



## Firepower Threat Defense OSPF

이 장에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 FTD을 구성하는 방법을 설명합니다.

- [Firepower Threat Defense OSPF, 1 페이지](#)
- [OSPF 요구 사항 및 사전 요건, 4 페이지](#)
- [OSPF에 대한 지침, 5 페이지](#)
- [OSPFv2 구성, 7 페이지](#)
- [OSPFv3 구성, 20 페이지](#)

## Firepower Threat Defense OSPF

이 장에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 FTD을 구성하는 방법을 설명합니다.

### OSPF 정보

OSPF는 경로 선택 시 거리 벡터 대신 링크 상태를 사용하는 내부 게이트웨이 라우팅 프로토콜입니다. OSPF는 라우팅 테이블 업데이트가 아닌 링크 상태 광고를 전파합니다. 전체 라우팅 테이블 대신 LSA만 교환되므로, OSPF 네트워크는 RIP 네트워크보다 더 빠르게 통합될 수 있습니다.

OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터에는 동일한 링크 상태 데이터베이스가 포함되며, 여기에는 각 라우터의 사용 가능한 인터페이스 및 연결 가능한 네이버 목록이 있습니다.

RIP를 능가하는 OSPF의 장점은 다음과 같습니다.

- OSPF 링크 상태 데이터베이스 업데이트는 RIP 업데이트보다 전송되는 빈도가 낮으며, 링크 상태 데이터베이스는 천천히 업데이트되지 않고 오래된 정보의 기간이 만료되는 즉시 업데이트됩니다.
- 라우팅 결정은 비용을 기준으로 하며, 이는 특정 인터페이스 전체에 패킷을 전송하는 데 필요한 오버헤드를 나타낸 것입니다. Firepower Threat Defense 디바이스에서는 목적지까지의 홉 개수가 아닌 링크 대역폭을 기준으로 인터페이스의 비용을 계산합니다. 비용을 구성하여 선호하는 경로를 지정할 수 있습니다.

최단 경로 우선 알고리즘의 단점은 CPU 주기 및 메모리가 많이 필요하다는 점입니다.

Firepower Threat Defense 디바이스에서는 OSPF 프로토콜의 프로세스 2개를 다른 인터페이스 집합에서 동시에 실행합니다. 동일한 IP 주소를 사용하는 인터페이스가 있을 경우 2개의 프로세스를 실행하고자 할 수 있습니다(NAT 사용 시 이러한 인터페이스가 공존할 수 있으나, OSPF에서는 중복 주소를 허용하지 않음). 또는 내부에서 한 프로세스를 실행하고 외부에서 다른 프로세스를 실행한 다음, 두 프로세스 간의 경로 하위 집합을 재분배하고자 할 수 있습니다. 이 경우에도 마찬가지로, 사설 주소를 공용 주소에서 분리해야 할 수 있습니다.

경로를 다른 OSPF 라우팅 프로세스, RIP 라우팅 프로세스 또는 OSPF 지원 인터페이스에서 구성된 고정 및 연결된 경로의 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

Firepower Threat Defense 디바이스에서는 다음과 같은 OSPF 기능을 지원합니다.

- 영역 내, 영역 간 및 외부(유형 I 및 유형 II) 경로
- 가상 링크
- LSA 플러딩
- OSPF 패킷에 대한 인증(비밀번호 및 MD5 인증)
- Firepower Threat Defense 디바이스를 전용 라우터 또는 전용 백업 라우터로 구성. Firepower Threat Defense 디바이스는 ABR로 설정할 수도 있습니다.
- 스텝 영역 및 not-so-stubby 영역
- 영역 경계 라우터 유형 3 LSA 필터링

OSPF에서는 MD5 및 일반 텍스트 인접 디바이스 인증을 지원합니다. OSPF와 다른 프로토콜(예: RIP) 간의 경로 재분배 시 공격자가 라우팅 정보를 교란시키기 위해 이를 이용할 우려가 있으므로, 가능한 경우 모든 라우팅 프로토콜에 인증을 사용해야 합니다.

NAT를 사용하면 OSPF가 공용 및 사설 영역에서 가동되며, 주소 필터링이 필요한 경우 2개의 OSPF 프로세스를 실행해야 합니다. 하나는 공용 영역에 사용되는 프로세스이고 다른 하나는 사설 영역에서 사용되는 프로세스입니다.

여러 영역에 인터페이스가 있는 라우터는 ABR(영역 경계선 라우터)라고 합니다. OSPF를 사용하는 라우터와 다른 라우팅 프로토콜을 사용하는 라우터 간에 트래픽을 재분배하는 게이트웨이 역할을 수행하는 라우터를 ASBR(자동 시스템 경계 라우터)이라고 합니다.

ABR에서는 LSA를 사용하여 사용 가능한 경로에 대한 정보를 다른 OSPF 라우터로 전송합니다. ABR 유형 3 LSA 필터링을 사용할 경우, ABR 역할을 수행하는 ASA를 통해 별도의 사설 및 공용 영역을 확보할 수 있습니다. 유형 3 LSA(영역 간 경로)는 한 영역에서 다른 영역으로 필터링할 수 있으며, 이렇게 하면 사설 네트워크를 알리지 않고도 NAT와 OSPF를 함께 사용할 수 있습니다.



**참고** 유형 3 LSA만 필터링할 수 있습니다. 사설 네트워크에서 Firepower Threat Defense 디바이스를 ASBR로 구성하면 사설 네트워크를 설명하는 유형 5 LSA가 전송되며, 이 경우 공용 영역을 비롯한 전체 AS에 플러딩이 발생합니다.

NAT가 적용되었으나 공용 영역에서 OSPF만 실행 중인 경우, 공용 네트워크에 대한 경로가 사설 네트워크 내부에 기본 또는 유형 5 AS 외부 LSA로서 재배포될 수 있습니다. 그러나 Firepower Threat Defense 디바이스에서 보호하는 사설 네트워크에 대한 고정 경로를 구성해야 합니다. 또는 동일한 Firepower Threat Defense 디바이스 인터페이스에서 공용 네트워크와 사설 네트워크를 혼합할 수 없습니다.

Firepower Threat Defense 디바이스에서 하나는 RIP 라우팅 프로세스, 다른 하나는 EIGRP 라우팅 프로세스로 된 2개의 OSPF 라우팅 프로세스를 동시에 실행할 수 있습니다.

## Fast Hello 패킷에 대한 OSPF 지원

OSPF의 Fast Hello 패킷 지원은 hello 패킷을 1초 미만의 간격으로 전송하도록 구성하는 방법을 제공합니다. 이러한 컨피그레이션을 통해 OSPF(Open Shortest Path First) 네트워크에서 통합 속도를 단축할 수 있습니다.

### OSPF의 Fast Hello 패킷 지원 사전 요구 사항

OSPF는 네트워크에서 기존에 구성해야 하거나 OSPF의 Fast Hello 패킷 지원 기능과 동시에 구성해야 합니다.

### OSPF Hello 간격 및 Dead 간격

OSPF Hello 패킷은 OSPF 프로세스에서 OSPF 네이버와의 연결을 유지하기 위해 이러한 네이버에 전송하는 패킷입니다. Hello 패킷은 구성 가능한 간격(초 단위)으로 전송됩니다. 기본값은 이더넷 링크의 경우 10초이고, 비 브로드캐스트 링크의 경우 30초입니다. Hello 패킷에는 Dead 간격 내에 수신된 Hello 패킷에 대한 모든 네이버 목록이 포함됩니다. Dead 간격도 구성 가능한 간격(초 단위)이며, 기본값은 Hello 간격 값의 4배로 설정됩니다. 모든 Hello 간격의 값은 네트워크 내에서 동일해야 합니다. 마찬가지로, 모든 Dead 간격의 값도 네트워크 내에서 동일해야 합니다.

이러한 두 간격의 상호 작용을 통해 링크가 작동 중임을 나타내어 연결을 유지할 수 있습니다. 라우터가 Dead 간격 내에 네이버에서 Hello 패킷을 수신하지 못할 경우, 해당 네이버는 중단된 것으로 선언됩니다.

### OSPF Fast Hello 패킷

OSPF Fast Hello 패킷은 1초 미만의 간격으로 전송되는 Hello 패킷을 참조합니다. Fast Hello 패킷에 대한 내용을 이해하려면 OSPF Fast Hello 패킷과 Dead 간격 간의 관계에 대해서도 숙지해야 합니다. [OSPF Hello 간격 및 Dead 간격, 3 페이지](#)의 내용을 참조하십시오.

OSPF Fast Hello 패킷 기능은 `ospf dead-interval` 명령을 사용하여 구현할 수 있습니다. Dead 간격은 1초로 설정되고, hello 송수 값은 1초 동안 전송하려는 Hello 패킷의 수로 설정되므로 1초 미만의 또는 "빠른" Hello 패킷이 제공됩니다.

Fast Hello 패킷이 인터페이스에서 구성되면, 이 인터페이스로 전송되는 Hello 패킷에서 광고되는 Hello 간격은 0으로 설정됩니다. 이 인터페이스를 통해 수신되는 Hello 패킷의 Hello 간격은 무시됩니다.

1초로 설정하든(Fast Hello 패킷의 경우) 다른 값으로 설정하든 Dead 간격은 세그먼트에서 일정해야 합니다. Hello 승수의 경우에는 Dead 간격 내에 최소 하나 이상의 Hello 패킷이 전송된다면 전체 세그먼트에서 동일하지 않아도 됩니다.

