Security Cloud Control에서 가상 프라이빗 네트워크 관리

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 섹션은 FDM 매니지드 디바이스의 원격 액세스 및 사이트 간 VPN에 적용됩니다. FTD에서 사이트 간 VPN 연결을 구축하기 위한 IPsec(Internet Protocol Security) 표준에 대해 설명합니다. 또한 FTD에서 VPN 연결을 구축하고 원격 액세스하는 데 사용되는 SSL 표준에 대해서도 설명합니다.

Security Cloud Control에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

사이트 간 가상 프라이빗 네트워크 소개

사이트간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 관리형 디바이스 및 관리형 디바이스와 모든 관련 표준을 준수하는 다른 Cisco 또는 타사 피어 간에 Site-to-Site IPsec 연결을 만들 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다 . Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

Security Cloud Control로 사이트 간 VPN 간소화

사이트 간 VPN은 인터넷을 통해 여러 네트워크를 안전하게 연결하는 신뢰할 수 있는 솔루션입니다. 이 프로세스를 더 쉽고 효율적으로 만들기 위해, Security Cloud Control는 통합된 사이트 간 **VPN** 마법사를 제공합니다. 이 직관적인 도구는 기존 VPN 구성의 복잡성을 줄이면서 안전한 VPN 터널의 생성 및 관리를 간소화하도록 설계되었습니다.

사이트 간 VPN 마법사는 다양한 관리 대상 디바이스 간에 VPN 터널을 구성하기 위한 단일 통합 인터페이스를 제공합니다. 이러한 일관성은 특정 디바이스나 네트워크 환경에 관계없이 관리자에게 간소화된 경험을 보장합니다. 위저드는 중앙 집중식이며 직관적인 구성 프로세스를 제공함으로써

조직이 운영 효율성을 높이고 오류를 줄이며 네트워크 인프라에서 높은 수준의 보안을 유지할 수 있도록 지원합니다.

아래 표는 관리 대상 디바이스에 허용되는 사이트 간 VPN 구성을 명시합니다.

	FDM 관리	클라우드 제공 **Firewall Management Center** 매니지드 **Firewall Threat Defense**	**Secure Firewall ASA**	**Multicloud Defense**
FDM 관리	예	아니요	아니요	아니요
클라우드 제공 **Firewall Management Center** 매니지드 **Firewall Threat Defense**	아니요	예	예	예
Secure Firewall ASA	아니요	예	예	예
Multicloud Defense	아니요	예	예	아니요

사이트 간 VPN 개념

VPN 토폴로지

새로운 사이트 간 VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다 및 인증 방법을 선택해야 합니다. 구성된 후 토폴로지를 FTD에 구축합니다.

IPsec 및 IKE 프로토콜

Security Cloud Control에서 사이트 간 VPN은 IKE 정책과 VPN 토폴로지에 할당된 IPsec 제안을 기반으로 구성됩니다. 정책 및 제안은 IPsec 터널에서 트래픽을 보호하는 데 사용되는 보안 프로토콜 및 알고리즘과 같은 사이트 간 VPN의 특성을 정의하는 파라미터 집합입니다. VPN 토폴로지에 할당할 수 있는 전체 구성 이미지를 정의하려면 몇 가지 정책 유형이 필요할 수 있습니다.

인증 VPN 터널

VPN 연결을 인증하려면 각 디바이스의 토폴로지에서 사전 공유 키를 구성합니다. 사전 공유 키를 사용하면 IKE 인증 단계에서 사용되는 보안 키를 두 피어 간에 공유할 수 있습니다.

Virtual Tunnel Interface(VTI)

Security Cloud Control는 현재 FTD에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 Security Cloud Control에 온보딩될 수 있지만

VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 Security Cloud Control는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다.

VPN 암호화 도메인

VPN의 암호화 도메인은 경로 기반 또는 정책 기반 트래픽 선택기라는 두 가지 방법으로 정의할 수 있습니다.

- 정책 기반: 암호화 도메인은 IPSec 터널에 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPSec 로컬 및 원격 트래픽 선택기는 0.0.0.0으로 설정됩니다. 즉, IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다. ASA는 암호화 맵을 사용하는 정책 기반 VPN을 지원합니다.
- 경로 기반: 암호화 도메인은 소스와 대상 모두에 대해 특정 IP 범위만 암호화하도록 설정됩니다. 이는 가상 IPsec 인터페이스를 생성하며, 해당 인터페이스에 들어오는 모든 트래픽은 암호화 및 암호 해독됩니다. ASA는 VTI(Virtual Tunnel Interface)를 사용하여 경로 기반 VPN을 지원합니다.

외부 디바이스 정보

비 시스코 또는 관리되지 않는 시스코 디바이스를 정적 또는 동적 IP 주소를 가진 "엑스트라넷" 디바이스로 VPN 토폴로지에 추가할 수 있습니다.

- 비 시스코 디바이스: Security Cloud Control을 사용하여 비 시스코 디바이스에 구성을 생성하거나 구축할 수 없습니다.
- 관리되지 않는 시스코 디바이스: 회사 내 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공업체 또는 파트너 네트워크에 대한 연결과 같이 조직에서 관리하지 않는 시스코 디바이스입니다.

전역 **IKE** 정책 정보

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 구축하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 Edit(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- IKEv1 정책 구성
- IKEv2 정책 구성

IKEv1 정책 관리

IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 구축하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics

IKEv1 정책 생성, 4 페이지

IKEv1 정책 생성

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 구축하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(**새 **IKE** 정책 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스  버튼을 클릭하고 **FDM** > **IKEv1 Policy(IKEv1** 정책**)**를 선택하여 새 IKEv1 정책을 생성합니다.

- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.

단계 **3** 개체 이름을 최대 128자로 입력합니다.

단계 **4** IKEv1 속성을 구성합니다.

- **Priority(우선순위)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(라이프타임)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication(인증)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 사용할 인증 방법 결정을 참조하십시오.
  - **Preshared Key(사전 공유 키)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
  - **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **5** **Add(추가)**를 클릭합니다.

IKEv2 정책 관리

IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 구축하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics

IKEv2 정책 생성, 6 페이지

IKEv2 정책 생성

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 구축하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy(**새 **IKEv2** 정책 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스  버튼을 클릭하고 **FTD** > **IKEv2 Policy(IKEv2** 정책**)**를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv2 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 개체 이름을 최대 128자로 입력합니다.

단계 **4** IKEv2 속성을 구성합니다.

- **Priority(**우선순위**)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec

피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.

- **State(**상태**)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman** 그룹**)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Integrity Hash(**무결성 해시**)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.
- **PRF(Pseudo-Random Function)** 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.
- **Lifetime(**라이프타임**)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

IPsec 제안 정보

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터

널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- IKEv1 IPsec 제안 개체 생성 및 편집
- IKEv2 IPsec 제안 개체 생성 및 편집

IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 Security Cloud Control는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

Related Topics

IKEv1 IPsec 제안 개체 생성, 8 페이지

IKEv1 IPsec 제안 개체 생성

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 Security Cloud Control는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal(**새 **IKEv1** 제안 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM** > **IKEv1 IPsec Proposal(IKEv1 IPsec** 제안**)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 새 개체의 개체 이름을 입력합니다.

단계 **4** IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPSec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPSec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 **5** 이 제안에 대한 **ESP Encryption(ESP** 암호화**)**(Encapsulating Security Protocol) 알고리즘을 선택합니다. 자세한 내용은 사용할 암호화 알고리즘 결정을 참조하십시오.

단계 **6** 인증에 사용할 **ESP Hash(ESP** 해시**)** 또는 무결성 알고리즘을 선택합니다. 자세한 내용은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **7** **Add(**추가**)**를 클릭합니다.

IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

Related Topics

IKEv2 IPsec 제안 개체 생성 또는 편집, 10 페이지

IKEv2 IPsec 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 Create New IPsec Proposal(새 IPsec 제안 생성) 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM** > **IKEv2 IPsec Proposal(IKEv2 IPsec** 제안**)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 새 개체의 개체 이름을 입력합니다.

단계 **4** IKE2 IPsec 제안 개체 구성:

- **Encryption(**암호화**)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Integrity Hash(**무결성 해시**)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **5** **Add(**추가**)**를 클릭합니다.

VPN에서 사용되는 암호화 및 해시 알고리즘

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPsec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

- AES-GCM - (IKEv2에만 해당됨) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다.
- AES-GMAC - (IKEv2 IPsec 제안에만 해당됨) AES-GMAC(Advanced Encryption Standard Galois Message Authentication Code)는 데이터 원본 인증 기능만 제공하는 블록 암호화 작동 모드입니다. 이 모드는 데이터를 암호화하지 않고 데이터 인증을 허용하는 AES-GCM의 변형입니다. AES-GMAC는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다.
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.
- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 라이선스 어카운트가 내보내기 제어에 대한 요건을 충족하지 않는 경우에는 이 옵션이 유일한 옵션입니다. 3DES보다 속도가 빠르며 시스템 리소스를 더 적게 사용하지

만 보안성은 더 낮습니다. 강력한 데이터 기밀 유지 기능이 필요하지 않으며 시스템 리소스나 속도가 중요한 경우에는 DES를 선택하십시오.

- 3DES - 56비트 키를 사용하여 암호화를 3회 수행하는 3DES(Triple DES)는 서로 다른 키를 사용하여 각 데이터 블록을 3회 처리하므로 DES보다 안전합니다. 그러나 시스템 리소스를 더 많이 사용하며 DES보다 속도가 느립니다.
- NULL - null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이 알고리즘은 대개 테스트용으로만 사용됩니다.

사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 표준 SHA(SHA-1)에서는 160비트 다이제스트를 생성합니다. SHA는 MD5보다 무차별 암호 대입 공격에 대한 방어력이 뛰어납니다. 그러나 MD5 보다 리소스를 더 많이 사용 합니다. 최고 보안 레벨이 필요한 구현의 경우 SHA 해시 알고리즘을 사용합니다.
- IKEv2 구성에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.
  - SHA-256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
- MD5(Message Digest 5) - 128비트 다이제스트를 생성합니다. MD5는 SHA보다 전반적으로 성능이 우수하여 처리 시간이 짧지만 SHA보다 취약한 것으로 간주됩니다.
- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 AES-GCM/GMAC 옵션 중 하나를 암호화 알고리즘으로 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

사용할 **Diffie-Hellman** 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책에서는 아래에 나열된 그룹을 모두 지원하지는 않습니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 2 - Diffie-Hellman 그룹 2: 1024비트 MODP(모듈식 지수) 그룹. 이 옵션은 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 5 - Diffie-Hellman 그룹 5: 1536비트 MODP 그룹. 전에는 이 옵션이 128비트 키에 대해 좋은 보호 방법으로 간주되었지만 이제는 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 19 - Diffie-Hellman 그룹 19: NIST(국내 표준 및 기술) 256비트 ECP(elliptic curve modulo a prime) 그룹
- 20 - Diffie-Hellman 그룹 20: NIST 384비트 ECP 그룹
- 21 - Diffie-Hellman 그룹 21: NIST 521비트 ECP 그룹
- 24 - Diffie-Hellman 그룹 24: 2048비트 MODP 그룹 및 256비트 소수 위수 하위 그룹. 이 옵션은 더 이상 권장되지 않습니다.

사용할 인증 방법 결정

다음과 같은 방법을 사용하여 Site-to-Site VPN 연결에서 피어를 인증할 수 있습니다.

사전 공유 키

사전 공유 키는 연결에서 각 피어에 구성된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다. IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 구성해야 합니다. IKEv2의 경우, 각 피어에 고유 키를 구성할 수 있습니다.

사전 공유 키는 인증서에 비해 확장성이 떨어집니다. 다수의 사이트 간 VPN 연결을 구성해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

FDM-관리에 대한 사이트 간 VPN 구성

Security Cloud Control는 FDM 관리 디바이스에서 사이트 간 VPN 기능의 다음 측면을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 사이트 간 VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.
- 엔드포인트로 작동하는 엑스트라넷 디바이스의 동적 IP 주소 지원.

동적 주소 지정 피어로 사이트 간 VPN 연결 구성

Security Cloud Control를 사용하면 피어의 VPN 인터페이스 IP 주소 중 하나를 알 수 없거나 인터페이스가 DHCP 서버에서 주소를 가져올 때 피어 간에 사이트 간 VPN 연결을 생성할 수 있습니다. 사전 공유 키, IKE 설정 및 IPsec 구성이 다른 피어와 일치하는 모든 동적 피어는 사이트 간 VPN 연결을 설정할 수 있습니다.

피어 A와 B를 고려하십시오. 고정 피어는 VPN 인터페이스의 IP 주소가 고정되어 있는 디바이스이고 동적 피어는 VPN 인터페이스의 IP 주소를 알 수 없거나 임시 IP 주소가 있는 디바이스입니다.

다음 사용 사례에서는 동적으로 주소가 지정된 피어를 사용하여 안전한 사이트 간 VPN 연결을 설정하는 다양한 시나리오를 설명합니다.

- A는 정적 피어이고 B는 동적 피어이거나 그 반대입니다.
- A는 고정 피어이고 B는 DHCP 서버에서 확인된 IP 주소를 사용하거나 그 반대로 하는 동적 피어입니다. **Bind VPN to the assigned IP(**할당된 **IP**에 **VPN** 바인딩**)**를 선택하여 고정 피어의 IP 주소와 동적 피어의 DHCP 할당 IP 주소 간에 VPN 연결을 설정할 수 있습니다.
- A 및 B는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 주소입니다. 이 경우 고정 피어의 IP 주소와 동적 피어의 DHCP 할당 IP 주소 간에 VPN 연결을 설정하려면 하나 이상의 피어에 대해 **Bind VPN to the assigned IP(**할당된 **IP**에 **VPN** 바인딩**)**을 선택해야 합니다.
- A는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.
- A는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다. **Bind VPN to the assigned IP(**할당된 **IP**에 **VPN** 바인딩**)**를 선택하여 고정 피어의 IP 주소와 동적 피어의 DHCP 할당 IP 주소 간에 VPN 연결을 설정할 수 있습니다.

Important **Bind VPN to the assigned IP(**할당된 **IP**에 **VPN** 바인딩**)**를 선택하면 VPN이 DHCP 할당 IP 주소에 고정으로 바인딩합니다. 그러나 이 동적 인터페이스는 피어가 재시작된 후 여러 개의 새 IP 주소를 수신할 수 있습니다. VPN 터널이 새 IP 주소를 업데이트하더라도 다른 피어는 새 구성으로 업데이트되지 않습니다. 다른 피어에서 대역 외 변경 사항을 적용하려면 사이트 간 구성을 다시 구축해야 합니다.

Note Firewall Device Manager과 같은 로컬 관리자를 사용하여 인터페이스의 IP 주소를 변경하면 Security Cloud Control에서 해당 피어의 **Configuration Status(**구성 상태**)**가 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. 이 대역 외 변경 사항을 해결하면 다른 피어의 **Configuration Status(**구성 상태**)**가 "Not Synced(동기화되지 않음)" 상태로 변경됩니다. "Not Synced(동기화되지 않음)" 상태인 디바이스에 Security Cloud Control 구성을 구축해야 합니다.

일반적으로 동적 피어는 연결을 시작하는 피어여야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.

Note 다음 시나리오에서는 사이트 간 VPN 연결을 구성할 수 없습니다.

- 두 피어 모두에 DHCP 할당 IP 주소가 있는 경우
  - 해결 방법: 피어 중 하나에 DHCP 서버에서 확인된 IP 주소가 있는 경우 사이트 간 VPN을 구성할 수 있습니다. 이 경우 **Bind VPN to the assigned IP(**할당된 **IP**에 **VPN** 바인딩**)**을 선택하여 사이트 간 VPN을 구성해야 합니다.
- 디바이스에 둘 이상의 동적 피어 연결이 있는 경우
  - 해결 방법: 다음 단계를 수행하여 사이트 간 VPN을 구성할 수 있습니다.
    - 3개의 디바이스 A, B 및 C를 고려하십시오.
    - A(고정 피어)와 B(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다.
    - 엑스트라넷 디바이스를 생성하여 A와 C(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다. A의 고정 VPN 인터페이스 IP 주소를 엑스트라넷 디바이스에 할당하고 C와의 연결을 설정합니다.

FDM-관리 디바이스 사이트 간 **VPN** 가이드 및 제한 사항

- Security Cloud Control는 S2S VPN에 대한 흥미로운 트래픽을 설계하기 위해 crypto-acl을 지원하지 않습니다. 이는 보호된 네트워크만 지원합니다.
- Security Cloud Control는 현재 ASA 또는 FDM 관리 디바이스에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 Security Cloud Control에 온보딩될 수 있지만 VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 Security Cloud Control는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다. VTI 터널에 대한 Security Cloud Control 지원이 곧 제공될 예정입니다.
- IKE 포트 500/4500이 사용 중이거나 활성화된 일부 PAT 변환이 있을 때마다 사이트 간 VPN을 동일한 포트에서 구성할 수 없으므로 해당 포트에서 서비스를 시작하는 데 실패합니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPSec이 구현되는 통상적인 방식입니다.
- 이 릴리스에서는 하나 이상의 VPN 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

FDM 관리 디바이스 사이에 사이트 간 VPN 터널 생성

참고로 FDM 관리 디바이스는 다른 FDM 관리 디바이스 또는 외부 네트워크 디바이스와 안전한 VPN 터널을 설정할 수 있는 기능을 갖추고 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 선택합니다.

단계 **2** 오른쪽 상단의 **Create Tunnel(**터널 생성**)(**  **)** 아이콘을 클릭하고 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 **3** **Peer Selection(**피어 선택**)** 영역에서 다음 정보를 입력합니다.

- **Configuration Name(**구성 이름**)**: 고유한 토폴로지 이름을 입력합니다.

  FDM 관리 디바이스 VPN 및 해당 토폴로지 유형임을 나타내도록 토폴로지의 이름을 지정하는 것이 좋습니다.

- 피어 **1**: **FDM** 탭을 클릭하고 FDM 관리 디바이스를 선택합니다.
- 피어 **2**: **FDM** 탭을 클릭하고 FDM 관리 디바이스를 선택합니다.

  엑스트라넷 디바이스를 선택하는 경우 **Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP**

주소)에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당)가 표시됩니다.

Note
엔드포인트 디바이스 중 하나 또는 둘 다에 동적 IP 주소가 있는 경우 추가 지침은 동적으로 주소가 지정된 피어를 사용하여 사이트 간 VPN 연결 구성을 참조하십시오.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** **Peer Details(**피어 세부 정보**)** 영역에서 다음 정보를 입력합니다.

- **VPN Access Interface(VPN** 액세스 인터페이스**)**: 피어 1과 피어 2 간의 연결을 설정할 인터페이스를 선택합니다.
- **Routing(**라우팅**)**: **Add Networks(**네트워크 추가**)**를 클릭하고 보호된 네트워크를 하나 이상 선택하여 피어 1과 피어 2의 보호된 네트워크 사이에 사이트 간 터널을 생성합니다.
- (선택 사항) **NAT Exempt Interface(NAT** 제외 인터페이스**)**: 피어 1과 피어 2에 대해 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외하려면 **NAT Exempt(NAT** 제외**)**를 선택합니다. 개별 피어에 대해 수동으로 구성해야 합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** **IKE Settings(IKE** 설정**)** 영역에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 전역 IKE 정책 구성을 참조하십시오.

Note
IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

a. 필요에 따라 두 옵션 중 하나를 선택하거나 두 옵션을 모두 선택합니다.

Note
기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

b. **Add IKEv2 Policy(IKEv2** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv2 정책을 선택합니다.

c. 디바이스에 대한 **Local Pre-Shared Key(**로컬 사전 공유 키**)** 및 **Remote Pre-Shared Key(**원격 사전 공유 키**)**가 자동으로 생성됩니다. 사전 공유 키는 연결에서 각 피어에 구성된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다.

d. **IKE Version 1(IKE** 버전 **1)**을 클릭하여 활성화합니다.

e. **Add IKEv1 Policy(IKEv1** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv1 정책을 선택합니다.

f. **IPEv1** 사전 공유 키가 자동으로 생성됩니다.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** **IPSec** 설정**)** 영역에서 피어 1 및 피어 2에 대한 IPSec 구성을 지정합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다.

IPSec 설정에 대한 자세한 내용은 IPsec 제안 정보의 내용을 참조하십시오.

a. **Add IKEv2 IPSec Proposals(IKEv2 IPSec** 제안 추가**)**를 클릭하고 피어 1 및 피어 2에 대해 원하는 IKEv2 제안을 선택합니다.

b. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.

c. **Next(**다음**)**를 클릭합니다.

단계 **10** **Finish(**마침**)** 영역에는 완료한 구성의 요약이 있습니다.

