



클래식 디바이스 관리 기본 사항

다음 주제는 Firepower System의 클래식 디바이스(7000 및 8000 시리즈 디바이스/ASA with FirePOWER Services/NGIPSv)를 관리하는 방법을 설명합니다.

- [클래식 디바이스 관리 요구 사항 및 사전 요건, 1 페이지](#)
- [원격 관리 구성\(클래식 디바이스\), 1 페이지](#)
- [인터페이스 설정, 4 페이지](#)

클래식 디바이스 관리 요구 사항 및 사전 요건

모델 지원

절차에 나와 있는 클래식 모델

지원되는 도메인

Leaf 달리 명시되지 않은 경우

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)

원격 관리 구성(클래식 디바이스)

7000 및 **8000** 시리즈를 제외한 모든 디바이스

기본 라이선스를 사용하는 디바이스의 원격 관리를 구성하는 방법은 디바이스에 맞는 빠른 시작 가이드를 참조하십시오.

7000 및 8000 시리즈 디바이스

디바이스를 FMC에 등록하기 전 로컬 웹 인터페이스를 사용하여 7000 또는 8000 Series 디바이스의 원격 관리를 구성합니다.

Firepower 디바이스를 관리하기 전에 Firepower Management Center와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. 어플라이언스는 채널을 사용하여 구성 및 이벤트 정보를 공유합니다. 고가용성 피어도 채널을 사용하며, 기본 포트는 8305/tcp입니다.

두 어플라이언스 간 커뮤니케이션을 활성화하려면 어플라이언스가 서로 인식할 수 있는 다음과 같은 방법을 제공해야 합니다.

- 호스트 이름 또는 사용자가 커뮤니케이션을 설정하려는 어플라이언스의 IP 주소
NAT 환경에서 다른 어플라이언스는 라우팅할 수 있는 주소가 없는 경우에도 원격 관리를 구성할 때 또는 관리 어플라이언스를 추가할 때 IP 주소 또는 호스트 이름을 제공해야 합니다.
- 연결을 식별하는 최대 37자의 자체 생성 영숫자 등록 키
- NAT 환경에서 이 커뮤니케이션을 설정하는 데 도움이 되는 선택적인 고유한 영숫자 NAT ID
NAT ID는 반드시 관리되는 어플라이언스 등록에 사용되는 모든 NAT ID 중에서 고유한 것이어야 합니다.

매니지드 디바이스에서 원격 관리 구성

이 절차는 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 1 관리하려는 디바이스의 웹 인터페이스에서 **System(시스템) > Integration(통합) > Remote Management(원격 관리)**를 선택합니다.

단계 2 미리 표시되지 않은 경우 **Remote Management(원격 관리)**를 클릭합니다.

단계 3 **Add Manager(관리자 추가)**를 클릭합니다.

단계 4 관리 호스트 필드에서 어플라이언스를 관리하는 데 사용할 Firepower Management Center에 대해 다음을 입력합니다.

- IP 주소
- FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 이름(즉 호스트 이름)

주의 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 IP 주소 대신 호스트 이름을 사용합니다.

NAT 환경에서 관리되는 어플라이언스를 추가할 때 IP 주소 또는 호스트 이름을 지정하려는 경우 여기에서 지정할 필요는 없습니다. 이 경우 Firepower System은 관리되는 어플라이언스의 웹 인터페이스에서 원격 관리자를 식별하기 위해 나중에 제공되는 NAT ID를 사용합니다.

단계 5 **Registration Key(등록 키)** 필드에 어플라이언스 간 커뮤니케이션을 설정하는 데 사용할 등록 키를 입력합니다.

단계 6 NAT 환경의 경우, **Unique NAT ID(고유 NAT ID)** 필드에 어플라이언스 간 커뮤니케이션을 설정하는데 사용할 고유한 영숫자 NAT ID를 입력합니다.

단계 7 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 어플라이언스가 서로 커뮤니케이션할 수 있는지 확인하면 **Pending Registration(등록 보류)** 상태가 표시됩니다.
- Firepower Management Center에 디바이스를 추가하려면 **FMC에 디바이스 추가**를 참조하십시오.

매니지드 디바이스에서 원격 관리 수정

이 절차는 7000 및 8000 Series 디바이스에 적용됩니다.

원격 관리자를 편집할 때는 다음에 주의하십시오.

