DHCP 및 DDNS

다음 주제는 DHCP 및 DDNS 서비스와 Threat Defense 디바이스에서 구성하는 방법을 설명합니다.

DHCP 및 DDNS 서비스 정보

다음 주제는 DHCP 서버, DHCP 릴레이 에이전트 및 DDNS 업데이트를 설명합니다.

DHCPv4 서버 정보

DHCP는 IP 주소와 같은 네트워크 컨피그레이션 매개변수를 DHCP 클라이언트에 제공합니다. 위협 방지 디바이스은 위협 방지 디바이스 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버를 제공할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 직접 네트워크 컨피그레이션 매개변수를 제공합니다.

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.

하지만 Ipv6의 DHCP 서버는 지원되지 않습니다. 그러나 IPv6 트래픽에 대한 DHCP 릴레이를 활성화할 수 있습니다.

DHCP 옵션

DHCP는 TCP/IP 네트워크에서 호스트할 구성 정보를 전달하기 위한 프레임워크를 제공합니다. 구성 파라미터는 DHCP 메시지의 Options(옵션) 필드에 저장된 태깅 항목으로 전달되며, 데이터는 옵션이

라고도 합니다. 벤더 정보는 Options(옵션)에도 저장되어 있으며 모든 벤더 정보는 확장하여 DHCP 옵션으로 사용될 수 있습니다.

Cisco IP Phone은 TFTP 서버에서 구성을 다운로드합니다. Cisco IP Phone이 시작할 때 IP 주소 및 TFTP 서버 IP 주소 모두 미리 구성되지 않았다면 이 정보를 얻고자 DHCP 서버에 옵션 150 또는 66으로 요청을 보냅니다.

- DHCP 옵션 150은 일련의 TFTP 서버의 IP 주소를 제공합니다.
- DHCP 옵션 66은 단일 TFTP 서버의 IP 주소 또는 호스트 이름을 제공합니다.
- DHCP 옵션 3은 기본 경로를 설정합니다.

하나의 요청에서 옵션 150과 66을 모두 포함할 수 있습니다. 이 경우, 두 옵션의 값이 이미 ASA에 구성되어 있다면 ASA DHCP 서버에서는 두 옵션을 모두 포함하여 응답합니다.

고급 DHCP 옵션을 사용하여 DHCP 클라이언트에 DNS, WINS, 도메인 이름 매개변수를 제공할 수 있습니다. DHCP 옵션 15는 DNS 도메인 접미사에 사용됩니다. 또한 DHCP 자동 컨피그레이션 설정을 사용하여 이 값을 얻거나 직접 정의할 수도 있습니다. 이 정보를 정의하는 데 둘 이상의 방법을 사용할 경우 다음 순서로 DHCP 클라이언트에 전달됩니다.

1. 직접 구성한 설정
2. 고급 DHCP 옵션 설정
3. DHCP 자동 컨피그레이션 설정

이를테면 DHCP 클라이언트에서 수신할 도메인 이름을 직접 정의한 다음 DHCP 자동 컨피그레이션을 활성화할 수 있습니다. DHCP 자동 컨피그레이션에서 DNS 및 WINS 서버와 함께 도메인을 검색하더라도, 수동으로 정의된 도메인 이름이 검색된 DNS 및 WINS 서버 이름과 함께 DHCP 클라이언트에 전달됩니다. DHCP 자동 컨피그레이션 프로세스에 의해 검색된 도메인 이름보다 수동 정의된 도메인 이름이 우선하기 때문입니다.

DHCPv6 스테이트리스 서버 정보

접두사 위임 기능(IPv6 접두사 위임 클라이언트 활성화)과 함께 SLAAC(StateLess Address Auto Configuration)를 사용하는 클라이언트의 경우, DHCP IPv6 풀을 정의하고 DHCPv6 서버에 할당하여 IR(정보 요청) 패킷을 threat defense에 보낼 때 DNS 서버 또는 도메인 이름 같은 정보를 제공하도록 threat defense를 구성할 수 있습니다. threat defense는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 클라이언트에서 IPv6 자동 구성을 활성화하여 자체 IPv6 주소를 생성하도록 클라이언트를 구성합니다. 클라이언트에서 스테이트리스 자동 구성을 사용하도록 설정하면 라우터 광고 메시지에서 수신된 접두사, 즉 threat defense가 접두사 위임을 사용하여 수신한 접두사를 기준으로 IPv6 주소를 구성합니다.

DHCP 릴레이 에이전트 소개

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 세

그먼트에 서버가 없을 경우, 위협 방지 디바이스는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다. DHCP 릴레이 에이전트를 사용하면 DHCP 요청을 다른 인터페이스의 DHCP 서버로 전송하는 브로드캐스트를 수신하는 위협 방지 디바이스의 인터페이스를 구성할 수 있습니다.

DHCP 및 DDNS 요구 사항 및 사전 요건

모델 지원

Threat Defense

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

DHCP 및 DDNS 서비스에 대한 지침

이 섹션에는 DHCP 및 DDNS 서비스를 구성하기 전에 확인해야 하는 제한사항 및 지침이 포함되어 있습니다.

방화벽 모드

- DHCP 릴레이는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.
- DHCP 서버는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드에서 지원됩니다. 라우팅 모드에서 DHCP 서버는 브리지 그룹 멤버 인터페이스가 아닌 BVI 인터페이스에서 지원됩니다. DHCP 서버가 작동하려면 BVI에 이름이 있어야 합니다.
- DDNS는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.

IPv6

DHCP 서버에 대해 IPv6 DHCP 릴레이에 대한 IPv6가 지원됩니다.

DHCPv4 서버

- 최대 가용 DHCP 풀은 주소 256개입니다.