## OSPF Fast Hello 패킷 기능의 이점

OSPF Fast Hello 패킷 기능의 이점은 OSPF 네트워크에서 Fast Hello 패킷을 사용하지 않는 경우와 비교했을 때 더 빠른 통합이 가능하다는 점입니다. 이 기능을 사용하면 1초 내에 손실된 네이버를 감지할 수 있습니다. 이 기능은 특히 OSI(Open System Interconnection) 물리적 레이어 및 데이터 링크 레이어로 감지할 수 없는 네이버가 손실된 LAN 세그먼트에 유용합니다.

## OSPFv2와 OSPFv3의 구현 차이점

OSPFv3는 이전 버전인 OSPFv2와 호환되지 않습니다. OSPF를 사용하여 IPv4와 IPv6 트래픽을 모두 라우팅하려면 OSPFv2와 OSPFv3를 동시에 실행해야 합니다. 이들은 서로 공존하지만 상호 작용을 수행하지는 않습니다.

OSPFv3에서 제공하는 추가 기능은 다음과 같습니다.

- 링크당 프로토콜 처리
- 주소 지정 시맨틱 제거
- 플러딩 범위 추가
- 링크당 다중 인스턴스 지원
- IPv6 링크-로컬 주소를 사용하여 네이버 검색 및 기타 기능 지원
- LSA를 접두사와 접두사 길이로 표시
- LSA 유형 2개 추가
- 알 수 없는 LSA 유형 처리
- RFC-4552에 지정된 대로, OSPFv3 라우팅 프로토콜 트래픽에 IPsec ESP 표준을 사용한 인증 지원

## OSPF 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할  
 관리자  
 액세스 관리자  
 Network Admin(네트워크 관리자)

## OSPF에 대한 지침

### 방화벽 모드 지침

OSPF에서는 라우팅 방화벽 모드만 지원합니다. OSPF에서는 투명 방화벽 모드를 지원하지 않습니다.

### 고가용성 지침

OSPFv2 및 OSPFv3는 스테이트풀 고가용성을 지원합니다.

### IPv6 지침

- OSPFv2에서는 IPv6을 지원하지 않습니다.
- OSPFv3에서는 IPv6을 지원합니다.
- OSPFv3에서는 인증에 IPv6을 사용합니다.
- Firepower Threat Defense 디바이스에서는 OSPFv3 경로가 최상의 경로인 경우, 이를 IPv6 RIB에 설치합니다.

### OSPFv3 Hello 패킷 및 GRE

일반적으로 OSPF 트래픽은 GRE 터널을 통과하지 않습니다. IPv6의 OSPFv3가 GRE 내부에서 캡슐화되는 경우 멀티캐스트 대상과 같은 보안 검사를 위한 IPv6 헤더 검증이 실패합니다. 이 패킷에는 대상 IPv6 멀티캐스트가 있으므로 암시적 보안 확인 검증으로 인해 패킷이 삭제됩니다.

GRE 트래픽을 우회하도록 사전 필터 규칙을 정의할 수 있습니다. 그러나 사전 필터 규칙을 사용하는 경우 검사 엔진에서 내부 패킷을 조사하지 않습니다.

### 클러스터링 지침

- OSPFv3 암호화는 지원되지 않습니다. 클러스터링 환경에서 OSPFv3 암호화를 구성하려고 할 경우 오류 메시지가 표시됩니다.
- Spanned 인터페이스 모드의 경우, 동적 라우팅은 관리 전용 인터페이스에서 지원되지 않습니다.
- 클러스터에서 마스터 역할이 변경될 경우 다음 동작이 발생합니다.
  - 스팬(spanned) 인터페이스 모드의 경우 라우터 프로세스는 제어 유닛에서만 액티브 상태이며 데이터 유닛에서는 일시 중단 상태입니다. 제어 유닛에서 구성이 동기화되었으므로 각

클러스터 유닛에서는 동일한 라우터 ID를 보유하게 됩니다. 결과적으로, 인접한 라우터에 서는 역할이 변경되는 동안 클러스터의 라우터 ID 변경을 알 수 없습니다.

### MPLS(Multiprotocol Label Switching) 및 OSPF 지침

MPLS 구성 라우터가 MPLS 헤더를 포함하는 불투명 Type-10 링크 상태 알림(LSA)이 포함된 링크 상태(LS) 업데이트 패킷을 전송하는 경우, 인증이 실패하고 어플라이언스가 이를 승인하지 않고 자동으로 업데이트 패킷을 삭제합니다. 결국 피어 라우터가 승인을 받지 않았기 때문에 피어 라우터는 네 이버 관계를 종료합니다.

네이버 관계를 안정적으로 유지하려면 NSF(중단 없이 전달)가 어플라이언스에서 비활성화되었는지 확인하십시오.

- Firepower Management Center(Devices(디바이스) > Device Management(디바이스 관리)(원하는 디바이스 선택) > Routing(라우팅) > OSPF > Advanced(고급) > Non Stop Forwarding(중단 없이 전달))에서 **Non Stop Forwarding(중단 없이 전달)** 페이지로 이동합니다.

**Non Stop Forwarding Capability(중단 없이 전달 기능)** 상자가 선택되어 있지 않은지 확인합니다.

### 경로 재배포 지침

OSPFv2 또는 OSPFv3에서 IPv4 또는 IPv6 접두사 목록을 사용하는 경로 맵 재배포는 지원되지 않습니다. 재배포를 위해 OSPF에서 연결된 경로를 사용합니다.

### 추가 지침

- OSPFv2 및 OSPFv3에서는 하나의 인터페이스에 여러 인스턴스를 지원합니다.
- OSPFv3에서는 클러스터링되지 않은 환경에서 ESP 헤더를 통해 암호화를 지원합니다.
- OSPFv3에서는 Non-Payload Encryption을 지원합니다.
- OSPFv2에서는 RFCs 4811, 4812 및 3623에서 각각 정의된 대로 Cisco NSF Graceful Restart 및 IETF NSF Graceful Restart 메커니즘을 지원합니다.
- OSPFv3에서는 RFC 5187에 정의된 대로 Graceful Restart 메커니즘을 지원합니다.
- 배포될 수 있는 내부 영역(유형 1) 경로의 수에는 제한이 있습니다. 이러한 경로의 경우, 단일 유형-1 LSA는 모든 접두사를 포함합니다. 시스템에서 패킷 크기에 35KB의 제한이 있으므로 3000개의 경로로 인해 패킷이 제한을 초과합니다. 2900개의 유형 1 경로를 지원되는 최대 수로 간주하십시오.
- 가상 라우팅을 사용하는 디바이스의 경우 전역 가상 라우터에 OSPFv2 및 OSPFv3를 구성할 수 있습니다. 그러나 사용자 정의 가상 라우터에서는 OSPFv2만 구성할 수 있습니다.
- 경로 업데이트가 링크의 최소 MTU보다 큰 경우 경로 업데이트가 삭제되어 인접성 플랩이 발생하지 않도록 하려면 링크의 양쪽에 있는 인터페이스에서 동일한 MTU를 구성해야 합니다.

## OSPFv2 구성

이 섹션에서는 OSPFv2 라우팅 프로세스 구성과 관련된 작업을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 전역 및 사용자 정의 가상 라우터에 대해 OSPFv2를 구성할 수 있습니다.

### OSPF 영역, 범위 및 가상 링크 구성

설정 인증, 스텝 영역 정의, 기본 요약 경로에 특정 비용 할당 등 여러 OSPF 영역 파라미터를 구성할 수 있습니다. 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다. 각 OSPF 프로세스에는 고유한 관련 영역 및 네트워크가 있습니다. 인증에서는 영역에 무단 액세스를 차단하는 비밀번호 기반의 보호 기능을 제공합니다.

스텝 영역은 외부 경로에 대한 정보가 전송되지 않는 영역입니다. 그 대신, 스텝 영역에는 ABR에서 생성된 기본 외부 경로가 있으며 이는 자동 시스템 외부의 목적지를 위한 경로입니다. OSPF 스텝 영역 지원을 사용하려면 스텝 영역에서 기본 라우팅을 사용해야 합니다.

프로시저

- 단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing(라우팅)**을 클릭합니다.
- 단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.
- 단계 4 **OSPF**를 클릭합니다.
- 단계 5 프로세스 1을 선택합니다. 각 컨텍스트/가상 라우터에 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다. 영역 파라미터를 구성하려면 OSPF 프로세스를 선택해야 합니다.  
디바이스에서 가상 라우팅을 사용하고 있다면 ID 필드에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 표시됩니다.
- 단계 6 드롭다운 목록에서 OSPF 역할을 선택하고 다음 필드에 설명을 입력합니다. 옵션으로는 내부, ABR 및 ASBR, ABR 및 ASBR이 있습니다. OSPF 역할에 대한 설명은 [OSPF 정보, 1 페이지](#)의 내용을 참조하십시오.
- 단계 7 **Area(영역) > Add(추가)**를 선택합니다.  
수정(✍)를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삼입, 삭제할 수 있습니다.
- 단계 8 각 OSPF 프로세스에 대한 다음 영역 옵션을 구성합니다.
  - **OSPF Process(OSPF 프로세스)** - 프로세스 ID를 선택합니다. 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
  - **영역 ID** - 경로를 요약할 영역을 지정합니다.
  - **영역 유형** - 옵션 중 하나를 선택합니다.