구성을 읽고 만족하면 **Submit(**제출**)**를 클릭합니다.

사이트 간 피어 사이에 보호된 트래픽에 대한 네트워킹 구성

사이트 간 연결 구성을 완료한 후에는 VPN이 모든 대상 디바이스에서 작동하도록 다음 구성을 수행해야 합니다.

Procedure

단계 **1** AC 정책을 구성합니다.

두 피어 뒤에 있는 보호된 네트워크 간의 양방향 트래픽을 허용하기 위해 AC 정책을 구성합니다. 이러한 정책은 패킷이 손실되지 않고 의도된 대상으로 이동하도록 도와줍니다.

Note
두 피어 모두에서 수신 및 발신 트래픽에 대한 AC 정책을 생성해야 합니다.

a. 왼쪽의 Security Cloud Control 탐색 모음에서 **Policies(**정책**)**를 클릭하고 원하는 옵션을 선택합니다.

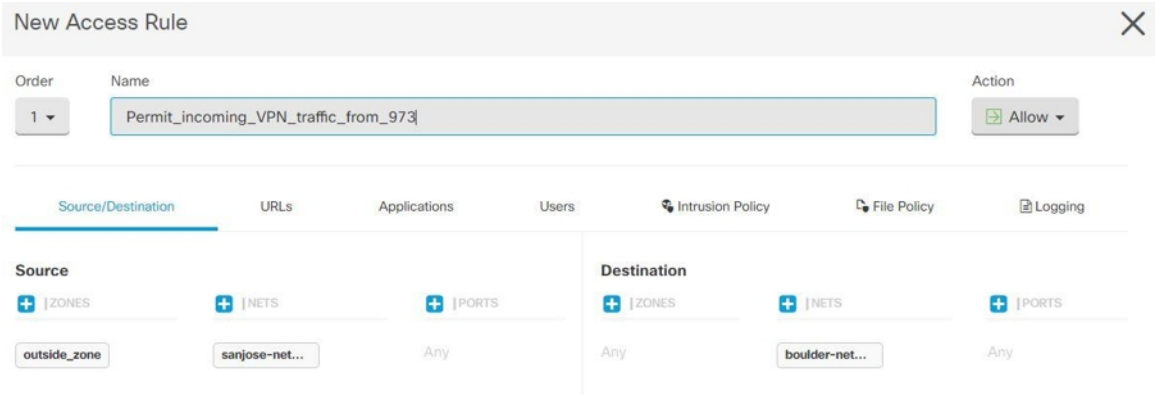
b. 두 피어 모두에서 수신 및 발신 트래픽에 대한 정책을 생성합니다.

다음 예는 두 피어 모두에서 AC 정책을 생성하는 단계를 보여줍니다.

각각 2개의 보호된 네트워크 'boulder-network' 및 'sanjose-network' 간에 사이트 간 VPN 연결을 사용하는 2개의 FDM 관리 디바이스 'FTD_BGL_972' 및 'FTD_BGL_973'을 고려하십시오.

수신 트래픽을 허용하기 위한 *AC* 정책 생성:

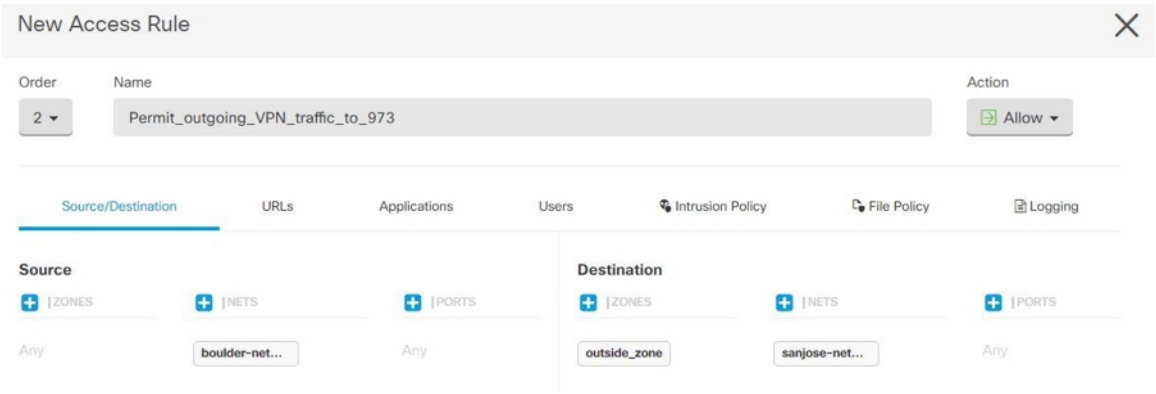
'FTD_BGL_972' 디바이스에서 피어('FTD_BGL_973')의 수신 트래픽을 허용하기 위해 'Permit_incoming_VPN_traffic_from_973' 정책이 생성됩니다.



- **Source Zone(**소스 영역**)**: 네트워크 트래픽이 시작되는 피어 디바이스의 영역을 설정합니다. 이 예에서 트래픽은 FTD_BGL_973에서 시작되어 FTD_BGL_972에 도달합니다.
- **Source Network(**소스 네트워크**)**: 네트워크 트래픽이 시작되는 피어 디바이스의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD_BGL_973) 뒤에 있는 보호되는 네트워크인 'sanjose-network'에서 시작됩니다.
- **Destination Network(**대상 네트워크**)**: 네트워크 트래픽이 도착하는 디바이스의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD_BGL_972) 뒤에 있는 보호되는 네트워크인 'boulder-network'에 도착합니다. 참고: 나머지 필드는 기본값("Any(모두)")을 사용할 수 있습니다.
- 정책에서 침입 및 기타 검사 설정의 영향을 받는 트래픽을 허용하려면 **Action(**작업**)**을 **Allow(**허용**)**으로 설정합니다.

발신 트래픽을 허용하기 위한 *AC* 정책 생성:

피어('FTD_BGL_973')로의 발신 트래픽을 허용하기 위해 'FTD_BGL_972' 디바이스에서 'Permit_outgoing_VPN_traffic_to_973' 정책이 생성됩니다.



- **Source Network(**소스 네트워크**)**: 네트워크 트래픽이 시작되는 피어 디바이스의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD_BGL_972) 뒤에 있는 보호되는 네트워크인 'boulder-network'에서 시작됩니다.

- **Destination Zone(**대상 영역**)**: 네트워크 트래픽이 도착하는 피어 디바이스의 영역을 설정합니다. 이 예에서는 트래픽이 FTD_BGL_972에서 도착하여 FTD_BGL_973에 도달하고 있습니다.
- **Destination Network(**대상 네트워크**)**: 네트워크 트래픽이 도착하는 피어의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD_BGL_972) 뒤에 있는 보호되는 네트워크인 'sanjose-network'에 도착합니다. 참고: 나머지 필드는 기본값("Any(모두)")을 사용할 수 있습니다.
- 정책에서 침입 및 기타 검사 설정의 영향을 받는 트래픽을 허용하려면 **Action(**작업**)**을 **Allow(**허용**)**으로 설정합니다.

한 디바이스에서 AC 정책을 생성한 후에는 해당 피어에서 유사한 정책을 생성해야 합니다.

단계 **2** NAT가 피어 디바이스 중 하나에 구성된 경우 NAT 제외 규칙을 수동으로 구성해야 합니다. NAT에서 사이트 간 VPN 트래픽 제외를 참조하십시오.

단계 **3** 각 피어에서 반환 VPN 트래픽을 수신하기 위한 라우팅을 구성합니다.

자세한 내용은 라우팅 구성을 참조하십시오.

a. **Gateway(**게이트웨이**)** — 대상 네트워크에 대해 게이트웨이의 IP 주소를 식별하는 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다.

b. **Interface(**인터페이스**)** — 트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 예에서 트래픽은 '외부' 인터페이스를 통해 전송됩니다.

c. **Destination Networks(**대상 네트워크**)** -대상 네트워크를 식별하는 하나 이상의 네트워크 개체를 선택합니다. 이 예에서 대상은 피어(FTD_BGL_973) 뒤에 있는 'sanjose-network'입니다.

한 디바이스에서 라우팅 설정을 구성한 후에는 해당 피어에서 유사한 설정을 구성해야 합니다.

기존 Security Cloud Control 사이트 간 VPN 편집

고급 구성 마법사는 기본적으로 기존 사이트 간 VPN 구성을 수정하는 데 사용됩니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 선택합니다.

단계 **2** 편집할 원하는 사이트 간 VPN 터널을 선택합니다.

단계 **3** **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.

Note
또는 다음을 수행하여 구성을 편집할 수 있습니다.

a. VPN 페이지를 열고 필터 패널에서 **Global View(**전역 보기**)** 버튼을 클릭합니다(자세한 내용은 전역 보기 참조).

   모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 그림이 나타납니다.

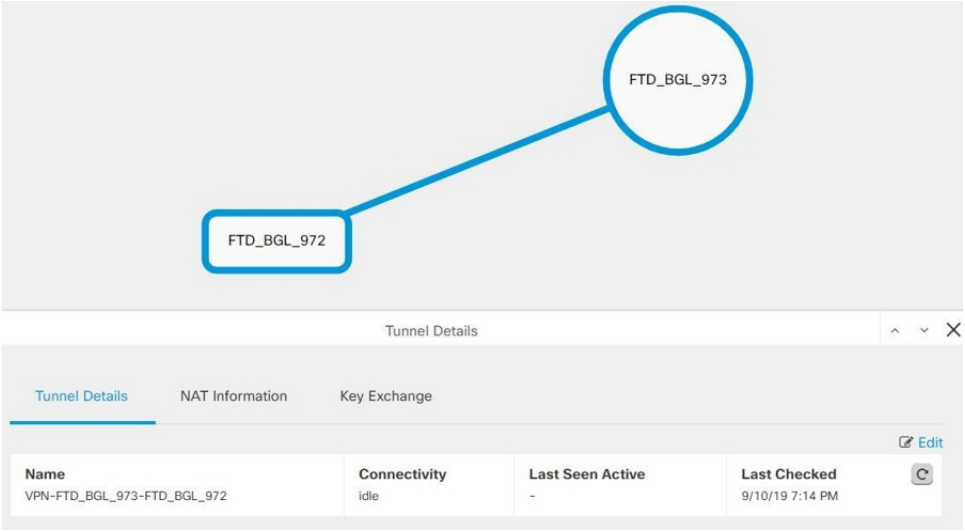
   구성을 편집하려면 피어 중 하나가 FDM 관리 디바이스여야 합니다.

b. 상자를 클릭하여 디바이스를 선택합니다.

c. **View details(**세부 정보 보기**)**를 클릭하여 피어를 확인합니다.

d. 터널 세부 정보를 보려면 피어 디바이스를 클릭합니다.

   디바이스와 관련된 터널 세부 정보, NAT 정보 및 키 교환 정보를 볼 수 있습니다.



e. **Tunnel Details(**터널 세부 정보**)**에서 **Edit(**편집**)**을 클릭합니다.

단계 **4** **Peer Devices(**피어 디바이스**)** 섹션에서 Configuration Name(구성 이름), VPN Access Interface(VPN 액세스 인터페이스) 및 Protected Networks(보호된 네트워크) 디바이스 구성을 수정할 수 있습니다.

Note
참여 디바이스는 변경할 수 없습니다.

단계 **5** **IKE Settings(IKE** 설정**)** 섹션에서 다음 IKEv2 정책 구성을 수정할 수 있습니다.

a. 각 디바이스에 대한 파란색 플러스 버튼을 클릭하고 새 IKEv2 정책을 선택합니다. 기존 IKEv2 정책을 삭제하려면 선택한 정책 위에 마우스를 놓고 **x** 아이콘을 클릭합니다.

b. 참여 디바이스에 대한 사전 공유 키를 수정합니다. 엔드포인트 디바이스의 사전 공유 키가 다른 경우 파란색 설정 버튼을 클릭하고 디바이스에 대한 적절한 사전 공유 키를 입력합니다.

c. **Next(**다음**)**를 클릭합니다.

단계 **6** **IPSec Settings(IPSec** 설정**)** 섹션에서 다음 IPSec 구성을 수정할 수 있습니다.

a. 파란색 플러스 버튼을 클릭하여 새 IKEv2 제안을 선택합니다. 기존 IKEv2 제안을 삭제하려면 선택한 제안 위에 마우스를 올려 놓고 **x** 아이콘을 클릭합니다.

b. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다.

c. **Edit VPN(VPN** 편집**)**을 클릭한 다음 **Finish(**마침**)**를 클릭합니다.

포인트 투 포인트 VPN이 수정되고 모든 변경 사항으로 업데이트됩니다.

Security Cloud Control 사이트 간 **VPN** 터널 삭제

Procedure

단계 **1** 왼쪽 창 에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** 삭제할 원하는 사이트 간 VPN 터널을 선택합니다.

단계 **3** 오른쪽의 **Actions(**작업**)** 창에서 **Delete(**삭제**)**를 클릭합니다.

선택한 사이트 간 VPN 터널이 삭제됩니다.

NAT에서 사이트 간 VPN 트래픽 제외

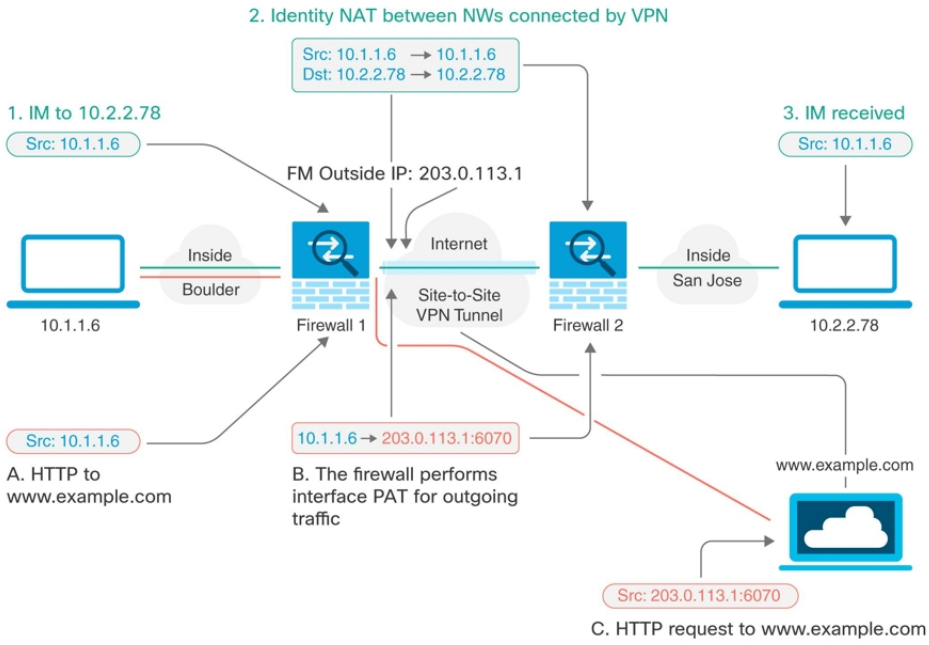
인터페이스에 사이트 간 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

VPN 연결을 생성할 때 **NAT Exempt(NAT** 제외**)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 간 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래 예에서는 인터페이스 PAT(Port Address Translation) 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 주소를 동일한 주소로 변환합니다.



다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.

Note 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

Procedure

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a. 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.

b. 파란색 플러스 버튼 을 클릭하여 개체를 생성합니다.

c. **FTD** > **Network(**네트워크**)**를 클릭합니다.

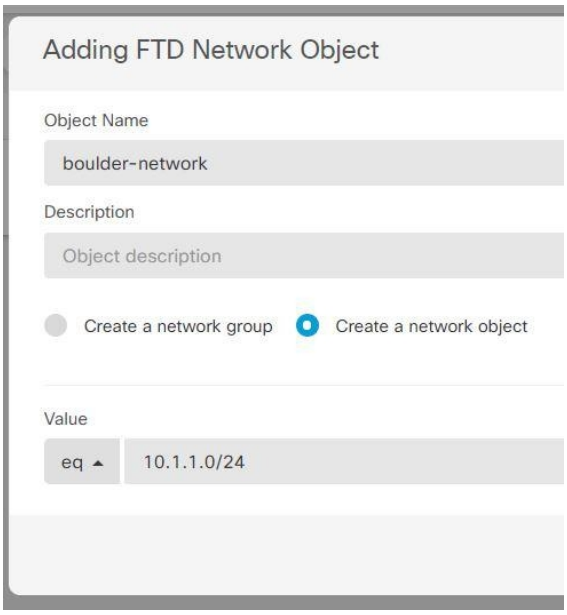
d. 볼더 내부 네트워크를 확인합니다.

e. 개체 이름을 입력합니다(예: boulder-network).

f. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

g. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.



h. **Add(**추가**)**를 클릭합니다.

i. 파란색 플러스 버튼 을 클릭하여 개체를 생성합니다.

j. 내부 산호세 네트워크를 정의합니다.

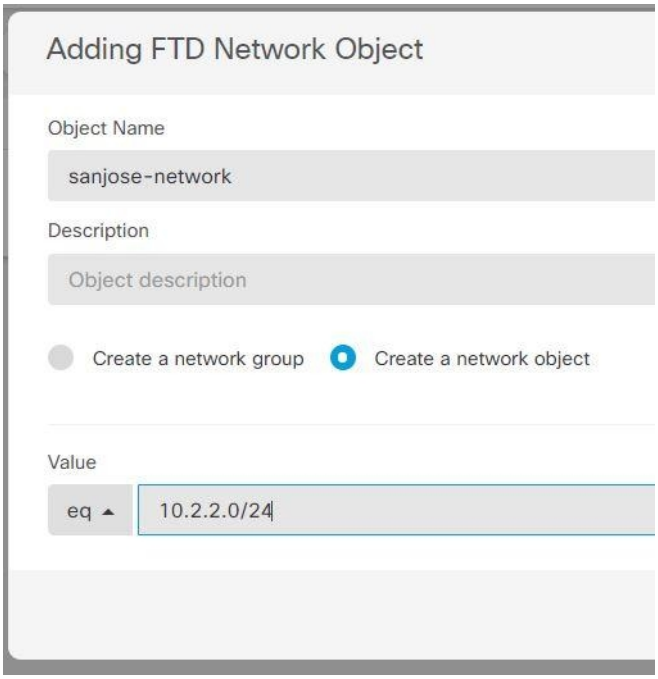
k. 개체 이름(예: san-jose)을 입력합니다.

l. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

m. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.

- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.



n. **Add(**추가**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

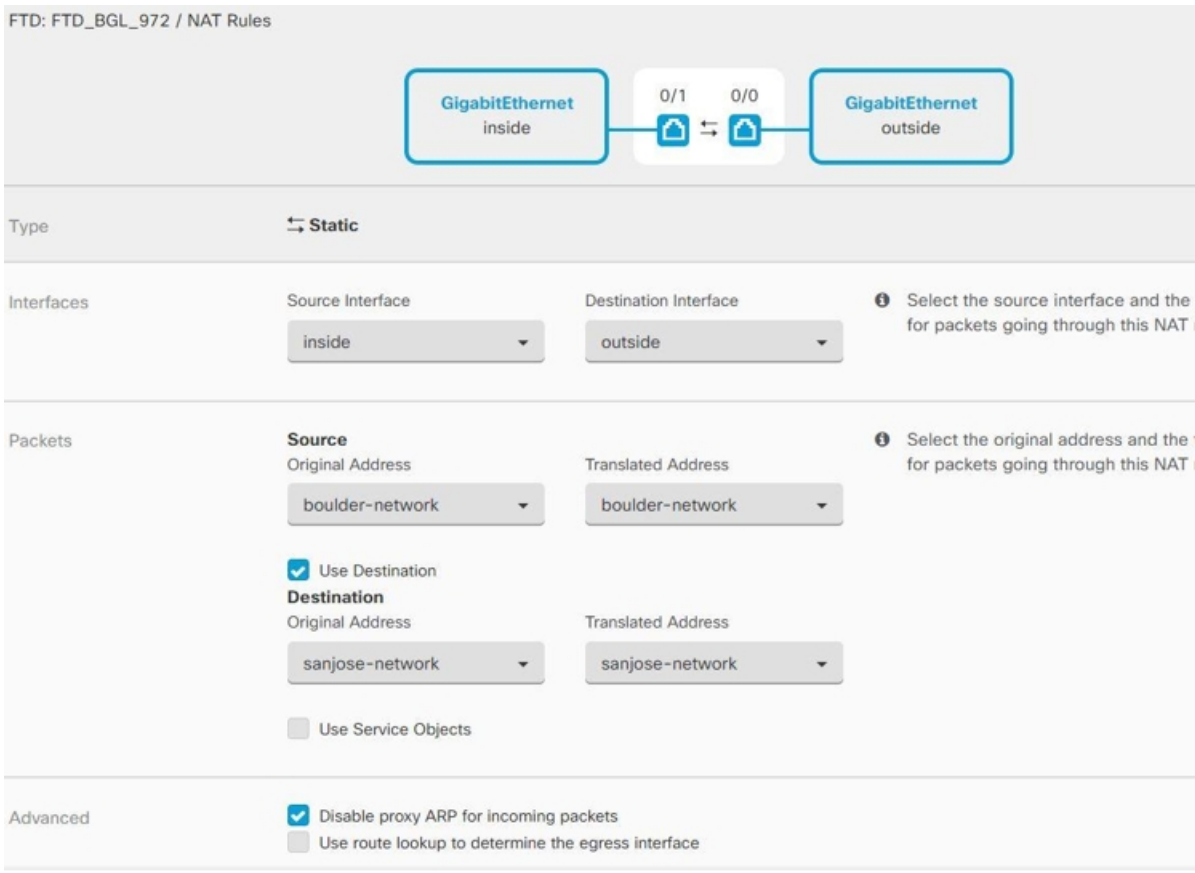
a. 왼쪽 창에서 **Security Devices(**보안 디바이스**)** > **All Devices(**모든 디바이스**)**를 클릭합니다.

b. 필터를 사용하여 NAT 규칙을 생성할 디바이스를 찾습니다.

c. 상세정보 패널의 Management(관리) 영역에서 **NAT** NAT를 클릭합니다.

d. + > **Twice NAT(2**회 **NAT)**를 클릭합니다.