- 각 인터페이스에서 DHCP 서버를 1개만 구성할 수 있습니다. 각 인터페이스는 자체 주소 풀을 두고 사용할 수 있습니다. 그러나 DNS 서버, 도메인 이름, 옵션, ping 시간 초과, WINS 서버와 같은 나머지 DHCP 설정은 전역으로 구성되며 모든 인터페이스에서 DHCP 서버에 의해 사용됩니다.
- 해당 인터페이스에서 DHCP 서버도 활성화된 경우, 인터페이스를 DHCP 클라이언트로 설정할 수 없습니다. 고정 IP 주소를 사용해야 합니다.
- 서로 다른 인터페이스에서 활성화하려 하더라도 동일한 디바이스에서 DHCP 서버와 DHCP 릴레이를 모두 설정할 수 없습니다. 단 하나의 서비스 유형만 구성 가능합니다.
- 위협 방지 디바이스 는 QIP DHCP 서버를 DHCP 프록시 서비스와 함께 사용하는 것을 지원하지 않습니다.
- DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

DHCP 릴레이

- 전역 서버와 인터페이스 특정 서버를 포함하여 최대 10개의 DHCPv4 릴레이 서버를 구성할 수 있으며, 각 인터페이스에는 최대 4개의 서버가 가능합니다.
- 단일 모드 및 각 상황를 구성할 수 있습니다. IPv6 인터페이스 특정 서버는 지원되지 않습니다.
- 서로 다른 인터페이스에서 활성화하려 하더라도 동일한 디바이스에서 DHCP 서버와 DHCP 릴레이를 모두 설정할 수 없습니다. 단 하나의 서비스 유형만 구성 가능합니다.
- DHCP 릴레이 서비스는 BVI 또는 브리지 그룹 멤버 인터페이스 또는 라우팅 모드에서 사용할 수 없습니다. 그러나 액세스 목록을 사용하는 방법으로 DHCP 트래픽을 허용할 수 있습니다. DHCP 요청과 응답이 위협 방지 디바이스를 지날 수 있게 하려면 2개의 액세스 규칙을 구성해야 합니다. 하나는 내부 인터페이스에서 외부(UDP 대상 포트 67)로 보내는 DHCP 요청을 허용하는 것이고 다른 하나는 반대 방향(UDP 대상 포트 68)으로 서버의 응답을 허용하는 것입니다.
- IPv4에서는 클라이언트가 위협 방지 디바이스에 직접 연결되어야 하며, 다른 릴레이 에이전트 또는 라우터를 통해 요청을 보낼 수 없습니다. IPv6에서는 위협 방지 디바이스가 다른 릴레이 서버에서 보낸 패킷을 지원합니다.
- DHCP 클라이언트는 위협 방지 디바이스에서 요청을 릴레이하는 DHCP 서버와 다른 인터페이스에 있어야 합니다.
- 트래픽 영역의 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.
- DHCP 릴레이는 VTI(Virtual Tunnel Interface)에서 지원되지 않습니다.

DHCPv4 서버 구성

DHCPv4 서버를 구성하려면 다음 단계를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **DHCP** > **DHCP** 서버를 선택합니다.

단계 **3** 다음 DHCP 서버 옵션을 구성합니다.

- **Ping** 시간 초과 - DHCP Ping 시도 시 시간 초과까지 threat defense 디바이스가 대기하는 시간의 양으로 밀리초 단위입니다. 유효한 값의 범위는 10밀리초 ~ 10000밀리초입니다. 기본값은 50밀리초입니다.

  주소 충돌을 방지하고자 threat defense 디바이스는 DHCP 클라이언트에 주소를 지정하기 전에 주소에 2개의 ICMP ping 패킷을 보냅니다.

- 임대 길이 - 클라이언트가 할당받은 IP 주소를 임대 만료 전까지 사용할 수 있는 시간으로 초 단위입니다. 유효한 값은 300초 ~ 9000초입니다. 기본값은 3600초(1시간)입니다.

- (라우팅된 모드) 자동 설정 - threat defense 디바이스에서 DHCP 자동 설정을 활성화합니다. 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. 그렇지 않은 경우 자동 설정을 비활성화하고 4단계에서 사용자가 직접 값을 추가할 수 있습니다.

- (라우팅된 모드) 인터페이스 - 자동 설정에 사용할 인터페이스를 지정합니다. 가상 라우팅 기능이 있는 디바이스의 경우, 이 인터페이스는 전역 가상 라우터 인터페이스만 될 수 있습니다.

단계 **4** 자동 구성된 설정을 오버라이드하려면 다음을 수행합니다.

- 인터페이스의 도메인 이름을 입력합니다. 장치가 Your_Company 도메인 내에 있을 수 있습니다.

- 드롭다운 목록에서 인터페이스에 구성된 DNS 서버(기본, 보조)를 선택합니다. 새 DNS 서버를 추가하려면 네트워크 개체 생성의 내용을 참조하십시오.

- 드롭다운 목록에서 인터페이스에 구성된 WINS 서버(기본, 보조)를 선택합니다. 새 WINS 서버를 추가 하려면 네트워크 개체 생성의 내용을 참조하십시오.

단계 **5** **Server(**서버**)**를 선택하고 **Add(**추가**)**를 클릭하여 탭에서 다음 옵션을 구성합니다.

- 인터페이스 - 드롭다운 목록에서 인터페이스를 선택합니다. 투명 모드에서 명명된 브리지 그룹 멤버 인터페이스를 지정합니다. 라우팅 모드에서 명명된 라우팅 인터페이스 또는 명명된 BVI를 지정합니다. 브리지 그룹 멤버 인터페이스는 지정하지 마십시오. 각 BVI의 브리지 그룹 구성원 인터페이스가 DHCP 서버에서 작동하려면 이름이 있어야 합니다.

- 주소 풀 - DHCP 서버에서 사용되는 최소 및 최대 IP 주소 범위입니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.

- **DHCP** 서버 활성화 - 선택한 인터페이스에서 DHCP 서버를 활성화합니다.

단계 **6** **OK**를 클릭하여 DHCP 서버 설정을 저장합니다.

단계 **7** (선택 사항) **Advanced(**고급**)**를 선택하고 **Add(**추가**)**를 클릭하여 옵션이 DHCP 클라이언트에 반환하려는 정보 유형을 지정하십시오.

- 옵션 코드 - threat defense 디바이스는 정보 전송을 위해 RFC 2132, RFC 2563, RFC 5510의 DHCP 옵션을 지원합니다. 1, 12, 50–54, 58–59, 61, 67, 82를 제외하고 모든 DHCP 옵션(1 ~ 255)이 지원됩니다. DHCP 옵션 코드에 대한 자세한 내용은 DHCPv4 서버 정보, 1 페이지을 참조하십시오.

  참고 threat defense 디바이스는 사용자가 제공하는 옵션의 유형 및 값이 RFC 2132에 정의된 옵션 코드의 예상 유형 및 값과 일치하는지 확인하지 않습니다. 옵션 코드와 그 유형 및 예상 값에 대한 자세한 내용은 RFC 2132를 참조하십시오.

