면 DNS 조회 테이블에서 항목이 제거됩니다. 항목 제거 시 테이블을 다시 컴파일해야 하므로 자주 제거하면 디바이스의 처리 부하가 증가할 수 있습니다. 일부 DNS 항목은 매우 짧은 TTL(3초 정도)을 가질 수 있으므로 이 설정을 사용하여 TTL을 가상으로 늘릴 수 있습니다. 기본값은 1분입니다(즉, TTL이 경과한지 1분 이후에 항목이 제거됨). 범위는 1~65535분입니다.

d) **Save(**저장**)**를 클릭합니다. 또한 컨피그레이션을 구축하여 디바이스에 변경 사항을 적용해야 합니다.

단계 **3** 관리 인터페이스용 DNS를 설정합니다.

a) 관리 인터페이스에서 사용할 서버를 정의하는 **DNS Group(DNS** 그룹**)**을 선택합니다. 그룹이 아직 없으면 **Create New DNS Group(**새 **DNS** 그룹 생성**)**을 클릭하여 바로 생성합니다.

b) **Save(**저장**)**를 클릭합니다. 관리 DNS 서버를 업데이트하려면 변경 사항을 구축해야 합니다.

일반 **DNS** 문제 문제 해결

DNS 서버는 관리 인터페이스 및 데이터 인터페이스에 대해 각기 별도로 설정해야 합니다. 일부 기능은 이 중 하나의 유형을 통해 이름 확인을 수행하지만 두 유형을 모두 사용하지는 않습니다. 그리고 사용 방식에 따라 특정 기능이 다른 확인 방법을 사용하는 경우도 있습니다.

예를 들어 **ping** *hostname* 및 **ping interface** *interface_name hostname* 명령에서는 데이터 인터페이스 DNS 서버를 사용하여 이름을 확인하는 반면, **ping system** *hostname* 명령에서는 관리 인터페이스 DNS 서버를 사용합니다. 따라서 특정 인터페이스 및 라우팅 테이블을 통해 연결을 테스트할 수 있습니다.

호스트 이름 조회 문제를 트러블슈팅할 때는 이 점에 유념하십시오.

관리 인터페이스용 DNS 문제 해결의 경우 관리 인터페이스용 DNS 문제 해결의 내용도 참조하십시오.

이름 확인이 수행되지 않는 경우

이름 확인이 전혀 수행되지 않는 경우의 몇 가지 트러블슈팅 팁은 다음과 같습니다.

- 관리 인터페이스 및 데이터 인터페이스 모두에 대해 DNS 서버를 구성했는지 확인합니다. 데이터 인터페이스의 경우 인터페이스로 Any(모두)를 사용합니다. 일부 인터페이스에서 DNS를 허용하지 않으려는 경우에만 인터페이스를 명시적으로 지정하십시오.
- 데이터 인터페이스에서 조회를 위해 진단 인터페이스를 사용하고 있는 경우, 인터페이스에 IP 주소를 컨피그레이션했는지 확인합니다. 조회하려면 인터페이스에 IP 주소가 있어야 합니다.
- 진단 인터페이스를 통해 또는 관리 전용 인터페이스를 통해 DNS 서버에 연결할 수 없는데, 경로 조회 시 데이터 라우팅 테이블에서 일치를 찾으므로 관리 전용 라우팅 테이블에 대한 폴백이 없기 때문입니다. 진단 인터페이스를 사용하려면 해당 인터페이스만 선택해야 합니다.

- 각 DNS 서버의 IP 주소에 대해 ping을 실행하여 해당 주소에 연결할 수 있는지 확인합니다. 특정 인터페이스를 테스트하려면 **system** 및 **interface** 키워드를 사용합니다. ping에 실패하면 정적 경로와 게이트웨이를 확인합니다. 서버에 정적 경로를 추가해야 할 수 있습니다.
- ping에 성공했으나 이름 확인에 실패하는 경우 액세스 제어 규칙을 확인합니다. 서버 연결에 사용하는 인터페이스에 대해 DNS 트래픽(UDP/53)을 허용하고 있는지 확인합니다. 시스템과 DNS 서버 사이에 있는 디바이스에 의해 이 트래픽이 차단될 수도 있으므로 다른 DNS 서버를 사용해야 할 수 있습니다.
- ping이 정상적으로 실행되고 적절한 경로가 있으며 액세스 제어 규칙에 문제가 없다면 DNS 서버에 FQDN에 대한 매핑이 없을 가능성을 고려하십시오. 이러한 경우에는 다른 서버를 사용해야 할 수 있습니다.

잘못된 이름이 확인되는 경우

이름이 확인되기는 하지만 이름의 IP 주소가 최신 정보가 아닌 경우 캐싱 문제가 있을 수 있습니다. 이 문제는 액세스 제어 규칙에 사용되는 FQDN 네트워크 개체 등의 데이터 인터페이스 기반 기능에만 영향을 줍니다.

시스템에는 이전 조회에서 가져온 DNS 정보의 로컬 캐시가 있습니다. 새 조회를 수행해야 하는 경우 시스템은 먼저 로컬 캐시를 확인합니다. 로컬 캐시에 해당 정보가 있으면 그 결과 IP 주소를 반환합니다. 로컬 캐시에서 요청을 해결하지 못하면 DNS 서버로 DNS 쿼리가 전송됩니다. 외부 DNS 서버에서 요청을 해결한 경우 그 결과 IP 주소는 해당 호스트 이름과 함께 로컬 캐시에 저장됩니다.

각 조회에는 DNS 서버에 의해 정의되며 캐시에서 자동으로 만료되는 TTL(Time to Live) 값이 있습니다. 또한 시스템은 액세스 제어 규칙에 사용되는 FQDN의 값을 주기적으로 새로 고칩니다. 이러한 새로 고침은 최소한 폴링 시간 간격(기본적으로 4시간마다)으로 수행되지만 항목의 TTL(Time to Live) 값에 따라 더 자주 수행될 수도 있습니다.

로컬 캐시를 확인하려면 **show dns-hosts** 및 **show dns** 명령을 사용합니다. FQDN의 IP 주소가 잘못된 경우, **dns update** [**host** *hostname*] 명령을 사용하여 시스템에서 정보를 새로 고치도록 강제할 수 있습니다. 호스트를 지정하지 않고 명령을 사용하면 모든 호스트 이름이 새로 고쳐집니다.

clear dns [**host** *fqdn*] 및 **clear dns-hosts cache** 명령을 사용하면 캐시된 정보를 제거할 수 있습니다.

관리 인터페이스 구성

관리 인터페이스는 물리적 관리 포트에 연결된 가상 인터페이스입니다. 물리적 인터페이스에는 진단 가상 인터페이스도 포함됩니다. 이 인터페이스는 다른 물리적 인터페이스를 사용하여 **Interfaces(**인터페이스**)** 페이지에서 구성할 수 있습니다. 진단 인터페이스에 대한 자세한 내용은 관리/진단 인터페이스를 참조하십시오.

관리 인터페이스는 다음과 같은 두 가지 용도로 사용됩니다.

- IP 주소에 대한 웹 및 SSH 연결을 열고 인터페이스를 통해 디바이스를 구성할 수 있습니다.
- 시스템은 이 IP 주소를 통해 스마트 라이선싱 및 데이터베이스 업데이트를 가져옵니다.

CLI 설정 마법사를 사용하는 경우 초기 시스템 컨피그레이션 중에 디바이스의 관리 주소 및 게이트웨이를 구성합니다. device manager 설정 마법사를 사용하는 경우에는 관리 주소와 게이트웨이가 기본값으로 유지됩니다.

필요한 경우 device manager를 통해 이러한 주소를 변경할 수 있습니다. **configure network ipv4 manual** 및 **configure network ipv6 manual** 명령을 사용하여 CLI에서 관리 주소 및 게이트웨이를 변경할 수도 있습니다. 기본 관리 인터페이스 설정을 복원하려면 **configure network** {**ipv4** | **ipv6**} **dhcp-dp-route** 명령을 사용하십시오.

고정 주소를 정의할 수도 있고, 관리 네트워크의 다른 디바이스가 DHCP 서버로 작동하는 경우에는 DHCP를 통해 주소를 가져올 수 있습니다. 대부분의 플랫폼에서 관리 인터페이스는 기본적으로 DHCP에서 IP 주소를 가져옵니다.