- 기본 - (기본값) 표준 OSPF 영역입니다.
- 스텝 - 스텝 영역의 경우 외부에 라우터 또는 영역이 없습니다. 스텝 영역은 AS(Autonomous System) 외부 LSA(Type 5 LSA)가 스텝 영역으로 플러딩되는 것을 방지합니다. 스텝 영역을 생성하면 스텝 요약 체크 박스의 선택을 취소하여 요약 LSA(Types 3 및 4)가 영역으로 플러딩되는 것을 방지할 수 있습니다.
- **NSSA** - NSSA(not-so-stubby) 영역을 지정합니다. NSSA는 Type 7 LSA를 승인합니다. 재분배 체크 박스의 선택을 취소하고 기본 정보 출처 체크 박스를 선택하여 경로 재분배를 비활성화할 수도 있습니다. **NSSA** 요약 체크 박스의 선택을 취소하고 LSA 요약이 영역으로 플러딩되는 것을 방지합니다.
- 메트릭 값 - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 기본값은 10입니다. 유효한 값의 범위는 0~16777214입니다.
- **Metric Type**(메트릭 유형) - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.
- 사용 가능한 네트워크 - 사용 가능한 네트워크 중 하나를 선택하고 **Add**(추가)를 클릭하거나 추가(+ )을 클릭하여 새 네트워크 개체를 추가합니다. 네트워크 추가 절차는 [네트워크 개체](#)를 참조하십시오.
- 인증 - OSPF 인증을 선택합니다.
  - 없음 - (기본) OSPF 영역 인증을 비활성화합니다.
  - 비밀번호 - 영역 인증에 일반 텍스트 비밀번호를 제공하며 보안이 중요한 경우 권장하지 않습니다.
  - **MD5** - MD5 인증을 허용합니다.
- 기본 비용 - 대상까지 최단 경로를 결정하는 데 사용되는 OSPF 영역에 대한 기본 비용입니다. 유효한 값의 범위는 0~65535입니다. 기본값은 1입니다.

단계 9 **OK**를 클릭하여 구성을 저장합니다.

단계 10 **Range**(범위) > **Add**(추가)를 선택합니다.

- 사용 가능한 네트워크 및 알림 여부를 선택하거나
- 네트워크 개체를 추가하려면 추가(+ )을 클릭합니다. 네트워크 추가 절차는 [네트워크 개체](#)의 내용을 참조하십시오.

단계 11 **OK**를 클릭하여 설정 범위를 저장합니다.

단계 12 **Virtual Link**(가상 링크)를 선택하고 **Add**(추가)를 클릭하여 각 OSPF 프로세스에 대해 다음 옵션을 구성합니다.

- 피어 라우터 - 피어 라우터의 IP 주소를 선택합니다. 새 피어 라우터를 추가하려면 추가(+ )을 클릭합니다. 네트워크 추가 절차는 [네트워크 개체](#)의 내용을 참조하십시오.



- **Hello 간격** - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. Hello 간격은 Hello 패킷에 광고되는 무부호 정수입니다. 이 값은 특정 네트워크의 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~65535입니다. 기본값은 10입니다.

Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다.

- **전송 지연** - 인터페이스에서 LSA 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 이 정수 값은 0보다 커야 합니다. 유효한 값의 범위는 1~8192입니다. 기본값은 1입니다.

업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.

- **재전송 간격** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값은 예상 왕복 지연 시간보다 커야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 5입니다.

라우터에서 LSA를 네이버로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

- **데드 간격** - 라우터가 중단되었음을 네이버가 나타내기까지 hello 패킷이 표시되지 않은 시간을 초 단위로 입력합니다. Dead 간격은 무부호 정수입니다. 기본값은 Hello 간격의 4배이거나 40초입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~65535입니다.

- **인증** - 다음 OSPF 가상 링크 인증 중 하나를 선택합니다.

- **없음** - (기본) 가상 링크 영역 인증을 비활성화합니다.

- **영역 인증** - MD5를 사용하여 활성화 영역을 인증합니다. **Add(추가)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(확인)**를 클릭합니다.

- **비밀번호** - 가상 링크 인증에 일반 텍스트 비밀번호를 제공하며 보안이 중요한 경우 권장하지 않습니다.

- **MD5** - MD5 인증을 허용합니다. **Add(추가)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(확인)**를 클릭합니다.

참고 MD5 키 ID는 숫자만 입력합니다.

- **키 체인** - 키 체인 인증을 허용합니다. **Add(추가)**를 클릭하고 키 체인을 생성한 뒤 **Save(저장)**를 클릭합니다. 자세한 절차는 **키 체인 개체 생성**을 참조하십시오. 피어에 대해 동일한 인증 유형(MD5 또는 키 체인)과 키 ID를 사용하여 성공적인 인접성을 설정합니다.

단계 13 **OK**를 클릭하여 설정을 저장합니다.

단계 14 Routing(라우팅) 페이지에서 **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPF 재배포 구성을 진행합니다.

## OSPF 재배포 구성

Firepower Threat Defense 디바이스는 OSPF 라우팅 프로세스 간의 경로 재분배를 제어할 수 있습니다. 하나의 라우팅 프로세스에서 OSPF 라우팅 프로세스로 경로를 재분배하기 위한 규칙이 표시됩니다. RIP 및 BGP에서 검색된 경로를 OSPF 라우팅 프로세스로 재분배할 수 있습니다. 고정 경로 및 연결된 경로도 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

프로시저

- 단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing(라우팅)**을 클릭합니다.
- 단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.
- 단계 4 **OSPF**를 클릭합니다.
- 단계 5 **Distribution(배포) > Add(추가)**를 선택합니다.
- 수정(✍)을 클릭하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 6 각 OSPF 프로세스에 대한 다음 재배포 옵션을 구성합니다.
- **OSPF Process(OSPF 프로세스)** - 프로세스 ID를 선택합니다. 가상 라우팅을 사용하는 디바이스의 드롭다운 목록에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 표시됩니다.
  - **경로 유형** - 다음 유형 중 하나를 선택합니다.
    - 고정 - 고정 경로를 OSPF 라우팅 프로세스에 재배포합니다.
    - 연결됨 - 연결된 경로(인터페이스에서 IP 주소를 활성화하여 자동으로 설정된 경로)를 OSPF 연결 프로세스에 재배포합니다. 연결된 경로는 AS에 외부 경로로 재분배할 수 있습니다. (옵션) 목록에서 서브넷을 사용할지 여부를 선택할 수 있습니다.
    - **OSPF** - 내부, 외부 1 및 2, NSSA 외부 1 및 2 또는 서브넷을 사용할지 여부 등 다른 OSPF 라우팅 프로세스의 재분배 경로입니다. (옵션) 목록 아래에서 다음 옵션을 선택할 수 있습니다.
    - **BGP** - BGP 라우팅 프로세스에서 경로를 재분배합니다. AS 번호 및 서브넷 사용 여부를 추가합니다.

- **RIP** - RIP 라우팅 프로세스에서 경로를 재분배합니다. (옵션) 목록에서 서브넷을 사용할지 여부를 선택할 수 있습니다.

참고 사용자 정의 가상 라우터는 RIP를 지원하지 않으므로 RIP에서 경로를 재배포할 수 없습니다.

- **메트릭 값** - 배포되는 경로의 메트릭 값입니다. 기본값은 10입니다. 유효한 값의 범위는 0 ~ 16777215입니다.

하나의 OSPF 프로세스에서 동일한 디바이스의 다른 OSPF 프로세스로 재분배할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재분배할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.

- **Metric Type(메트릭 유형)** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.
- **태그 값** - OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값입니다. 아무것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값은 0 ~ 4294967295입니다.
- **Route Map(경로 맵)** - 드롭다운 목록에서 경로 맵을 선택하여 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜로 경로 가져오기를 필터링합니다. 이 매개변수를 지정하지 않으면 모든 경로가 재분배됩니다. 이 매개변수를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. 또는 추가(+)를 클릭하여 새 경로 맵을 추가할 수 있습니다. 새 경로 맵을 추가하려면 **구성 경로 맵 항목**을 참조하십시오.

단계 7 **OK(확인)**를 클릭하여 재배포 구성을 저장합니다.

단계 8 **Routing(라우팅)** 페이지에서 **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

[OSPF 영역 간 필터링 구성, 11 페이지](#)를 계속 진행합니다.

## OSPF 영역 간 필터링 구성

ABR Type 3 LSA 필터링은 OSPF를 실행하여 서로 다른 OSPF 영역 간 Type 3 LSA를 필터링하는 ABR의 기능을 확장합니다. 일단 접두사 목록이 구성되면 지정된 접두사만 하나의 OSPF 영역에서 다른 OSPF 영역으로 전송됩니다. 모든 다른 접두사는 OSPF 영역으로 제한됩니다. 이 영역 필터링 유형을 OSPF 영역에서 수신 또는 발신 트래픽에 적용하거나 해당 영역의 수신 및 발신 트래픽 모두에 적용할 수 있습니다.

접두사 목록의 여러 엔트리가 주어진 접두사와 일치하는 경우 순차 번호가 가장 낮은 엔트리가 사용됩니다. 목록 상단 근처의 가장 일반적인 일치 또는 거부에 가장 낮은 순차 번호를 할당하는 것이 효율적일 수 있습니다. 기본적으로 순차 번호는 5부터 시작하여 5씩 증가하며 자동으로 생성됩니다.