- 유형 - DHCP 옵션 유형입니다. 사용 가능한 옵션에는 **IP**, **ASCII**및 **16** 진수가 있습니다. IP를 선택한 경우에 IP 주소 필드에 IP 주소를 추가해야 합니다. ASCII를 선택한 경우에 ASCII 필드에 ASCII 값을 추가해야 합니다. 16 진수를 선택한 경우 HEX 필드에 16 진수 값을 추가해야 합니다.
- **IP** 주소 **1** 및 **IP** 주소 **2** - 이 옵션 코드로 반환될 IP 주소입니다. 새 IP 주소를 추가하려면 네트워크 개체 생성의 내용을 참조하십시오.
- **ASCII** - DHCP 클라이언트에 반환될 ASCII 값입니다. 이 문자열은 공백을 포함할 수 없습니다.
- **16** 진수 - DHCP 클라이언트에 반환될 16 진수 값입니다. 문자열은 짝수여야 하며 공백이 없어야 합니다. 0x 접두사를 사용할 필요 없습니다.

단계 **8** **OK**를 클릭하여 옵션 코드 설정을 저장합니다.

단계 **9** 변경 사항을 저장하려면 DHCP 페이지에서 저장을 클릭합니다.

DHCPv6 스테이트리스 서버 구성

접두사 위임 기능과 함께 SLAAC(StateLess Address Auto Configuration)를 사용하는 클라이언트의 경우, IR(정보 요청) 패킷을 threat defense에 보낼 때 DNS 서버 또는 도메인 이름 같은 정보를 제공하도록 threat defense를 구성할 수 있습니다.

DHCP IPv6 풀 생성

DHCPv6 서버에서 사용할 DHCP IPv6 풀을 생성합니다. DHCPv6 서버는 클라이언트가 IR(정보 요청) 패킷을 threat defense로 보낼 때 DNS 서버 또는 도메인 이름과 같은 정보를 제공합니다. DHCP IPv6 풀은 IR 메시지에서 전송할 매개 변수를 정의합니다.

이 기능은 라우팅 모드에서만 지원됩니다. 이 기능은 클러스터링 또는 고가용성에서 지원되지 않습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **DHCP IPv6 Pool(DHCP IPv6 풀)**을 선택합니다.

단계 **3** **Add(추가)** ( ) 버튼을 클릭합니다.

단계 **4** **DNS Server(DNS 서버)** 및 **Domain Name(도메인 이름)**을 구성합니다.

값을 수동으로 정의하고 **Add(추가)**를 클릭하거나 **Import(가져오기)**를 선택하여 threat defense가 접두사 위임 클라이언트 인터페이스의 DHCPv6 서버에서 가져온 하나 이상의 매개변수를 사용할 수 있습니다. 수동으로 구성한 매개변수를 가져온 매개변수와 혼합하고 일치시킬 수 있습니다. 그러나 동일한 매개변수를 수동으로 구성할 수 없으며 **Import(가져오기)**도 사용할 수 없습니다.

그림 ***1:*** 수동으로 값 정의

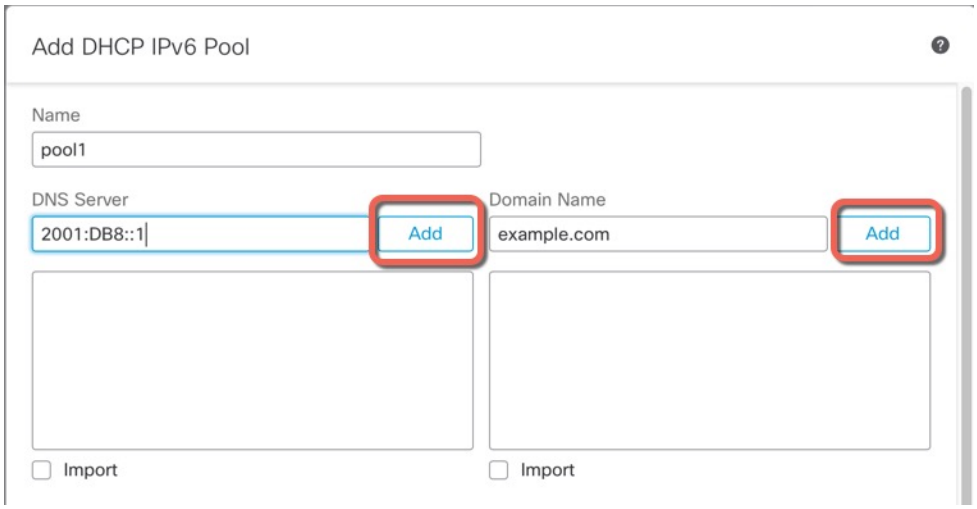
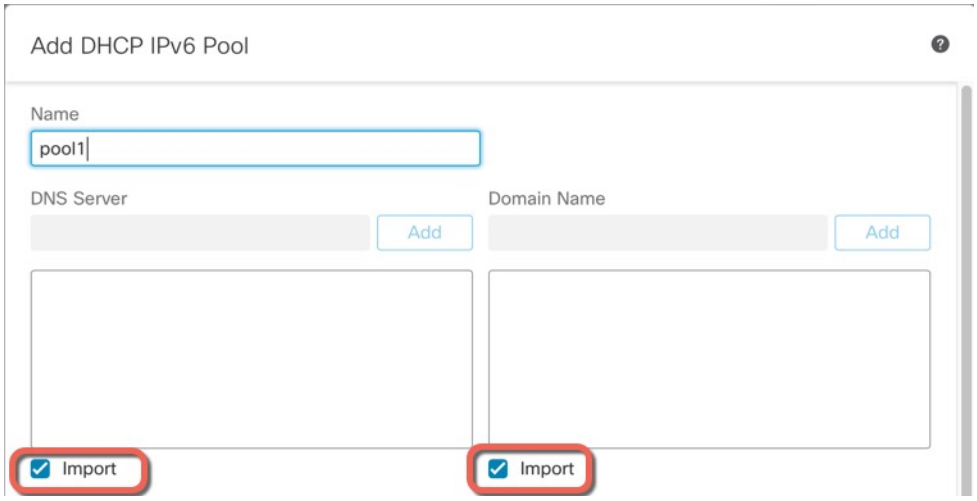


그림 ***2:*** 값 가져오기



단계 **5** 기타 서버 옵션을 정의합니다.

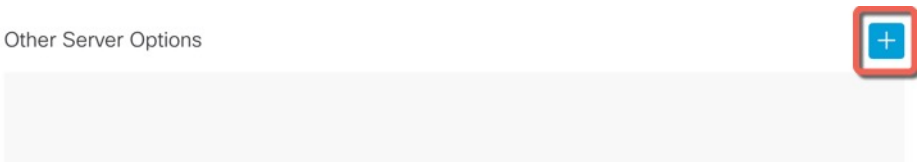
다음 서버에 대해 도메인 이름 및 IP 주소를 정의할 수 있습니다.