- 섹션 1에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 2에서 **Source Interface(**소스 인터페이스**)** = **inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**)** = **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'boulder-network'를 선택합니다.
- **Use Destination(**대상 사용**)**을 선택합니다.
- **Destination Original Address(**대상 원본 주소**)** = 'sanjose-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'sanjose-network'를 선택합니다. 참고: 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.



- **Disable proxy ARP for Incoming packet(**수신 패킷에 대해 프록시 **ARP** 비활성화**)**을 선택합니다.
- **Save(**저장**)**를 클릭합니다.
- 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

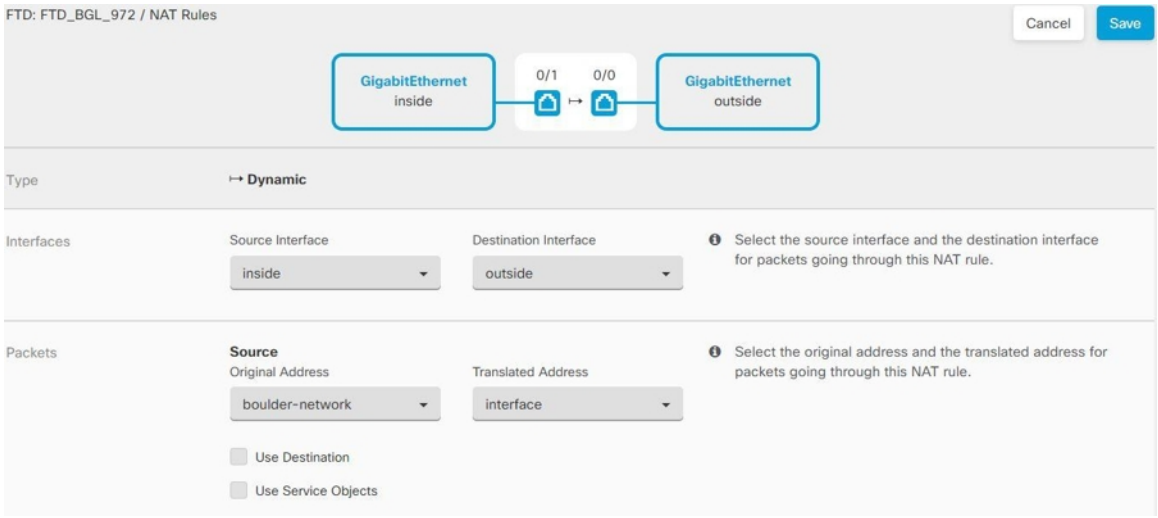
단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다. 참고: 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 구성 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 구성을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뜁니다.

a. + **> Twice NAT(2**회 **NAT)**를 클릭합니다.

b. 섹션 1에서 **Dynamic(**동적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

c. 섹션 2에서 **Source Interface(**소스 인터페이스**) = inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**) = outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

d. 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'interface'를 선택합니다.



e. **Save(**저장**)**를 클릭합니다.

f. 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **4** Security Cloud Control에 구성 변경 사항을 구축합니다. 자세한 내용은 Security Cloud Control에서 FTD로 구성 변경 사항 구축을 참조하십시오.

단계 **5** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

FDM-관리 디바이스에 대한 고정 및 기본 경로 구성

시스템의 인터페이스에 직접 연결되지 않은 네트워크에 바인딩된 패킷을 보낼 위치를 알 수 있도록 FTD(Firepower Threat Defense) 디바이스에 정적 경로를 정의합니다.

기본 경로 생성을 고려하십시오. 이는 네트워크 0.0.0.0/0에 대한 경로입니다. 이 경로는 기존 NAT 변환이나 고정 NAT 규칙 또는 기타 정적 경로를 통해 이그레스 인터페이스를 확인할 수 없는 패킷을 전송할 위치를 정의합니다.

기본 게이트웨이를 사용하여 모든 네트워크에 액세스할 수 없는 경우 다른 고정 경로가 필요할 수 있습니다. 예를 들어 기본 경로는 대개 외부 인터페이스의 업스트림 라우터입니다. 디바이스에 직접 연결되지 않는 추가 내부 네트워크가 있으며 기본 게이트웨이를 통해 해당 네트워크에 액세스할 수 없는 경우에는 이러한 각 내부 네트워크에 대해 고정 경로가 필요합니다.

시스템 인터페이스에 직접 연결된 네트워크에 대해서는 고정 경로를 정의할 수 없습니다. 시스템에서 이러한 경로를 자동으로 생성합니다.

클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense용 사이트 간 VPN 구성

클라우드 제공 Firewall Management Center매니지드 Firewall Threat Defense 디바이스와 다음 디바이스 간에 사이트 간 IPsec 연결을 생성할 수 있습니다.

- Firewall Threat Defense
- Secure Firewall ASA
- Multicloud Defense

클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense 디바이스 사이에 사이트 간 VPN 터널 생성

클라우드 제공 Firewall Management Center에 의해 관리되는 두 Firewall Threat Defense 사이에 사이트 간 VPN 터널을 생성하려면 다음 절차를 수행합니다.

시작하기 전에

Firewall Threat Defense 디바이스에 보류 중인 구축이 없어야 합니다.

프로시저

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 선택합니다.

단계 2 오른쪽 상단의 **Create Tunnel(**터널 생성**)(**  **)** 아이콘을 클릭하고 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 3 **Peer Selection(**피어 선택**)** 영역에서 다음 정보를 입력합니다.

- **Configuration Name(**구성 이름**)**: 고유한 토폴로지 이름을 입력합니다.

  Firewall Threat Defense 디바이스 VPN 및 해당 토폴로지 유형임을 나타내도록 토폴로지의 이름을 지정하는 것이 좋습니다.

- 피어 **1**: **FTD** 탭을 클릭하고 Firewall Threat Defense 디바이스를 선택합니다.
- 피어 **2**: **FTD** 탭을 클릭하고 Firewall Threat Defense 디바이스를 선택합니다.

  엑스트라넷 디바이스를 선택하는 경우 **Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당**)**가 표시됩니다.

단계 4 **Next(**다음**)**를 클릭합니다.

단계 5 **Peer Details(**피어 세부 정보**)** 영역에서 다음 정보를 입력합니다.

- **VPN Access Interface(VPN** 액세스 인터페이스**)**: 연결을 설정할 피어 1 및 피어 2의 인터페이스를 선택합니다.
- **LAN Interfaces(LAN** 인터페이스**)**: LAN 서브넷을 제어하는 피어 1 및 피어 2의 인터페이스를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.
- **Routing(**라우팅**)**: **Add Networks(**네트워크 추가**)**를 클릭하고 보호된 네트워크를 하나 이상 선택하여 선택한 네트워크 및 사이트 간 터널을 생성합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** **IKE Settings(IKE** 설정**)** 영역에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 전역 IKE 정책 구성을 참조하십시오.

참고
IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

1. 필요에 따라 두 옵션 중 하나를 선택하거나 두 옵션을 모두 선택합니다.

   참고
   기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

2. **Add IKEv2 Policy(IKEv2** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv2 정책을 선택합니다.
3. 디바이스에 대한 **Local Pre-Shared Key(**로컬 사전 공유 키**)** 및 **Remote Pre-Shared Key(**원격 사전 공유 키**)**가 자동으로 생성됩니다. 사전 공유 키는 연결에서 각 피어에 구성된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다.
4. **IKE Version 1(IKE** 버전 **1)**을 클릭하여 활성화합니다.
5. **Add IKEv1 Policy(IKEv1** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv1 정책을 선택합니다.
6. **IPEv1** 사전 공유 키가 자동으로 생성됩니다.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** **IPSec** 설정**)** 영역에서 피어 1 및 피어 2에 대한 IPSec 구성을 지정합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다.

IPSec 설정에 대한 자세한 내용은 IPsec 제안 구성에 대한 정보를 참조하십시오.

1. **Add IKEv2 IPSec Proposals(IKEv2 IPSec** 제안 추가**)**를 클릭하고 피어 1 및 피어 2에 대해 원하는 IKEv2 제안을 선택합니다.
2. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 VPN에서 사용되는 암호화 및 해시 알고리즘, 11 페이지을 참조하십시오.
3. **Next(**다음**)**를 클릭합니다.

단계 **10** **Finish(**마침**)** 영역에는 완료한 구성의 요약이 있습니다.

구성을 읽고 만족하면 **Submit(**제출**)**를 클릭합니다.

단계 **11**

단계 **12** 다음 단계를 수행하여 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense 디바이스에 구성을 구축합니다.

a) **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 선택합니다.
b) **Cloud-Delivered FMC(**클라우드 제공 **FMC)**에 해당하는 확인란이 선택되었는지 확인하고 오른쪽의 **Actions(**작업**)** 창에서 **Deployment(**구축**)**를 클릭합니다.
c) 사이트 간 VPN 구성에 참여하는 디바이스를 선택하고 **Deploy(**구축**)**를 클릭합니다.
d) **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)**를 선택합니다. Security Cloud Control에 구성된 것과 동일한 VPN 토폴로지를 확인할 수 있습니다.

클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense와 Multicloud Defense 사이에 사이트 간 VPN 터널 생성

모든 관련 표준을 준수하는 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense와 Security Cloud Control 대시보드의 Multicloud Defense 사이에 사이트 간 IPsec 연결을 생성할 수 있습니다. VPN 연결이 설정되면 방화벽 뒤에 있는 호스트는 보안 VPN 터널을 통해 게이트웨이 뒤에 있는 호스트에 연결할 수 있습니다.

Multicloud Defense에서는 현재 AWS(Amazon Web Services), Azure, GCP(Google Cloud Platform) 및 Oracle OCI 클라우드 어카운트를 지원합니다.

다음 절차를 수행하여 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense 디바이스와 Security Cloud Control 대시보드의 Multicloud Defense 사이에 VPN 터널을 생성합니다.

시작하기 전에

다음 사전 요건이 충족되는지 확인합니다.

- 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense 디바이스에는 보류 중인 변경 사항이 없어야 합니다.
- Multicloud Defense이 Security Cloud Control에 온보딩되어야 합니다. 클라우드 어카운트 연결을 참조하십시오.
- Multicloud Defense 게이트웨이 기호는 활성 상태여야 합니다.
- Multicloud Defense 게이트웨이는 VPN 활성화 상태여야 합니다. 게이트웨이 내에서 VPN 활성화를 참조하십시오.
- 자세한 내용은 마이그레이션에 대한 Multicloud Defense 게이트웨이 사전 요건 및 제한 사항을 읽어보십시오.

프로시저

단계 1 탐색창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 선택합니다.

단계 2 오른쪽 상단의 **Create Tunnel(**터널 생성**)(**  **)** 아이콘을 클릭하고 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 3 **Peer Selection(**피어 선택**)** 영역에서 다음 정보를 입력합니다.

- **Configuration Name(**구성 이름**)**: 고유한 토폴로지 이름을 입력합니다.
- 피어 **1**: **FTD** 탭을 클릭하고 Firewall Threat Defense 디바이스를 선택합니다.
- 피어 **2**: Multicloud Defense 탭을 클릭하고 원하는 게이트웨이를 선택합니다.

  엑스트라넷 디바이스를 선택하는 경우 **Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당**)**가 표시됩니다.

단계 4 **Next(**다음**)**를 클릭합니다.

단계 5 **Peer Details(**피어 세부 정보**)** 영역에서 다음 정보를 입력합니다.

- **VPN Access Interface(VPN** 액세스 인터페이스**)**: Firewall Threat Defense의 인터페이스를 선택하여 게이트웨이와의 연결을 설정합니다.
- **Public IP(**퍼블릭 **IP)(**선택 사항**)**: 선택한 Firewall Threat Defense의 외부 인터페이스에 매핑되는 네트워크 주소 변환 의 공용 IP 주소를 지정합니다.
- **Routing (**라우팅**)**: **Add Networks(**네트워크 추가**)**를 클릭하고 Firewall Threat Defense에서 보호된 네트워크를 하나 이상 선택하여 선택한 네트워크 및 Multicloud Defense 게이트웨이 사이에 사이트 간 터널을 생성합니다.

단계 6 **Next(**다음**)**를 클릭합니다.

단계 7 **Tunnel Details(**터널 상세정보**)** 영역에서 다음 정보를 제공합니다.

- **Virtual Tunnel Interface IP(**가상 터널 인터페이스 **IP)**: 피어에서 새 가상 터널 인터페이스의 주소를 지정합니다. 이 디바이스에서 현재 사용되지 않는 미사용 IP 주소를 할당할 수 있습니다.
- **Autonomous System Number(**자동 시스템 번호**)**: 네트워크 자동 시스템 번호를 지정합니다.

단계 8 **Next(**다음**)**를 클릭합니다.

단계 9 **IKE Settings(IKE** 설정**)** 영역에서 **Add IKEv2(IKEv2** 추가**)**를 클릭하고 IKE(인터넷 키 교환) 협상을 위한 IKE 버전을 추가하고 프라이버시 구성을 지정합니다.

Security Cloud Control는 기본적으로 **Local Pre-Shared Key(**로컬 사전 공유 키**)**를 생성합니다, 이것은 피어에 구성된 암호 키 문자열입니다. IKE는 인증 단계 중에 이 키를 사용합니다. 피어 간에 터널을 설정할 때 서로를 확인하는 데 사용됩니다.

단계 **10** **Next(**다음**)**를 클릭합니다.

단계 **11** **IPSec Settings(IPSec** 설정**)** 영역 에서 IKEv2 IPSec 제안 추가를 클릭하고 IKE IPSec 구성을 선택합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 제안을 사용할 수 있습니다. IPsec 제안 구성을 참조하십시오.

단계 **12** **Next(**다음**)**를 클릭합니다.

단계 **13** **Finish(**완료**)** 영역에서 구성을 검토하고 구성에 만족하는 경우에만 계속 진행합니다.

단계 **14** **Submit(**제출**)**를 클릭합니다.

구성은 Multicloud Defense 게이트웨이로 푸시됩니다.

단계 **15** 다음 단계를 수행하여 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense 디바이스에 구성을 구축합니다.

a) **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 선택합니다.
b) **Cloud-Delivered FMC(**클라우드 제공 **FMC)**에 해당하는 확인란이 선택되었는지 확인하고 오른쪽의 **Actions(**작업**)** 창에서 **Deployment(**구축**)**를 클릭합니다.
c) 사이트 간 VPN 구성에 참여하는 디바이스를 선택하고 **Deploy(**구축**)**를 클릭합니다.
d) **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)**를 선택합니다. Security Cloud Control에 구성된 것과 동일한 VPN 토폴로지를 확인할 수 있습니다.

클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense와 Secure Firewall ASA 사이에 사이트 간 VPN 생성

시작하기 전에

Firewall Threat Defense 디바이스에 보류 중인 구축이 없어야 합니다.

프로시저

단계 **1** 탐색창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 선택합니다.

단계 **2** 오른쪽 상단의 **Create Tunnel(**터널 생성**)(**  **)** 아이콘을 클릭하고 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 **3** **Peer Selection(**피어 선택**)** 영역에서 다음 정보를 입력합니다.

- **Configuration Name(**구성 이름**)**: 고유한 토폴로지 이름을 입력합니다.

  Firewall Threat Defense 디바이스 VPN 및 해당 토폴로지 유형임을 나타내도록 토폴로지의 이름을 지정하는 것이 좋습니다.

- 피어 **1**: **FTD** 탭을 클릭하고 Firewall Threat Defense 디바이스를 선택합니다.
- 피어 **2**: **ASA** 탭을 클릭하고 Secure Firewall ASA 디바이스를 선택합니다.

  엑스트라넷 디바이스를 선택하는 경우 **Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당**)**가 표시됩니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** **Peer Details(**피어 세부 정보**)** 영역에서 다음 정보를 입력합니다.

- **VPN Access Interface(VPN** 액세스 인터페이스**)**: 연결을 설정할 피어 1 및 피어 2의 인터페이스를 선택합니다.
- **LAN Interfaces(LAN** 인터페이스**)**: LAN 서브넷을 제어하는 피어 1 및 피어 2의 인터페이스를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.
- **Routing(**라우팅**)**: **Add Networks(**네트워크 추가**)**를 클릭하고 보호된 네트워크를 하나 이상 선택하여 선택한 네트워크 및 사이트 간 터널을 생성합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** **Tunnel Details(**터널 상세정보**)** 영역에서 다음 정보를 제공합니다.

- **Virtual Tunnel Interface IP(**가상 터널 인터페이스 **IP)**: Secure Firewall ASA에 대한 새 가상 터널 인터페이스의 주소를 지정합니다. Security Cloud Control는 충돌이 발생하는 경우 변경할 수 있는 Secure Firewall ASA에 대한 샘플 주소를 제공합니다. 이 디바이스에서 현재 사용되지 않는 미사용 IP 주소를 할당할 수 있습니다.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** **IKE Settings(IKE** 설정**)** 영역에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 전역 IKE 정책 구성을 참조하십시오.

참고
IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

1. 필요에 따라 두 옵션 중 하나를 선택하거나 두 옵션을 모두 선택합니다.

   참고
   기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

2. **Add IKEv2 Policy(IKEv2** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv2 정책을 선택합니다.
3. 디바이스에 대한 **Local Pre-Shared Key(**로컬 사전 공유 키**)** 및 **Remote Pre-Shared Key(**원격 사전 공유 키**)**가 자동으로 생성됩니다. 사전 공유 키는 연결에서 각 피어에 구성된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다.

4. **IKE Version 1(IKE** 버전 **1)**을 클릭하여 활성화합니다.
5. **Add IKEv1 Policy(IKEv1** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv1 정책을 선택합니다.
6. **IPEv1** 사전 공유 키가 자동으로 생성됩니다.

단계 **10** **Next(**다음**)**를 클릭합니다.

단계 **11** **IPSec** 설정**)** 영역에서 피어 1 및 피어 2에 대한 IPSec 구성을 지정합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다.

IPSec 설정에 대한 자세한 내용은 IPsec 제안 구성에 대한 정보를 참조하십시오.

1. **Add IKEv2 IPSec Proposals(IKEv2 IPSec** 제안 추가**)**를 클릭하고 피어 1 및 피어 2에 대해 원하는 IKEv2 제안을 선택합니다.
2. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.

단계 **12** **Next(**다음**)**를 클릭합니다.

단계 **13** **Finish(**마침**)** 영역에는 완료한 구성의 요약이 있습니다.

구성을 읽고 만족하면 **Submit(**제출**)**를 클릭합니다.

단계 **14** 다음 단계를 수행하여 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense 디바이스에 구성을 구축합니다.

a) **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 선택합니다.
b) **Cloud-Delivered FMC(**클라우드 제공 **FMC)**에 해당하는 확인란이 선택되었는지 확인하고 오른쪽의 **Actions(**작업**)** 창에서 **Deployment(**구축**)**를 클릭합니다.
c) 사이트 간 VPN 구성에 참여하는 디바이스를 선택하고 **Deploy(**구축**)**를 클릭합니다.
d) **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)**를 선택합니다. Security Cloud Control에 구성된 것과 동일한 VPN 토폴로지를 확인할 수 있습니다.

Secure Firewall ASA에 대한 사이트 간 VPN

Security Cloud Control는 Secure Firewall ASA 디바이스에서 사이트 간 VPN 기능의 다음 측면을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 사이트 간 VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.