⚠

주의 현재 연결된 주소를 변경할 경우 변경 사항을 저장하면 즉시 적용되므로 device manager 또는 CLI에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다. 관리 네트워크에서 새 주소가 유효하며 사용 가능한지 확인합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **Management Interface(**관리 인터페이스**)**를 클릭하면 됩니다.

단계 **2** 관리 게이트웨이를 정의할 방법을 선택합니다.

게이트웨이는 시스템에서 스마트 라이선스 및 데이터베이스 업데이트(VDB, 규칙, 지리위치, URL 등)를 받고 관리 DNS 및 NTP 서버에 접속하기 위해 인터넷에 연결할 수 있는 방법을 결정합니다. 다음 옵션 중에서 선택합니다.

정적 **IP** 옵션**:**

- 데이터 인터페이스를 게이트웨이로 사용 - 별도의 관리 네트워크를 관리 인터페이스에 연결하지 않은 경우 이 옵션을 선택합니다. 라우팅 테이블에 따라 트래픽이 인터넷에 라우팅되며, 대개 외부 인터페이스를 거칩니다. 이 옵션은 threat defense virtual 디바이스에서는 지원되지 않습니다.
- 관리 인터페이스에 고유 게이트웨이 사용 - 별도의 관리 네트워크를 관리 인터페이스에 연결한 경우 IPv4 및 IPv6를 위한 고유 게이트웨이(아래)를 지정합니다.

DHCP IP 옵션**:**

- 데이터 인터페이스에 대체 시스템을 가진 관리 인터페이스에 고유한 게이트웨이 사용-DHCP 서버가 게이트웨이를 제공하는 경우 시스템은 관리 인터페이스를 통해 게이트웨이를 통과하는 관리 트래픽을 라우팅합니다. DHCP 서버가 게이트웨이를 제공하지 않는 경우, 시스템은 데이터

인터페이스 라우팅 테이블에 따라 관리 트래픽을 라우팅합니다. 일반적으로 외부 인터페이스를 통해 트래픽을 전송합니다. 이 옵션은 threat defense virtual 디바이스에서는 지원되지 않습니다.

- 관리 인터페이스에 고유한 게이트웨이 사용**(**대체 시스템 없음**)**— 시스템은 관리 인터페이스를 통해 DHCP 서버에서 제공하는 게이트웨이로 관리 트래픽을 라우팅합니다. DHCP 서버가 게이트웨이를 제공하지 않는 경우 시스템은 관리 인터페이스의 로컬 호스트에만 연결할 수 있습니다. 데이터 인터페이스를 통해 라우팅하려면 Fallback(대체 시스템) 옵션을 선택합니다.

단계 **3** IPv4, IPv6 중 하나 또는 둘 다의 관리 주소, 서브넷 마스크 또는 IPv6 접두사 및 게이트웨이(필요한 경우)를 구성합니다.

속성 집합을 하나 이상 구성해야 합니다. 특정 집합의 주소 지정 방법을 비활성화하려면 해당 집합을 비워 둡니다.

Type(유형**)** > **DHCP**를 선택하여 DHCP 또는 IPv6 자동 컨피그레이션을 통해 주소와 게이트웨이를 가져옵니다.

단계 **4** (선택 사항). 정적 IPv4 주소를 구성하는 경우 인터페이스에서 DHCP 서버를 구성합니다.

관리 인터페이스에서 DHCP 서버를 구성하는 경우, 관리 네트워크의 클라이언트가 DHCP 풀에서 주소를 가져올 수 있습니다. 이 옵션은 threat defense virtual 디바이스에서는 지원되지 않습니다.

a) **Enable DHCP Server(DHCP** 서버 활성화**)** > **On(**켜기**)**을 클릭합니다.
b) 서버의 주소 풀을 입력합니다.

주소 풀은 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 이 IP 주소 범위는 관리 주소와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 192.168.45.46-192.168.45.254와 같이 지정합니다.

단계 **5** **Save(**저장**)**를 클릭하고 경고를 확인한 후에 **OK(**확인**)**를 클릭합니다.

디바이스 호스트 이름 구성

디바이스 호스트 이름을 변경할 수 있습니다.

configure network hostname 명령을 사용하여 CLI에서 호스트네임을 변경할 수도 있습니다.

⚠

주의 호스트 이름을 사용하여 시스템에 연결할 때 호스트 이름을 변경하는 경우 변경 사항을 저장하면 즉시 적용되므로 device manager에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **Hostname(**호스트네임**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 호스트 이름을 클릭하면 됩니다.

단계 **2** 새 호스트 이름을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

일부 시스템 프로세스의 경우에는 호스트 이름 변경 사항이 즉시 적용됩니다. 그러나 모든 시스템 프로세스에서 같은 이름이 사용되도록 하려면 변경 사항을 구축하여 업데이트를 완료해야 합니다.

시간 서비스(NTP, PTP) 구성

시스템은 NTP(Network Time Protocol)를 사용하여 시스템 시간을 설정합니다. NTP를 구성해야 합니다.

디바이스가 Cisco ISA 3000 어플라이언스인 경우, 네트워크에서 PTP를 사용하는 경우에도 PTP(Precision Time Protocol)를 구성할 수 있습니다.

NTP(Network Time Protocol) 구성

시스템에서 시간을 정의하려면 NTP(Network Time Protocol) 서버를 구성해야 합니다. NTP 서버는 초기 시스템 설정 시 구성하지만, 다음 절차를 통해 변경할 수 있습니다. NTP 연결에 문제가 있는 경우, NTP 트러블슈팅를 참조하십시오.

threat defense 디바이스는 NTPv4를 지원합니다.

참고 Firepower 4100/9300의 경우, device manager을 통해 NTP를 설정하지 않습니다. FXOS에서 NTP를 컨피그레이션하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Time Services(**시간 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Time Services(**시간 서비스**)**를 클릭하면 됩니다.

단계 **2** **NTP Time Server(NTP** 시간 서버**)**에서 자체 시간 서버를 사용할지 아니면 Cisco 시간 서버를 사용할지를 선택합니다.

- **Default NTP Servers(**기본 **NTP** 서버**) -** 이 옵션을 선택하는 경우 서버 목록에는 NTP에 사용되는 서버 이름이 표시됩니다.
- **User-Defined NTP Servers(**사용자 정의 **NTP** 서버**) -** 이 옵션을 선택하는 경우 사용하려는 NTP 서버의 IPv4 또는 IPv6 주소 또는 FQDN(Fully Qualified Domain Name)을 입력합니다. 예를 들어 ntp1.example.com 또는 10.100.10.10을 입력합니다. NTP 서버를 3개까지 추가할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

PTP(Precision Time Protocol) 구성(ISA 3000)

PTP(Precision Time Protocol)는 패킷 기반 네트워크에서 다양한 디바이스의 클록을 동기화하기 위해 개발된 시간 동기화 프로토콜입니다. 이러한 디바이스 클록은 일반적으로 정밀도와 안정성이 다양합니다. 이 프로토콜은 산업, 네트워크에 연결된 측정 및 제어 시스템을 위해 특별히 설계되었으며 최소한의 대역폭 및 적은 처리 오버헤드를 필요로 하기 때문에 분산 시스템에서 사용하기에 가장 적합합니다.

PTP 시스템은 PTP 및 비 PTP 디바이스의 조합으로 구성된 분산형, 네트워크에 연결된 시스템입니다. PTP 디바이스에는 일반 클록, 경계 클록 및 투명 클록이 있습니다. 비 PTP 디바이스에는 네트워크 스위치, 라우터 및 기타 인프라 디바이스가 있습니다.

threat defense 디바이스를 투명 클록이 되도록 구성할 수 있습니다. threat defense 디바이스에서는 클록을 PTP 클록과 동기화하지 않습니다. threat defense 디바이스에서는 PTP 클록에 정의된 대로 PTP 기본 프로필을 사용합니다.

PTP 디바이스를 구성할 때 함께 작동할 디바이스의 도메인 번호를 정의합니다. 따라서 여러 PTP 도메인을 구성한 다음, 하나의 특정 도메인에 대해 PTP 클록을 사용하도록 비 PTP 디바이스를 각각 구성할 수 있습니다.