- NIS

- NISP
- SIP
- SNTP

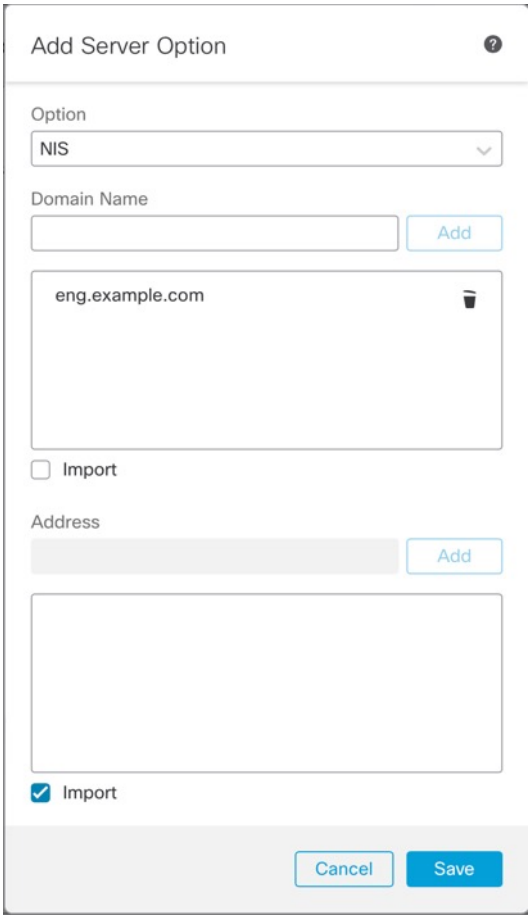
a) **Add(**추가**)** ( ) 버튼을 클릭합니다.

그림 ***3:*** 기타 서버 옵션



b) **Option(**옵션**)** 아래에서 서버 유형을 선택하고 **Domain Name(**도메인 이름**)** 및 **Address(**주소**)**를 수동으로 정의하거나 **Import(**가져오기**)**를 선택합니다.

그림 ***4:*** 서버 도메인 이름 및 주소 정의



Import(가져오기**)**는 threat defense가 접두사 위임 클라이언트 인터페이스의 DHCPv6 서버에서 획득한 한 개 이상의 매개변수를 사용합니다. 수동으로 구성한 매개변수를 가져온 매개변수와 혼합하고 일치시킬 수 있습니다. 그러나 동일한 매개변수를 수동으로 구성할 수 없으며 **Import(**가져오기**)**도 사용할 수 없습니다.

c) **Save(**저장**)**를 클릭합니다.

d) 각 서버 유형에 대해 반복합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 이 풀을 DHCPv6 서버와 함께 사용합니다. DHCPv6 스테이트리스 서버 활성화, 9 페이지의 내용을 참조하십시오.

DHCPv6 스테이트리스 서버 활성화

접두사 위임 기능(IPv6 접두사 위임 클라이언트 활성화)과 함께 SLAAC(StateLess Address Auto Configuration)를 사용하는 클라이언트의 경우, IR(정보 요청) 패킷을 threat defense에 보낼 때 DNS 서버 또는 도메인 이름 같은 정보를 제공하도록 threat defense를 구성할 수 있습니다. threat defense는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 클라이언트에서 IPv6 자동 구성을 활성화하여 자체 IPv6 주소를 생성하도록 클라이언트를 구성합니다. 클라이언트에서 스테이트리스 자동 구성을 사용하도록 설정하면 라우터 광고 메시지에서 수신된 접두사, 즉 threat defense가 접두사 위임을 사용하여 수신한 접두사를 기준으로 IPv6 주소를 구성합니다.

이 기능은 라우팅 모드에서만 지원됩니다. 이 기능은 클러스터링 또는 고가용성에서 지원되지 않습니다.

시작하기 전에

DHCP IPv6 풀 개체를 추가합니다. DHCP IPv6 풀 생성, 6 페이지을 참조하십시오. 이 개체는 IR 메시지에 포함된 서버 매개변수를 정의합니다.

프로시저

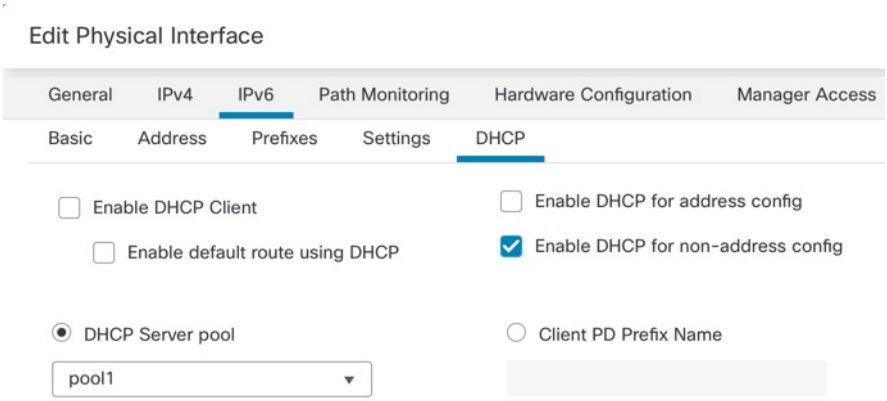
단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **IPv6** 페이지를 클릭한 다음 **DHCP**를 클릭합니다.

단계 **4** **DHCP Server Pool(DHCP** 서버 풀**)**을 클릭하고 이전에 생성한 개체를 선택합니다.

그림 *5: DHCPv6* 서버 활성화



단계 **5** **Enable DHCP for non-address config(**비 주소 구성에 **DHCP** 활성화**)**를 선택하여 SLAAC 클라이언트에 DHCPv6 서버에 대해 알립니다.

이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

DHCP 릴레이 에이전트 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.

브로드캐스트를 수신하는 threat defense 디바이스의 인터페이스를 구성하여 DHCP 요청을 다른 인터페이스의 DHCP 서버에 전달하게 함으로써 이러한 문제를 해결할 수 있습니다.

참고 DHCP 릴레이는 투명 방화벽 모드에서 지원되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **DHCP** > **DHCP** 릴레이를 선택합니다.

단계 **3** **IPv4 Relay Timeout(IPv4** 릴레이 시간 초과**)** 및 **IPv6 Relay Timeout(IPv6** 릴레이 시간 초과**)** 필드에 DHCP 릴레이 에이전트가 시간 초과될 때까지 threat defense 디바이스가 대기하는 시간을 초 단위로 입력합니다. 유효한 값의 범위는 1초 ~ 3600초입니다. 기본값은 60초입니다.