## 프로시저

- 
- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing**(라우팅)을 클릭합니다.
- 단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.
- 단계 4 **OSPF**를 클릭합니다.
- 단계 5 **InterArea**(영역 간) > **Add**(추가)를 선택합니다.
- 수정(✍)을 클릭하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 6 각 OSPF 프로세스에 대한 다음 필터링 옵션을 구성합니다.
- **OSPF Process**(OSPF 프로세스) - 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
  - **영역 ID** - 경로를 요약할 영역을 지정합니다.
  - **PrefixList** - 접두사의 이름입니다. 새 접두사 목록 개체를 추가하려면 5 단계를 참조하십시오.
  - **트래픽 방향** - 인바운드 또는 아웃바운드입니다. OSPF 영역에 들어오는 LSA를 필터링하려면 **Inbound**(인바운드)를 선택하고, OSPF 영역 밖으로 나가는 LSA를 필터링하려면 **Outbound**(아웃바운드)를 선택합니다. 기존 필터 항목을 편집할 경우 이 설정은 변경할 수 없습니다.
- 단계 7 추가(+ )을 클릭하고 새 접두사 목록에 대한 이름을 입력하고 덮어쓰기 허용 여부를 선택합니다. 접두사 규칙을 구성하기 전에 접두사 목록을 구성해야 합니다.
- 단계 8 접두사 규칙을 구성하려면 추가를 클릭하고 다음 파라미터를 구성합니다.
- **작업** - 재배포 액세스에 대한 차단 또는 허용을 선택합니다.
  - **시퀀스 없음** - 라우팅 시퀀스 번호입니다. 기본적으로 순차 번호는 5부터 시작하여 5씩 증가하며 자동으로 생성됩니다.
  - **IP 주소** - IP 주소 형식의 접두사 번호/마스크 길이를 지정합니다.
  - **최소 접두사 길이** - (선택 사항) 최소 접두사 길이입니다.
  - **최대 접두사 길이** - (선택 사항) 최대 접두사 길이입니다.
- 단계 9 **확인** 을 클릭하여 영역 간 필터링 구성을 저장합니다.
- 단계 10 **Routing**(라우팅) 페이지에서 **Save**(저장)를 클릭하여 변경 사항을 저장합니다.
- 

다음에 수행할 작업

[OSPF 필터 규칙 구성, 13 페이지](#)를 계속 진행합니다.

## OSPF 필터 규칙 구성

각 OSPF 프로세스에 대한 ABR Type 3 LSA 필터를 구성할 수 있습니다. ABR Type 3 LSA 필터는 지정된 접두사만 한 영역에서 다른 영역으로 전송되도록 허용하며 다른 모든 접두사는 제한합니다. 이러한 유형의 영역 필터링은 특정 OSPF 영역의 외부 또는 특정 OSPF 영역의 내부에 적용하거나, 동일한 OSPF 영역의 내부와 외부에 동시에 적용할 수 있습니다. OSPF ABR Type 3 LSA 필터링은 OSPF 영역 간의 경로 재분배 제어 기능을 개선합니다.

프로시저

- 
- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing**(라우팅)을 클릭합니다.
- 단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.
- 단계 4 **OSPF**를 클릭합니다.
- 단계 5 **Filter Rule**(필터 규칙) > **Add**(추가)를 선택합니다.
- 수정(✍)을 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 필터 규칙을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 6 각 OSPF 프로세스에 대한 다음 필터 규칙 옵션을 구성합니다.
- **OSPF Process**(OSPF 프로세스) - 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
  - 액세스 목록 - 이 OSPF 프로세스에 대한 액세스 목록입니다. 새 표준 액세스 목록 개체를 추가하려면 추가(+)을 클릭합니다. [표준 ACL 개체 설정](#)의 내용을 참조하십시오.
  - 트래픽 방향 - 필터링할 트래픽 방향을 선택합니다. OSPF 영역에 들어오는 LSA를 필터링하려면 In을 선택하고, OSPF 영역 밖으로 나가는 LSA를 필터링하려면 Out을 선택합니다. 기존 필터 항목을 편집할 경우 이 설정은 변경할 수 없습니다.
  - 인터페이스 - 이 필터 규칙에 대한 인터페이스입니다.
- 단계 7 확인을 클릭하여 필터 규칙 구성을 저장합니다.
- 단계 8 **Routing**(라우팅) 페이지에서 **Save**(저장)를 클릭하여 변경 사항을 저장합니다.
- 

다음에 수행할 작업

[OSPF 요약 주소 구성, 14 페이지](#)를 계속 진행합니다.

## OSPF 요약 주소 구성

다른 프로토콜의 경로가 OSPF에 재분배될 경우, 각 경로는 외부 LSA에 개별적으로 광고됩니다. 그러나 Firepower Threat Defense 디바이스를 구성하여 지정된 네트워크 주소 및 마스크에 포함되는 모든 재분배된 경로에 대한 단일 경로를 광고할 수 있습니다. 이렇게 구성하면 OSPF 링크 상태 데이터베이스의 크기가 줄어듭니다. 지정된 IP 주소 마스크 쌍과 일치하는 경로는 억제할 수 있습니다. 태그 값을 일치 값으로 사용하여 경로 맵을 통한 재분배를 제어할 수 있습니다.

다른 라우팅 프로토콜에서 학습된 경로를 요약할 수 있습니다. 요약 광고에 사용되는 메트릭은 특정 경로 중에서도 가장 작은 메트릭입니다. 요약 경로는 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

OSPF에 요약 경로를 사용하면 OSPF ASBR에서는 단일한 외부 경로를 해당 주소에서 다루는 모든 재분배 경로의 취합본으로 광고하게 됩니다. OSPF로 재분배되는 다른 라우팅 프로토콜의 경로만 요약할 수 있습니다.

프로시저

- 
- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing**(라우팅)을 클릭합니다.
- 단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.
- 단계 4 **OSPF**를 클릭합니다.
- 단계 5 **Summary Address**(요약 주소) > **Add**(추가)를 선택합니다.
- 수정(✍)을 클릭하거나 메뉴를 오른쪽 클릭하여 주소를 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 6 각 OSPF 프로세스에 대한 다음 요약 주소 옵션을 구성합니다.
- **OSPF Process**(OSPF 프로세스) - 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
  - **사용 가능한 네트워크** - 요약 주소의 IP 주소입니다. 사용 가능한 네트워크 목록에서 하나를 선택하고 추가를 클릭하거나 새 네트워크를 추가하려면 추가(+)를 클릭 합니다. 네트워크 추가 절차는 **네트워크 개체**의 내용을 참조하십시오.
  - **태그** - 각 외부 경로에 연결된 32비트 십진수 값이 표시됩니다. 이 값은 OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있습니다.
  - **알림** - 요약 경로 알림입니다. 이 확인란의 선택을 취소하면 요약 주소에 속하는 경로가 억제됩니다. 기본적으로 이 확인란은 선택되어 있습니다.
- 단계 7 **OK**를 클릭하여 주소 구성을 저장합니다.
- 단계 8 **Routing**(라우팅) 페이지에서 **Save**(저장)를 클릭하여 변경 사항을 저장합니다.
-

다음에 수행할 작업

OSPF 인터페이스 및 네이버 구성, 15 페이지를 계속 진행합니다.

## OSPF 인터페이스 및 네이버 구성

필요한 경우 일부 인터페이스별 OSPFv2 매개변수를 변경할 수 있습니다. 이러한 파라미터는 변경할 필요가 없지만, hello 간격 및 dead 간격과 같은 인터페이스 파라미터는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 컨피그레이션할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

고정 OSPFv2 네이버를 정의하여 포인트-투-포인트 비 브로드캐스트 네트워크를 통해 OSPFv2 경로를 광고할 수 있습니다. 이 기능을 사용하면 GRE 터널에 광고를 캡슐화하지 않고도 기존 VPN 연결 전체에 OSPFv2 광고를 브로드캐스트할 수 있습니다.

프로시저

- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing**(라우팅)을 클릭합니다.
- 단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.
- 단계 4 **OSPF**를 클릭합니다.
- 단계 5 **Interface**(인터페이스) > **Add**(추가)를 선택합니다.  
수정(✍)를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 6 각 OSPF 프로세스에 대한 다음 인터페이스 옵션을 구성합니다.
  - **Interface**(인터페이스) - 구성 중인 인터페이스입니다.  
참고 디바이스에서 가상 라우팅을 사용하는 경우 이 드롭다운 목록에는 라우터에 속하는 인터페이스만 표시됩니다.
  - 기본 비용 - 인터페이스를 통한 패킷 전송의 비용입니다. 기본값은 10입니다.
  - 우선 순위 - 네트워크의 라우터 우선 순위를 결정합니다. 유효한 값의 범위는 0~255입니다. 기본값은 1입니다. 이 설정을 0으로 입력하면 해당 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다.  
네트워크에 라우터가 2개 연결될 경우, 두 라우터 모두 전용 라우터가 되려고 시도합니다. 라우터 우선 순위가 더 높은 디바이스가 전용 라우터가 됩니다. 연관성이 있을 경우, 라우터 ID가 더 높은 라우터가 전용 라우터가 됩니다. 이 설정은 포인트-투-포인트 인터페이스로 구성된 인터페이스에는 적용되지 않습니다.
  - **MTU 무시** - OSPF에서는 네이버가 공통 인터페이스의 동일한 MTU를 사용하고 있는지 여부를 확인합니다. 네이버가 DBD 패킷을 교환할 때 이러한 확인이 이루어집니다. DBD 패킷에 수신되는 MTU가 수신 인터페이스에 구성된 IP MTU보다 클 경우, OSPF 인접성이 설정되지 않습니다.