- 엔드포인트로 작동하는 엑스트라넷 디바이스의 정적 또는 동적 IP 주소 지원.

동적 주소 지정 피어로 사이트 간 **VPN** 연결 구성

Security Cloud Control를 사용하면 피어의 VPN 인터페이스 IP 주소 중 하나를 알 수 없거나 인터페이스가 DHCP 서버에서 주소를 가져올 때 피어 간에 사이트 간 VPN 연결을 생성할 수 있습니다. 사전 공유 키, IKE 설정 및 IPsec 구성이 다른 피어와 일치하는 모든 동적 피어는 사이트 간 VPN 연결을 설정할 수 있습니다.

피어 A와 B를 고려하십시오. 고정 피어는 VPN 인터페이스의 IP 주소가 고정되어 있는 디바이스이고 동적 피어는 VPN 인터페이스의 IP 주소를 알 수 없거나 임시 IP 주소가 있는 디바이스입니다.

다음 사용 사례에서는 동적으로 주소가 지정된 피어를 사용하여 안전한 사이트 간 VPN 연결을 설정하는 다양한 시나리오를 설명합니다.

- A는 정적 피어이고 B는 동적 피어이거나 그 반대입니다.
- A는 고정 피어이고 B는 DHCP 서버에서 확인된 IP 주소를 사용하거나 그 반대로 하는 동적 피어입니다.
- A는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.
- A는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.

참고 ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 인터페이스의 IP 주소를 변경하면 Security Cloud Control에서 해당 피어의 **Configuration Status(**구성 상태**)**에 "Conflict Detected(충돌 탐지됨)"가 표시됩니다. 이 대역 외 변경 사항을 해결하면 다른 피어의 **Configuration Status(**구성 상태**)**가 "Not Synced(동기화되지 않음)" 상태로 변경됩니다. "Not Synced(동기화되지 않음)" 상태인 디바이스에 Security Cloud Control 구성을 구축해야 합니다.

일반적으로 동적 피어는 연결을 시작하는 피어여야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.

참고 다음 시나리오에서는 사이트 간 VPN 연결을 구성할 수 없습니다.

디바이스에 둘 이상의 동적 피어 연결이 있는 경우

- 3개의 디바이스 A, B 및 C를 고려하십시오.
- A(고정 피어)와 B(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다.
- 엑스트라넷 디바이스를 생성하여 A와 C(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다. A의 고정 VPN 인터페이스 IP 주소를 엑스트라넷 디바이스에 할당하고 C와의 연결을 설정합니다.

Secure Firewall ASA 사이트 간 VPN 지침 및 제한 사항

- Security Cloud Control는 S2S VPN에 대한 흥미로운 트래픽을 설계하기 위해 crypto-acl을 지원하지 않습니다. 이는 보호된 네트워크만 지원합니다.
- IKE 포트 500/4500이 사용 중이거나 활성화된 일부 PAT 변환이 있을 때마다 사이트 간 VPN을 동일한 포트에서 구성할 수 없으므로 해당 포트에서 서비스를 시작하는 데 실패합니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPSec이 구현되는 통상적인 방식입니다.
- 이 릴리스에서는 하나 이상의 VPN 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

Virtual Tunnel Interface에 대한 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다. Secure Firewall ASA에서의 GRE 터널 종료는 지원되지 않습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다. 그러나 VTI가 활성화된 후 물리적 인터페이스 MTU를 변경하는 경우, 새 MTU 설정을 사용하려면 VTI를 비활성화했다가 다시 활성화해야 합니다.
- 네트워크 주소 변환을 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.
- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.

- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있으며 암호화 맵에 구성된 피어 주소를 제공하며 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통과하는 모든 트래픽이 암호화됩니다.
- 기본적으로 VTI 인터페이스의 보안 레벨은 0입니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI에서는 BGP만 지원됩니다.
- Secure Firewall ASA가 IOS IKEv2 VTI 클라이언트를 종료하는 경우, IOS에서 config-exchange 요청을 비활성화합니다. Secure Firewall ASA는 IOS VTI 클라이언트에서 시작한 이 L2L 세션에 대한 mode-CFG 속성을 검색할 수 없기 때문입니다.
- IPv6은 지원되지 않습니다.

관련 정보:

- Secure Firewall ASA 사이에 사이트 간 VPN 터널 생성, 37 페이지

Secure Firewall ASA 사이에 사이트 간 VPN 터널 생성

두 ASA 또는 엑스트라넷 디바이스를 사용하는 ASA 간에 사이트 간 VPN 터널을 생성하려면 다음 절차를 수행합니다.

프로시저

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Site to Site VPN(**사이트 간 **VPN)** > **ASA & FDM**을 클릭합니다.

단계 2 오른쪽 상단의 **Create Tunnel(**터널 생성**)(**  **)** 아이콘을 클릭하고 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 3

단계 4 **Peer Selection(**피어 선택**)** 영역에서 다음 정보를 입력합니다.

- **Configuration Name(**구성 이름**)**: 고유한 토폴로지 이름을 입력합니다.
- 피어 **1**: **ASA** 탭을 클릭하고 Secure Firewall ASA 디바이스를 선택합니다.
- 피어 **2**: **ASA** 탭을 클릭하고 Secure Firewall ASA 디바이스를 선택합니다.

  엑스트라넷 디바이스를 선택하는 경우 **Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당**)**가 표시됩니다.

단계 5 **Next(**다음**)**를 클릭합니다.

단계 **6** **Peer Details(**피어 세부 정보**)** 영역에서 다음 정보를 입력합니다.

- 새 정책 기반 또는 경로 기반 사이트 간 VPN을 생성하는 옵션 중 하나를 선택합니다.
- **VPN Access Interface(VPN** 액세스 인터페이스**)**: 연결을 설정할 피어 1 및 피어 2의 인터페이스를 선택합니다.
- (경로 기반에 적용 가능)**LAN Interfaces(LAN** 인터페이스**)**: LAN 서브넷 제어하는 피어 1 및 피어 2의 인터페이스를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.
- **Routing(**라우팅**)**: **Add Networks(**네트워크 추가**)**를 클릭하고 보호된 네트워크를 하나 이상 선택하여 선택한 네트워크 및 사이트 간 터널을 생성합니다.
- (정책 기반에 적용 가능) **NAT Exempt(NAT** 제외**)**: 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외하려면 선택합니다. 개별 피어에 대해 수동으로 구성해야 합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 ASA 사이트 간 VPN 트래픽 제외를 참조하십시오.

단계 **7** **Next(**다음**)**를 클릭합니다.

단계 **8** (라우트 기반에 적용 가능) 이전 단계에서 피어 디바이스가 구성되면 터널 세부 정보에서 **VTI** 주소 필드가 자동으로 채워집니다. 필요한 경우 새 VTI로 사용할 IP 주소를 수동으로 입력할 수 있습니다.

단계 **9** **IKE Settings(IKE** 설정**)** 영역에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 전역 IKE 정책 정보의 내용을 참조하십시오.

참고
IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

1. 필요에 따라 두 옵션 중 하나를 선택하거나 두 옵션을 모두 선택합니다.

   참고
   기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

2. **Add IKEv2 Policy(IKEv2** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv2 정책을 선택합니다.
3. 디바이스에 대한 **Local Pre-Shared Key(**로컬 사전 공유 키**)** 및 **Remote Pre-Shared Key(**원격 사전 공유 키**)**가 자동으로 생성됩니다. 사전 공유 키는 연결에서 각 피어에 구성된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다.
4. **IKE Version 1(IKE** 버전 **1)**을 클릭하여 활성화합니다.
5. **Add IKEv1 Policy(IKEv1** 정책 추가**)**를 클릭하고 피어 1과 피어 2에 대한 IKEv1 정책을 선택합니다.

6. **IPEv1** 사전 공유 키가 자동으로 생성됩니다.

단계 **10** **Next(**다음**)**를 클릭합니다.

단계 **11** **IPSec** 설정**)** 영역에서 피어 1 및 피어 2에 대한 IPSec 구성을 지정합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다.

IPSec 설정에 대한 자세한 내용은 전역 IKE 정책 정보의 내용을 참조하십시오.

1. **Add IKEv2 IPSec Proposals(IKEv2 IPSec** 제안 추가**)**를 클릭하고 피어 1 및 피어 2에 대해 원하는 IKEv2 제안을 선택합니다.
2. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 VPN에서 사용되는 암호화 및 해시 알고리즘, 11 페이지을 참조하십시오.

단계 **12** **Finish(**완료**)** 영역에서 구성을 검토하고 구성에 만족하는 경우에만 계속 진행합니다.

기본적으로 **Deploy changes to ASA immediately(ASA**에 즉시 변경 사항 구축**)** 확인란이 선택되어 **Submit(**제출**)**를 클릭한 후 ASA 디바이스에 즉시 구성을 구축합니다.

나중에 수동으로 설정을 검토하고 구축하려면 이 확인란의 선택을 취소합니다 .

새로 구성된 사이트 간 VPN 터널을 표시하는 VPN Tunnels(VPN 터널) 페이지로 이동합니다. 변경 사항이 준비되며 수동으로 구축해야 합니다. VTI 터널을 통해 디바이스 간에 VTI 트래픽을 자동으로 라우팅하도록 라우팅 정책이 생성됩니다. 이 정책을 보려면 **Security Devices(**보안 디바이스**)** 페이지에서 디바이스를 선택하고 **Configuration(**구성**)** > **Diff(**차이**)**를 선택합니다.

ASA와 Multicloud Defense 게이트웨이 사이에 사이트 간 VPN 터널 생성

모든 관련 표준을 준수하는 ASA와 Multicloud Defense 게이트웨이 사이에 사이트 간 IPsec 연결을 생성할 수 있습니다. VPN 연결이 설정되면 방화벽 뒤에 있는 호스트는 보안 VPN 터널을 통해 게이트웨이 뒤에 있는 호스트에 연결할 수 있습니다.

Multicloud Defense에서는 현재 AWS(Amazon Web Services), Azure, GCP(Google Cloud Platform) 및 Oracle OCI 클라우드 어카운트를 지원합니다.

다음 절차를 수행하여 Security Cloud Control에 의해 관리되는 ASA 디바이스와 Security Cloud Control 대시보드의 Multicloud Defense 게이트웨이 사이에 VPN 터널을 생성합니다.

시작하기 전에

다음 사전 요건이 충족되는지 확인합니다.

- ASA 디바이스에는 보류 중인 변경 사항이 없어야 합니다.
- VPN 터널을 생성하기 전에 ASA 콘솔에서 BGP 프로파일을 생성합니다. 자세한 내용은 ASA Border 게이트웨이 프로토콜 설정을 참조하십시오.
- Multicloud Defense 게이트웨이가 **Active(**활성**)** 상태여야 합니다.

- Multicloud Defense 게이트웨이는 VPN 활성화 상태여야 합니다. 게이트웨이 내에서 VPN 활성화를 참조하십시오.
- 자세한 내용은 ASA 사이트 간 VPN 제한 사항 및 지침을 참조하십시오.
- 자세한 내용은 마이그레이션에 대한 Multicloud Defense 게이트웨이 사전 요건 및 제한 사항을 읽어보십시오.

프로시저

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 선택합니다.

단계 **2** 오른쪽 상단의 **Create Tunnel(**터널 생성**)(**  **)** 아이콘을 클릭하고 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 **3** **Peer Selection(**피어 선택**)** 영역에서 다음 정보를 입력합니다.

- **Configuration Name(**구성 이름**)**: 고유한 토폴로지 이름을 입력합니다.
- 피어 **1**: **ASA** 탭을 클릭하고 Secure Firewall ASA 디바이스를 선택합니다.
- 피어 **2**: **Multicloud Defense** 탭을 클릭하고 멀티클라우드게이트웨이를 선택합니다.

  엑스트라넷 디바이스를 선택하는 경우 **Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당**)**가 표시됩니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** **Peer Details(**피어 세부 정보**)** 영역에서 다음 정보를 입력합니다.

- **VPN Access Interface(VPN** 액세스 인터페이스**)**: Secure Firewall ASA의 인터페이스를 선택하여 Multicloud Defense 게이트웨이와의 연결을 설정합니다.
- **LAN Interfaces(LAN** 인터페이스**)**: LAN 서브넷을 제어하는 Secure Firewall ASA의 인터페이스를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.
- **Public IP(**퍼블릭 **IP)(**선택 사항**)**: 선택한 Secure Firewall ASA의 외부 인터페이스에 매핑되는 네트워크 주소 변환 의 공용 IP 주소를 지정합니다.
- **Routing(**라우팅**)**: **Add Networks(**네트워크 추가**)**를 클릭하고 Secure Firewall ASA에 대해 보호된 네트워크를 하나 이상 선택하여 Multicloud Defense 게이트웨이과의 사이트 간 터널을 설정합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** **Tunnel Details(**터널 상세정보**)** 영역에서 다음 정보를 제공합니다.

- **Virtual Tunnel Interface IP(**가상 터널 인터페이스 **IP)**: 피어에서 새 가상 터널 인터페이스의 주소를 지정합니다. Security Cloud Control는 충돌이 발생하는 경우 변경할 수 있는 Secure Firewall ASA에 대한 샘플 주소를 제공합니다. 이 디바이스에서 현재 사용되지 않는 미사용 IP 주소를 할당할 수 있습니다.
- 자동 시스템 번호(피어 1): Secure Firewall ASA 디바이스에 자동 시스템 번호가 구성되어 있지 않은 경우Security Cloud Control 는 디바이스에 대해 자동 시스템 번호를 제안하며, 이 번호는 수정할 수 있습니다. 디바이스에 이미 자동 시스템 번호가 구성된 경우 현재 값이 표시되고 수정할 수 없습니다.
- 자동 시스템 번호(피어 2): BGP 프로파일이 Multicloud Defense 게이트웨이에 할당된 경우 프로파일과 연결된 자동 번호가 표시되며 이는 수정할 수 없습니다. Multicloud Defense 게이트웨이 추가를 참조하십시오.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** **IKE Settings(IKE** 설정**)** 영역에서 Security Cloud Control는 **Local Pre-Shared Key(**로컬 사전 공유 키**)**를 생성합니다. 이것은 피어에 구성된 암호 키 문자열입니다. IKE는 인증 단계 중에 이 키를 사용합니다. 피어 간에 터널을 설정할 때 서로를 확인하는 데 사용됩니다.

단계 **10** **Finish(**완료**)** 영역에서 구성을 검토하고 구성에 만족하는 경우에만 계속 진행합니다.

기본적으로 **Deploy changes to ASA immediately(ASA**에 즉시 변경 사항 구축**)** 확인란이 선택되어 **Submit(**제출**)**를 클릭한 후 ASA 디바이스에 즉시 구성을 구축합니다.

나중에 수동으로 설정을 검토하고 구축하려면 이 확인란의 선택을 취소합니다 .

단계 **11** **Submit(**제출**)**를 클릭합니다.

구성은 Multicloud Defense 게이트웨이로 푸시됩니다.

Security Cloud Control의 VPN 페이지에는 피어 간에 생성된 사이트 간 터널이 표시됩니다. Multicloud Defense 게이트웨이 포털에서 해당 터널을 확인할 수 있습니다.

NAT에서 사이트 간 VPN 트래픽 제외

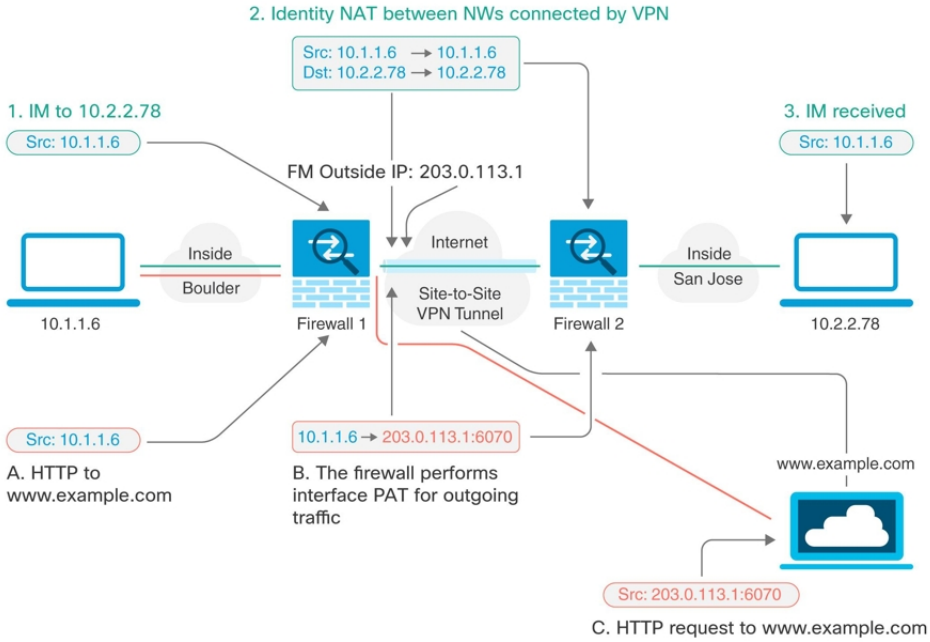
인터페이스에 사이트 간 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

VPN 연결을 생성할 때 **NAT Exempt(NAT** 제외**)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 간 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래 예에서는 인터페이스 PAT(Port Address Translation) 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 주소를 동일한 주소로 변환합니다.



다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.

Note 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

Procedure

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a. 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.

b. 파란색 플러스 버튼 을 클릭하여 개체를 생성합니다.

c. **FTD** > **Network(**네트워크**)**를 클릭합니다.

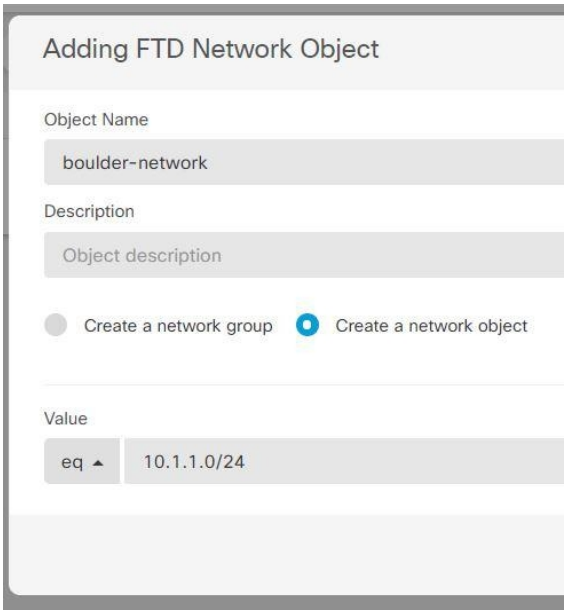
d. 볼더 내부 네트워크를 확인합니다.

e. 개체 이름을 입력합니다(예: boulder-network).

f. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

g. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.



h. **Add(**추가**)**를 클릭합니다.

i. 파란색 플러스 버튼 을 클릭하여 개체를 생성합니다.

j. 내부 산호세 네트워크를 정의합니다.

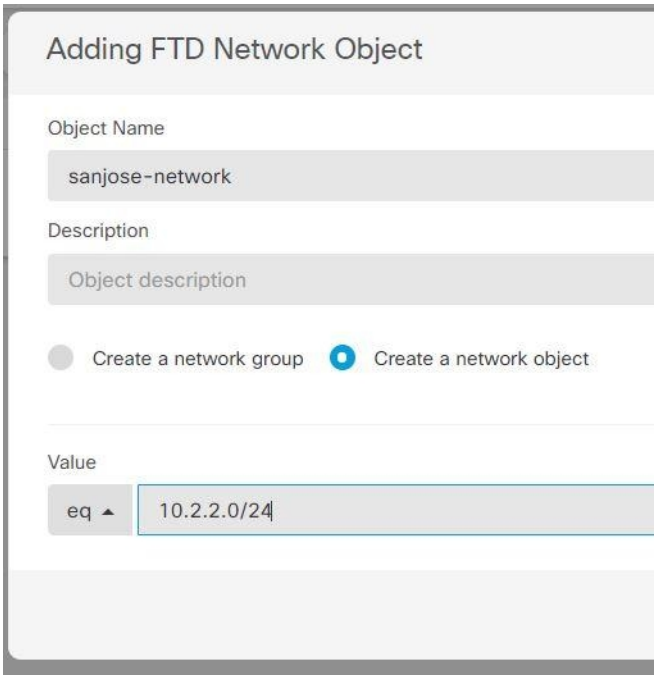
k. 개체 이름(예: san-jose)을 입력합니다.

l. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

m. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.

- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.



n. **Add(**추가**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

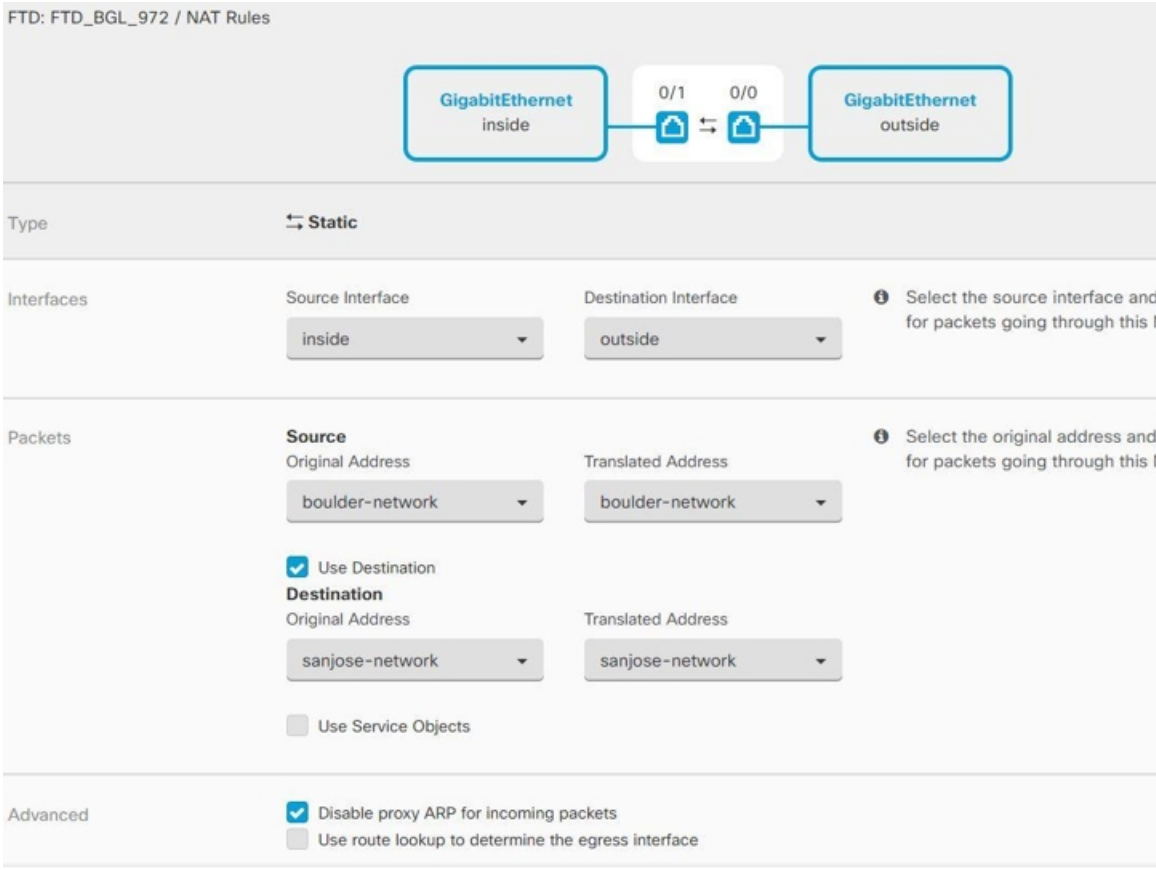
a. 왼쪽 창에서 **Security Devices(**보안 디바이스**)** > **All Devices(**모든 디바이스**)**를 클릭합니다.

b. 필터를 사용하여 NAT 규칙을 생성할 디바이스를 찾습니다.

c. 상세정보 패널의 Management(관리) 영역에서 **NAT** NAT를 클릭합니다.

d. + > **Twice NAT(2**회 **NAT)**를 클릭합니다.

- 섹션 1에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 2에서 **Source Interface(**소스 인터페이스**)** = **inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**)** = **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'boulder-network'를 선택합니다.
- **Use Destination(**대상 사용**)**을 선택합니다.
- **Destination Original Address(**대상 원본 주소**)** = 'sanjose-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'sanjose-network'를 선택합니다. 참고: 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.



- **Disable proxy ARP for Incoming packet(**수신 패킷에 대해 프록시 **ARP** 비활성화**)**을 선택합니다.
- **Save(**저장**)**를 클릭합니다.
- 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

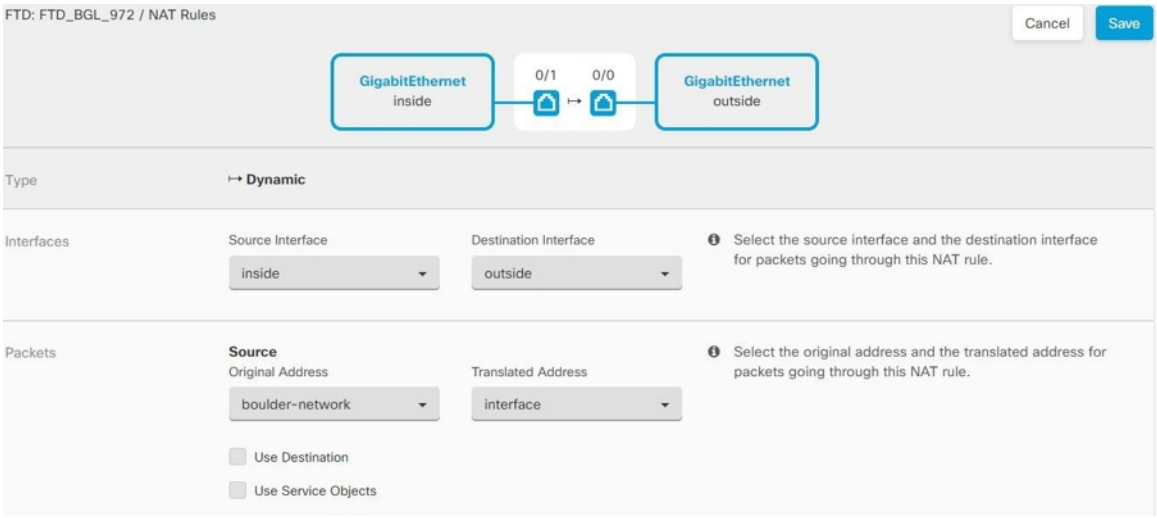
단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다. 참고: 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 구성 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 구성을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뜁니다.

a. **>** **Twice NAT(2**회 **NAT)**를 클릭합니다.

b. 섹션 1에서 **Dynamic(**동적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

c. 섹션 2에서 **Source Interface(**소스 인터페이스**) = inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**) = outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

d. 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'interface'를 선택합니다.



e. **Save(**저장**)**를 클릭합니다.

f. 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **4** Security Cloud Control에 구성 변경 사항을 구축합니다. 자세한 내용은 Security Cloud Control에서 FTD로 구성 변경 사항 구축을 참조하십시오.

단계 **5** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

사이트 간 가상 프라이빗 네트워크 모니터링

Security Cloud Control를 사용하면 온보드딩된 FDM 관리 디바이스에서 기존 또는 새로 생성된 사이트 간 VPN 구성을 모니터링, 수정 및 삭제할 수 있습니다.

사이트 간 **VPN** 터널 연결 확인

Check Connectivity(연결 확인**)** 버튼을 사용하여 터널에 대한 실시간 연결 확인을 트리거하여 터널이 현재 활성 상태인지 유휴 상태인지를 식별합니다. 온디맨드 연결 확인 버튼을 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 1시간에 한 번 수행됩니다.

Note

- Security Cloud Control는 FTD에서 이 연결성 검사 명령을 실행하여 터널이 활성 상태인지 유휴 상태인지를 확인합니다.

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- 모델 ASA 디바이스 터널은 항상 유휴로 표시됩니다.

VPN 페이지에서 터널 연결을 확인하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **2** 사이트 간 VPN 터널에 대한 터널 목록을 검색 및 필터링하고 선택합니다.

단계 **3** 오른쪽의 작업 창에서 **Check Connectivity(**연결 확인**)**를 클릭합니다.

사이트 간 **VPN** 대시보드

Security Cloud Control에서는 테넌트에서 생성된 사이트 간 VPN 연결에 대한 통합 정보를 제공합니다.

1. 왼쪽 창 에서 **Secure Connections** (보안 연결) > **Site to Site VPN(**사이트 간 **VPN**)을 클릭합니다. 사이트 간 **VPN**은 다음 위젯의 정보를 제공합니다.

   - **Sessions and Insights(**세션 및 인사이트**)**: 활성 VPN 터널 및 유휴 VPN 터널을 나타내는 막대 그래프를 적절한 색상으로 표시합니다.
   - **Issues(**문제**)**: 문제로 탐지된 총 터널 수를 표시합니다.
   - **Pending Deploy(**구축 보류**)**: 보류 중인 구축이 있는 총 터널 수를 표시합니다.

원형 차트 또는 위젯의 링크를 클릭하면 선택한 값에 따라 필터가 적용된 사이트 간 VPN 목록 페이지가 표시됩니다. 예를 들어 **VPN** 터널 상태 위젯에서 **Active VPN Tunnels(**활성 **VPN** 터널**)**을 클릭하면 활성 상태 필터가 적용된 사이트 간 VPN 목록 페이지로 이동하며 활성 터널만 표시됩니다.

VPN 문제 식별

Security Cloud Control는 FTD에서 VPN 문제를 식별할 수 있습니다. (이 기능은 아직 AWS VPC 사이트 간 VPN 터널에 사용할 수 없습니다.) 이 문서에서는 다음을 설명합니다.

- 누락된 피어가 있는 VPN 터널 찾기
- 암호화 키 문제가 있는 VPN 피어 찾기
- 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기

- 터널 구성에서 문제 찾기

터널 구성 문제 해결, on page 50

누락된 피어가 있는 VPN 터널 찾기

"Missing IP Peer" 상태는 FDM 관리 디바이스보다 ASA 디바이스에서 발생할 가능성이 높습니다.

Procedure

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table View(**테이블 보기**)**를 선택합니다.

단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 4 감지된 문제를 확인합니다.

단계 5 문제 ⚠를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 하나의 피어 이름이 나열됩니다. Security Cloud Control는 다른 피어 이름을 "[Missing peer IP.]"로 보고합니다.

암호화 키 문제가 있는 VPN 피어 찾기

이 접근 방식을 사용하여 다음과 같은 암호화 키 문제가 있는 VPN 피어를 찾습니다.

- IKEv1 또는 IKEv2 키가 잘못되었거나 누락되었거나 일치하지 않습니다.
- 사용되지 않거나 낮은 암호화 터널

Procedure

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table View(**테이블 보기**)**를 선택합니다.

단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 4 문제 ⚠를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.

단계 5 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭합니다.

단계 6 Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 7 하단의 Tunnel Details(터널 세부 정보) 창에서 **Key Exchange(**키 교환**)**를 클릭합니다. 두 디바이스를 모두 보고 해당 지점에서 주요 문제를 진단할 수 있습니다.

터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기

"불완전하거나 잘못 구성된 액세스 목록" 상태는 ASA 디바이스에서만 발생할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 **4** 문제 ⚠를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.

단계 **5** 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭합니다.

단계 **6** Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 **7** 하단의 Tunnel Details(터널 세부 정보) 패널에서 **Tunnel Details(**터널 세부 정보**)**를 클릭합니다. "Network Policy: Incomplete(네트워크 정책: 완료되지 않음)" 메시지가 표시됩니다.

터널 구성에서 문제 찾기

터널 구성 오류는 다음 시나리오에서 발생할 수 있습니다.

- 사이트 간 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 **4** 터널 문제에서 탐지된 문제를 클릭하여 오류를 보고하는 VPN 구성을 봅니다. 구성 보고 문제 ⚠를 볼 수 있습니다.

단계 **5** VPN 구성 보고 문제를 선택합니다.

단계 **6** 오른쪽의 피어 창에 문제가 있는 피어에 대한 ⚠ 아이콘이 나타납니다. ⚠ 아이콘 위로 마우스를 가져가면 문제와 해결 방법을 볼 수 있습니다.

다음 단계: 터널 구성 문제 해결.

터널 구성 문제 해결

이 절차는 다음과 같은 터널 구성 문제를 해결하려고 시도합니다.

- 사이트 간 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

자세한 내용은 터널 구성에서 문제 찾기를 참조하십시오.

프로시저

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 적절한 디바이스 유형 탭을 클릭하고 문제를 보고하는 VPN 구성과 연결된 디바이스를 선택합니다.
단계 **4** 디바이스 변경 사항을 수락합니다.
단계 **5** 왼쪽 창에서, **VPN** > **ASA/FDM** 사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.
단계 **6** 이 문제를 보고하는 VPN 구성을 선택합니다.
단계 **7** **Actions(**작업**)**창에서 **Edit**(편집) 아이콘을 클릭합니다.
단계 **8** 4단계에서 **Finish(**마침**)** 버튼을 클릭할 때까지 각 단계에서 **Next(**다음**)**를 클릭합니다.
단계 **9** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

사이트 간 **VPN** 터널 검색 및 필터링

필터 사이드바 를 검색 필드와 함께 사용하여 VPN 터널 다이어그램에 표시된 VPN 터널 검색에 집중할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** 필터 아이콘 을 클릭하여 필터 창을 엽니다.
단계 **3** 다음 필터를 사용하여 검색을 구체화합니다.

- **Filter by Device(**디바이스별 필터링**)** - **Filter by Device(**디바이스별 필터링**)**를 클릭하고 디바이스 유형 탭을 선택한 후 필터링을 통해 찾으려는 디바이스를 선택합니다.
- **Tunnel Issues(**터널 문제**)** - 터널의 양쪽에 문제가 있음을 탐지했는지 여부입니다. 디바이스에 문제가 있는 몇 가지 예로는 연결된 인터페이스 또는 피어 IP 주소 또는 액세스 목록 누락, IKEv1 제안 불일치 등이 있습니다(AWS VPC VPN 터널에서는 터널 문제 탐지를 아직 사용할 수 없음).

- **Devices/Services(**디바이스/서비스**)** -디바이스 유형을 기준으로 필터링합니다.
- **Status(**상태**)** – 터널 상태는 활성 또는 유휴 상태일 수 있습니다.
  - **Active(**활성**)** - 네트워크 패킷이 VPN 터널을 통과하는 열린 세션이 있거나 성공적인 세션이 설정되었고 아직 시간 초과되지 않았습니다. Active(활성)는 터널이 활성 상태이고 관련성이 있음을 나타내는 데 도움이 될 수 있습니다.
  - 유휴 - Security Cloud Control는 이 터널에 대해 열려 있는 세션을 검색할 수 없습니다. 터널이 사용 중이 아니거나 이 터널에 문제가 있을 수 있습니다.
- **Onboarded(**온보딩됨**)** - Security Cloud Control에서 디바이스를 관리하거나 Security Cloud Control에서 관리하지 않을 수 있습니다(관리되지 않음).
  - **Managed(**관리됨**)** - Security Cloud Control가 관리하는 디바이스별로 필터링합니다.
  - **Unmanaged(**관리되지 않음**)** - Security Cloud Control가 관리하지 않는 디바이스로 필터링합니다.
- **Device Types(**디바이스 유형**)** - 터널의 한쪽이 라이브(연결된 디바이스) 디바이스인지 아니면 모델 디바이스인지 여부입니다.

단계 **4** 검색 창에 디바이스 이름 또는 IP 주소를 입력하여 필터링된 결과를 검색할 수도 있습니다. 검색은 대/소문자를 구분하지 않습니다.

관리되지 않는 사이트 간 **VPN** 피어 온보딩

Security Cloud Control는 피어 중 하나가 온보딩될 때 사이트 간 VPN 터널을 검색 합니다. 두 번째 피어가 Security Cloud Control에서 관리되지 않는 경우 VPN 터널 목록을 필터링하여 관리되지 않는 디바이스를 찾아 온보딩할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3**  를 클릭하여 필터 패널을 엽니다.

단계 **4** **Unmanaged(**관리되지 않음**)**를 선택합니다.

단계 **5** 결과의 테이블에서 터널을 선택합니다.

단계 **6** 오른쪽의 **Peers(**피어**)** 창에서 **Onboard Device(**온보드 디바이스**)**를 클릭하고 화면의 지침을 따릅니다.

관련 정보**:**

- Security Cloud Control에 디바이스 온보딩
- 디바이스 온보딩

사이트 간 VPN 터널의 IKE 개체 세부 정보 보기

선택한 터널의 피어/디바이스에 구성된 IKE 개체의 세부 정보를 볼 수 있습니다. 이러한 세부 정보는 IKE 정책 개체의 우선 순위에 따라 계층 구조의 트리 구조로 나타납니다.

Note 엑스트라넷 디바이스는 IKE 개체 세부 정보를 표시하지 않습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **VPN Tunnels(VPN** 터널**)** 페이지에서 피어를 연결하는 VPN 터널의 이름을 클릭합니다.

단계 **3** 오른쪽의 **Relationships(**관계**)** 아래에 세부 정보를 보려는 개체를 확장합니다.

마지막으로 성공한 사이트 간 VPN 터널 설정 날짜 보기

이 정보는 일반적으로 VPN 터널이 마지막으로 성공적으로 설정된 날짜와 시간을 제공하여 두 사이트 간의 연결성을 보장합니다. 이 데이터에 접근하면 VPN 상태를 모니터링하고 발생할 수 있는 연결 문제를 해결하는 데 도움이 될 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **VPN Tunnels(VPN** 터널**)** 페이지에는 매니지드 디바이스에 구성된 모든 사이트 간 VPN 터널이 표시됩니다. 터널을 클릭하여 오른쪽 창 에서 추가 세부 정보를 볼 수 있습니다.

Note
Search and Filter Site-to-Site VPN Tunnels(사이트 간 VPN 터널 검색 및 필터링)를 사용하여 특정 터널을 찾습니다.

Last Active(마지막 활성**)** 필드에는 VPN 터널이 성공적으로 설정된 날짜와 시간이 표시됩니다.

사이트 간 VPN 터널 정보 보기

사이트 간 VPN 테이블 보기는 Security Cloud Control에 온보딩된 모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 전체 목록입니다. 터널은 이 목록에 한 번만 존재합니다. 테이블에 나열된 터널을 클릭하면 추가 조사를 위해 터널의 피어로 직접 이동할 수 있는 옵션이 오른쪽 사이드바에 제공됩니다.

Security Cloud Control가 터널의 양쪽을 모두 관리하지 않는 경우 Onboard Device(디바이스 온보딩)를 클릭하여 언매니지드 피어의 온보드 기본 온보딩 페이지를 열 수 있습니다. Security Cloud Control가 터널의 양쪽을 모두 관리하는 경우 Peer 2(피어 2) 열에 매니지드 디바이스의 이름이 포함됩니다. 그러나 AWS VPC의 경우 Peer 2 열에 VPN 게이트웨이의 IP 주소가 포함됩니다.

테이블 보기에서 사이트 간 VPN 연결을 보려면 다음을 수행합니다.

Procedure

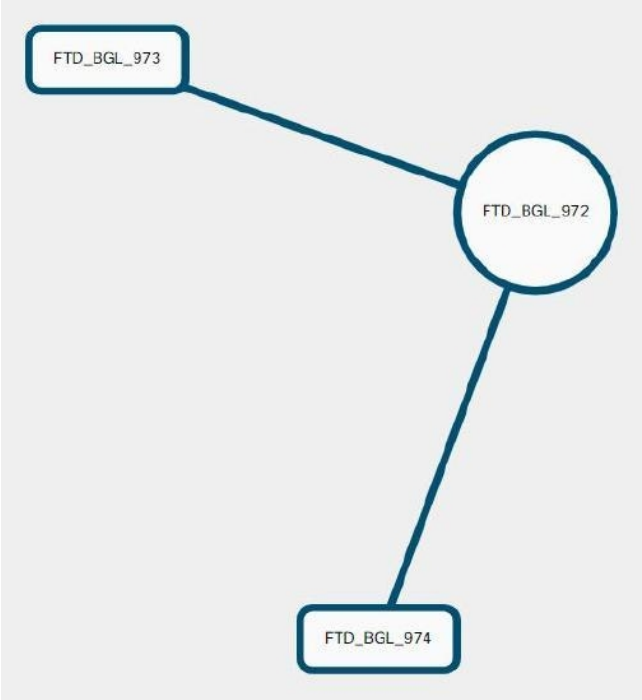
단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **VPN Tunnels(VPN** 터널**)** 페이지에는 매니지드 디바이스에 구성된 모든 사이트 간 VPN 터널이 표시됩니다. 터널을 클릭하여 오른쪽 창 에서 추가 세부 정보를 볼 수 있습니다.

Note
Search and Filter Site-to-Site VPN Tunnels(사이트 간 VPN 터널 검색 및 필터링)를 사용하여 특정 터널을 찾습니다.