시간 초과는 로컬 DHCP 릴레이 에이전트를 통한 주소 협상에 필요합니다.

단계 **4** (선택 사항) 모든 클라이언트 인터페이스를 신뢰할 수 있는 인터페이스로 설정하려면 **Trust All Information(**모든 정보 신뢰**)**을 선택합니다.

DHCP Option 82를 보존하기 위해 인터페이스를 신뢰받는 인터페이스로 구성할 수 있습니다. DHCP Option 82는 다운스트림 스위치 및 라우터에서 DHCP 스누핑과 IP 소스 가드에 사용합니다. 일반적으로 threat defense DHCP 릴레이 에이전트에서 Option 82가 이미 설정된 DHCP 패킷을 수신하지만 giaddr 필드(서버에 패킷을 전달하기 전에 릴레이 에이전트에 의해 설정되는 DHCP 릴레이 에이전트 주소 지정)가 0으로 설정된 경우 threat defense는 기본적으로 그 패킷을 폐기합니다. 인터페이스를 신뢰받는 인터페이스로 지정하여 Option 82를 보존하고 패킷을 전달할 수 있습니다.

단계 **5** **DHCP Relay Agent(DHCP** 릴레이 에이전트**)**에서 **Add(**추가**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

- 인터페이스 - DHCP 클라이언트에 연결된 인터페이스입니다.
- **IPv4** 릴레이 활성화 - 이 인터페이스에서 IPv4 DHCP 릴레이를 활성화합니다.
- 경로 설정 - (IPv4의 경우) 서버에서 전송한 DHCP 메시지 내의 기본 게이트웨이 주소를 초기 DHCP 요청을 릴레이한 DHCP 클라이언트와 가장 가까운 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 threat defense 디바이스는 인터페이스 주소를 포함하는 것을 추가합니다.
- **IPv6** 릴레이 활성화 - 이 인터페이스에서 IPv6 DHCP 릴레이를 활성화합니다.

단계 **6** DHCP 릴레이 에이전트 변경 사항을 저장하려면 **OK**를 클릭합니다.

단계 **7** **DHCP Servers(DHCP** 서버**)**에서 **Add(**추가**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

동일한 서버에 속해 있는 경우에도 IPv4 및 IPv6 서버 주소를 개별 항목으로 추가합니다.

- 서버 - DHCP 서버의 IP 주소입니다. 드롭다운 목록에서 IP 주소를 선택합니다. 새로 추가하려는 경우 네트워크 개체 생성를 참조하십시오.
- 인터페이스 - 드롭다운 목록에서 지정된 DHCP 서버가 연결된 인터페이스입니다. DHCP 릴레이 에이전트 및 DHCP 서버는 동일한 인터페이스에 구성될 수 없습니다.

단계 **8** DHCP 서버 변경 사항을 저장하려면 **OK**를 클릭합니다.

단계 **9** 변경 사항을 저장하려면 DHCP 페이지에서 저장을 클릭합니다.

동적 DNS 구성

인터페이스에서 DHCP IP 주소 지정을 사용하는 경우, DHCP 리스가 갱신될 때 할당된 IP 주소가 변경될 수 있습니다. FQDN(Fully Qualified Domain Name)을 사용하여 인터페이스에 연결해야 하는 경우, IP 주소를 변경하면 DNS 서버 리소스 레코드(RR)가 오래 될 수 있습니다. DDNS(Dynamic DNS)는 IP 주소 또는 호스트네임이 변경될 때마다 DNS RR을 업데이트하는 메커니즘을 제공합니다. 고정 또는 PPPoE IP 주소 지정에 DDNS를 사용할 수도 있습니다.

DDNS는 DNS 서버에서 다음 RR을 업데이트합니다. A RR은 이름-IP 주소 매핑을 포함하고 PTR RR은 주소를 이름에 매핑합니다.

threat defense는 다음 DDNS 업데이트 방법을 지원합니다.

- 표준 DDNS - 표준 DDNS 업데이트 방법은 RFC 2136에 의해 정의됩니다.

  이 방법을 사용하는 경우, threat defense 및 DHCP 서버는 DNS 요청을 사용하여 DNS RR을 업데이트합니다. threat defense 또는 DHCP 서버는 호스트 이름에 대한 정보를 얻기 위해 DNS 요청을 로컬 DNS 서버로 전송하고, 응답에 따라 RR을 소유한 기본 DNS 서버를 결정합니다. 그런 다음 threat defense 또는 DHCP 서버는 기본 DNS 서버로 직접 업데이트 요청을 보냅니다. 다음과 같은 일반적인 시나리오를 참조하십시오.

  - threat defense가 A RR을 업데이트하고, DHCP 서버가 PTR RR을 업데이트합니다.

    일반적으로 threat defense는 A RR을 "소유"하고 DHCP 서버는 PTR RR을 "소유"하므로 두 엔티티 모두 업데이트를 별도로 요청해야 합니다. IP 주소 또는 호스트 이름이 변경되면 threat defense는 DHCP 요청(FQDN 옵션 포함)을 DHCP 서버에 전송하여 PTR RR 업데이트를 요청해야 함을 알립니다.

  - DHCP 서버가 A RR과 PTR RR을 모두 업데이트합니다.

    threat defense에 A RR을 업데이트 할 권한이 없는 경우, 이 시나리오를 사용합니다. IP 주소 또는 호스트 이름이 변경되면 threat defense는 DHCP 요청(FQDN 옵션 포함)을 DHCP 서버에 전송하여 A RR 및 PTR RR 업데이트를 요청해야 함을 알립니다.

  보안 요구 사항과 기본 DNS 서버의 요구 사항에 따라 다른 소유권을 설정할 수 있습니다. 예를 들어 고정 주소의 경우, threat defense는 두 레코드의 업데이트를 모두 소유해야 합니다.

- 웹 - 웹 업데이트 방법은 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 활용합니다.

  이 방법을 사용하면 IP 주소 또는 호스트 이름이 변경될 때 threat defense에서 계정이 있는 DNS 제공자에게 직접 HTTP 요청을 보냅니다.

참고 외부 인터페이스에서 로우 터치(low-touch) 프로비저닝을 사용하여 등록된 디바이스의 경우 DDNS가 웹 방법과 유사한 "fmcOnly" 방법을 사용하여 자동으로 활성화됩니다. 이 방법은 로우 터치 프로비저닝 디바이스에만 사용할 수 있습니다. 이 화면에서 이 방법에 대한 일부 옵션을 편집하거나, 이 방법을 삭제하고 다른 옵션을 구성할 수 있습니다. 로우 터치 프로비저닝에 대한 자세한 내용은 일련 번호(로우 터치 프로비저닝)를 사용하여 Management Center에 디바이스 추가 항목을 참고하십시오.