- 호스트 필드는 FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 유효한 IP 주소(즉 호스트 이름)를 정의합니다.
- 이름 필드는 관리하는 어플라이언스의 표시 이름을 정의하며 이는 Firepower System의 컨텍스트 내에서만 사용됩니다. 다른 표시 이름을 입력해도 관리하는 디바이스의 호스트 이름은 변경되지 않습니다.

프로시저

단계 1 디바이스의 웹 인터페이스에서 **System(시스템) > Integration(통합)**을 선택합니다.

단계 2 미리 표시되지 않은 경우 **Remote Management(원격 관리)**를 클릭합니다.

단계 3 다음 작업을 수행할 수 있습니다.

- 원격 관리 비활성화 - 활성화를 하거나 비활성화하려면 관리자 옆의 슬라이더를 클릭합니다. 관리를 비활성화하면 Firepower Management Center와 디바이스 간 연결이 차단되지만 Firepower Management Center에서 디바이스가 삭제되지는 않습니다. 디바이스를 더 이상 관리하지 않으려면 **FMC에서 디바이스 삭제**를 참조하십시오.
- 관리자 정보 편집 - 수정하려는 관리자 옆의 수정(✎)을 클릭하여 **Name(이름)** 및 **Host(호스트)** 필드를 수정하고 **Save(저장)**를 클릭합니다.

관리 포트 변경

어플라이언스는 기본적으로 포트 8305를 사용하는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

Cisco는 기본 설정을 유지할 것을 적극 권장하지만 관리 포트가 네트워크의 다른 통신과 충돌하는 경우 다른 포트를 선택할 수 있습니다. 일반적으로 관리 포트 변경은 설치 중에 수행합니다.



주의 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 어플라이언스의 설정을 변경해야 합니다.

전역 도메인에서 이 작업을 수행해야 합니다.

프로시저

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

단계 2 관리 인터페이스를 클릭합니다.

단계 3 공유 설정 섹션의 원격 관리 포트 필드에 사용하려는 포트 번호를 입력합니다.

단계 4 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

어플라이언스와 통신해야 할 구축 시 모든 어플라이언스에 대해 이 절차를 반복합니다.

인터페이스 설정

어플라이언스 편집기의 인터페이스 페이지에 자세한 인터페이스 설정 정보가 표시됩니다. 페이지는 물리적 하드웨어 보기와 인터페이스 테이블 보기로 구성되며 설정 세부사항을 드릴다운할 수 있습니다. 이 페이지에서 인터페이스를 추가하고 편집할 수 있습니다.

물리적 하드웨어 보기

인터페이스 페이지 상단에는 7000 또는 8000 Series 디바이스에 대한 물리적 하드웨어 보기가 그림 형태로 표시됩니다.

물리적 하드웨어 보기를 사용하면 다음을 할 수 있습니다.

- 네트워크 모듈, 부품 번호 및 일련 번호 보기
- 인터페이스 테이블 보기에서 인터페이스 선택
- 인터페이스 편집기 열기
- 인터페이스의 이름, 인터페이스의 유형, 인터페이스의 링크 포함 여부, 인터페이스의 속도 설정, 인터페이스가 현재 우회 모드에 있는지 여부 보기
- 오류 또는 경고에 대한 세부 사항 보기

인터페이스 페이지

Interfaces(인터페이스) 페이지에는 디바이스에서 사용 가능한 모든 인터페이스가 나와 있습니다. 테이블에는 구성된 모든 인터페이스를 볼 때 사용할 수 있는 확장 가능한 탐색 트리가 포함되어 있습니다. 인터페이스 옆의 화살표 아이콘을 클릭하여 인터페이스를 확장하거나 축소하면 하위 구성 요소를 보거나 숨길 수 있습니다. 인터페이스 테이블 보기는 각 인터페이스에 대해 요약된 정보를 제공합니다.