- **필터 해제** - 이 설정을 사용하여 동기화 및 플러딩이 진행되는 동안 발신 LSA 인터페이스를 필터링합니다. 기본적으로 OSPF에서는 새로운 LSA를 동일한 영역의 모든 인터페이스로 플러딩 하며, LSA가 도달하는 인터페이스는 제외입니다. 완전히 메시된 토폴로지의 경우, 이러한 플러딩이 실행되면 대역폭을 낭비하고 링크 및 CPU를 과도하게 사용할 수 있습니다. 이 확인란을 선택하면 OSPF에서 선택된 인터페이스에 LSA 플러딩을 수행하지 않습니다.
- **Hello Interval(Hello 간격)** - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. 유효한 값은 1초 ~ 8192초입니다. 기본값은 10초입니다.  
Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다. 이 값은 특정 인터페이스의 모든 라우터 및 액세스 서버에서 동일해야 합니다.
- **전송 지연** - 인터페이스에서 LSA 패킷을 전송하는 예상 시간을 초 단위로 지정합니다. 유효한 값은 1초 ~ 65535초입니다. 기본값은 1초입니다.  
업데이트 패킷의 LSA에는 전송 전에 이 필드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.
- **Retransmit Interval(재전송 간격)** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 5초입니다.  
라우터에서 LSA를 네이버로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.
- **Dead Interval(중단 간격)** - 인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간 기간(초)입니다. 값은 네트워크의 모든 노드에 대해 동일 해야 하며 1 ~ 65535 범위를 사용할 수 있습니다.
- **Hello Multiplier** - 필드에서 1초당 전송되는 Hello 패킷의 수를 지정합니다. 유효한 값은 3초 ~ 20초입니다.
- **Point-to-Point** - VPN 터널을 통해 OSPF 경로를 전송할 수 있습니다.
- **인증** - 다음에서 OSPF 인증 인터페이스를 선택합니다.
  - **None (없음)** - (기본) 비활성화 인터페이스 인증합니다.
  - **영역 인증** - MD5를 사용하여 활성화 인터페이스를 인증합니다. **Add(추가)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(확인)**를 클릭합니다.
  - **비밀번호** - 가상 링크 인증에 일반 텍스트 비밀번호를 제공하며 보안이 중요한 경우 권장하지 않습니다.
  - **MD5** - MD5 인증을 허용합니다. **Add(추가)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(확인)**를 클릭합니다.



참고 MD5 키 ID는 숫자만 입력합니다.

- 키 체인 - 키 체인 인증을 허용합니다. **Add(추가)**를 클릭하고 키 체인을 생성한 뒤 **Save(저장)**을 클릭합니다. 자세한 절차는 **키 체인 개체 생성**을 참조하십시오. 피어에 대해 동일한 인증 유형(MD5 또는 키 체인)과 키 ID를 사용하여 성공적인 인접성을 설정합니다.

- 비밀 번호 입력 - 비밀 번호 인증 유형으로 비밀 번호를 선택하는 경우를 구성합니다.
- 암호 확인 - 선택한 암호를 확인합니다.

단계 7 **Neighbor(네이버) > Add(추가)**를 선택합니다.

수정(✍)를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 8 각 OSPF 프로세스에 대해 다음 파라미터를 구성합니다.

- **OSPF Process(OSPF 프로세스)** - 1 또는 2를 선택합니다.
- **네이버-드롭다운** 목록에서 네이버 중 하나를 선택하거나 추가(+)을 클릭하여, 새로운 네이버를 추가 하고, 이름, 설명, 네트워크, 오버라이드 허용 여부를 입력하고 저장을 클릭합니다.
- **Interface(인터페이스)** - 필드에서 고정 네이버와 관련된 인터페이스를 선택합니다.

단계 9 **OK**를 클릭하여 네이버 구성을 저장합니다.

단계 10 Routing(라우팅) 페이지에서 **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

## OSPF 고급 속성 구성

Advanced Properties(고급 속성)를 사용하면 시스템 로그 메시지 생성, 관리 경로 거리, LSA 타이머 및 Graceful Restart와 같은 옵션을 구성할 수 있습니다.

### Graceful Restart

Firepower Threat Defense 디바이스에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(Non-Stop Forwarding) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 무중단(Hitless) 소프트웨어 업그레이드가 예정되어 있을 때 유용합니다. NSF Cisco(RFC 4811 및 RFC 4812) 또는 NSF IETF(RFC 3623)를 사용하여 OSPFv2에서 Graceful Restart를 구성할 수 있습니다.



참고 NSF 기능은 HA 모드 및 클러스터링에도 유용합니다.

NSF Graceful Restart 기능을 구성하려면 기능을 구성하고, 디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. NSF 지원 디바이스는 해당 디바이스의 재시

작 작업을 네이버에 나타낼 수 있으며, NSF 인식 디바이스는 네이버를 초기화하도록 지원할 수 있습니다.

디바이스는 몇 가지 조건에 따라 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다.

- 디바이스는 현재 속한 모드에 관계없이 NSF 인식 디바이스로 구성할 수 있습니다.
- NSF 지원 디바이스로 구성하려면 디바이스가 Failover 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.
- NSF 인식 또는 NSF 지원 디바이스가 되려면, 필요에 따라 불투명 LSA(Link State Advertisements)/LLS(Link Local Signaling) 블록 처리 기능과 함께 디바이스를 구성해야 합니다.

## 프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing**(라우팅)을 클릭합니다.

단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 4 **OSPF** > **Advanced Settings**(고급 설정)를 클릭합니다.

단계 5 **General**(일반)을 선택하고 다음을 설정합니다.

- **라우터 ID**— 선택 자동 또는 라우터 ID에 대한 IP 주소 IP 주소를 선택하는 경우 IP Address(IP 주소) 필드에 IP 주소를 입력합니다.
- **LSA MOSFP 무시** - 경로가 지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷을 수신하면 syslog 메시지를 차단합니다.
- **RFC 1583 호환**— 요약 경로 비용을 계산하는 데 사용하는 방법으로 호환성 RFC 1583를 구성합니다. RFC 1583 호환성이 활성화된 라우팅 루프가 발생할 수 있습니다. 라우팅 루프를 방지하기 위해 비활성화합니다. OSPF 라우팅 도메인의 모든 OSPF 라우터는 동일한 RFC 호환성이 있어야 합니다.
- **Adjacency Changes**(인접성 변경사항) - 시스템 로그 메시지가 전송될 수 있는 인접성 변경 사항을 정의합니다.

OSPF 네이버가 작동 또는 중단될 경우 기본적으로 시스템 로그 메시지가 생성됩니다. OSPF 인접 노드가 중단될 때 시스템 로그 메시지를 보내고 각 상태에 대해 시스템 로그를 보내도록 라우터를 구성할 수 있습니다.

- **로그 인접성 변경** - OSPF 네이버가 변경되면 Firepower Threat Defense 디바이스가 syslog 메시지를 전송합니다. 이 설정은 기본적으로 선택되어 있습니다.
- **로그 인접성 변경 세부 사항** - OSPF 네이버가 변경될 때 뿐 아니라 상태 변화가 있을 때마다 Firepower Threat Defense 디바이스가 syslog 메시지를 전송합니다. 이 설정은 기본적으로 선택되어 있지 않습니다.

- **Administrative Route Distances**(관리 경로 거리) - 영역 간, 영역 내 및 외부 IPv6 경로에 대한 관리 경로 거리를 구성하는 데 사용된 설정을 수정할 수 있습니다. 관리 경로 영역의 값은 10 ~ 254의 정수입니다. 기본값은 110입니다.
- **LSA Group Pacing**(LSA 그룹 속도) - LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 10 ~ 1800입니다. 기본값은 240입니다.
- **Default information originate**(기본 정보 생성) - OSPFv3 라우팅 도메인에 기본 외부 경로를 생성하고 다음 옵션을 구성하려면 **Enable**(활성화) 확인란을 선택합니다.
  - 항상 기본 경로 광고—기본 경로 광고 항상 보장 합니다.
  - 를 클릭합니다.(메트릭 값) - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 유효한 값의 범위는 0 ~ 16777214입니다. 기본값은 10입니다.
  - **Metric Type**(메트릭 유형) - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형입니다. 유효한 값은 1(유형 1 외부 경로) 및 2(유형 2 외부 경로)입니다. 기본값은 Type 2 외부 경로입니다.
  - **RouteMap**(경로 맵) - 경로 맵이 적절한 경우 기본 경로를 생성하는 라우팅 프로세스를 선택하거나 추가(+)을 클릭하여 새 경로를 추가합니다. 새 경로 맵을 추가하려면 **구성 경로 맵 항목**을 참조하십시오.

단계 6 **OK**(확인)를 클릭하여 일반 구성을 저장합니다.

단계 7 **Non Stop Forwarding**(정지 없이 전송)을 선택하고 NSF 가능 또는 NSF 인식 디바이스에서 OSPFv2에 대해 Cisco NSF graceful restart를 구성합니다.

참고 OSPFv2에 사용할 수 있는 두 가지 Graceful Restart 메커니즘은 Cisco NSF 및 IETF NSF입니다. ospf 인스턴스에는 Graceful Restart 메커니즘을 한 번에 하나만 구성할 수 있습니다. NSF 인식 장치는 Cisco NSF 헬퍼 및 IETF NSF 헬퍼 둘 다로 구성 될 수 있으나 NSF 지원 장치는 OSPF 인스턴스를 위해 한 번에 Cisco NSF 또는 IETF NSF 모드에서 구성할 수 있습니다.

- a) **Enable Cisco 비 Stop Forwarding** 기능 체크 박스 선택합니다.
- b) (선택 사항) 필요한 경우 **Cancels NSF restart when non-NSF-aware neighboring networking devices are detected**(NSF 이외 인식 인접 네트워킹 디바이스가 감지된 경우 NSF 재시작 취소) 확인란을 선택합니다.
- c) (선택 사항) **Enable Cisco 비 Stop Forwarding 헬퍼 모드** 체크 박스 NSF 인식 디바이스에서 헬퍼 모드를 비활성화하려면 선택하지 않았는지 확인합니다.

단계 8 NSF 지원 또는 NSF 인식 디바이스에 대해 OSPFv2용 IETF NSF 정상 재시작을 구성합니다.

- a) **Enable IETF 비 Stop Forwarding** 기능 확인란을 선택합니다.
- b) (선택 사항) **Length of graceful restart interval**(정상 재시작 간격 길이) 필드에 재시작 간격을 초 단위로 입력합니다. 기본값은 120초입니다. 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.
- c) (선택 사항) **Enable IETF nonstop** 착신 전환 (NSF) 헬퍼 모드에 대한 체크 박스 NSF 인식 디바이스에서 IETF NSF 헬퍼 모드를 비활성화 하려면 선택 하지 않은 있는지 확인합니다.