시작하기 전에

디바이스에서 사용해야 하는 PTP 클록에 구성된 도메인 번호를 결정합니다. 또한 시스템에서 도메인의 PTP 클록에 연결하기 위해 통과하는 인터페이스를 결정합니다.

다음은 PTP 구성에 대한 지침입니다.

- 이 기능은 Cisco ISA 3000 어플라이언스에서만 사용할 수 있습니다.
- Cisco PTP는 멀티캐스트 PTP 메시지만 지원합니다.
- PTP는 IPv4 네트워크용으로만 사용할 수 있으며 IPv6 네트워크용으로는 사용할 수 없습니다.
- PTP 구성은 라우팅 또는 브리지 그룹 멤버에 관계없이 물리적 이더넷 데이터 인터페이스에서 지원됩니다. 이는 관리 인터페이스, 하위 인터페이스, EtherChannel, BVI(Bridge Virtual Interfaces) 또는 기타 가상 인터페이스에서 지원되지 않습니다.
- VLAN 하위 인터페이스에서 이동하는 PTP가 지원되며 이때 적절한 PTP 구성이 현재 상위 인터페이스에 있다고 가정합니다.

- PTP 패킷이 디바이스를 통해 이동할 수 있는지 확인해야 합니다. PTP 트래픽은 UDP 대상 포트 319 및 320과 대상 IP 주소 224.0.1.129로 식별되므로 이 트래픽을 허용하는 액세스 제어 규칙이 작동해야 합니다.
- 라우팅 인터페이스 간에 PTP 패킷이 이동할 경우, 멀티캐스트 라우팅을 활성화해야 하며 각 인터페이스는 224.0.1.129 IGMP 멀티캐스트 그룹에 조인해야 합니다. 동일한 브리지 그룹에 있는 인터페이스 간에 PTP 패킷이 이동할 경우에는 멀티캐스트 라우팅을 활성화하고 IGMP 그룹을 구성하지 않아도 됩니다.

프로시저

단계 **1** PTP 클록 연결 인터페이스의 구성을 확인합니다.

기본 구성에서는 모든 인터페이스를 동일한 브리지 그룹에 배치하지만, 브리지 그룹에서 인터페이스를 제거할 수 있습니다. 멀티캐스트 IGMP 그룹과 관련하여 다르게 구성해야 하므로 인터페이스가 라우팅되었는지 아니면 브리지 그룹 멤버인지 여부를 확인하는 것이 중요합니다.

다음 절차에서는 브리지 그룹에 포함된 인터페이스를 확인하는 방법에 대해 설명합니다. PTP용으로 구성하는 인터페이스가 브리지 그룹 멤버인지 확인합니다.

a) **Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 **View All Interfaces(**모든 인터페이스 보기**)**를 클릭합니다.
b) 목록에서 인터페이스를 찾고 Mode(모드) 열을 선택합니다. BridgeGroupMember는 브리지 그룹의 일부임을 의미하며, 그 외의 경우에는 라우팅되어야 합니다.

단계 **2** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Time Services(**시간 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **Time Services(**시간 서비스**)**를 클릭하면 됩니다.

단계 **3** PTP 설정을 구성합니다.

- **Domain Number(**도메인 번호**)** — 네트워크의 PTP 디바이스에 구성된 도메인 번호(0~255)입니다. 다른 도메인에서 수신한 패킷은 일반 멀티캐스트 패킷으로 처리되며 PTP 처리를 거치지 않습니다.
- **Clock Mode(**클록 모드**)** — **EndToEndTransparent**를 선택합니다. 이 디바이스는 PTP 투명 클록으로만 작동할 수 있습니다.

  또는 **Forward(**포워드**)**를 선택할 수 있지만, 이는 PTP를 구성하지 않는 것과 같습니다. 도메인 번호가 무시됩니다. PTP 패킷은 멀티캐스트 트래픽에 대한 라우팅 테이블을 기준으로 디바이스를 통과합니다. 이는 기본 PTP 컨피그레이션입니다.
- **Interfaces(**인터페이스**)** — 시스템이 네트워크의 PTP 클록에 연결할 때 통과하는 모든 인터페이스를 선택합니다. PTP는 이러한 인터페이스에서만 활성화됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 선택한 인터페이스 중에서 라우팅된 인터페이스, 즉 브리지 그룹 구성원이 아닌 인터페이스의 경우에는 FlexConfig를 사용하여 멀티캐스트 라우팅을 활성화하고 라우팅된 인터페이스를 올바른 IGMP 그룹에 조인해야 합니다.

선택한 모든 인터페이스가 브리지 그룹 구성원인 경우 이 단계를 완료하지 마십시오. 브리지 그룹 구성원에서 IGMP를 구성하려고 하면 구축 오류가 발생합니다.

a) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

c) 멀티캐스트 라우팅을 활성화하고 라우팅된 인터페이스에 대한 IGMP 조인을 구성하는 데 필요한 개체를 생성합니다.

다음은 개체에 대한 기본 템플릿이 될 수 있습니다. 이 예시에서 GigabitEthernet1/2는 PTP를 활성화하는 하나의 라우팅된 인터페이스입니다. 인터페이스 하드웨어 이름을 적절하게 변경하고, 라우팅된 인터페이스가 두 개 이상 있을 경우 각각의 추가 인터페이스에 **interface** 및 **igmp** 명령을 반복합니다.

igmp 명령은 224.0.1.129 IGMP 그룹에 조인합니다. 이 주소는 네트워크 주소와 관계없이 모든 인터페이스에 대한 올바른 IP 주소입니다.

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

무효화 템플릿은 다음과 같이 표시됩니다.

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭하고, 이 개체를 FlexConfig 정책에 추가한 후 **Save(**저장**)**를 클릭합니다.

미리보기에 개체의 정상적인 명령이 표시되는지 확인합니다.

다음에 수행할 작업

변경 사항을 구축한 후에 PTP 설정을 확인할 수 있습니다. device manager CLI 콘솔에서 또는 SSH나 콘솔 세션에서 다양한 **show ptp** 명령을 실행합니다. 예를 들어 GigabitEthernet1/2에만 도메인 10에 대한 PTP를 구성한 경우, 출력은 다음과 같이 표시될 수 있습니다.