DDNS 페이지는 DDNS와 관련된 DHCP 서버 설정도 지원합니다.

참고 DDNS는 브리지 그룹 멤버 인터페이스 또는 BVI에서 지원되지 않습니다.

시작하기 전에

- **Objects(**개체**)** > **Object Management(**개체 관리**)** > **DNS Server Group(DNS** 서버 그룹**)**에서 DNS 서버 그룹을 설정한 다음 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS**에서 인터페이스에 대해 그룹을 활성화합니다. DNS의 내용을 참조하십시오.
- 디바이스 호스트네임을 설정합니다. threat defense 초기 설정을 수행할 때 또는 **configure network hostname** 명령을 사용하여 호스트 이름을 구성할 수 있습니다. 인터페이스당 호스트네임을 지정하지 않으면 디바이스 호스트네임이 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **DHCP** > **DDNS**를 선택합니다.

단계 **3** 표준 DDNS 방법: threat defense에서 DNS 요청을 활성화하도록 DDNS 업데이트 방법을 구성합니다.

DHCP 서버가 모든 요청을 수행할 경우, DDNS 업데이트 방법을 설정할 필요가 없습니다.

a) **DDNS Update Methods(DDNS** 업데이트 방법**)**에서 **Add(**추가**)**를 클릭합니다.
b) 방법 이름을 설정합니다.
c) **DDNS**를 클릭합니다.
d) (선택 사항) DNS 요청 간 업데이트 간격을 설정합니다. 기본적으로 모든 값이 0으로 설정된 경우, IP 주소 또는 호스트네임이 변경될 때마다 업데이트 요청이 전송됩니다. 요청을 정기적으로 보내려면 일(0~364), 시간, 분 및 초를 설정합니다.
e) threat defense에서 업데이트할 **Update Records(**업데이트 레코드**)**를 설정합니다.

이 설정은 threat defense에서 직접 업데이트하려는 레코드에만 적용됩니다. DHCP 서버가 업데이트할 레코드를 결정하려면 인터페이스당 또는 전역적으로 DHCP 클라이언트 설정을 구성합니다. 참고, 단계 5, 14 페이지.

- **Not Defined(**정의되지 않음**)** - threat defense에서 DNS 업데이트를 비활성화합니다.

- **Both A and PTR Records(A** 및 **PTR** 레코드 모두**)** - A RR 및 PTR RR을 모두 업데이트하도록 threat defense를 설정합니다. 고정 또는 PPPoE IP 주소 지정에 이 옵션을 사용합니다.
- **A Records(A** 레코드**)** - A RR만 업데이트하도록 threat defense를 설정합니다. DHCP 서버가 PTR RR을 업데이트하도록 하려면 이 옵션을 사용합니다.

f) **OK(**확인**)**를 클릭합니다.

g) 이 방법을 단계 5, 14 페이지의 인터페이스에 할당합니다.

단계 **4** 웹 방법: threat defense에서 HTTP 업데이트 요청을 활성화하도록 DDNS 업데이트 방법을 구성합니다.

a) **DDNS Update Methods(DDNS** 업데이트 방법**)**에서 **Add(**추가**)**를 클릭합니다.

b) 방법 이름을 설정합니다.

c) **Web(**웹**)**을 클릭합니다.

d) IPv4, IPv6 또는 두 주소 유형을 모두 업데이트하도록 웹 업데이트 유형을 설정합니다.

e) 웹 **URL**을 설정합니다. 업데이트 URL을 지정합니다. 필요한 URL은 DNS 제공자에 확인하십시오.

다음 구문을 사용합니다.

https://*username***:***password***@***provider-domain/path***?hostname=<h>&myip=<a>**

예제**:**

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) (선택 사항) DNS 요청 간 업데이트 간격을 설정합니다. 기본적으로 모든 값이 0으로 설정된 경우, IP 주소 또는 호스트네임이 변경될 때마다 업데이트 요청이 전송됩니다. 요청을 정기적으로 보내려면 일(0~364), 시간, 분 및 초를 설정합니다.

g) **OK(**확인**)**를 클릭합니다.

h) 이 방법을 단계 5, 14 페이지의 인터페이스에 할당합니다.

i) DDNS용 웹 유형 방법에서는 또한 DDNS 서버 루트 CA를 식별하여 HTTPS 연결을 위해 DDNS 서버 인증서를 검증해야 합니다. 참고, 단계 9, 16 페이지.

단계 **5** 업데이트 방법 설정, DHCP 클라이언트 설정, 해당 인터페이스의 호스트네임 등 DDNS에 대한 인터페이스 설정을 구성합니다.

a) **DDNS Interface Settings(DDNS** 인터페이스 설정**)**에서 **Add(**추가**)**를 클릭합니다.

b) 드롭다운 목록에서 **Interface(**인터페이스**)**를 선택합니다.

c) **DDNS Update Methods(DDNS** 업데이트 방법**)** 페이지에서 생성한 방법 이름을 선택합니다.

(표준 DDNS 방법) DHCP 서버가 모든 업데이트를 수행하도록 하려면 방법을 할당할 필요가 없습니다.

d) 이 인터페이스의 호스트네임을 설정합니다.

호스트네임을 설정하지 않으면 디바이스 호스트네임이 사용됩니다. FQDN을 지정하지 않으면 DNS 서버 그룹의 기본 도메인이 추가되거나(고정 또는 PPPoE IP 주소 지정) DHCP 서버의 도메인 이름이 추가됩니다(DHCP IP 주소 지정용).

e) 표준 DDNS 방법: DHCP 서버가 업데이트할 레코드를 결정하기 위해 **DHCP Client requests DHCP server to update requests(**요청을 업데이트하도록 **DHCP** 클라이언트 요청 **DHCP** 서버**)**를 설정합니다.

threat defense는 DHCP 서버에 DHCP 클라이언트 요청을 전송합니다. DDNS를 지원하도록 DHCP 서버도 설정해야 합니다. 클라이언트 요청을 준수하도록 서버를 설정하거나 클라이언트를 재정의할 수 있습니다(이 경우, 클라이언트가 서버에 수행 중인 업데이트를 수행하지 않도록 클라이언트에 응답함).

고정 또는 PPPoE IP 주소 지정의 경우, 이러한 설정은 무시됩니다.