- d) 엄격 링크 상태 알림 확인 활성화 - 활성화하면 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.
- e) **Enable IETF** 비 **Stop Forwarding**— 활성화 되지 않은 전환에 따라 라우팅 프로토콜 정보를 복원되는 동안 알려진 경로 계속 하려면 데이터 패킷 전달할 수 있는 작신 전환 중단 방법입니다. OSPF 네이버 OSPF 디바이스에서의 상태를 복구 하기 위해 OSPF 프로토콜 확장을 사용합니다. 작동 하려면 복구를 위한 네이버 NSF 프로토콜 확장을 지원 하고 다시 시작 되는 디바이스에 "helper" 역할을 할 수 해야 합니다. 네이버는 프로토콜 상태 복구 수행 하는 동안 다시 시작 되는 디바이스에 데이터 트래픽 전달 계속 해야 합니다.

## OSPFv3 구성

이 섹션에서는 OSPFv3 라우팅 프로세스 구성과 관련된 작업을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 OSPFv3는 전역 가상 라우터에만 구성할 수 있으며 사용자 정의 가상 라우터에는 구성할 수 없습니다.

### OSPFv3 영역, 경로 요약 및 가상 링크 구성

OSPFv3를 활성화하려면 OSPFv3 라우팅 프로세스를 생성하고, OSPFv3에 대한 영역을 생성하고, OSPFv3에 대한 인터페이스를 활성화하고, 경로를 대상 OSPFv3 라우팅 프로세스에 재분배해야 합니다.

프로시저

- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing**(라우팅) > **OSPFv3**을 선택합니다.
- 단계 3 기본적으로 활성화 프로세스 1 선택 되어 있습니다. 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다.
- 단계 4 드롭다운 목록에서 OSPF 역할을 선택하고 다음 필드에 설명을 입력합니다. 옵션으로는 내부, ABR 및 ASBR, ABR 및 ASBR이 있습니다. 참조 [OSPF 정보, 1 페이지](#) OSPFv3 역할에 대한 설명입니다.
- 단계 5 **Area**(영역) > **Add**(추가)를 선택합니다.  
수정(✍)를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 6 **General**(일반)을 선택하고 각 OSPF 프로세스에 대해 다음 옵션을 구성합니다.
  - 영역 ID - 경로를 요약할 영역을 지정합니다.
  - 비용 - 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 요약 경로의 메트릭 또는 비용을 입력합니다. 유효한 값의 범위는 0 ~ 16777215입니다.

- 유형-Normal, NSSA, Stub 지정 합니다. 일반을 선택 하는 경우에 다른 매개 변수가 구성 합니다. Stub을 선택 하는 경우 영역에 요약 Lsa를 전송 하도록 선택할 수 있습니다. NSSA를 선택 하는 경우에 다음 세 가지 옵션을 구성할 수 있습니다.
  - 요약 LSA를 영역으로 전송하도록 허용하려면 **Allow sending of summary LSAs into the area**(요약 LSA를 영역으로 전송하도록 허용) 확인란을 선택합니다.
  - 재배포 시 경로를 Normal 및 not-so-stubby 영역으로 가져오도록 허용하려면 **Redistribution imports routes to normal and NSSA areas**(재배포시 일반 및 NSSA 영역으로 경로 가져오기) 확인란을 선택합니다.
  - **default-information originate** - OSPF 라우팅 도메인에 기본 외부 경로를 생성합니다.
- **Metric**(메트릭) - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 기본값은 10입니다. 유효한 값의 범위는 0 ~ 16777214입니다.
- **메트릭 유형** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.

단계 7 **OK**(확인)를 클릭하여 일반 구성을 저장합니다.

단계 8 **Route Summary**(경로 요약) > **Add Route Summary**(경로 요약 추가)를 선택합니다.

수정(✍)을 클릭하거나 메뉴를 오른쪽 클릭하여 라우트 요약을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 9 각 OSPF 프로세스에 대한 다음 경로 요약 옵션을 구성 합니다.

- **IPv6/Prefix-length-IPv6** 접두사. 네트워크 개체를 새로 추가하려면 추가(+ )을 클릭합니다. 네트워크 추가 절차는 **네트워크 개체**의 내용을 참조하십시오.
- **비용** - 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 요약 경로의 메트릭 또는 비용을 입력합니다. 유효한 값의 범위는 0 ~ 16777215입니다.
- **알림** - 요약 경로 알림입니다. 이 확인란의 선택을 취소하면 요약 주소에 속하는 경로가 억제됩니다. 기본적으로 이 확인란은 선택되어 있습니다.

단계 10 확인 을 클릭 하여 경로 요약 구성을 저장 합니다.

단계 11 가상 링크를 선택하고 추가를 클릭하여 각 OSPF 프로세스에 대해 다음 옵션을 구성합니다.

- **피어 RouterID**-피어 라우터 IP 주소를 선택합니다. 네트워크 개체를 새로 추가하려면 추가(+ )을 클릭합니다. 네트워크 추가 절차는 **네트워크 개체**의 내용을 참조하십시오.
- **TTL 보안**— 활성화 TTL 보안 검사 합니다. Hop count에 대한 값은 1에서 254 사이의 숫자입니다. 기본값은 1입니다.

OSPF에서 0에서 255 TTL (Live) 값으로 IP 헤더 시간으로 발신 패킷을 전송하고 가능한 임계값보다 작은 TTL 값이 있는 수신 패킷을 구성합니다. 장치별 전달 하는 IP 패킷을 TTL 감소, 때문에 직접 (1 홉) 연결을 통해 수신 된 패킷 255의 값을 갖습니다. 두 개의 홉을 통과 하는 패킷은 254 등의 값을 갖고 있습니다. 수신 임계값은 패킷을 거리 있을 수 있는 홉의 최대 수 형태로 구성됩니다.

- **데드 간격** - 라우터가 중단되었음을 네이버가 나타내기까지 hello 패킷이 표시되지 않은 시간을 초 단위로 입력합니다. 기본값은 Hello 간격의 4배이거나 40초입니다. 유효한 값의 범위는 1 ~ 65535입니다.

Dead 간격은 무부호 정수입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다.

- **Hello 간격** - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. 유효한 값의 범위는 1 ~ 65535입니다. 기본값은 10입니다.

Hello 간격은 Hello 패킷에 광고되는 무부호 정수입니다. 이 값은 특정 네트워크의 모든 라우터 및 액세스 서버에서 동일해야 합니다. Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다.

- **재전송 간격** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값은 예상 왕복 지연 시간보다 커야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 5입니다.

라우터에서 LSA를 네이버로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

- **전송 지연** - 인터페이스에서 LSA 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 이 정수 값은 0보다 커야 합니다. 유효한 값의 범위는 1 ~ 8192입니다. 기본값은 1입니다.

업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.

단계 12 **OK**를 클릭하여 설정을 저장합니다.

단계 13 변경 사항을 저장 하려면 라우터 페이지에서 저장 을 클릭 합니다.

다음에 수행할 작업

[OSPFv3 재배포 구성](#) 진행 합니다.

## OSPFv3 재배포 구성

Firepower Threat Defense 디바이스는 OSPF 라우팅 프로세스 간의 경로 재분배를 제어할 수 있습니다. 하나의 라우팅 프로세스에서 OSPF 라우팅 프로세스로 경로를 재분배하기 위한 규칙이 표시됩니다. RIP 및 BGP에서 검색된 경로를 OSPF 라우팅 프로세스로 재분배할 수 있습니다. 고정 경로 및 연결된 경로도 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

## 프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.

단계 2 라우팅 > **OSPF**를 선택합니다.

단계 3 **Redistribution**(재배포)을 선택하고 **Add**(추가)를 누릅니다.

수정(✍)을 클릭하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 4 각 OSPF 프로세스에 대한 다음 재배포 옵션을 구성합니다.

- **소스 프로토콜** - 경로를 재배포하는 소스 프로토콜. 지원되는 프로토콜은 **connected**, **static**, **OSPF**입니다. OSPF를 선택 하는 경우에 프로세스 **ID** 필드에 프로세스 **ID**를 입력 해야 합니다. BCP를 선택 하는 경우에 **AS** 번호 필드에 **AS** 번호를 추가해야 합니다.

- **메트릭** - 배포 되는 경로의 메트릭 값입니다. 기본값은 10입니다. 유효한 값의 범위는 0~16777215입니다.

하나의 OSPF 프로세스에서 동일한 디바이스의 다른 OSPF 프로세스로 재분배할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재분배할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.

- **Metric Type**(메트릭 유형) - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 **Type 1** 외부 경로는 1, **Type 2** 외부 경로는 2입니다.

- **Tag**(태그) - 태그는 OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값을 지정합니다. 아무것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값은 0 ~ 4294967295입니다.

- **Route Map**(경로 맵) - 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜까지 경로 가져오기의 필터링을 확인합니다. 이 매개변수를 지정하지 않으면 모든 경로가 재분배됩니다. 이 매개변수를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. 또는 추가(+)를 클릭하여 새 경로 맵을 추가할 수 있습니다. **경로 맵**의 절차를 참조하여 새로운 경로 맵을 추가합니다.

- **Process ID**(프로세스 ID) - OSPF 프로세스 ID(1 또는 2)입니다.

참고 프로세스 ID가 활성화되면 OSPFv3 프로세스가 다른 OSPFv3 프로세스에서 학습한 경로를 재배포합니다.

- **Match**(연결) - 다른 라우팅 도메인에 재배포할 수 있도록 OSPF 경로를 활성화합니다.

- **Internal**(내부) - 특정 자동 시스템의 내부에 있는 경로입니다.

- **External 1**(외부 1) - 자동 시스템의 외부에 있지만, OSPFv3에 Type 1 외부 경로로서 가져온 경로입니다.