사이트 간 VPN 전역 보기

다음은 전역 보기의 예입니다. 그림에서 'FTD_BGL_972'에는 FTD_BGL_973 및 FTD_BGL_974 디바이스와의 사이트 간 연결이 있습니다.



Procedure

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭합니다.

단계 2 **Global view(**전역 보기**)** 버튼을 클릭합니다.

단계 3 Search and Filter Site-to-Site VPN Tunnels(사이트 간 VPN 터널 검색 및 필터링)를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

단계 4 전역 보기에 표시된 피어 중 하나를 선택합니다.

단계 5 **View Details(**세부사항 보기**)**를 클릭합니다.

단계 6 VPN 터널의 다른 쪽 끝을 클릭하면 Security Cloud Control에 해당 연결에 대한 Tunnel Details(터널 세부 정보), NAT Information(NAT 정보) 및 Key Exchange(키 교환) 정보가 표시됩니다.

- **Tunnel Details(**터널 세부 정보**)** - 터널에 대한 이름 및 연결 정보를 표시합니다. Refresh(새로 고침) 아이콘을 클릭하면 터널에 대한 연결 정보가 업데이트됩니다.
- **Tunnel Details specific to AWS connections(AWS** 연결 관련 터널 세부 정보**)** -AWS 사이트 간 연결에 대한 터널 세부 정보는 다른 연결과 약간 다릅니다. AWS VPC에서 VPN 게이트웨이로의 각 연결에 대해 AWS는 2개의 VPN 터널을 생성합니다. 이는 고가용성을 위한 것입니다.
  - 터널의 이름은 VPN 게이트웨이가 연결된 VPC의 이름을 나타냅니다. 터널에 이름이 지정된 IP 주소는 VPN 게이트웨이가 VPC로 인식하는 IP 주소입니다.

- Security Cloud Control 연결 상태가 **active(**활성**)**로 표시되면 AWS 터널 상태가 **Up(**가동 중**)**입니다. Security Cloud Control 연결 상태가 **inactive(**비활성**)**인 경우 AWS 터널 상태는 **Down(**중단**)**입니다.

- **NAT Information(NAT** 정보**)** - 사용 중인 NAT 규칙의 유형, 원래 및 변환된 패킷 정보를 표시하고, 해당 터널에 대한 NAT 규칙을 볼 수 있는 NAT 테이블에 대한 링크를 제공합니다. (AWS VPC 사이트 간 VPN에는 아직 사용할 수 없습니다.)
- **Key Exchange(**키 교환**)** - 터널 및 키 교환 문제에서 사용 중인 암호화 키를 표시합니다. (AWS VPC 사이트 간 VPN에는 아직 사용할 수 없습니다.)

사이트 간 **VPN** 터널 창

Tunnels(터널) 창에는 특정 VPN 게이트웨이와 연결된 모든 터널의 목록이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 사이트 간 VPN 연결의 경우, tunnels(터널) 창에는 VPN 게이트웨이에서 VPC로의 모든 터널이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 각 사이트 간 VPN 연결에는 2개의 터널이 있으므로 다른 디바이스에 대해 일반적으로 표시되는 터널 수가 두 배입니다.

VPN 게이트웨이 세부 정보

VPN 게이트웨이에 연결된 피어의 수 및 VPN 게이트웨이의 IP 주소를 표시합니다. 이는 VPN Tunnels(VPN 터널) 페이지에만 표시됩니다.

피어 보기

사이트 간 VPN 피어 쌍을 선택하면 Peers(피어) 창에 쌍의 두 디바이스가 나열되며 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭할 수 있습니다. **View Peers(**피어 보기**)**를 클릭하면 디바이스가 연결된 다른 사이트 간 피어가 표시됩니다. 이는 Table(테이블) 보기 및 Global(전역) 보기에 표시됩니다.

Security Cloud Control 사이트 간 VPN 터널 삭제

Procedure

단계 **1** 왼쪽 창 에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** 삭제할 원하는 사이트 간 VPN 터널을 선택합니다.

단계 **3** 오른쪽의 **Actions(**작업**)** 창에서 **Delete(**삭제**)**를 클릭합니다.

선택한 사이트 간 VPN 터널이 삭제됩니다.

원격 액세스 가상 프라이빗 네트워크 소개

사용자는 원격 액세스 VPN(원격 액세스 가상 프라이빗 네트워크) 기능을 통해 물리적 사무실 건물 외부의 위치에서 기업 네트워크에 연결할 수 있습니다. 즉, 사용자는 인터넷에 연결되어 있는 지원되는 iOS/ Android 디바이스 또는 컴퓨터를 사용하여 네트워크 리소스에 안전하게 액세스 수 있습니다. 이 기능은 데이터를 안전하게 보호하면서 홈 네트워크 또는 공용 Wifi 네트워크 에서 연결해야 하는 모바일 근무자에게 특히 유용합니다.

관련 정보:

-
- FTD에 대한 원격 액세스 VPN 구성

FDM 매니지드 디바이스에 대한 원격 액세스 VPN 구성

Security Cloud Control는 새로운 원격 액세스 VPN(Remote Access Virtual Private Network)을 구성하기 위한 직관적인 사용자 인터페이스를 제공합니다. 또한 Security Cloud Control에 온보딩된 여러 FDM 관리 디바이스에 대해 원격 액세스 VPN 연결을 빠르고 쉽게 구성할 수 있습니다. AnyConnect는 FDM 관리 디바이스에 대한 RA VPN 연결을 위해 엔드포인트 디바이스에서 지원되는 유일한 클라이언트입니다.

AnyConnect 클라이언트는 FDM 관리 디바이스와 SSL VPN 연결을 협상할 때 TLS(Transport Layer Security: 전송 계층 보안) 또는 DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다. 클라이언트 및 FDM 관리 디바이스에서는 사용할 TLS/DTLS 버전을 협상합니다. 클라이언트가 지원하는 경우 DTLS가 사용됩니다.

Security Cloud Control는 FDM 관리 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- SSL 클라이언트 기반 원격 액세스
- IPv4 및 IPv6 주소 지정
- 여러 FDM 관리 디바이스에서 공유 RA VPN 구성

Important 온보딩 FDM 관리 디바이스(소프트웨어 버전 6.7 이상에서 실행)에 SAML 서버가 인증 소스인 원격 액세스 VPN 구성이 포함된 경우, Security Cloud Control는 현재 릴리스에서 SAML 서버 개체를 관리하지 않으므로 연결 프로파일의 AAA 세부 정보를 채우지 않습니다. . 따라서 Security Cloud Control에서 이러한 원격 액세스 VPN 구성을 관리할 수 없습니다. 그러나 Security Cloud Control는 원격 액세스 VPN 연결 프로파일 및 연결된 신뢰할 수 있는 CA 인증서 및 SAML 서버 개체를 읽습니다.

관련 정보:

- RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어, on page 58
- FDM-관리 디바이스에 대한 말단 간 원격 액세스 VPN 구성 프로세스, on page 73

RA VPN 사용자를 위한 스플릿 터널링(헤어 피닝)

이 문서에서는 RA VPN에 대한 스플릿 터널링에 대해 설명합니다.

일반적으로 원격 액세스 VPN에서는 VPN 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 VPN 사용자가 RA VPN에 연결되어 있는 동안 외부 네트워크에 액세스하도록 허용할 수 있습니다. 이 기술을 스플릿 터널링 또는 헤어피닝이라고도 합니다. 스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수

있습니다. 스플릿 터널링은 FTD 디바이스의 네트워크 부하를 줄이고 외부 인터페이스의 대역폭을 늘립니다.

스플릿 터널 목록을 구성하려면 표준 액세스 목록 또는 확장 액세스 목록을 생성해야 합니다. 디바이스가 실행 중인 버전에 대해 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드 VPN(Virtual Private Network) 장의 외부 인터페이스에서 원격 액세스 **VPN** 사용자를 위한 외부 인터페이스에서 인터넷 액세스를 제공하는 방법**(**헤어 피닝**)** 섹션에 설명된 지침을 따르십시오. 실행 중입니다.

RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어

이 문서에서는 외부 RADIUS 서버 또는 그룹 정책에서 RA VPN 연결에 특성을 적용하는 방법에 대한 정보를 제공합니다.

외부 RADIUS 서버 또는 FDM 관리 디바이스에 정의된 그룹 정책에서 RA VPN 연결에 사용자 인증 속성(사용자 자격 또는 권한이라고도 함)을 적용할 수 있습니다. FDM 관리 디바이스에서 그룹 정책에 구성된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

FDM 관리 디바이스에서는 다음 순서로 속성을 적용합니다.

Procedure

단계 **1** 외부 AAA 서버에 정의된 사용자 속성 - 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이 속성을 반환합니다.

단계 **2** FDM 관리 디바이스에 구성된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=group-policy) 값을 반환하면, FDM 관리 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.

단계 **3** 연결 프로파일에서 할당한 그룹 정책 - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다. FDM 관리 디바이스에 처음 접속하는 모든 사용자는 이 그룹에 속하며, 이를 통해 AAA 서버에서 반환한 사용자 속성 또는 사용자에게 할당된 그룹 정책에 없는 모든 속성을 제공합니다.

FDM 관리 디바이스에서는 벤더 ID가 3076인 RADIUS 속성을 지원합니다. 사용하는 RADIUS 서버에 이러한 속성이 정의되지 않은 경우, 수동으로 정의해야 합니다. 특성을 정의하려면 특성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

다음 주제에서는 값이 RADIUS 서버에 정의되어 있는지 또는 값이 시스템에서 RADIUS 서버로 전송하는 값인지 여부에 따라 지원되는 속성을 설명합니다.

RADIUS 서버로 전송되는 속성

RADIUS 속성 146 및 150은 인증 및 권한 부여 요청을 위해 FDM 관리 디바이스에서 RADIUS 서버로 전송됩니다. 다음 속성 모두 어카운트 관리 시작, 중간 업데이트, 중단 요청을 위해 FDM 관리 디바이스에서 RADIUS 서버로 전송됩니다.

*Table 1: Secure Firewall Threat Defense*에서 *RADIUS*로 전송하는 속성

특성	특성	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
클라이언트 유형	150	정수	단일	VPN에 접속 중인 클라이언트의 유형: 2= AnyConnect 클라이언트 SSL VPN
세션 유형	151	정수	단일	연결 유형: 1 = AnyConnect Client SSL VPN
터널 그룹 이름	146	문자열	단일	FDM 관리 디바이스에 정의된 대로 세션을 설정하는 데 사용된 연결 프로파일의 이름입니다. 이름은 1~253자일 수 있습니다.

RADIUS 서버에서 수신한 속성

다음 사용자 권한 부여 속성은 RADIUS 서버에서 FDM 관리 디바이스로 전송됩니다.

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Access-List-Inbound	86	문자열	단일	두 Acess-List(액세스 목록) 속성 모두 FDM 관리 디바이스에 구성된 ACL의 이름을 따릅니다. 스마트 CLI 확장 액세스 목록 개체 유형을 사용해 Firewall Device Manager에서 이 ACL을 생성합니다(Firewall Device Manager에 로그인하고 **Device(**디바이스**)**> **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)**> **Objects(**개체**)** 선택). 이 ACL에서는 인바운드(FDM 관리 디바이스로 들어가는 트래픽) 또는 아웃바운드(FDM 관리 디바이스에서 나가는 트래픽) 방향으로 트래픽 플로우를 제어합니다.
Access-List-Outbound	87	문자열	단일	
Address-Pools	217	문자열	단일	RA VPN에 접속하는 클라이언트에 대한 주소 풀로 사용될 서브넷을 식별하는 FDM 관리 디바이스에 정의된 네트워크 개체의 이름입니다. **Objects(**개체**)** 페이지에서 네트워크 개체를 정의합니다.

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Banner1	15	문자열	단일	사용자가 로그인하면 표시할 배너입니다.
Banner2	36	문자열	단일	사용자가 로그인하면 표시할 배너의 두 번째 부분입니다. 배너2는 배너1에 추가됩니다.
Group-Policy	25	문자열	단일	연결에 사용할 그룹 정책입니다. RA VPN **Group Policy(**그룹 정책**)** 페이지에서 그룹 정책을 생성해야 합니다. 다음 형식 중 하나를 사용할 수 있습니다. • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	정수	단일	사용자가 설정할 수 있는 별도의 동시 연결 개수입니다(0~2147483647).
VLAN	140	정수	단일	사용자의 연결을 제한할 VLAN입니다(0~4094). 또한 FDM 관리 디바이스의 하위 인터페이스에 이 VLAN을 구성해야 합니다.

2단계 인증

RA VPN에 대한 2단계 인증을 구성할 수 있습니다. 2단계 인증의 경우, 사용자는 사용자 이름 및 정적 암호뿐 아니라 Duo 암호와 같은 추가 항목도 제공해야 합니다. 2단계 인증이 두 번째 인증 소스를 사

용하는 것과 다른 점은 두 가지 인증 요소가 기본 인증 소스와 연결된 Duo 서버와의 관계에 따라 단일 인증 소스에서 구성된다는 것입니다. 보조 인증 소스로 Duo LDAP 서버를 구성하는 Duo LDAP은 예외입니다.

- RADIUS를 사용하는 Duo 2단계 인증, 62 페이지
- LDAP를 사용하는 Duo 2단계 인증, 66 페이지

RADIUS를 사용하는 Duo 2단계 인증

듀오 RADIUS 서버를 기본 인증 소스로 구성할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다.

듀오를 구성하는 세부 절차는 https://duo.com/docs/cisco-firepower의 내용을 참조하십시오.

그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 Microsoft AD(Active Directory) 서버를 첫 번째 인증 요소로 사용하고 Duo 클라우드 서비스는 두 번째 요소로 사용하도록 Duo를 구성합니다.

이 접근 방식을 사용하는 경우, 사용자는 듀오 인증 프록시 및 연결된 RADIUS/AD 서버 둘 다에 구성된 사용자 이름과 RADIUS/AD 서버에 구성된 사용자 이름의 암호(다음 듀오 코드 중 하나가 바로 뒤에 나옴)를 사용해 인증해야 합니다.

Dou-passcode. 예: my-password,12345.

push. 예: *my-password*,**push**. **push(**푸시**)**를 사용하여 듀오에게 듀오 모바일 앱으로 푸시 인증을 전송하도록 지시합니다. 사용자는 이미 이 앱을 설치하여 등록했어야 합니다.

SMS. 예: *my-password*,**SMS**. SMS를 사용하여 듀오에게 사용자의 모바일 디바이스로 새로운 암호 배치가 포함된 SMS 메시지를 전송하도록 지시합니다. SMS를 사용하는 경우, 사용자의 인증 시도가 실패합니다. 그러면 사용자는 다시 인증하고 두 번째 요인으로 새 암호를 입력해야 합니다.

phone(전화**)**. 예: *my-password*,**phone**. 전화를 사용해 듀오에게 전화 콜백 인증을 수행하도록 지시합니다.

사용자 이름과 비밀번호가 인증된 경우 Duo Authentication Proxy는 Duo 클라우드 서비스에 연결하여 요청이 구성된 유효한 프록시 디바이스에서 왔는지 확인한 다음, 지시에 따라 사용자의 모바일 디바이스로 임시 패스코드를 푸시합니다. 사용자가 이 암호를 수락하면 듀오에서 세션을 인증된 것으로 표시하고 RA VPN이 설정됩니다.

자세한 설명은 Duo RADIUS를 사용하여 2단계 인증을 구성하는 방법, 62 페이지의 내용을 참조하십시오.

*Duo RADIUS*를 사용하여 *2*단계 인증을 구성하는 방법

듀오 RADIUS 서버를 기본 인증 소스로 구성할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다.

그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 AD 서버를 첫 번째 인증 요소로 사용하고 듀오 클라우드 서비스는 두 번째 요소로 사용하도록 구성합니다.

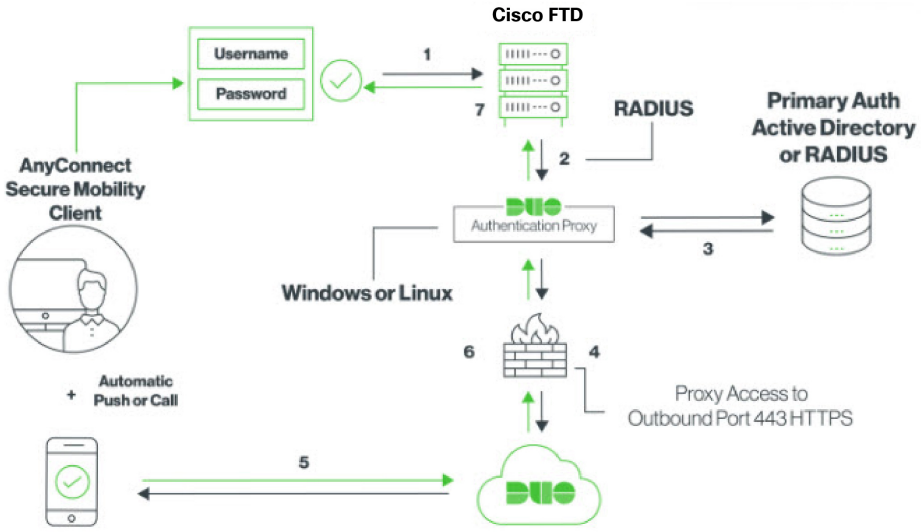
다음 주제에서는 구성에 대해 자세히 설명합니다.

- Duo RADIUS 보조 인증을 위한 시스템 플로우, 63 페이지

• Security Cloud Control을 사용하여 Duo RADIUS용 디바이스 구성, 64 페이지

Duo RADIUS 보조 인증을 위한 시스템 플로우

다음은 시스템 플로우에 대한 설명입니다



다.

1. 사용자는 FDM 관리 디바이스에 원격 액세스 VPN을 연결하고 RADIUS/AD 서버와 연결된 사용자 이름, RADIUS/AD 서버에 구성된 사용자 이름의 비밀번호, DUO 코드, Duo 비밀번호, 푸시, SMS 또는 전화 중 하나를 제공합니다. 자세한 정보는 RADIUS를 사용하는 Duo 2단계 인증, 62 페이지의 내용을 참조하십시오.
2. FDM 관리 디바이스에서 Duo Authentication Proxy에 인증 요청을 전송합니다.
3. Duo Authentication Proxy에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.
4. 자격 증명이 인증되면 Duo Authentication Proxy가 TCP 포트 443을 통해 Duo Security에 연결됩니다.
5. 그런 다음 Duo에서 푸시 알림, 패스코드를 사용한 문자 메시지 또는 전화 통화를 통해 사용자를 개별적으로 인증합니다. 사용자는 이 인증을 성공적으로 완료해야 합니다.
6. Duo Authentication Proxy가 인증 응답을 수신합니다.
7. 보조 인증에 성공하면 FDM 관리 디바이스에서 사용자의 AnyConnect 클라이언트와 원격 액세스 VPN 연결을 설정합니다.

Duo RADIUS 보조 인증 구성

Duo Authentication Proxy에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.

Duo 어카운트 생성

Duo 어카운트를 생성하고 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다.

프로세스는 간단히 다음과 같습니다. 자세한 내용은 Duo 웹 사이트를 참조하십시오.

프로시저

단계 **1** Duo 어카운트에 등록합니다.

단계 **2** Duo Admin Panel에 로그인하여 **Applications(**애플리케이션**)**로 이동합니다.

단계 **3** 애플리케이션 목록에서 **Protect an Application(**애플리케이션 보호**)**을 클릭하고 **Cisco Firepower Threat Defense VPN**을 찾습니다.

단계 **4** **Protect this Application(**이 애플리케이션 보호**)**을 클릭하여 통합 키, 암호 키 및 API 호스트 이름을 가져옵니다. 프록시를 구성할 때 이 정보가 필요합니다. 도움이 필요한 경우 *Duo* 시작하기 가이드 (https://duo.com/docs/getting-started)를 참조하십시오.

단계 **5** Duo 인증 프록시를 설치하고 구성합니다. 자세한 내용은 https://duo.com/docs/cisco-firepower의 "Duo Authentication Proxy 설치" 섹션을 참조하십시오.

단계 **6** 인증 프록시를 시작합니다. 자세한 내용은 https://duo.com/docs/cisco-firepower의 "프록시 시작" 섹션을 참조하십시오.

Duo에 새 사용자를 등록하는 방법은 https://duo.com/docs/enrolling-users를 참조하십시오.

Security Cloud Control을 사용하여 Duo RADIUS용 디바이스 구성

프로시저

단계 **1** FTD Radius 서버 개체를 구성합니다.

a) 왼쪽 창에서 개체를 클릭합니다.

b)  > **RA VPN Objects (ASA & FTD)(RA VPN** 개체**(ASA** 및 **FTD))** > **Identity Source(ID** 소스**)**를 클릭합니다.

c) 이름을 입력하고 **Device Type(**디바이스 유형**)**을 **FTD**로 설정합니다.