참고 **DDNS** 페이지의 모든 인터페이스에 대해 이러한 값을 전역적으로 설정할 수도 있습니다. 인터페이스별 설정이 전역 설정보다 우선합니다.

- **Not Selected(**선택하지 않음**)** - DHCP 서버에 대한 DDNS 요청을 비활성화합니다. 클라이언트가 DDNS 업데이트를 요청하지 않더라도 DHCP 서버가 업데이트를 보내도록 설정할 수 있습니다.
- **No Update(**업데이트 없음**)** - 업데이트를 수행하지 않도록 DHCP 서버에 요청합니다. 이 설정은 **A** 및 **PTR** 레코드 모두가 활성화된 DDNS 업데이트 방법과 함께 작동합니다.
- **Only PTR(PTR** 만**)** - DHCP 서버가 PTR RR 업데이트를 수행하도록 요청합니다. 이 설정은 **A** 레코드가 활성화된 DDNS 업데이트 방법과 함께 작동합니다.
- **Both A and PTR Records(A** 및 **PTR** 레코드 모두**)** - DHCP 서버가 A 및 PTR RR 업데이트를 모두 수행하도록 요청합니다. 이 설정에서는 DDNS 업데이트 방법을 인터페이스와 연결할 필요가 없습니다.

f) **OK(**확인**)**를 클릭합니다.

참고 **Dynamic DNS Update(**동적 **DNS** 업데이트**)** 설정은 threat defense에서 DHCP 서버를 활성화할 때 DHCP 서버 설정과 관련이 있습니다. 자세한 내용은 단계 6, 15 페이지를 참조하십시오.

단계 **6** threat defense에서 DHCP 서버를 활성화하는 경우, DDNS에 대한 DHCP 서버 설정을 구성할 수 있습니다.

DHCP 서버를 활성화하려면 DHCPv4 서버 구성, 4 페이지의 내용을 참조하십시오. DHCP 클라이언트가 표준 DDNS 업데이트 방법을 사용할 때 서버 동작을 설정할 수 있습니다. 서버가 업데이트를 수행하는 경우, 클라이언트 리스가 만료되고 갱신되지 않으면 서버는 DNS 서버가 담당했던 RR을 제거하도록 요청합니다.

a) 전역적으로 또는 인터페이스별로 서버 설정을 구성할 수 있습니다. 전역 설정은 기본 **DDNS** 페이지를 참조하십시오. 인터페이스별 설정은 **DDNS Interface Settings(DDNS** 인터페이스 설정**)** 페이지를 참조하십시오. 인터페이스 설정이 전역 설정보다 우선합니다.

b) DHCP 서버가 **Dynamic DNS Update(**동적 **DNS** 업데이트**)**에서 업데이트할 DNS RR을 설정합니다.

- **Not Selected(**선택하지 않음**)** - 클라이언트가 요청하는 경우에도 DDNS 업데이트가 비활성화됩니다.

- **Only PTR(PTR만)** - DDNS 업데이트를 활성화합니다. **Override DHCP Client Requests(DHCP 클라이언트 요청 재정의)** 설정을 활성화하면 서버가 PTR RR만 업데이트합니다. 활성화하지 않으면 서버는 클라이언트가 요청하는 RR을 업데이트합니다. 클라이언트가 FQDN 옵션과 함께 업데이트 요청을 보내지 않으면 서버는 DHCP 옵션 12에서 검색된 호스트네임을 사용하여 A 및 PTR RR 모두에 대한 업데이트를 요청합니다.
- **Both A and PTR Records(A 및 PTR 레코드 모두)** - DDNS 업데이트를 활성화합니다. **Override DHCP Client Requests(DHCP 클라이언트 요청 재정의)** 설정을 활성화하면 서버가 A 및 PTR RR을 모두 업데이트합니다. 활성화하지 않으면 서버는 클라이언트가 요청하는 RR을 업데이트합니다. 클라이언트가 FQDN 옵션과 함께 업데이트 요청을 보내지 않으면 서버는 DHCP 옵션 12에서 검색된 호스트네임을 사용하여 A 및 PTR RR 모두에 대한 업데이트를 요청합니다.

c) DHCP 클라이언트에서 요청한 업데이트 작업을 재정의하려면 **Override DHCP Client Requests(DHCP 클라이언트 요청 재정의)**를 선택합니다.

서버는 요청이 재정의되었다고 클라이언트에 응답하므로, 클라이언트는 서버가 수행 중인 업데이트도 수행하지 않습니다.

단계 **7** (선택 사항) 일반 DHCP 클라이언트 설정을 구성합니다. 이러한 설정은 DDNS와 관련이 없지만, DHCP 클라이언트의 동작 방식과 관련이 있습니다.

a) **DDNS** 페이지에서 **Enable DHCP Client Broadcast(DHCP 클라이언트 브로드캐스트 활성화)**를 선택하여 DHCP 서버가 DHCP 응답을 브로드캐스트하도록 요청합니다(DHCP 옵션 1).

b) **DDNS** > **DHCP Client ID Interface(DHCP 클라이언트 ID 인터페이스)**에서 MAC 주소가 내부에서 생성된 기본 문자열 대신 옵션 61에 대한 DHCP 요청 패킷 내부에 저장되도록 하려면 **Available Interfaces(사용 가능한 인터페이스)** 목록에서 인터페이스를 선택한 다음 **Add(추가)**를 클릭하여 **Selected Interfaces(선택한 인터페이스)** 목록으로 이동합니다.

일부 ISP의 경우 옵션 61이 인터페이스 MAC 주소가 됩니다. MAC 주소가 DHCP 요청 패킷에 포함되지 않은 경우 IP 주소는 지정되지 않습니다. 이 설정은 DDNS와 직접 관련이 없지만, 일반적인 DHCP 클라이언트 설정입니다.

단계 **8** 변경 사항을 저장하려면 Device(디바이스) 페이지에서 **Save(저장)**를 클릭합니다.

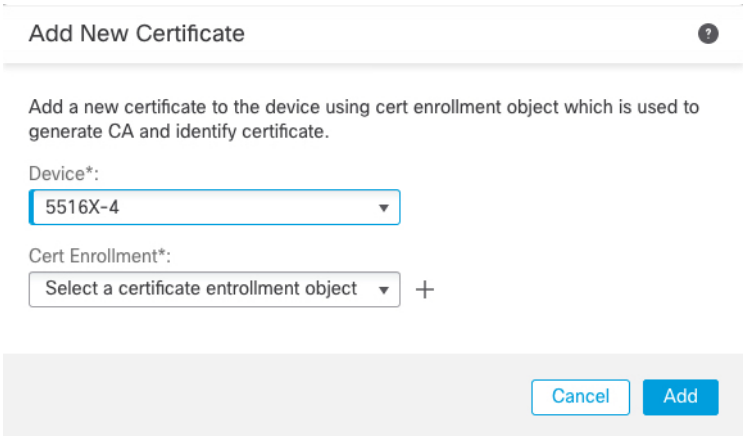
단계 **9** DDNS용 웹 방법에서는 또한 DDNS 서버 루트 CA를 식별하여 HTTPS 연결을 위한 DDNS 서버 인증서를 검증해야 합니다.