- **External 2(외부 2)** - 자동 시스템의 외부에 있지만, OSPFv3에 Type 2 외부 경로로서 가져온 경로입니다.
- **NSSA External 1(NSSA 외부 1)** - 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 1 외부 경로로서 가져온 경로입니다.
- **NSSA External(NSSA 외부)** - 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 2 외부 경로로서 가져온 경로입니다.

단계 5 **OK(확인)**를 클릭하여 재배포 구성을 저장합니다.

단계 6 Routing(라우팅) 페이지에서 **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

[OSPFv3 요약 접두사 설정, 24 페이지](#)를 계속 진행합니다.

## OSPFv3 요약 접두사 설정

지정된 IPv6 접두사 및 마스크 쌍과 일치하는 경로를 알리도록 Firepower Threat Defense 디바이스를 구성할 수 있습니다.

프로시저

단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing(라우팅) > OSPFv3**을 선택합니다.

단계 3 **Summary Prefix(요약 접두사) > Add(추가)**를 선택합니다.

수정(✍)을 클릭하거나 메뉴를 오른쪽 클릭하여 요약 접두사를 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 4 각 OSPF 프로세스에 대한 다음 요약 접두사 옵션을 구성합니다.

- **IPv6 Prefix/Length(IPv6 접두사/길이)** - IPv6 접두사 및 프리픽스 길이 라벨입니다. 목록에서 하나를 선택하거나 추가(+)을 클릭하여 새 네트워크 개체를 추가합니다. 네트워크 추가 절차는 [네트워크 개체](#)를 참조하십시오.
- **Advertise(알림)** - 지정된 접두사 및 마스크 쌍과 일치하는 경로를 알립니다. 지정된 접두사 및 마스크 쌍과 일치하는 경로를 억제하려면 이 확인란의 선택을 취소합니다.
- (선택 사항) **Tag(태그)** - 경로 맵을 통해 재배포를 제어하기 위한 일치 값으로 사용할 수 있는 값입니다.

단계 5 **OK(확인)**를 클릭하여 요약 접두사 구성을 저장합니다.



단계 6 Routing(라우팅) 페이지에서 **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPFv3 인터페이스, 인증 및 네이버 설정, 25 페이지를 계속 진행합니다.

## OSPFv3 인터페이스, 인증 및 네이버 설정

필요한 경우 특정 인터페이스별 OSPFv3 매개변수를 변경할 수 있습니다. 이러한 파라미터는 변경할 필요가 없지만, hello 간격 및 dead 간격과 같은 인터페이스 파라미터는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 구성할 경우, 네트워크의 모든 라우터 구성에 호환되는 값이 있는지 확인해야 합니다.

프로시저

- 단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2 **Routing(라우팅) > OSPFv3**을 선택합니다.
- 단계 3 **Interface(인터페이스) > Add(추가)**를 선택합니다.
- Edit(편집)**를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.
- 단계 4 각 OSPFv3 프로세스에 대해 다음 인터페이스 옵션을 구성합니다.
- **Interface(인터페이스)** - 구성 중인 인터페이스입니다.
  - **Enable OSPFv3(OSPFv3 활성화)** - OSPFv3을 활성화합니다.
  - **OSPF Process(OSPF 프로세스)** - 1 또는 2를 선택합니다.
  - **Area(영역)** - 이 프로세스에 대한 영역 ID입니다.
  - **Instance(인스턴스)** - 인터페이스에 할당할 영역 인스턴스 ID를 지정합니다. 하나의 인터페이스에는 하나의 OSPFv3 영역만 포함할 수 있습니다. 여러 인터페이스에서 동일한 영역을 사용할 수 있으며, 각 인터페이스에서는 다른 영역 인스턴스 ID를 사용할 수 있습니다.
- 단계 5 **Properties(속성)**를 선택하고 각 OSPFv3 프로세스에 대해 다음 옵션을 구성합니다.
- **Filter Outgoing Link Status Advertisements(발송 링크 상태 알림 필터링)** - OSPFv3 인터페이스에 발신되는 LSA를 필터링합니다. 기본적으로 모든 발신 LSA는 인터페이스에 플러딩됩니다.
  - **Disable MTU mismatch detection(MTU 불일치 감지 비활성화)** - DBD 패킷이 수신될 때 OSPF MTU 불일치 감지를 비활성화합니다. OSPF MTU 불일치 감지는 기본적으로 활성화되어 있습니다.
  - **Flood Reduction(플러딩 감소)** - 정상 LSA를 Do not Age LSAs(LSA 기간 적용 안 함)로 변경하여 3600초마다 영역에 플러딩되지 않도록 합니다.

OSPF LSA는 3600초마다 새로 고침됩니다. 대규모 OSPF 네트워크에서 이는 영역 간에 많은 양의 불필요한 LSA 플러딩을 유발할 수 있습니다.

- **Point-to-Point Network(포인트-투-포인트 네트워크)** - VPN 터널을 통해 OSPF 경로를 전송할 수 있습니다. 인터페이스가 포인트-투-포인트 비 브로드캐스트로 구성된 경우, 다음과 같은 제한이 적용됩니다.
  - 인터페이스에 대해 하나의 네이버만 정의할 수 있습니다.
  - 네이버를 수동으로 구성해야 합니다.
  - 암호화 엔드포인트를 가리키는 고정 경로를 정의해야 합니다.
  - 인터페이스에서 터널을 통해 OSPF가 실행 중일 경우, 업스트림 라우터가 있는 일반 OSPF를 동일한 인터페이스에서 실행할 수 없습니다.
  - OSPF 네이버를 지정하기 전에 암호화 맵을 인터페이스에 바인딩하여 OSPF 업데이트가 VPN 터널을 통해 전달되도록 해야 합니다. OSPF 네이버를 지정한 후에 암호화 맵을 인터페이스에 바인딩한 경우, **clear local-host all** 명령을 사용하여 OSPF 연결을 지워 OSPF 인접성이 VPN 터널을 통해 설정될 수 있도록 합니다.
- **Broadcast(브로드캐스트)** - 인터페이스의 브로드캐스트 인터페이스 여부를 지정합니다. 기본적으로 이 확인란은 이더넷 인터페이스에 선택되어 있습니다. 인터페이스를 포인트-투-포인트 비 브로드캐스트 인터페이스로 지정하려면 이 확인란의 선택을 취소합니다. 인터페이스를 포인트-투-포인트 비 브로드캐스트 인터페이스로 지정하면 OSPF 경로를 VPN 터널을 통해 전송할 수 있습니다.
- **Cost(비용)** - 인터페이스에서 패킷을 전송하는 비용을 지정합니다. 이 설정의 유효한 값 범위는 0~255입니다. 기본값은 1입니다. 이 설정을 0으로 입력하면 해당 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다. 이 설정은 포인트-투-포인트 비 브로드캐스트 인터페이스로 구성된 인터페이스에는 적용되지 않습니다.
 

네트워크에 라우터가 2개 연결될 경우, 두 라우터 모두 전용 라우터가 되려고 시도합니다. 라우터 우선 순위가 더 높은 디바이스가 전용 라우터가 됩니다. 연관성이 있을 경우, 라우터 ID가 더 높은 라우터가 전용 라우터가 됩니다.
- **Priority(우선 순위)** - 네트워크의 전용 라우터를 결정합니다. 유효한 값의 범위는 0~255입니다.
- **Dead Interval(중단 간격)** - 인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간 기간(초)입니다. 이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다.
- **Poll Interval(폴링 간격)** - 네이버와의 인접성이 설정되기 전에 라우터가 전송할 OSPF 패킷 사이의 시간 기간(초)입니다. 라우팅 디바이스가 활성 네이버를 감지하면 hello 패킷 간격은 폴링 간격에 지정된 시간에서 hello 간격에 지정된 시간으로 변경됩니다. 유효한 값의 범위는 1초~65535초입니다.
- **Retransmit Interval(재전송 간격)** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1초~65535초입니다. 기본값은 5초입니다.

- **Transmit Delay**(전송 지연) - 필드에 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간(초)입니다. 유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 1초입니다.

단계 6 **OK**(확인)를 클릭하여 구성을 저장합니다.

단계 7 **Authentication**(인증)을 선택하고 각 OSPFv3 프로세스에 대해 다음 옵션을 구성합니다.

- **Type**(유형) - 인증 유형입니다. 사용 가능한 옵션은 **Area**(영역), **Interface**(인터페이스), **None**(없음)입니다. **None**(없음) 옵션은 사용 중인 인증이 없음을 나타냅니다.
- **Security Parameters Index**(보안 파라미터 색인) - 256~4294967295 사이의 숫자입니다. 유형으로 **Interface**(인터페이스)를 선택한 경우 구성합니다.
- **Authentication**(인증) - 인증 알고리즘의 유형입니다. 지원되는 값은 **SHA-1** 및 **MD5**입니다. 유형으로 **Interface**(인터페이스)를 선택한 경우 설정합니다.
- **Authentication Key**(인증 키) - MD5 인증을 사용할 경우, 키는 32자 길이의 16진수 숫자(16바이트)여야 합니다. SHA-1 인증을 사용할 경우, 키는 40자 길이의 16진수 숫자(20바이트)여야 합니다.
- **Encrypt Authentication Key**(인증 키 암호화) - 인증 키 암호화를 활성화합니다.
- **Include Encryption**(암호화 포함) - 암호화를 활성화합니다.
- **Encryption Algorithm**(암호화 알고리즘) - 암호화 알고리즘의 유형입니다. 지원되는 값은 **DES**입니다. **Null** 항목은 암호화가 없음을 나타냅니다. **Include Encryption**(암호화 포함)을 선택하는 경우 구성합니다.
- **Encryption Key**(인증 키) - 인증 키를 입력합니다. **Include Encryption**(암호화 포함)을 선택하는 경우 구성합니다.
- **Encrypt Key**(키 암호화) - 키가 암호화되도록 활성화합니다.