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
```

```
PTP PORT DATASET: GigabitEthernet1/1
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 1
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/2
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 2
 PTP version: 2
 Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/3
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 3
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 4
 PTP version: 2
 Port state: Disabled
```

관리 연결용 HTTP 프록시 구성

시스템과 인터넷 사이에 직접 연결이 없는 경우 관리 인터페이스에 대한 HTTP 프록시를 설정할 수 있습니다. 그러면 시스템에서 데이터베이스 업데이트를 다운로드하기 위해 device manager에 대한 연결 및 시스템에서 Cisco로의 연결을 비롯한 모든 관리 연결에 프록시를 사용합니다.

configure network http-proxy 명령을 사용하여 threat defense CLI에서 HTTP 프록시를 구성할 수도 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **HTTP Proxy(HTTP** 프록시**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **HTTP Proxy(HTTP** 프록시**)**를 클릭하면 됩니다.

단계 **2** 토글을 클릭하여 프록시를 활성화한 다음, 프록시 설정을 구성합니다.

- **HTTP Proxy(HTTP** 프록시**)** — 프록시 서버의 IP 주소입니다.
- **Port(**포트**)** — 프록시 서버가 HTTP 연결을 수신 대기하도록 구성된 포트 번호입니다.
- **Use Proxy authentication(**프록시 인증 사용**)** — 서버가 프록시 연결에 대한 인증을 요구하도록 구성된 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우에는 프록시 서버에 로그인할 수 있는 어카운트의 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**도 입력합니다.

단계 **3** **Save(**저장**)**를 클릭한 다음, 변경할 사항을 확인합니다.

변경 사항은 즉시 적용됩니다. 구축 작업은 필요하지 않습니다.

시스템에서 관리 연결을 완료하는 방법을 변경하고 있으므로 device manager에 대한 연결이 끊어집니다. 변경을 완료하려면 몇 분 정도 기다린 다음, 브라우저 창을 새로 고침하시고 다시 로그인하십시오.

클라우드 서비스 구성

Cisco Defense Orchestrator, Cisco Threat Response 및 CDO와 같은 다양한 클라우드 기반 애플리케이션을 사용할 수 있도록 클라우드 서비스에 등록할 수 있습니다.

클라우드에 등록되면 페이지에 등록 상태와 테넌시 유형 및 디바이스가 등록된 어카운트 이름이 표시됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

디바이스가 등록되지 않은 경우 이 페이지에는 Cisco 클라우드에 등록하기 위한 등록 방법이 표시됩니다. 클라우드에 등록한 후에는 개별 클라우드 서비스를 활성화 또는 비활성화할 수 있습니다.

단계 **2** Cisco 클라우드에 등록하려면(평가 모드에서 또는 클라우드 서비스에서 등록을 취소한 후) 다음 옵션 중 하나를 선택합니다.

- **Security/CDO Account(**보안/**CDO** 계정**)** — 다음 방법 중 하나를 사용할 수 있습니다.

  참고 CDO는 클라우드 제공 관리 센터를 사용해 threat defense 디바이스를 관리할 수 있습니다. CDO의 간소화된 디바이스 관리자 기능은 이미 이 모드에서 threat defense를 관리하고 있는 기존 사용자만 사용할 수 있습니다.

  - **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator**에서 테넌시로 자동 등록**)**(Firepower 1000, 2100, Secure Firewall 3100만 해당). 등록 키를 얻는 대신 자동 등록을 사용할 수 있습니다. 먼저, CDO로 이동하여 디바이스의 일련 번호를 사용하여 디바이스를 추가합니다. 그 다음 device manager에서 이 체크 박스를 선택하고 등록을 시작합니다. 디바이스 섀시 또는 포장 전표에서 일련 번호를 확인합니다. FXOS의 경우 FXOS CLI로 이동하고 **show chassis detail** 명령을 사용하여 일련 번호(SN)로 레이블이 표시된 올바른 일련 번호를 검색할 수 있습니다. threat defense 명령 **show serial-number**은 CDO 등록에 권장되지 않는 다른 일련 번호를 제공합니다. 이 방법은 CDO의 클라우드 제공 관리 센터 및 CDO의 레거시 디바이스 관리자 모드에서 작동합니다.
  - CDO 또는 보안 계정에 로그인하여 등록 키를 생성합니다. 그런 다음 이 페이지로 돌아와서 **Cloud Services Region(**클라우드 서비스 영역**)**을 선택하고 **Registration Key(**등록 키**)**에 붙여

넣습니다. 이 방법은 CDO의 레거시 디바이스 관리자 모드에서만 작동합니다. CDO의 클라우드 제공 관리 센터는 Device Manager에서 Management Center 또는 CDO로 전환, 36 페이지를 참조하십시오.

이때 **Cisco Defense Orchestrator** 및 **Cisco Success Network**를 활성화할 수도 있습니다. 이는 기본적으로 활성화됩니다.

- 스마트 라이선스—(CDO 미사용 시에만 해당) 링크를 클릭하여 Smart Licensing(스마트 라이선싱) 페이지로 이동하고 CSSM에 등록합니다. 등록 프로세스 중에 Cisco Success Network를 활성화하는 경우

  참고 클라우드 서비스에서 등록을 취소했거나 등록을 위한 스마트 라이선스 접근 방식에 몇 가지 추가 단계가 있습니다. 이 경우 **Cloud Services Region(**클라우드 서비스 지역**)**을 선택한 다음, **Register (**등록**)**를 클릭합니다. 공개된 내용을 읽고 **Accept(**수락**)**를 클릭합니다.

단계 **3** 클라우드 서비스에 등록한 후에는 필요에 따라 기능을 활성화하거나 비활성화할 수 있습니다. 다음 주제를 참고하십시오.

- 활성화 또는 비활성화 CDO (레거시 디바이스 관리자 모드), 31 페이지
- Cisco Success Network에 연결, 32 페이지
- Cisco Cloud로 이벤트 전송, 33 페이지
- 클라우드 서비스에서 등록 취소, 34 페이지

활성화 또는 비활성화 CDO (레거시 디바이스 관리자 모드)

참고 이 섹션은 CDO의 레거시 디바이스 관리자 모드에만 적용되며 클라우드 제공 관리 센터에는 적용되지 않습니다.

클라우드 서비스 구성, 30 페이지에서 권장하는 대로 CDO의 등록 키를 사용하여 클라우드 서비스에 등록한 경우, 디바이스가 이미 CDO에 등록되어 있습니다. 나중에 필요에 따라 연결을 비활성화하거나 다시 활성화할 수 있습니다.

디바이스가 스마트 라이선싱을 사용하여 클라우드 서비스에 등록된 경우 CDO를 활성화하면 문제가 발생합니다. 디바이스가 CDO 인벤토리에 표시되지 않습니다. 먼저 클라우드 서비스에서 디바이스 등록을 해제하는 것이 좋습니다. 기어(⚙) 드롭다운 목록에서 **Unregister Cloud Services(**클라우드 서비스 등록 해제**)**를 선택합니다. 등록을 취소한 후에는 CDO에서 등록 토큰을 가져오고 클라우드 서비스 구성, 30 페이지에서 설명하는 것과 같이 토큰과 보안 어카운트를 사용하여 다시 등록합니다.

클라우드 관리 방식에 대한 자세한 내용을 확인하려면 CDO 포털(http://www.cisco.com/go/cdo)을 참조하거나 서비스를 받고 있는 리셀러 또는 파트너에게 문의하십시오.

시작하기 전에