필드	설명
이름	<p>각 인터페이스 유형은 해당 유형 및 링크 상태(해당되는 경우)를 나타내는 고유한 아이콘으로 표시됩니다. 이름이나 아이콘 위에 포인터를 올려 놓으면 추가 정보를 제공하는 도구 설명이 표시됩니다. 인터페이스 아이콘에 대해서는 인터페이스 아이콘, 6 페이지에 설명되어 있습니다.</p> <p>아이콘은 인터페이스의 다음 세 가지 상태 중 하나인 현재 링크 상태를 나타내기 위해 배지 표기 규칙을 사용합니다.</p> <ul style="list-style-type: none"> • Error • Fault(결함) • 사용할 수 없음 <p>논리적 인터페이스는 상위 물리적 인터페이스와 동일한 링크 상태를 가집니다. ASA FirePOWER 모듈은 링크 상태를 표시하지 않습니다. 비활성화된 인터페이스는 반투명 아이콘으로 표시됩니다.</p> <p>아이콘 오른쪽에 나타나는 인터페이스 이름은 하이브리드 및 사용자가 정의한 ASA FirePOWER 인터페이스를 제외하면 자동으로 생성됩니다. ASA FirePOWER 인터페이스의 경우 시스템은 활성화되고 이름이 있으며 링크가 있는 인터페이스만 표시합니다.</p> <p>물리적 인터페이스는 물리적 인터페이스의 이름을 표시합니다. 논리적 인터페이스는 물리적 인터페이스의 이름 및 할당된 VLAN 태그를 표시합니다.</p> <p>ASA FirePOWER 여러 보안 컨텍스트가 있는 경우 인터페이스는 보안 컨텍스트의 이름 및 인터페이스의 이름을 표시합니다. 보안 컨텍스트가 하나인 경우 시스템은 인터페이스의 이름만 표시합니다.</p>
보안 영역	인터페이스가 할당된 보안 영역 보안 영역을 추가 또는 편집하려면 수정(✎)을 클릭합니다.
에서 사용(NGIPSv만 해당)	인터페이스가 할당된 인라인 집합, 가상 스위치 또는 가상 라우터
MAC Address(MAC 주소)	<p>스위치 또는 라우팅 기능이 활성화되었을 때 인터페이스에 표시되는 MAC 주소</p> <p>NGIPSv 디바이스의 경우 디바이스에 구성된 네트워크 어댑터를 인터페이스 페이지에 나타나는 인터페이스에 일치시킬 수 있는 MAC 주소가 표시됩니다.</p>

필드	설명
IP 주소(7000/8000 시리즈만 해당)	인터페이스에 할당된 IP 주소 활성화 여부를 확인하려면 IP 주소 위로 포인터를 옮깁니다. 비활성 IP 주소는 회색으로 표시됩니다.

인터페이스 아이콘

표 1: 인터페이스 아이콘 유형 및 설명

아이콘	Interface Type	설명	확인
물리적	물리적	설정되지 않은 물리적 인터페이스	물리적 스위치 인터페이스 설정 또는 물리적 라우팅 인터페이스 설정
수동	수동	패시브 구축 시 트래픽을 분석하도록 설정된 센싱 인터페이스	패시브 인터페이스 구성
인라인	인라인	인라인 구축 시 트래픽을 처리하도록 설정된 센싱 인터페이스	인라인 인터페이스 구성
전환됨	전환됨	Layer 2 구축 시 트래픽을 전환하도록 설정된 인터페이스	스위치 인터페이스 구성
라우팅 모드	라우팅 모드	Layer 3 구축 시 트래픽을 라우팅하도록 설정된 인터페이스	라우팅 인터페이스
집계	집계	단일 논리적 링크로서 설정된 여러 물리적 인터페이스	집계 인터페이스 정보
집계 전환	집계 전환	Layer 2 구축 시 단일 논리적 링크로서 설정된 여러 물리적 인터페이스	집계 스위치 인터페이스 추가
집계 라우팅	집계 라우팅	Layer 3 구축 시 단일 논리적 링크로서 설정된 여러 물리적 인터페이스	집계 라우팅 인터페이스 추가
하이브리드	하이브리드	가상 라우터와 가상 스위치 간 트래픽을 연결하도록 설정된 논리적 인터페이스	논리적 하이브리드 인터페이스
ASA FirePOWER	ASA FirePOWER	ASA FirePOWER 모듈이 설치된 ASA 디바이스에 설정된 인터페이스	Cisco ASA FirePOWER 인터페이스 관리, 10 페이지

물리적 하드웨어 보기 사용

이 작업은 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 관리하려는 디바이스 옆의 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 다음 경우에 그래픽 인터페이스를 사용합니다.

- 선택 - 인터페이스를 선택하려면 인터페이스를 클릭합니다. 시스템은 인터페이스 테이블에서 관련된 항목을 강조 표시합니다.
- 편집 - 인터페이스 편집기를 열려는 경우 인터페이스를 두 번 클릭합니다.
- 오류 또는 경고 정보 보기 - 오류 또는 경고에 대한 세부 정보를 확인하려는 경우 네트워크 모듈에서 영향을 받은 포트 위에 마우스 커서를 이동합니다.
- 인터페이스 정보 보기 - 인터페이스 이름, 인터페이스 유형, 인터페이스의 링크 포함 여부, 인터페이스의 속도 설정, 인터페이스가 현재 우회 모드에 있는지 여부를 확인하려면 인터페이스 위에 커서를 올립니다.
- 네트워크 모듈 정보 보기 - 네트워크 모듈 유형, 부품 번호, 일련 번호를 보려면 네트워크 모듈 하단 왼쪽의 어두운 원 위에 커서를 올립니다.