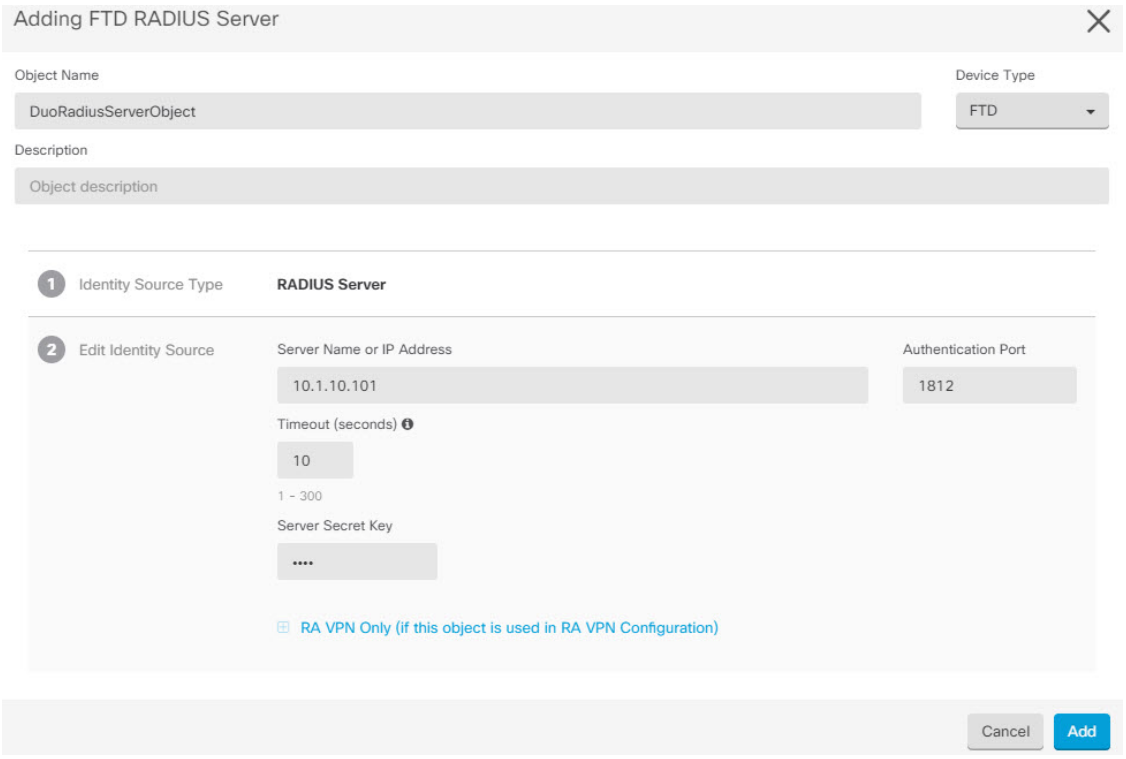
d) **Radius Server Group(Radius** 서버 그룹**)**을 선택하고 **Continue(**계속**)**를 클릭합니다.

자세한 내용은 RADIUS 서버 그룹 생성의 6단계를 참조하십시오.

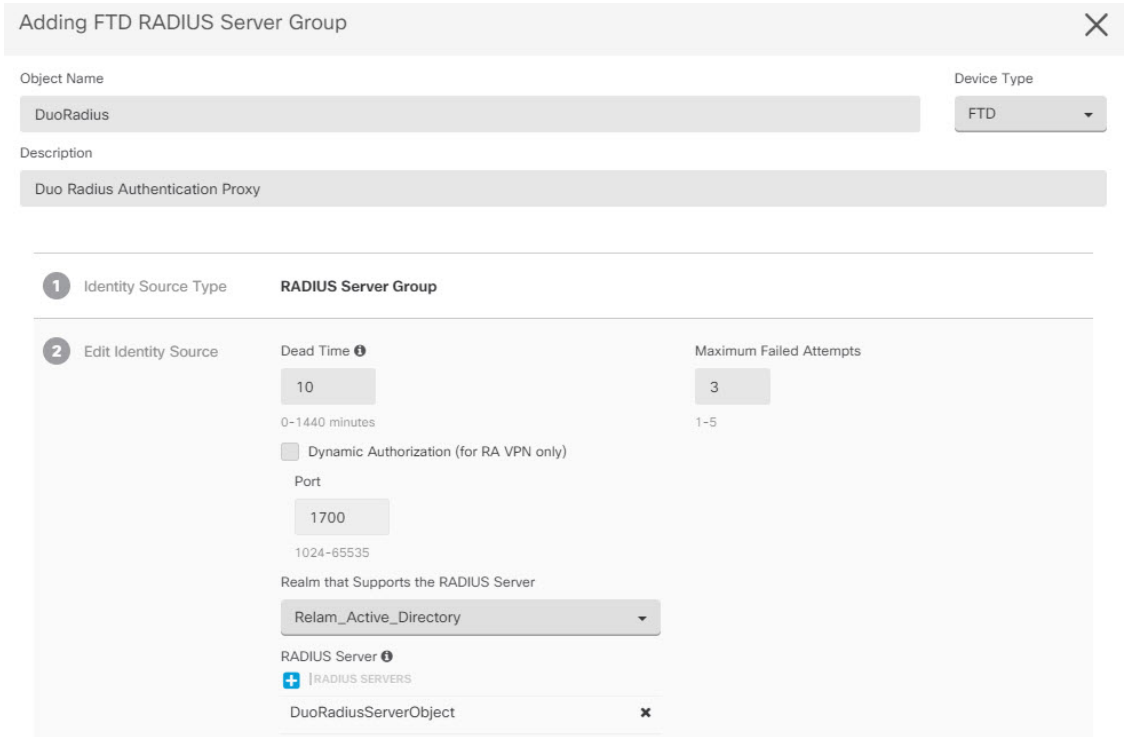
e) **Radius Server(Radius** 서버**)** 섹션에서 **Add(**추가**)** 버튼을 클릭하고 **Create New Radius Server(**새 **Radius** 서버 생성**)**를 클릭합니다.

RADIUS 서버 개체 생성을 참조하십시오.

Server Name(서버 이름**)** 또는 **IP Address(IP** 주소**)** 필드에 Duo Authentication Proxy 서버의 정규화된 호스트 이름 또는 IP 주소를 입력합니다.



f) Duo RADIUS 서버를 그룹에 추가했으면 **Add(**추가**)**를 클릭하여 새 Duo RADIUS 서버 그룹을 생성합니



단계 **2** Remote Access VPN Authentication Method(원격 액세스 VPN 인증 방법)를 Duo RADIUS로 변경합니다.

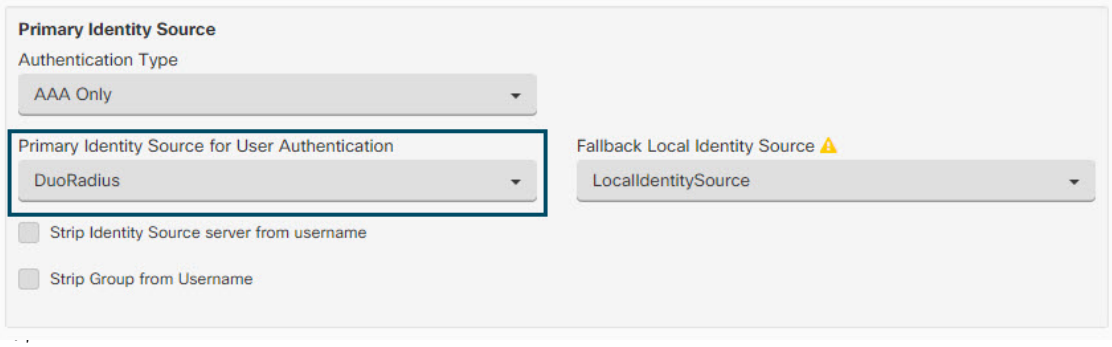
a) 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 클릭합니다.

b) VPN 구성을 확장하고 Duo를 추가할 연결 프로파일을 클릭합니다.

c) 오른쪽의 **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.

d) **Authentication Type(**인증 유형**)**은 **AAA** 또는 **AAA and Client Certificate(AAA** 및 클라이언트 인증서**)**가 될 수 있습니다.

e) **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)** 목록에서 이전에 생성한 서버 그룹을 선택합니



f) 일반적으로 "Authorization Server(권한 부여 서버)" 또는 "Accounting Server(과금 서버)"를 선택할 필요가 없습니다.

g) **Continue(**계속**)**를 클릭합니다.

h) **Summary and Instructions(**요약 및 지침**)** 단계에서 **Done(**완료**)**을 클릭하여 구성을 저장합니다.

단계 **3** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

LDAP를 사용하는 Duo 2단계 인증

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 패스코드, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

참고 Duo 2단계 인증 기능은 Firepower Threat 6.5 이상 버전을 실행하는 디바이스의 Security Cloud Control에서 사용할 수 있습니다.

FDM 관리 디바이스에서는 TCP/636 포트를 통해 LDAPS를 사용하여 Duo LDAP과 통신합니다.

이 접근 방식을 사용하는 경우 사용자는 AD/RADIUS 서버 및 Duo LDAP 서버에 구성된 사용자 이름을 사용하여 인증해야 합니다. AnyConnect에서 로그인하라는 프롬프트가 표시되면 사용자는 기본 Password(비밀번호) 필드에 AD/RADIUS 비밀번호를 입력하고 Secondary Password(보조 비밀번호)에는 Duo를 사용하여 인증하기 위해 다음 중 하나를 입력합니다. 자세한 내용은 https://guide.duo.com/anyconnect의 "요소 선택을 위한 두 번째 비밀번호" 섹션을 참조하십시오.

- *Duo passcode(Duo 암호)* - Duo Mobile을 통해 생성되었거나 SMS를 통해 전송되었거나 하드웨어 토큰에 의해 생성되었거나 관리자가 제공한 암호를 사용하여 인증합니다. 예: 1234567.
- **push(푸시)** - Duo Mobile 앱을 설치하고 활성화한 경우 전화기에 로그인 요청을 푸시합니다. 요청을 검토하고 **Approve(승인)**를 눌러 로그인합니다.
- **phone(전화기)** - 전화기 콜백을 사용하여 인증합니다.
- **sms** - 텍스트 메시지로 Duo 암호를 요청합니다. 로그인 시도가 실패합니다. 새 암호를 사용하여 다시 로그인합니다.

자세한 설명은 Duo LDAP를 사용하여 2단계 인증을 구성하는 방법, 67 페이지의 내용을 참조하십시오.

*Duo LDAP*를 사용하여 *2*단계 인증을 구성하는 방법

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 패스코드, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

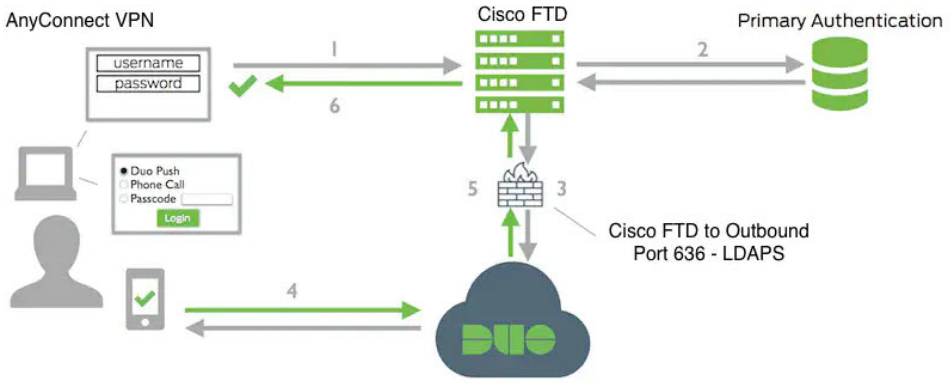
다음 주제에서는 구성에 대해 자세히 설명합니다.

- Duo LDAP 보조 인증을 위한 시스템 플로우, 67 페이지
- Duo LDAP 보조 인증 구성, 68 페이지

Duo LDAP 보조 인증을 위한 시스템 플로우

다음 그래픽에는 LDAP를 사용하여 2단계 인증을 제공하기 위해 Firewall Threat Defense 및 Duo가 함께 작동하는 방법이 나와 있습니다.

다음은 시스템 플로우에 대한 설명입니다.



1. 사용자는 FDM 관리 디바이스에 대한 원격 액세스 VPN 연결을 설정하고 사용자 이름과 비밀번호를 입력합니다.
2. FDM 관리 디바이스에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.

3. 기본 인증이 작동하는 경우 FDM 관리 디바이스에서는 보조 인증에 대한 요청을 Duo LDAP 서버로 전송합니다.
4. 그런 다음 Duo에서 푸시 알림, 패스코드를 사용한 문자 메시지 또는 전화 통화를 통해 사용자를 개별적으로 인증합니다. 사용자는 이 인증을 성공적으로 완료해야 합니다.
5. Duo에서는 사용자가 성공적으로 인증되었는지 여부를 나타내기 위해 FDM 관리 디바이스에 응답합니다.
6. 보조 인증에 성공하면 FDM 관리 디바이스에서 사용자의 AnyConnect 클라이언트와 원격 액세스 VPN 연결을 설정합니다.

Duo LDAP 보조 인증 구성

다음 절차에서는 Duo LDAP를 보조 인증 소스로 사용하여 원격 액세스 VPN에 2단계 인증을 구성하는 엔드 투 엔드 프로세스에 대해 설명합니다. 이 구성을 완료하려면 Duo를 사용하는 어카운트가 있어야 하며 Duo에서 일부 정보를 얻어야 합니다.

Duo 어카운트 생성

Duo 어카운트를 생성하고 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다.

프로세스는 간단히 다음과 같습니다. 자세한 내용은 Duo 웹 사이트를 참조하십시오.

프로시저

단계 **1** Duo 어카운트에 등록합니다.

단계 **2** Duo Admin Panel에 로그인하여 **Applications(**애플리케이션**)**로 이동합니다.

단계 **3** 애플리케이션 목록에서 **Protect an Application(**애플리케이션 보호**)**을 클릭하고 **Cisco Firepower Threat Defense VPN**을 찾습니다.

단계 **4** **Protect this Application(**이 애플리케이션 보호**)**을 클릭하여 통합 키, 암호 키 및 **API** 호스트 이름을 가져옵니다. 도움이 필요한 경우 *Duo* 시작하기 가이드(https://duo.com/docs/getting-started)를 참조하십시오.

Duo에 새 사용자를 등록하는 방법은 https://duo.com/docs/enrolling-users를 참조하십시오.

FDM-관리 디바이스에 신뢰할 수 있는 CA 인증서 업로드

FDM 관리 디바이스에는 Duo LDAP 서버에 대한 연결을 검증하는 데 필요한 신뢰할 수 있는 CA 인증서가 있어야 합니다. https://www.digicert.com/digicert-root-certificates.htm으로 직접 이동하여 **DigiCertSHA2HighAssuranceServerCA** 또는 **DigiCert High Assurance EV** 루트 **CA**를 다운로드하고 Firewall Device Manager(FDM)을 사용하여 업로드할 수 있습니다.

프로시저

단계 1 FDM 관리 디바이스의 Firewall Device Manager 페이지에 액세스하여 **Objects(**개체**)** > **Certificates(**인증서**)**를 선택합니다.

단계 2 **+** > **Add Trusted CA Certificate(**신뢰받는 **CA** 인증서 추가**)**를 클릭합니다.

단계 3 인증서의 이름(예: DigiCert_High_Assurance_EV_Root_CA)을 입력합니다. 공백은 허용되지 않습니다.

단계 4 **Upload Certificate(**인증서 업로드**)**를 클릭하고 다운로드한 파일을 선택합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

단계 6 아직 온보딩하지 않은 경우 Security Cloud Control에 디바이스를 온보딩합니다.

단계 7 FTD에서 Security Cloud Control로 구성 변경 사항 읽기

Security Cloud Control에서 Duo LDAP용 FTD 구성

프로시저

단계 1 Duo LDAP 서버의 Duo LDAP ID 소스 개체를 생성합니다.

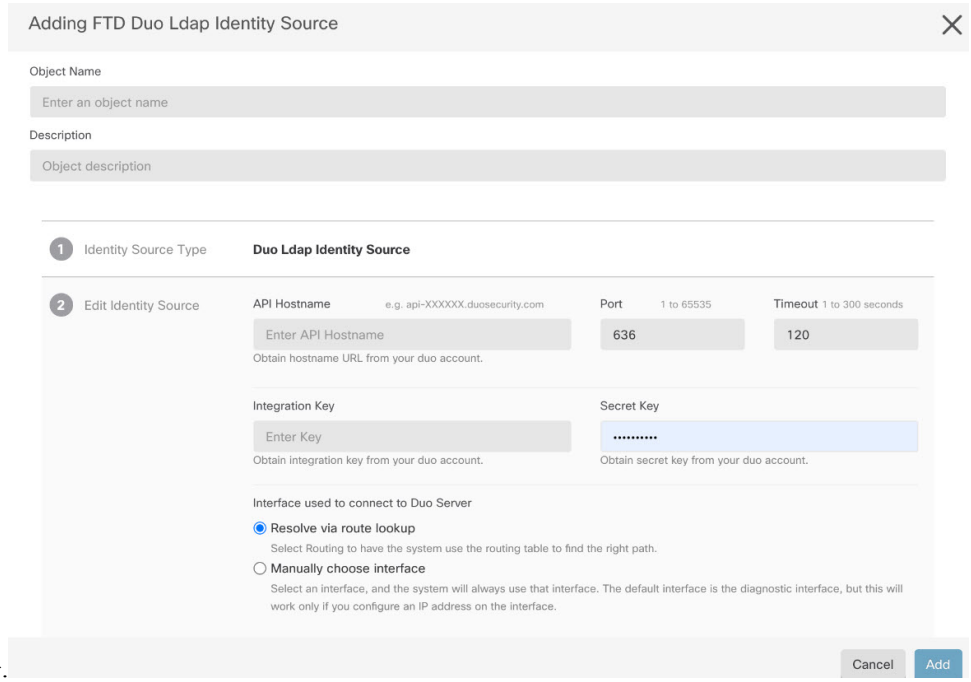
a) 왼쪽 Security Cloud Control 탐색 모음에서 개체를 클릭합니다.

b)  을 클릭하여 개체를 열고 **RA VPN Objects (ASA & FTD)(RA VPN** 개체**(ASA** 및 **FTD))** > **Identity Source(ID** 소스**)**를 클릭합니다.

c) 개체의 이름을 입력합니다(예: Duo-LDAP-server).

d) **Device Type(**디바이스 유형**)**을 **FTD**로 선택합니다.

e) **Duo LDAP Identity Source(Duo LDAP ID 소스)**를 클릭하고 **Continue(계속)**를 클릭합니



다.

f) **Edit Identity Source(ID 소스 편집)** 영역에서 다음 세부 정보를 입력합니다.

- **API Hostname(API 호스트 이름)**: Duo 어카운트에서 가져온 API 호스트 이름을 입력합니다. 호스트 이름은 X가 고유한 값으로 교체되면 API-XXXXXXXX.DUOSECURITY.COM과 유사하게 표시되어야 합니다. 대문자는 필요하지 않습니다.
- **Port(포트)**: LDAPS에 사용할 TCP 포트를 입력합니다. 포트는 다른 포트를 사용하도록 Duo에서 지시한 경우를 제외하고는 636이어야 합니다. 액세스 제어 목록에서 이 포트를 통해 Duo LDAP 서버에 대한 트래픽을 허용하는지 확인해야 합니다.
- **Timeout(시간 초과)**: Duo 서버에 연결할 시간 제한(초)을 입력합니다. 이 값은 1~300초일 수 있습니다. 기본값은 120입니다. 기본값을 사용하려면 120을 입력하거나 특성 줄을 삭제합니다.
- **Integration Key(통합 키)**: Duo 어카운트에서 가져온 통합 키를 입력합니다.
- **Secret Key(암호 키)**: Duo 어카운트에서 가져온 암호 키를 입력합니다. 이 키는 이후에 마스킹됩니다.
- **Interface used to connect to Duo Server(Duo 서버에 연결하는 데 사용되는 인터페이스)**: Duo 서버에 연결하는 데 사용할 인터페이스를 선택합니다.
  - **Resolve via route lookup(경로 조회를 통해 확인)**: 라우팅 테이블을 사용하여 올바른 경로를 찾으려면 이 옵션을 선택합니다. 라우팅 테이블을 생성하는 방법은 라우팅을 참조하십시오.
  - **Manually choose interface(수동으로 인터페이스 선택)**: 이 옵션을 선택하고 목록에서 인터페이스 중 하나를 선택합니다. 기본 인터페이스는 진단 인터페이스지만, 이는 인터페

이스의 IP 주소를 구성하는 경우에만 작동합니다. 참고: 선택한 인터페이스가 Duo 서버에 연결하려는 동일한 디바이스에 있는지 확인합니다.