고가용성을 구성하려는 경우 고가용성 그룹에서 사용할 두 디바이스를 모두 등록해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 CDO 기능의 **Enable(**활성화**)**/**Disable(**비활성화**)** 버튼을 클릭합니다.

Cisco Success Network에 연결

디바이스를 등록할 때 Cisco Success Network에 대한 연결을 활성화할지를 결정합니다. 디바이스 등록의 내용을 참조하십시오.

Cisco Success Network를 활성화하면 Cisco가 기술 지원을 제공하는 데 필수적인 사용자 정보 및 통계를 Cisco에 제공하게 됩니다. 또한, 이 정보를 통해 Cisco는 제품을 개선할 수 있으며 사용 가능하지만 사용되지 않은 기능을 알려 네트워크의 제품 가치를 최대화하도록 할 수 있습니다.

연결을 활성화하는 경우, 디바이스에서는 기술 지원 서비스, 클라우드 관리 및 모니터링 서비스와 같은 Cisco의 추가 제공 서비스에 참여할 수 있도록 Cisco Cloud에 대한 보안 연결을 설정합니다. 디바이스는 이 안전한 연결을 설정하고 항상 유지합니다. 클라우드에서 연결을 완전히 해제하는 방법에 대한 내용은 클라우드 서비스에서 등록 취소, 34 페이지를 참조하십시오.

디바이스를 등록하고 나면 Cisco Success Network 설정을 변경할 수 있습니다.

참고 시스템에서 Cisco에 데이터를 전송할 때 작업 목록에는 텔레메트리 작업이 표시됩니다.

시작하기 전에

Cisco Success Network를 활성화하려면 디바이스를 클라우드에 등록해야 합니다. 디바이스를 등록하려면 디바이스를 Cisco Smart Software Manager(Smart Licensing(스마트 라이선싱) 페이지)에 등록(등록 중 Cisco Success Network 옵션 선택)하거나, 등록 키를 입력(CDO 전용 레거시 디바이스 관리자 모드)하여 CDO에 등록하십시오.

참고 고가용성 그룹의 액티브 유닛에서 Cisco Success Network를 활성화하면 스탠바이 유닛에서도 연결이 활성화됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 Cisco Success Network 기능의 **Enable**/**Disable(**활성화/비활성화**)** 제어를 클릭합니다.

sample data(샘플 데이터**)** 링크를 클릭하면 Cisco에 전송된 정보 유형을 확인할 수 있습니다.

연결을 활성화하는 경우 공개되는 내용을 읽고 **Accept(**수락**)**를 클릭합니다.

Cisco Cloud로 이벤트 전송

Cisco Cloud 서버에 이벤트를 전송할 수 있습니다. 여기서는 다양한 Cisco Cloud 서비스에서 이벤트에 액세스할 수 있습니다. 그러면 이러한 클라우드 애플리케이션(예: SecureX threat response)을 사용하여 이벤트를 분석하고 디바이스에 발생했을 가능성이 있는 위협을 평가할 수 있습니다.

클라우드 툴은 전송하는 이벤트의 사용 여부를 결정합니다. 사용하지 않는 이벤트를 클라우드로 보내지 않으면서 대역폭 및 스토리지 공간을 모두 낭비하지 않도록 툴의 설명서를 참조하거나 이벤트 데이터를 검토하십시오. 툴은 동일한 소스에서 이벤트를 가져오므로 선택 시 가장 제한적인 툴이 아니라 사용하는 모든 툴을 반영해야 합니다. 대표적인 예는 다음과 같습니다.

- CDO의 보안 애널리틱스 및 로깅 툴은 모든 연결 이벤트를 사용할 수 있습니다.
- SecureX threat response 및 SecureX는 우선순위가 높은 연결 이벤트만 사용하므로 이러한 툴만 사용하는 경우에는 모든 연결 이벤트를 클라우드로 전송할 필요가 없습니다. 또한 이러한 툴은 보안 인텔리전스 우선순위가 높은 이벤트만 사용합니다.

시작하기 전에

디바이스를 클라우드 서비스에 등록해야 이 서비스를 활성화할 수 있습니다.

미국 지역의 경우 https://visibility.amp.cisco.com/에서, EU 지역의 https://visibility.eu.amp.cisco.com경우에는 에서, APJC 지역의 경우 https://visibility.apjc.amp.cisco.com에서 SecureX threat response에 연결할 수 있습니다. http://cs.co/CTRvideos에서 YouTube를 통해 애플리케이션의 용도와 이점에 대한 비디오를 볼 수 있습니다. SecureX threat response와 함께 threat defense를 사용하는 방법에 대한 자세한 내용은 *Cisco Secure Firewall Threat Defense* 및 *SecureX threat* 통합 가이드(https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 확인 가능)를 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 **Send Events to the Cisco Cloud(Cisco Cloud**에 이벤트 전송**)** 옵션의 **Enable**/**Disable(**활성화/비활성화**)** 제어를 클릭합니다.

단계 **3** 서비스를 활성화하는 경우 클라우드에 전송할 이벤트를 선택하라는 메시지가 표시됩니다. 나중에 선택한 이벤트 목록 옆에 있는 **Edit(**수정**)**를 클릭하여 이러한 선택 사항을 변경할 수 있습니다. 전송할 이벤트 유형을 선택하고 **OK(**확인**)**를 클릭합니다.

- **File/Malware(**파일/악성코드**)** - 액세스 제어 규칙에 적용한 모든 파일 정책에 해당합니다.
- **Intrusion(**침입**)** - 액세스 제어 규칙에 적용한 모든 침입 정책에 해당합니다.
- **Connection(**연결**)** - 기록을 활성화한 액세스 제어 규칙에 해당합니다. 이 옵션을 선택하는 경우 모든 연결 이벤트를 전송하거나 높은 우선순위 연결 이벤트만 전송하도록 선택할 수도 있습니다. 높은 우선순위 연결 이벤트는 침입, 파일 또는 악성코드 이벤트를 트리거하는 연결이나 보안 인텔리전스 차단 정책과 일치하는 연결과 관련된 이벤트입니다.

클라우드 서비스에서 등록 취소

더 이상 클라우드 서비스를 사용하지 않으려는 경우 클라우드에서 디바이스 등록을 취소할 수 있습니다. 디바이스를 서비스에서 제거하거나 달리 삭제하는 경우 등록을 취소할 수 있습니다. 클라우드 서비스 지역을 변경해야 하는 경우 등록을 취소한 후 다시 등록할 때 새 지역을 선택합니다.

이 절차를 사용하여 클라우드에서 등록을 취소해도 스마트 라이선싱 등록에는 영향을 주지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 기어(⚙) 드롭다운 목록에서 **Unregister Cloud Services(**클라우드 서비스 등록 취소**)**를 선택합니다.

단계 **3** 경고를 읽고 **Unregister(**등록 취소**)**를 클릭합니다.

활성화한 클라우드 서비스는 자동으로 비활성화되며 해당 서비스를 다시 활성화할 수 있는 기능은 제거됩니다. 그러나 이제 클라우드에 등록하기 위한 컨트롤이 표시되고 다시 등록할 수 있습니다.

웹 분석 활성화 또는 비활성화

웹 분석을 활성화하면 페이지 조회 수를 기반으로 하는 익명 제품 사용 정보가 Cisco에 제공됩니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Web Analytics(**웹 분석**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Web Analytics(**웹 분석**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 **Web Analytics(**웹 분석**)** 기능의 **Enable**/**Disable(**활성화/비활성화**)** 제어를 클릭합니다.

URL Filtering(URL 필터링) 기본 설정 컨피그레이션

시스템에서는 CSI(Cisco 종합적 보안 인텔리전스)(Cisco Talos Intelligence Group(Talos))에서 URL 카테고리 및 평판 데이터베이스를 가져옵니다. 이러한 환경 설정은 데이터베이스 업데이트 및 시스템이 카테고리나 평판을 알 수 없는 URL을 처리하는 방법을 제어합니다. 이러한 환경 설정을 지정하려면 URL 필터링 라이선스를 활성화해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 환경 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **URL** 필터링 기본 설정을 클릭하면 됩니다.