센싱 인터페이스 설정

Firepower 구축에 따라 어플라이언스 편집기의 인터페이스 페이지에서 관리되는 디바이스의 센싱 인터페이스를 구성할 수 있습니다. 관리되는 디바이스에는 총 1024개의 인터페이스만 구성할 수 있습니다.



참고 ASA FirePOWER 디바이스를 SPAN 포트 모드에서 구축한 경우 Firepower Management Center에는 ASA 인터페이스가 표시되지 않습니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)을(를) 선택합니다.

단계 2 인터페이스를 구성하려는 디바이스 옆의 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 구성하려는 인터페이스 옆의 수정(✎)을 클릭합니다.

단계 4 인터페이스 편집기를 사용하여 다음과 같이 센싱 인터페이스를 구성합니다.

- HA 링크 - 7000/8000 시리즈 디바이스의 고가용성 쌍에서 각 멤버에 구성된 인터페이스가 이중 통신 채널 또는 고가용성 링크 인터페이스로 기능하도록 하는 경우 **HA 링크**를 클릭하고 **HA 링크 인터페이스 설정, 8 페이지**의 설명에 따라 진행합니다.
- 인라인 - 인터페이스가 인라인 구축에서 트래픽을 처리하도록 구성하려는 경우 인라인을 클릭하고 **인라인 인터페이스 구성**의 설명에 따라 진행합니다.
- 패시브 - 인터페이스가 패시브 구축에서 트래픽을 분석하도록 구성하려는 경우 패시브를 클릭하고 **패시브 인터페이스 구성**의 설명에 따라 진행합니다.
- 라우티드 - 인터페이스가 7000/8000 시리즈 Layer 3 구축 시 트래픽을 라우팅하도록 구성하려면 라우티드를 클릭하고 **라우팅 인터페이스**의 설명에 따라 진행합니다.
- 스위치드 - 인터페이스가 7000/8000 시리즈 Layer 2 구축 시 트래픽을 전환하도록 구성하려는 경우 스위치드를 클릭하고 **스위치 인터페이스 구성**의 설명에 따라 진행합니다.

단계 5 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. **컨피그레이션 변경 사항 구축**의 내용을 참조하십시오.

HA 링크 인터페이스 설정

7000 또는 8000 Series 디바이스를 고가용성 쌍으로 설정한 후 물리적 인터페이스를 고가용성(HA) 링크 인터페이스로 구성해야 합니다. 이 링크는 페어링된 디바이스 간 상태 정보 공유를 위한 이중 통신 채널 역할을 합니다. 하나의 디바이스에서 HA 링크 인터페이스를 구성하면 두 번째 디바이스에서도 자동으로 인터페이스가 구성됩니다. 동일한 브로드캐스트 도메인에서는 HA 링크를 모두 구성해야 합니다.

동적 NAT는 다른 IP 주소 및 포트를 매핑할 때 동적 할당 IP 주소 및 포트에 의존합니다. HA 링크가 없는 경우 페일오버 시 매핑이 손실되어 현재 고가용성 쌍의 액티브 디바이스를 통해 라우팅된 모든 변환 연결에 실패하게 됩니다.

마찬가지로 고가용성 상태 공유 중인 7000 또는 8000 Series 디바이스, 동적 NAT 또는 VPN은 HA 링크 인터페이스를 요구합니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)을(를) 선택합니다.

단계 2 HA 링크 인터페이스를 설정하려는 피어 옆의 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 HA 링크 인터페이스로 설정하려는 인터페이스 옆의 수정(✎)을 클릭합니다.

단계 4 **HA** 링크를 클릭합니다.

단계 5 활성화 확인란을 선택합니다.

체크 박스의 선택을 취소하는 경우 시스템은 이를 비활성화하고 관리를 위해 인터페이스를 종료합니다.

단계 6 모드 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 자동 협상을 선택하여 인터페이스의 자동 협상 속도 및 양방향 설정을 구성합니다.

단계 7 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다.