다음 예에서는 DDNS 서버의 CA를 신뢰 지점으로 추가하는 방법을 보여줍니다.

a) DDNS 서버 CA 인증서를 가져옵니다. 이 절차에서는 PEM 형식을 사용하는 수동 가져오기를 보여주지만, PKCS12를 사용할 수도 있습니다.

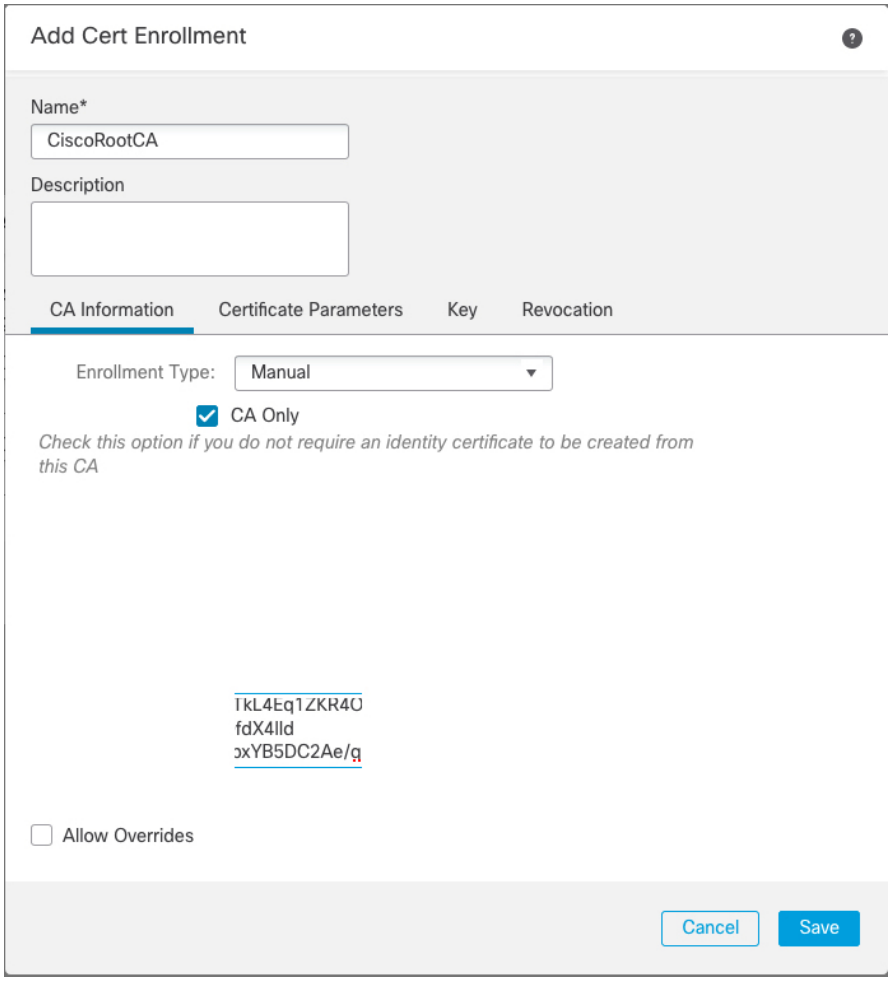
b) management center에서 **Devices(디바이스)** > **Certificates(인증서)**를 선택하고 **Add(추가)**를 클릭합니다.

c) **Device(디바이스)**를 선택하고 **Add(추가)** (+)을(를) 클릭합니다.



Add Cert Enrollment(인증서 등록 추가**)** 대화 상자가 나타납니다.

d) 다음 필드에 입력하고 **Save(**저장**)**를 클릭합니다.



- **Name(**이름**)**을 입력합니다.

- **Enrollment Type(**등록 유형**)** > **Manual(**수동**)**을 선택합니다.
- **CA Only(CA** 전용**)**를 클릭합니다.
- 9.a, 16 페이지단계의 CA 텍스트에 붙여 넣습니다.

e) **Save(**저장**)**를 클릭합니다.

DHCP 및 DDNS 기록

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
Management Center 웹 인터페이스에서 DHCP 릴레이 신뢰 인터페이스를 구성합니다.	7.4.1	Any(모든)	업그레이드 영향**.** 업그레이드 후 관련 **FlexConfig**를 다시 실행합니다**.** 이제 Management Center 웹 인터페이스를 통해 인터페이스를 신뢰할 수 있는 인터페이스로 구성하여 DHCP 옵션 82를 유지할 수 있습니다. 이렇게 하면 기존 FlexConfig를 제거해야 하지만, 이러한 설정은 모든 FlexConfig를 재정의합니다. DHCP Option 82는 다운스트림 스위치 및 라우터에서 DHCP 스누핑과 IP 소스 가드에 사용합니다. 일반적으로 Threat Defense DHCP 릴레이 에이전트에서 Option 82가 이미 설정된 DHCP 패킷을 수신하지만, giaddr 필드(서버에 패킷을 전달하기 전에 릴레이 에이전트에 의해 설정되는 DHCP 릴레이 에이전트 주소 지정)가 0으로 설정된 경우 Threat Defense는 기본적으로 해당 패킷을 폐기합니다. 인터페이스를 신뢰받는 인터페이스로 지정하여 Option 82를 보존하고 패킷을 전달할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add/Edit Device(**디바이스 추가/편집**)** > **DHCP** > **DHCP Relay(DHCP** 릴레이**)**

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
DHCPv6 스테이트리스 서버	7.3.0	7.3.0	이제 threat defense는 DHCPv6 접두사 위임 클라이언트를 사용할 때 경량 DHCPv6 스테이트리스 서버를 지원합니다. threat defense는 SLAAC 클라이언트가 threat defense에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 도메인 이름 등의 기타 정보를 제공합니다. threat defense는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Add/Edit Interfaces(**인터페이스 추가/편집**)** > **IPv6** > **DHCP** • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **DHCP IPv6 Pool(DHCP IPv6** 풀**)** 신규/수정된 명령: **show ipv6 dhcp**