단계 8 **OK**(확인)를 클릭하여 구성을 저장합니다.

단계 9 **Neighbor**(네이버)를 선택하고 **Add**(추가)를 클릭하여 각 OSPFv3 프로세스에 대해 다음 옵션을 구성합니다.

- **Link Local Address**(로컬 주소 연결) - 고정 네이버의 IPv6 주소입니다.
- **Cost**(비용) - 비용을 활성화합니다. **Cost**(비용) 필드에 비용을 입력한 다음, 알려려면 **Filter Outgoing Link State Advertisements**(발송 링크 상태 알림 필터링)를 선택합니다.
- (선택 사항) **Poll Interval**(폴링 간격) - 폴링 간격을 활성화합니다. **Priority**(우선 순위) 레벨 및 **Poll Interval**(폴링 간격)을 초 단위로 입력합니다.

단계 10 네이버를 추가하려면 **Add**(추가)를 클릭합니다.

단계 11 **OK**(확인)를 클릭하여 인터페이스 구성을 저장합니다.

## OSPFv3 고급 속성 설정

Advanced Properties(고급 속성)를 사용하면 시스템 로그 메시지 생성, 관리 경로 거리, 수동 OSPFv3 라우팅, LSA 타이머 및 Graceful Restart와 같은 옵션을 설정할 수 있습니다.

### Graceful Restart

Firepower Threat Defense 디바이스에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(Non-Stop Forwarding) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 무중단(Hitless) 소프트웨어 업그레이드가 예정되어 있을 때 유용합니다. graceful-restart(RFC 5187)를 사용하여 OSPFv3에서 Graceful Restart를 구성할 수 있습니다.



참고 NSF 기능은 HA 모드 및 클러스터링에도 유용합니다.

NSF Graceful Restart 기능을 구성하려면 기능을 구성하고, 디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. NSF 지원 디바이스는 해당 디바이스의 재시작 작업을 네이버에 나타낼 수 있으며, NSF 인식 디바이스는 네이버를 초기화하도록 지원할 수 있습니다.

디바이스는 몇 가지 조건에 따라 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다.

- 디바이스는 현재 속한 모드에 관계없이 NSF 인식 디바이스로 구성할 수 있습니다.
- NSF 지원 디바이스로 구성하려면 디바이스가 Failover 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.
- NSF 인식 또는 NSF 지원 디바이스가 되려면, 필요에 따라 불투명 LSA(Link State Advertisements)/LLS(Link Local Signaling) 블록 처리 기능과 함께 디바이스를 구성해야 합니다.

### 프로시저

- 단계 1** **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스를 수정합니다.
- 단계 2** **Routing**(라우팅) > **OSPFv3** > **Advanced**(고급)를 선택합니다.
- 단계 3** **Router ID**(라우터 ID)에서 **Automatic**(자동) 또는 **IP address**(IP 주소)를 선택합니다. IP 주소를 선택하는 경우 IP Address(IP 주소) 필드에 IP 주소를 입력합니다.
- 단계 4** 경로가 지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷을 수신할 때 시스템 로그 메시지를 표시하지 않으려면 **Ignore LSA MOSPF**(LSA MOSPF 무시) 확인란을 선택합니다.
- 단계 5** **General**(일반)을 선택하고 다음을 설정합니다.
  - **Adjacency Changes**(인접성 변경사항) - 시스템 로그 메시지가 전송될 수 있는 인접성 변경 사항을 정의합니다.

OSPF 네이버가 작동 또는 중단될 경우 기본적으로 시스템 로그 메시지가 생성됩니다. OSPF 인접 노드가 중단될 때 시스템 로그 메시지를 보내고 각 상태에 대해 시스템 로그를 보내도록 라우터를 구성할 수 있습니다.

- **Adjacency Changes**(인접성 변경사항) - OSPF 네이버가 작동 또는 중단될 때마다 Firepower Threat Defense 디바이스에서 시스템 로그 메시지를 전송하도록 합니다. 이 설정은 기본적으로 선택되어 있습니다.
- **Include Details**(상세정보 포함) - Firepower Threat Defense 디바이스의 작동 또는 중단 뿐만 아니라 모든 상태가 변경될 때마다 에서 syslog 메시지를 전송하게 됩니다. 이 설정은 기본적으로 선택되어 있지 않습니다.
- **Administrative Route Distances**(관리 경로 거리) - 영역 간, 영역 내 및 외부 IPv6 경로에 대한 관리 경로 거리를 구성하는 데 사용된 설정을 수정할 수 있습니다. 관리 경로 영역의 값은 10~254의 정수입니다. 기본값은 110입니다.
- **Default information originate**(기본 정보 생성) - OSPFv3 라우팅 도메인에 기본 외부 경로를 생성하고 다음 옵션을 구성하려면 **Enable**(활성화) 확인란을 선택합니다.
  - **Always advertise**(항상 알림) - 기본 경로의 존재 여부에 상관없이 항상 기본 경로를 광고합니다.
  - **Metric**(메트릭) - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 유효한 값의 범위는 0~16777214입니다. 기본값은 10입니다.
  - **Metric Type**(메트릭 유형) - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형입니다. 유효한 값은 1(유형 1 외부 경로) 및 2(유형 2 외부 경로)입니다. 기본값은 Type 2 외부 경로입니다.
  - **Route Map**(경로 맵) - 경로 맵이 적절한 경우, 기본 경로를 생성하는 라우팅 프로세스를 선택하거나 추가(+)를 클릭하여 새 경로를 추가합니다. **경로 맵**을 참조하여 새로운 경로 맵을 추가합니다.

단계 6 **OK**(확인)를 클릭하여 일반 구성을 저장합니다.

단계 7 **Passive Interface**(패시브 인터페이스)를 선택하고 **Available Interfaces**(사용 가능한 인터페이스) 목록에서 패시브 OSPFv3 라우팅을 활성화할 인터페이스를 선택한 다음 **Add**(추가)를 클릭하여 **Selected Interfaces**(선택한 인터페이스) 목록으로 이동합니다.

패시브 라우팅에서는 OSPFv3 라우팅 정보의 광고를 제어할 수 있도록 지원하고, 인터페이스에서 OSPFv3 라우팅 업데이트의 전송 및 수신을 비활성화합니다.

단계 8 **OK**(확인)를 클릭하여 패시브 인터페이스 구성을 저장합니다.

단계 9 **Timer**(타이머)를 선택하고 다음 LSA 속도 및 SPF 계산 타이머를 설정합니다.

- **Arrival**(도착) - 네이버에서 도착하는 동일한 LSA를 수락하는 동안 소요될 수밖에 없는 최소 지연 시간을 밀리초 단위로 지정합니다. 범위는 0밀리초~6000,000밀리초입니다. 기본값은 1000밀리초입니다.

- **Flood Pacing**(플러딩 속도) - 업데이트 중 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5밀리초 ~ 100밀리초입니다. 기본값은 33밀리초입니다.
- **Group Pacing**(그룹 속도) - LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 10 ~ 1800입니다. 기본값은 240입니다.
- **Retransmission Pacing**(재전송 속도) - 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5밀리초 ~ 200밀리초입니다. 기본값은 66밀리초입니다.
- **Throttle Initial**(제한 초기) - LSA의 첫 번째 어커런스를 생성하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. 기본값은 0밀리초입니다. 최소값은 동일한 LSA를 시작하는 데 필요한 최소 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다. 최대값은 동일한 LSA를 시작하는 데 필요한 최대 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다.

참고 LSA 제한의 경우 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3이 첫 번째 어커런스 값으로 자동으로 수정됩니다. 마찬가지로 지정된 최대 지연 시간이 최소 지연 시간보다 작으면 OSPFv3이 최소 지연 시간 값으로 자동으로 수정됩니다.

- **SPF Throttle**(SPF 제한) - SPF 계산의 변경 사항을 수신하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다. 최소값은 첫 번째와 두 번째 SPF 계산 사이의 지연 시간을 밀리초 단위로 지정합니다. 기본값은 10000밀리초입니다. 최대값은 SPF 계산에 소요되는 최대 대기 시간을 밀리초 단위로 지정합니다. 기본값은 10000밀리초입니다.

참고 SPF 제한의 경우, 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3에서 첫 번째 어커런스 값을 자동으로 수정합니다. 마찬가지로 지정된 최대 지연 시간이 최소 지연 시간보다 작으면 OSPFv3이 최소 지연 시간 값으로 자동으로 수정됩니다.

단계 10 **OK**(확인)를 클릭하여 LSA 타이머 구성을 저장합니다.

단계 11 **Non Stop Forwarding**(무제한 전달)을 선택하고 **Enable graceful-restart helper**(Graceful-Restart 헬퍼 활성화) 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다. NSF 인식 디바이스에서 Graceful-Restart 헬퍼 모드를 비활성화하려면 이 확인란의 선택을 취소합니다.

단계 12 **Enable link state advertisement**(링크 상태 알림 활성화) 확인란을 선택하여 strict 링크 상태 알림 확인을 활성화합니다.

이를 활성화하면 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.

단계 13 **Enable graceful-restart (Use when Spanned Cluster or Failover Configured)**(스팬 클러스터 또는 페일 오버가 구성된 경우 사용) 확인란을 선택하고 Graceful Restart 간격을 초 단위로 입력합니다. 범위는 1~1800입니다. 기본값은 120초입니다. 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.

단계 14 **OK**(확인)를 클릭하여 Graceful Restart 구성을 저장합니다.

단계 15 Routing(라우팅) 페이지에서 **Save**(저장)를 클릭하여 변경 사항을 저장합니다.

---