일반적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

단계 8 **MTU** 필드에 최대 전송 단위 (MTU)를 입력합니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 [7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위, 11 페이지](#)를 참조하십시오.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 **Snort** 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 [Snort® 재시작 트래픽 동작](#)을 참조하십시오.

단계 9 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

인터페이스 비활성화

인터페이스 유형을 **None**으로 설정하여 인터페이스를 비활성화할 수 있습니다. 비활성화된 인터페이스는 인터페이스 목록에서 회색으로 표시됩니다.

이 절차는 NGIPSv 및 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택합니다.

단계 2 인터페이스를 비활성화하려는 디바이스 옆의 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 비활성화하려는 인터페이스 옆의 수정(✎)을 클릭합니다.

단계 4 **None**을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

Cisco ASA FirePOWER 인터페이스 관리

ASA FirePOWER 인터페이스를 수정할 때, Firepower Management Center에서 인터페이스의 보안 영역만 구성할 수 있습니다.

ASA 전용 소프트웨어 및 CLI를 사용하면 ASA FirePOWER 인터페이스를 완전히 구성할 수 있습니다. ASA FirePOWER을 편집하여 다중 컨텍스트 모드에서 단일 컨텍스트 모드(또는 그 반대로) 전환하면 ASA FirePOWER는 모든 인터페이스의 이름을 변경합니다. 업데이트된 ASA FirePOWER 인터페이스 이름을 사용하려면 모든 Firepower System 보안 영역, 상관관계 규칙 및 관련 설정을 재구성해야 합니다. ASA FirePOWER 인터페이스 설정에 대한 자세한 내용은 ASA 설명서를 참조하십시오.



참고 ASA FirePOWER 인터페이스의 유형을 변경하거나 Firepower Management Center에서 인터페이스를 비활성화할 수 없습니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)을(를) 선택합니다.

단계 2 인터페이스를 비활성화하려는 디바이스 옆에 있는 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 미리 표시되지 않은 경우 인터페이스를 클릭합니다.

단계 4 편집하려는 인터페이스 옆에 있는 수정(✎)을 클릭합니다.

단계 5 보안 영역 드롭다운 목록에서 기존 보안 영역을 선택하거나 새 보안 영역을 추가하기 위해 새로 만들기를 선택합니다.

단계 6 저장을 클릭하여 보안 영역을 구성합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

7000 및 8000 Series 디바이스 및 NGIPsv의 MTU 범위

디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 **Snort** 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 **Snort® 재시작 트래픽 동작**를 참조하십시오.



참고 시스템은 구성된 MTU 값을 18바이트 크기로 줄입니다. IPv4 MTU를 594 이하로 설정하거나 IPv6 MTU를 1298 이하로 설정하지 마십시오.

플랫폼	MTU 범위
7000 및 8000 Series	576-9234(관리 인터페이스) 576 10172(인라인 집합, 패시브 인터페이스) 576-9922(기타 모두)
NGIPsv	576-9018(모든 인터페이스, 인라인 집합)

관련 항목

[MTU 정보](#)

보안 영역 개체의 수정 버전 동기화

보안 영역 개체를 업데이트하면 시스템은 개체의 새 개정을 저장합니다. 따라서 인터페이스에 각기 다른 수정 버전의 보안 영역 개체가 구성되어 있는 매니지드 디바이스가 동일한 보안 영역에 있는 경우 중복 연결로 보이는 항목이 로깅될 수 있습니다.

이중 연결 보고가 발견되면 개체의 동일한 개정을 사용하도록 모든 매니지드 디바이스를 업데이트할 수 있습니다.

이 절차는 NGIPsv 및 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 보안 영역 선택을 업데이트하려는 디바이스 옆에 있는 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 중복 연결 이벤트를 로깅하는 각 인터페이스에 대해 **Security Zone**(보안 영역)을 다른 영역으로 변경하고, **Save**(저장)를 클릭한 다음 원하는 영역으로 다시 변경하고 **Save**(저장)를 다시 클릭합니다.

단계 4 이중 이벤트를 로깅하는 각 디바이스에 대해 2단계와 3단계를 반복합니다. 계속 진행하기 전에 모든 디바이스를 수정해야 합니다.

다음에 수행할 작업

- 컨피그레이션 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)를 참고하십시오.



주의 동기화하려는 모든 디바이스에서 인터페이스에 대한 영역 설정을 수정하기 전에는 구성 변경 사항을 디바이스에 구축하지 마십시오. 모든 매니지드 디바이스에 동시에 구축해야 합니다.