단계 **2** 다음 옵션을 구성합니다.

- **Enable Automatic Updates(**자동 업데이트 활성화**)** - 업데이트된 URL 데이터를 시스템에서 자동으로 확인하고 다운로드할 수 있도록 합니다. 이 데이터에는 카테고리 및 평판 정보가 포함됩니다. 시스템은 30분마다 업데이트를 확인하지만, 데이터는 대개 매일 한 번씩 업데이트됩니다. 기

본적으로는 업데이트가 활성화됩니다. 이 옵션을 선택 취소하는 경우 범주 및 평판 필터링을 사용 중이라면 자동 업데이트를 주기적으로 활성화하여 새 URL 데이터를 가져옵니다.

- **Query Cisco CSI for Unknown URLs(Cisco CSI**에서 알 수 없는 **URL** 쿼리**)** - 로컬 URL 필터링 데이터베이스에 범주 및 평판 데이터가 없는 URL에 대해 Cisco CSI에 업데이트된 정보를 확인할지를 선택합니다. 조회에서 적절한 시간제한 이내에 이 정보가 반환되면 URL 조건을 기준으로 액세스 규칙을 선택할 때 해당 정보가 사용됩니다. 그렇지 않으면 URL은 미분류 범주와 일치합니다. 메모리 제한으로 인해 더 작은 URL 데이터베이스를 설치하는 저가형 시스템에서는 이 옵션을 반드시 선택해야 합니다.
- **URL Time to Live(Query Cisco CSI for Unknown URLs(**알 수 없는 **URL**의 경우 **Cisco CSI**에 쿼리**)**를 선택하면 사용 가능함) - 지정된 URL에 대해 카테고리 및 평판 조회 값을 캐시할 기간입니다. TTL(Time to Live)이 만료되면 다음 번에 URL 액세스를 시도할 때 카테고리/평판을 새로 조회합니다. 이 시간이 짧을수록 URL 필터링 정확도가 높아지고, 시간이 길수록 알 수 없는 URL에 대한 필터링 성능이 향상됩니다. TTL은 2, 4, 8, 12, 24, 48시간, 1주 또는 Never(안 함, 기본값)로 설정할 수 있습니다.

단계 **3** 필요에 따라 **Check the Category for a URL(URL**의 카테고리 확인**)**이 가능합니다.

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. **URL to Check(**확인할 **URL)** 상자에서 URL을 입력하고 **Go(**이동**)**를 클릭하십시오. 결과를 볼 수 있는 외부 웹 사이트로 연결됩니다. 분류에 동의하지 않는 경우 **Submit a URL Category Dispute(URL** 카테고리 이의 제출**)** 링크를 클릭하고 저희에게 알려주십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

Device Manager에서 Management Center 또는 CDO로 전환

device manager에서 전환하고자 하는 경우 관리를 위해 threat defense 디바이스가 management center 또는 CDO에 연결되도록 구성할 수 있습니다.

참고 CDO는 클라우드 제공 관리 센터를 사용해 threat defense 디바이스를 관리할 수 있습니다. CDO의 간소화된 디바이스 관리자 기능은 이미 이 모드에서 threat defense를 관리하고 있는 기존 사용자만 사용할 수 있습니다. 이 절차는 클라우드 제공 관리 센터에만 적용됩니다.

device manager을 사용하여 management center/CDO 설정을 수행할 때 관리를 위해 management center/CDO로 전환하면 관리 인터페이스 및 관리자 액세스 설정과 더불어 device manager에서 완료된 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책 또는 보안 영역과 같은 기타 기본 구성 설정은 유지되지 않습니다. threat defense CLI를 사용하는 경우 관리 및 management center/CDO 액세스 설정만 유지됩니다(예: 기본 내부 인터페이스 구성은 유지되지 않음).

management center/CDO/로 전환한 후에는 더 이상 device manager를 사용하여 threat defense 디바이스를 관리할 수 없습니다.

시작하기 전에

방화벽이 고가용성으로 구성된 경우에는 먼저 device manager(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 구성을 해제해야 합니다. 액티브 유닛에서 고가용성을 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** Cisco Smart Software Manager에 방화벽을 등록한 경우 관리자를 전환하기 전에 등록을 취소해야 합니다. 디바이스 등록 취소을 참조하십시오.

방화벽 등록을 취소하면 기본 라이선스와 모든 기능 라이선스가 해제됩니다. 방화벽을 등록 취소하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 방화벽에 할당된 상태로 유지됩니다.

단계 **2** (필요할 수 있음) 관리 인터페이스를 구성합니다. 관리 인터페이스 구성, 22 페이지 섹션을 참조하십시오.

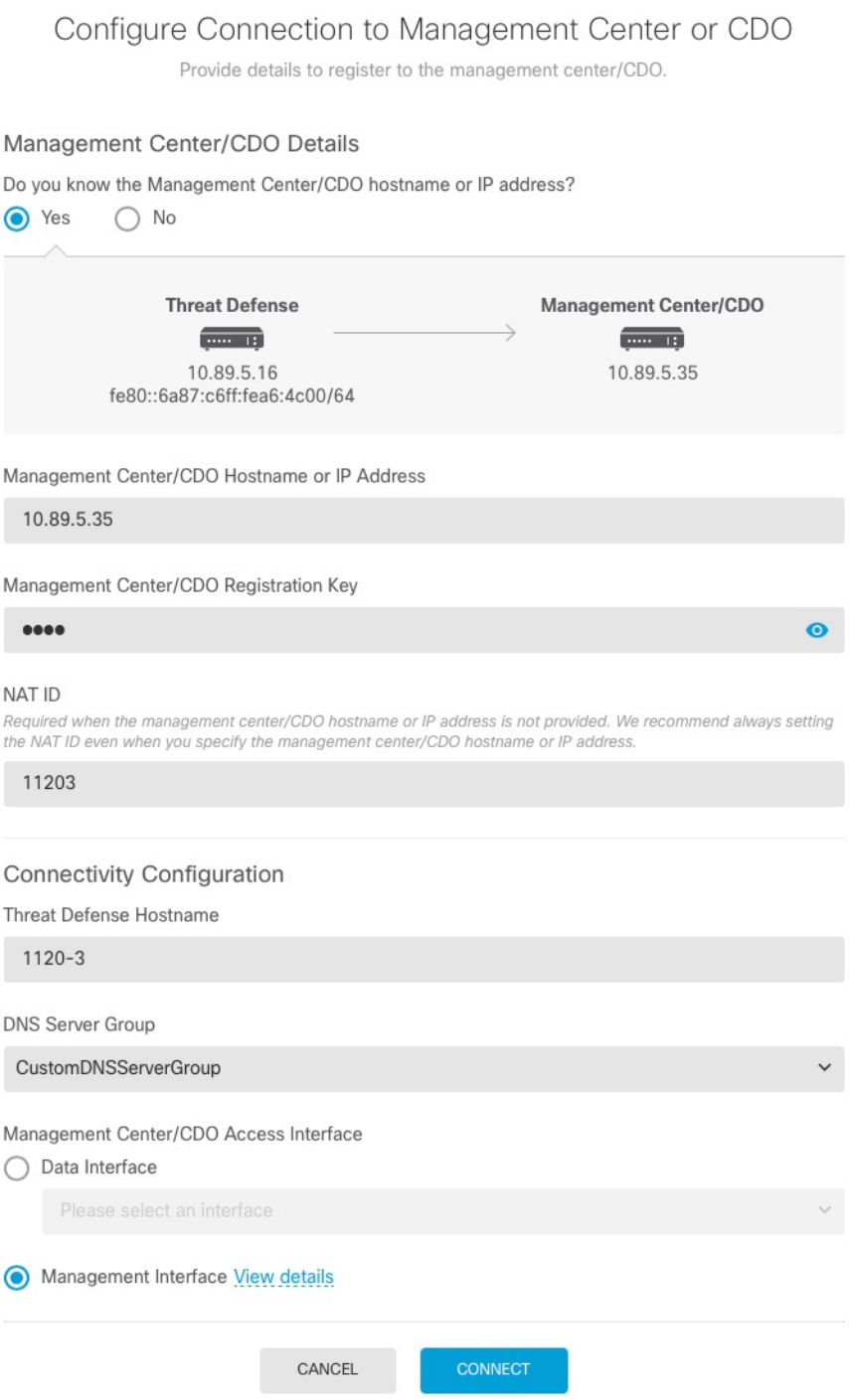
관리자 액세스에 데이터 인터페이스를 사용하려는 경우에도 관리 인터페이스 구성을 변경해야 할 수 있습니다. device manager 연결을 위해 관리 인터페이스를 사용하는 경우 device manager에 다시 연결해야 합니다.

- 관리자 액세스용 데이터 인터페이스 - 관리 인터페이스에 데이터 인터페이스로 설정된 게이트웨이가 있어야 합니다. 기본적으로 관리 인터페이스는 DHCP에서 IP 주소 및 게이트웨이를 수신합니다. DHCP에서 게이트웨이를 수신하지 못한 경우(예: 이 인터페이스를 네트워크에 연결하지 않은 경우) 게이트웨이는 기본적으로 데이터 인터페이스로 설정되며, 아무것도 구성할 필요가 없습니다. DHCP에서 게이트웨이를 수신한 경우 대신 고정 IP 주소로 이 인터페이스를 구성하고 게이트웨이를 데이터 인터페이스로 설정해야 합니다.
- 관리자 액세스용 관리 인터페이스 - 고정 IP 주소를 구성하려면 기본 게이트웨이도 데이터 인터페이스 대신 고유한 게이트웨이로 설정해야 합니다. DHCP를 사용하는 경우 DHCP에서 게이트웨이를 성공적으로 가져오면 어떤 것도 구성할 필요가 없습니다.

단계 **3** **Device**(디바이스) > **System Settings**(시스템 설정) > **Central Management**(중앙 관리)를 선택하고 **Proceed**(계속)을 눌러 management center/CDO 관리를 설정합니다.

단계 **4** **Management Center/CDO Details**(관리 센터/**CDO** 세부 정보)를 구성합니다.

그림 *1: Management Center/CDO* 세부 정보



a) **Do you know the Management Center/CDO hostname or IP address(**관리 센터**/CDO** 호스트 이름 또는 **IP** 주소를 알고 있습니까**)**에 대해 IP 주소 또는 호스트 이름을 사용하여 management center/CDO에 도달할 수 있으면 **Yes(**예**)**를, management center/CDO에 퍼블릭 IP 주소 또는 호스트 이름이 없거나 NAT 뒤에 있는 경우 **No(**아니요**)**를 클릭합니다.

하나 이상의 디바이스(management center/CDO 또는 threat defense)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다.

b) **Yes(**예**)**를 선택한 경우 **Management Center/CDO Hostname/IP Address(**관리 센터**/CDO** 호스트 이름**/IP** 주소**)**를 입력합니다.

c) **Management Center/CDO Registration Key(**관리 센터**/CDO** 등록 키**)**를 지정합니다.

threat defense 디바이스 등록 시에 management center/CDO에서 지정할 일회용 등록 키입니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center/CDO에 등록하는 여러 디바이스에 사용할 수 있습니다.

d) **NAT ID**를 지정합니다.

이 ID는 management center/CDO에서 지정할 고유한 일회성 문자열을 지정합니다. 이 필드는 디바이스 중 하나의 IP 주소만 지정하는 경우 입력해야 합니다. 두 디바이스의 IP 주소를 모두 알고 있는 경우에도 NAT ID를 지정하는 것이 좋습니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center/CDO에 등록하는 다른 디바이스에 사용할 수 없습니다. NAT ID는 연결이 올바른 디바이스에서 오는지 확인하기 위해 IP 주소와 함께 사용됩니다. IP 주소/NAT ID 인증 후에만 등록 키가 확인됩니다.

단계 **5** 연결성 설정을 구성합니다.

a) **FTD** 호스트 이름을 지정합니다.

Management Center/CDO Access Interface 액세스를 위해 데이터 인터페이스를 사용하는 경우 이 FQDN이 이 인터페이스에 사용됩니다.

b) **DNS** 서버 그룹을 지정합니다.

기존 그룹을 선택하거나 새로 생성합니다. 기본 DNS 그룹은 **CiscoUmbrellaDNSServerGroup**이며, 여기에는 OpenDNS 서버가 포함됩니다.

관리 센터**/CDO** 액세스 인터페이스에 대한 데이터 인터페이스를 선택하려는 경우 이 설정은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 마법사를 사용하여 설정하는 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다. 관리 및 데이터 트래픽이 모두 외부 인터페이스를 통해 DNS 서버에 연결되므로 관리에 사용한 것과 동일한 DNS 서버 그룹을 선택할 수 있습니다.

management center/CDO에서 이 threat defense 디바이스에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. management center/CDO에 threat defense 디바이스를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense 디바이스에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. management center/CDO와 threat defense 디바이스를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 management center/CDO에 의해 유지됩니다.

관리 센터**/CDO** 액세스 인터페이스관리 인터페이스를 선택하려는 경우 이 설정은 관리 DNS 서버를 구성합니다.

c) **Management Center/CDO Access Interface(**관리 센터**/CDO** 액세스 인터페이스**)**의 경우 구성된 인터페이스를 선택합니다.

threat defense 디바이스를 management center/CDO에 등록한 후 관리자 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.

단계 **6** (선택 사항) 데이터 인터페이스를 선택했는데 외부 인터페이스가 아닌 경우 기본 경로를 추가합니다.

인터페이스를 통과하는 기본 경로가 있는지 확인하라는 메시지가 표시됩니다. 외부를 선택한 경우 설정 마법사의 일부로 이 경로를 이미 구성한 것입니다. 다른 인터페이스를 선택한 경우 management center/CDO에 연결하기 전에 기본 경로를 수동으로 구성해야 합니다.정적 경로 구성에 대한 자세한 내용은 고정 경로 구성 항목을 참조하십시오.

관리 인터페이스를 선택한 경우 이 화면에서 계속 진행하기 전에 게이트웨이를 고유한 게이트웨이로 구성해야 합니다. 관리 인터페이스 구성, 22 페이지 섹션을 참조하십시오.

단계 **7** (선택 사항) 데이터 인터페이스를 선택한 경우 **Add a Dynamic DNS (DDNS) method(**동적 **DNS(DDNS)** 메서드 추가**)**를 클릭합니다.

DDNS는 management center/CDO 의 IP 주소가 변경될 경우 threat defense 디바이스가 FQDN(Fully-Qualified Domain Name)에서 에 연결할 수 있도록 합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)**를 참조하여 DDNS를 구성합니다.

management center/CDO에 threat defense 디바이스를 추가하기 전에 DDNS를 구성할 경우 threat defense 디바이스가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 threat defense 디바이스가 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. Threat Defense는 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.

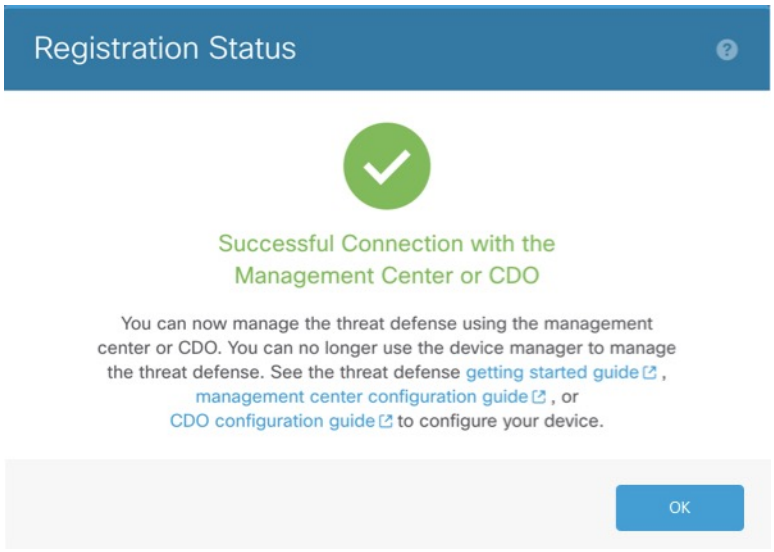
관리자 액세스용 관리 인터페이스를 사용할 때는 DDNS가 지원되지 않습니다.

단계 **8** **Connect(**연결**)**를 클릭합니다. 등록 상태**(Registration Status)** 대화 상자는 management center/CDO 전환에 대한 현재 상태를 보여줍니다. **Saving Management Center/CDO Registration Settings(**관리 센터**/CDO** 등록 설정 저장**)** 단계에서 management center/CDO로 이동하여 방화벽을 추가합니다.

management center/CDO에 대한 전환을 취소하려면 **Cancel Registration(**등록 취소**)**을 클릭합니다. 아니면 **Saving Management Center/CDO Registration Settings(**관리 센터**/CDO** 등록 설정 저장**)** 단계까지 device manager 브라우저를 닫지 마십시오. 이렇게 하면 프로세스가 일시 중지되며, device manager에 다시 연결할 때만 재개됩니다.

Save Management Center/CDO Registration Settings(관리 센터**/CDO** 등록 설정 저장**)** 단계를 수행한 후 device manager에 연결된 상태로 유지되는 경우, 마지막으로 **Successful Connection with Management Center or CDO(**관리 센터 또는 **CDO**와의 연결 성공**)** 대화 상자가 표시된 뒤 device manager으로부터 연결이 해제됩니다.

그림 2: 연결 성공



Management Center에서 또는 CDO에서 Device Manager로 전환

대신 device manager를 사용하도록 온프레미스 또는 클라우드 제공management center에서 현재 관리 중인 threat defense 디바이스를 구성할 수 있습니다.

소프트웨어를 다시 설치하지 않고 management center에서 device manager로 전환할 수 있습니다. management center에서 device manager로 전환하기 전에 device manager에서 모든 구성 요건을 충족하는지 확인하십시오. device manager에서 management center로 전환하려면 Device Manager에서 Management Center 또는 CDO로 전환, 36 페이지의 내용을 참조하십시오.

주의 device manager 전환 시 디바이스 구성이 지워지며 시스템이 기본 구성으로 돌아갑니다. 하지만 관리 IP 주소 및 호스트 이름은 유지됩니다.

프로시저

단계 1 management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 방화벽을 삭제합니다.

단계 2 SSH 또는 콘솔 포트를 사용하여 threat defense CLI에 연결합니다. SSH의 경우 관리 **IP** 주소에 대한 연결을 열고, 관리자 사용자 이름(또는 관리자 권한이 있는 다른 사용자)을 사용하여 threat defense CLI에 로그인합니다.

콘솔 포트는 기본적으로 FXOS CLI를 사용합니다. **connect ftd** 명령을 사용하여 threat defense CLI에 연결합니다. SSH 세션은 threat defense CLI에 직접 연결됩니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. **configure network ipv4/ipv6 manual** 명령을 사용하십시오.

단계 **3** 현재 원격 관리 모드 상태인지 확인합니다.

show managers

예제**:**

```
> show managers
Type                        : Manager
Host                        : 10.89.5.35
Display name                : 10.89.5.35
Identifier                  : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration                : Completed
```

단계 **4** 원격 관리자를 삭제하고 관리자 없음 모드를 설정합니다.

configure manager delete *uuid*

원격 관리에서 로컬 관리로 직접 이동할 수는 없습니다.둘 이상의 관리자가 정의된 경우 식별자(UUID라고도 함, **show managers** 명령 참조)를 지정해야 합니다. 각 관리자 항목을 개별적으로 삭제합니다.

예제**:**

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

단계 **5** 로컬 관리자를 구성합니다.

configure manager local

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

예제**:**

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

TLS / SSL 암호 설정 설정

SSL 암호 설정은 디바이스에 대한 TLS/SSL 연결에 허용되는 TLS 버전 및 암호화 암호 그룹을 제어합니다. 특히 이러한 설정은 원격 액세스 VPN 연결을 설정할 때 클라이언트가 사용할 수 있는 암호를 제어합니다.

일반적으로 설정하는 암호 그룹에는 사용 가능한 암호화 암호 그룹이 두 개 이상 있어야 합니다. 시스템은 클라이언트 및 threat defense 디바이스가 모두 지원하는 가장 높은 TLS 버전을 확인한 다음 TLS 버전과 호환되는 두 가지를 모두 지원하는 암호 그룹을 선택합니다. 시스템은 사용자가 허용하는 암호 중에서 가장 안전한 연결을 보장하기 위해 두 엔드포인트 모두에서 지원하는 가장 강력한 TLS 버전 및 암호 그룹을 선택합니다.

시작하기 전에

기본적으로 시스템은 DefaultSSLCipher 개체를 사용하여 허용되는 암호 그룹을 정의합니다. 이 개체에 포함된 암호는 내보내기 제어 기능에 대해 스마트 라이선스 어카운트가 활성화되었는지 여부에 따라 달라집니다. 이 기본값은 가능한 많은 클라이언트가 연결을 완료할 수 있도록 낮은 보안 레벨을 설정합니다. 기본 Diffie-Hellman 그룹도 있습니다. 기본값이 요구 사항에 맞지 않는 경우에만 이러한 설정을 지정해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **SSL Settings(SSL** 설정**)** 링크를 클릭합니다.

단계 **2** 다음 옵션을 구성합니다.

- **Ciphers(**암호**)** - 허용되는 TLS 버전 및 암호화 알고리즘을 정의하는 SSL 암호 개체를 선택합니다. DefaultSSLCipher 개체는 낮은 보안 레벨을 설정합니다. 더 높은 요구 사항을 구현하려면 이 개체를 CiscoRecommendedCipher 또는 맞춤형 암호 개체로 교체하십시오. 허용하려는 모든 TLS 버전과 암호만 포함하는 단일 개체를 생성하는 것이 이상적입니다.

  지금 개체를 생성해야 하는 경우 목록 하단에서 **Create New Cipher(**새 암호 생성**)**를 클릭합니다.

- **Ephemeral Diffie-Hellman Group(**일회성 **Diffie-Hellman** 그룹**)** - 일회성 암호화 알고리즘에 사용할 DH 그룹입니다. DH 그룹에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정의 내용을 참조하십시오. 기본값은 14입니다.

- **Elliptical Curve DH Group(**타원 곡선 **DH** 그룹**)** - 타원 곡선 암호화 알고리즘에 사용할 DH 그룹입니다. 기본값은 19입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

TLS / SSL 암호 개체 설정

SSL 암호 개체는 threat defense 디바이스에 대한 SSL 연결을 설정할 때 사용할 수 있는 보안 레벨, TLS/DTLS 프로토콜 버전 및 암호화 알고리즘의 조합을 정의합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **SSL Settings(SSL** 설정**)**에서 이러한 개체를 사용하여 상자에 SSL 연결을 수행하는 사용자에 대한 보안 요구 사항을 정의합니다.

선택할 수 있는 TLS 버전 및 암호는 스마트 라이선스 어카운트에 의해 제어됩니다. 내보내기 규정 준수 요건을 충족하는 경우 옵션의 조합을 선택할 수 있습니다. 라이선스가 내보내기를 준수하지 않는 경우 가장 낮은 보안 옵션인 TLSv1.0 및 DES-CDC-SHA로 제한됩니다. 평가 모드는 비호환 모드로 간주되므로 시스템 라이선스를 받을 때까지 옵션이 제한됩니다.

시스템에는 사전 정의된 개체가 여러 개 포함되어 있습니다. 사전 정의된 개체가 보안 요건에 맞지 않는 경우에만 새 개체를 생성해야 합니다. 개체는 다음과 같습니다.

- DefaultSSLCipher - 낮은 보안 레벨 그룹입니다. 가능한 많은 클라이언트가 시스템에 대한 연결을 완료할 수 있도록 SSL 설정에서 사용되는 기본값입니다. 여기에는 시스템에서 지원하는 모든 프로토콜 버전 및 암호가 포함됩니다.
- CiscoRecommendedCipher - 보안 레벨이 높은 그룹으로, 가장 안전한 암호 및 TLS 버전만 포함됩니다. 이 그룹은 가장 높은 보안을 제공하지만 클라이언트가 일치하는 암호를 사용할 수 있도록 해야 합니다. 암호 불일치 문제로 인해 일부 클라이언트가 연결을 완료할 수 없을 가능성이 더 높습니다.

프로시저

단계 **1** 콘텐츠 테이블에서 **Objects(**개체**)**를 선택하고 **SSL Ciphers(SSL** 암호**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Security Level(**보안 레벨**)** - 개체의 상대적 보안 레벨입니다. 보안 레벨을 선택한 후 프로토콜 버전 또는 암호 그룹 목록을 수정하면 개체에서 제공하는 실제 보안 레벨이 보안 레벨과 일치하지 않을 수 있습니다. 다음 중 하나를 선택합니다.
  - **All(**모두**)** - 낮음부터 높음까지 개체의 모든 TLS 레벨 및 암호 그룹을 포함합니다.
  - **Low(**낮음**)** - 모든 TLS 버전 및 암호를 포함하므로 사용자가 최소 보안 암호로 연결을 완료할 수 있습니다. 내보내기 미준수 라이선스의 경우 TLSv1.0 및 DES-CBC-SHA가 포함됩니다.

- **Medium(**중간**)** - 모든 TLS 버전을 포함하지만 상대적으로 안전하지 않은 일부 암호를 제거합니다. 이 옵션과 Low(낮음)/All(모두) 옵션 사이에는 최소한의 차이만 있습니다. 내보내기 미준수 라이선스에 이 옵션을 사용할 수 없습니다.
- **High(**높음**)** - 최신 DTLS 및 TLS 버전과 이러한 버전에서 작동하는 암호만 허용합니다. 이 옵션은 현재 사용 가능한 가장 안전한 암호로 연결을 제한합니다. 내보내기 미준수 라이선스에 이 옵션을 사용할 수 없습니다.
- **Custom(**맞춤형**)** - TLS 버전과 암호를 개별적으로 선택하려면 이 옵션을 선택합니다. 선택하는 옵션에 따라 높거나 낮은 보안 암호화 설정을 정의할지 여부가 결정됩니다. 맞춤형 개체에 대한 기본값은 없지만 맞춤형을 선택하기 전에 다른 레벨을 선택한 경우 편의상 이전에 표시된 옵션이 선택된 상태로 유지됩니다.

- **Protocol Versions(**프로토콜 버전**)** - threat defense 디바이스에 대한 TLS/SSL 연결을 설정할 때 클라이언트에서 사용할 수 있는 TLS/DTLS 버전입니다. 맞춤형 개체의 경우 지원하고자 하는 버전을 선택합니다. 다른 보안 레벨의 경우에는 목록을 수정하지 않는 것이 좋지만 원하는 대로 버전을 추가 또는 제거할 수 있습니다.
- **Applicable Cipher Suites(**적용 가능한 암호 그룹**)** - 클라이언트가 사용할 수 있는 암호화 알고리즘입니다. **+**를 클릭하여 새 그룹을 추가하고, 그룹에서 **x**를 클릭하면 그룹을 제거합니다.

  선택한 프로토콜 버전은 이 목록에서 사용 가능한 그룹을 제어합니다. 프로토콜 버전을 변경하면 선택한 버전에서 더 이상 작동하지 않는 선택한 그룹에 플래그가 지정됩니다. 이러한 그룹을 제거하거나 필요한 프로토콜 버전을 다시 추가해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.