- **Add(**추가**)**를 클릭합니다.

단계 **2** (선택 사항) 인증 시간 초과에 60초 이상을 지정하는 프로파일을 생성하려면 AnyConnect 프로파일 편집기를 사용합니다.

사용자에게 Duo 암호를 얻고 보조 인증을 완료할 추가 시간을 제공해야 합니다. 60초 이상 제공하는 것이 좋습니다. 다음 절차에서는 인증 시간 초과만 구성한 후 프로파일을 FDM 관리 디바이스에 업로드하는 방법에 대해 설명합니다. 다른 설정을 변경하려는 경우 지금 하면 됩니다.

a) 아직 작업을 수행하지 않은 경우, AnyConnect 프로파일 편집기 패키지를 다운로드하여 설치합니다. 이는 Cisco Software Center(software.cisco.com)(AnyConnect 버전용 폴더)에서 찾을 수 있습니다. 이 문서를 작성할 시점의 기본 경로는 **Downloads Home(**다운로드 홈**)** > **Security(**보안**)** > **VPN and Endpoint Security Clients(VPN** 및 엔드포인트 보안 클라이언트**)** > **Cisco VPN Clients(Cisco VPN** 클라이언트**)** > **AnyConnect Secure Mobility Client(AnyConnect Secure Mobility** 클라이언트**)** 입니다.

b) AnyConnect **VPN Profile Editor(VPN** 프로파일 편집기**)**를 엽니다.

c) 목차에서 **Preferences(Part 2)(**환경설정**(**파트 **2))**를 선택하고 페이지 끝으로 스크롤한 다음, **Authentication Timeout(**인증 시간 제한**)**을 60 이상으로 변경합니다. 다음 이미지는 AnyConnect 4.7 VPN 프로파일 편집기의 이미지입니다(이전 버전 또는 후속 버전의 경우 다를 수 있음).

d) **File(**파일**)** > **Save(**저장**)**를 선택하고 프로파일 XML 파일을 적절한 이름(예: duo-ldap-profile.xml)의 워크스테이션에 저장합니다.

e) 이제 **VPN** 프로파일 편집기 애플리케이션을 닫으면 됩니다.

f) Security Cloud Control에서 원격 액세스 VPN AnyConnect 클라이언트 프로파일을 업로드합니다.

단계 **3** 그룹 정책을 생성하고 정책에서 AnyConnect 프로파일을 선택합니다.

사용자에게 할당하는 그룹 정책으로 인해 연결의 여러 측면이 제어됩니다. 다음 절차에서는 프로파일 XML 파일을 그룹에 할당하는 방법에 대해 설명합니다. 자세한 내용은 새 FTD RA VPN 그룹 정책 생성을 참조하십시오.

a) 왼쪽 Security Cloud Control 탐색 모음에서 개체를 클릭합니다.

b) 기존 그룹 정책을 편집하려면 **RA VPN** 그룹 정책 필터를 사용하여 기존 그룹 정책만 확인한 후 원하는 정책을 수정하고 저장합니다.

c) 새 그룹 정책을 생성하려면 **RA VPN Objects (ASA & FTD)(RA VPN** 개체**(ASA** 및 **FTD))** > **RA VPN Group Policy(RA VPN** 그룹 정책**)**를 클릭합니다.

d) **General(**일반**)** 페이지에서 다음 속성을 구성합니다.

- **Name(**이름**)** - 새 프로파일의 경우 이름을 입력합니다. 예를 들어, Duo-LDAP-group과 같이 입력합니다.
- **AnyConnect Client Profiles(AnyConnect** 클라이언트 프로파일**)** - 생성한 AnyConnect 클라이언트 프로파일 개체를 선택합니다.

e) **Add(**추가**)**를 클릭하여 개체를 저장합니다.

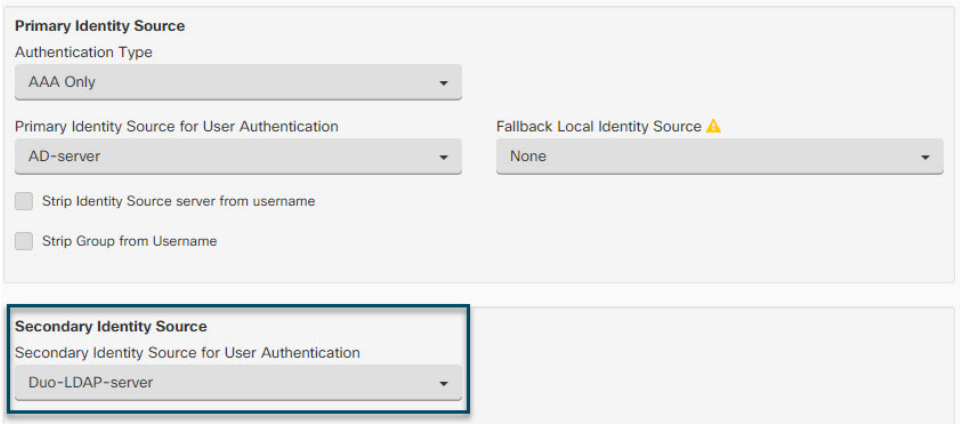
f) **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM** 버튼을 클릭합니다.
g) 업데이트할 원격 액세스 VPN 구성을 클릭합니다.
h) 오른쪽의 **Actions(**작업**)** 창에서 **Group Policies(**그룹 정책**)**를 클릭합니다.
i) +를 클릭하여 VPN 구성과 연결할 그룹 정책을 선택합니다.
j) **Save(**저장**)**를 클릭하여 그룹 정책을 저장합니다.

단계 **4** Duo-LDAP 보조 인증에 사용할 원격 액세스 VPN 연결 프로파일을 생성하거나 수정합니다.

다음 절차에서는 Duo-LDAP를 보조 인증 소스로 활성화하고 AnyConnect 클라이언트 프로파일을 적용하기 위한 주요 변경 사항에 대해서만 설명합니다. 새 연결 프로파일의 경우 나머지 필수 필드를 구성해야 합니다. 이 절차에서는 기존 연결 프로파일을 편집하는 중이며 이러한 두 가지 설정만 변경하면 된다고 가정합니다.

a) Security Cloud Control 내비게이션 페이지에서 **VPN** > **Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.
b) 원격 액세스 VPN 구성을 확장하고 업데이트할 연결 프로파일을 클릭합니다.
c) 오른쪽의 **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.
d) **Primary Identity Source(**기본 **ID** 소스**)** 아래에서 다음을 구성합니다.

- **Authentication Type(**인증 유형**)** - AAA Only(AAA 전용) 또는 AAA and Client Certificate(AAA 및 클라이언트 인증서) 중 하나를 선택합니다. AAA를 사용하지 않는 한, 2단계 인증을 구성할 수 없습니다.
- **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)** - 기본 Active Directory 또는 RADIUS 서버를 선택합니다. Duo-LDAP ID 소스를 기본 소스로 선택할 수 있습니다. 그러나 Duo-LDAP에서는 인증 서비스만 제공하며 ID 서비스는 제공하지 않습니다. 따라서 이를 기본 인증 소스로 사용하는 경우, 어떠한 대시보드에도 RA VPN 연결과 관련된 사용자 이름이 표시되지 않으며, 이러한 사용자에 대한 액세스 제어 규칙을 작성할 수 없게 됩니다. 원하는 경우 로컬 ID 소스로의 대체 기능을 구성할 수 있습니다.
- **Secondary Identity Source(**보조 **ID** 소스**)** - Duo-LDAP ID 소스를 선택합니다.



참고
Primary Identity Source(기본 **ID** 소스**)** 및 **Secondary Identity Source(**보조 **ID** 소스**)**의 사용자 이름이 동일한 경우, Connection Profile(연결 프로파일)의 **Advanced(**고급**)** 옵션에서 **Use**

Primary username for Secondary login(보조 로그인에 기본 사용자 이름 사용**)**을 활성화하는 것이 좋습니다. 이 방법으로 구성하면 엔드 유저는 기본 및 보조 ID 소스 모두에 단일 사용자 이름을 사용할 수 있습니다.

e) **Continue(**계속**)**를 클릭합니다.

f) **Group Policy(**그룹 정책**)** 페이지에서 사용자가 생성했거나 편집한 그룹 정책을 선택합니

g) **Continue(**계속**)**를 클릭합니다.

h) **Done(**완료**)**을 클릭하여 연결 프로파일에 변경 사항을 저장합니다.

단계 **5** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

FDM-관리 디바이스에 대한 말단 간 원격 액세스 VPN 구성 프로세스

이 섹션에서는 Security Cloud Control에 온보딩된 FDM 관리 디바이스에서 원격 액세스 가상 프라이빗망(RA VPN)을 구성하기 위한 엔드 투 엔드 절차를 제공합니다.

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스를 제공합니다.

Procedure

단계 **1** 두 개의 라이선스를 활성화합니다.

- 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager 어카운트를 사용하여 등록을 수행해야 합니다. 라이선스는 원격 액세스 VPN을 구성하기 전에 수출 통제 요구 사항을 충족해야 합니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다. FDM 관리 디바이스 구매에 라이선스가 자동으로 포함됩니다. 라이선스는 선택적 라이선스가 적용되지 않는 모든 기능을 포함합니다. 영구 라이선스입니다. 디바이스를 Secure Firewall Device Manager에 등록해야 합니다. 디바이스가 실행 중인 버전에 대해서는 Secure Firewall Threat Defense Cisco 구성 가이드의 시스템 라이선싱 장에서 디바이스 등록 섹션을 참조하십시오.
- 라이선스. 자세한 내용은 원격 액세스 VPN에 대한 라이선스 요구 사항을 참조하십시오.
  - 라이선스를 활성화하려면 디바이스가 실행 중인 버전에 대한 Secure Firewall Threat Defense 구성 가이드의 시스템 라이선스 섹션에서 선택적 라이선스 활성화 또는 비활성화 섹션을 참조하십시오.

단계 **2** 인증서를 구성합니다.

클라이언트와 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN에 대해 미리 정의된 DefaultInternalCertificate를 사용하거나 직접 만들 수 있습니다.

인증에 사용되는 디렉터리 영역에 대해 암호화된 연결을 사용하는 경우에는 신뢰할 수 있는 CA 인증서를 업로드해야 합니다. 인증서 및 업로드 방법에 대한 자세한 내용은 인증서 구성을 참조하십시오.

단계 **3** 원격 사용자 인증에 사용되는 ID 소스를 구성합니다.

다음 소스를 사용하여 RA VPN을 사용하여 네트워크에 연결을 시도하는 사용자를 인증할 수 있습니다. 또한 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- AD(Active Directory) ID 영역: 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성을 참조하십시오. Active Directory 영역 개체 생성 및 편집을 참조하십시오.
- RADIUS 서버 그룹: 기본 또는 보조 인증 소스로서, 권한 부여 및 어카운트 관리를 위한 것입니다. RADIUS 서버 개체 또는 그룹 만들기 또는 편집을 참조하십시오.
- Local Identity Source(로컬 사용자 데이터베이스): 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 설명한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다.

  Note
  Secure Firewall Device Manager에서만 FDM 관리 디바이스에서 직접 사용자 어카운트를 만들 수 있습니다. 로컬 사용자 구성을 참조하십시오.

단계 **4** (선택 사항). 새 RA VPN 그룹 정책을 생성합니다.

그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 구성할 수 있습니다. 또는 모든 연결에 기본 정책을 사용합니다.

단계 **5** RA VPN 구성을 생성합니다.

단계 **6** RA VPN 연결 프로파일을 구성합니다.

단계 **7** 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

단계 **8** 원격 액세스 VPN을 통한 트래픽을 허용합니다.

단계 **9** (선택 사항). ID 정책을 활성화하고 패시브 인증에 사용할 규칙을 생성합니다. 패시브 사용자 인증을 활성화하는 경우 원격 액세스 VPN을 통해 로그인한 사용자는 대시보드에 표시되며 정책에서 트래픽 일치 기준으로도 사용할 수 있게 됩니다. 패시브 인증을 활성화하지 않는 경우 RA VPN 사용자는 활성 인증 정책과 일치하는 경우에만 사용 가능합니다. 대시보드에서 또는 트래픽 일치용으로 사용자 이름 정보를 가져오려면 ID 정책을 활성화해야 합니다. ID 정책 구성을 참조하십시오.

Important Secure Firewall Device Manager와 같은 로컬 관리자를 사용하여 원격 액세스 VPN 구성을 변경하면, Security Cloud Control에서 해당 디바이스의 구성 상태가 "충돌 감지됨"으로 표시됩니다. FDM-관리 디바이스의 대역외 변경을 참조하십시오. 이 FDM 관리 디바이스에서 구성 충돌을 해결할 수 있습니다.

What to do next

RA VPN 구성이 FDM 관리 디바이스에 다운로드되면 사용자는 인터넷에 연결된 컴퓨터나 지원되는 다른 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 테넌트의 모든 온보딩 RA VPN 헤드엔드에서 실시간 AnyConnect 원격 액세스 RA VPN(가상 프라이빗망) 세션을 모니터링할 수 있습니다.

원격 액세스 가상 프라이빗 네트워크 세션 모니터링을 참조하십시오.

AnyConnect 클라이언트 소프트웨어 패키지 다운로드

원격 액세스 VPN를 구성하려면 먼저 AnyConnect 소프트웨어 패키지를 https://software.cisco.com/download/home/283000185에서 워크스테이션에 다운로드해야 합니다. 원하는 운영 체제에 대한 "AnyConnect 헤드엔드 구축 패키지"를 다운로드했는지 확인합니다. 나중에 VPN을 정의할 때 이러한 패키지를 FTD(Firepower Threat Defense) 디바이스에 업로드할 수 있습니다.

항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 수정 및 보안 패치가 있는지 확인합니다. 디바이스에서 패키지를 정기적으로 업데이트합니다.

Note 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드

Firewall Device Manager API 탐색기를 사용하여 FDM 관리 디바이스 버전 6.4.0에 AnyConnect 소프트웨어 패키지를 업로드할 수 있습니다. RA VPN 연결을 생성하려면 디바이스에 최소 하나의 AnyConnect 소프트웨어 패키지가 있어야 합니다.

Important 해당 절차는 Firewall Device Manager 버전 6.4에만 적용됩니다. Firewall Device Manager 버전 6.5 이상를 사용하는 경우 Security Cloud Control 인터페이스를 사용하여 AnyConnect 패키지를 업로드합니다.

Firewall Device Manager 버전 6.4.0에 AnyConnect 패키지를 업로드하려면 다음 절차를 따르십시오.

Procedure

단계 1 https://software.cisco.com/download/home/283000185에서 AnyConnect 패키지를 다운로드합니다.

- EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
- 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 Webs Deploy 패키지가 있습니다.

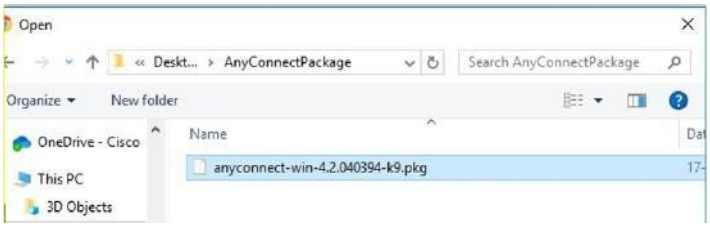
단계 2 브라우저를 사용하여 시스템의 홈페이지를 엽니다. 예를 들어 https://ftd.example.com입니다.

단계 3 Firewall Device Manager에 로그인합니다.

단계 4 /#/api-explorer를 가리키도록 URL을 수정합니다(예: https://ftd.example.com/#/api-explorer).

단계 5 아래로 스크롤하여 **Upload(업로드)** > **/action/uploaddiskfile**를 클릭합니다.

단계 6 **fileToUpload** 필드에서 파일 선택**(Choose File)**을 클릭하고 필요한 AnyConnect 패키지를 선택합니다. 패키지를 한 번에 하나씩 업로드할 수 있습니다.



단계 7 **Open(**열기**)**를 클릭합니다.

단계 8 아래로 스크롤하여 **TRY IT OUT!(**사용해보세요**!)**를 클릭합니다. 패키지가 완전히 업로드될 때까지 기다리십시오. **Response Body(**응답 본문**)**에서 API 응답은 다음 형식으로 나타납니다.

{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "fileuploadstatus",
"links": {
"self":

https://ftd.example.com:972/api/fdm/...90d111e9-a361- cf32937ce0df.pkg

} }

POST 작업을 수행할 때 동일한 문자열을 입력해야 하므로 응답에서 패키지의 **fileName**을 기록합니다. 이 예에서 파일 이름은 **691f47e1-90c7-11e9-a361-79e2452f0c57.pkg**입니다.

단계 9 Firewall Threat Defense REST API 페이지 상단 근처에서 위로 스크롤하고 **AnyConnectPackageFile** > **POST /object/anyconnectpackagefiles**를 클릭합니다. 페이로드에 있는 패키지 파일의 임시 준비 diskFilename 및 OS 유형을 제공하는 API에 대해 POST 작업을 수행합니다. 이 작업은 AnyConnect 패키지 파일을 생성합니다.

단계 10 본문 필드에 패키지 세부 정보를 다음 형식으로만 입력합니다.

{ "platformType": "WINDOWS",
"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "anyconnectpackagefile",
"name": "AnyConnectWindowsBGL" }

a. **platformType** 필드에 OS 플랫폼을 WINDOWS, MACOS 또는 LINUX로 입력합니다.

b. **diskFileName** 필드에는 디스크 파일을 업로드한 후 기록한 **fileName**을 입력합니다.

c. **name** 필드에 원하는 패키지 이름을 입력합니다.

d. **TRY IT OUT!(**사용해 보세요**!)**를 클릭합니다.

Response Body(응답 본문**)** 필드에서 API 응답은 성공적인 POST 작업 후 다음 형식으로 나타납니다.

{ "version": "ni7xeneslft3p",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":

" https://>/ftd.example.com:972...1-cf32937ce0df "https://bglgrp1224-pod.cisco.com:972/api/fdm/v3/object/anyconnectpackagefiles/7f8248c7-90d1-11e9-a361-cf32937ce0df

}
}

AnyConnect 패키지는 Firewall Device Manager에서 생성됩니다.

단계 **11** **AnyConnectPackageFile** > **GET /object/anyconnectpackagefiles** > **TRY IT OUT!(**사용해 보세요**!)** 를 클릭합니다**.**

Response Body(응답 본문**)**에는 모든 AnyConnect 패키지 파일이 표시됩니다.

샘플 응답은 다음과 같습니다.

{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {
"self":
"https://ftd.example.com:972...1-23534f081c43"
}
}
],

단계 **12** OS 유형별로 기타 AnyConnect 패키지를 업로드합니다. 4~10단계를 반복합니다.

단계 13 웹 페이지를 가리키도록 URL(예: https://ftd.example.com)을 수정합니다.

단계 14 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다. 구축되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

단계 15 변경 사항에 만족하는 경우 **Deploy Now(**지금 구축**)**를 클릭하여 작업을 즉시 시작할 수 있습니다. 창에는 구축이 진행 중임이 표시됩니다. 창을 닫을 수도 있고 구축이 완료될 때까지 기다릴 수도 있습니다.

Note FDM 관리디바이스에서 패키지를 삭제하려면, **AnyConnectPackageFile** > **Delete(**삭제**)** 를 클릭합니다. **objID** 필드에 패키지 ID를 입력하고 **TRY IT OUT!**을 클릭합니다.

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법, on page 112을 참조하십시오.

버전 6.5 이상을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드

버전 6.5 이상을 실행하는 FDM 관리 디바이스를 사용하여 RA VPN을 구성하는 경우, Security Cloud Control의 RA VPN 마법사를 사용하여 AnyConnect 소프트웨어 패키지를 디바이스에 업로드할 수 있습니다. RA VPN 마법사에서 AnyConnect 패키지가 미리 로드된 원격 HTTP 또는 HTTPS 서버의 URL을 제공해야 합니다.

Note FDM API 절차를 사용하여 AnyConnect 패키지를 업로드할 수도 있습니다.

Security Cloud Control 저장소에서 *AnyConnect* 패키지 업로드

원격 액세스 VPN 구성 마법사는 Security Cloud Control 저장소에서 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다. 디바이스가 인터넷 및 적절한 DNS 구성에 액세스할 수 있는지 확인합니다.

참고 표시된 목록에서 원하는 패키지를 사용할 수 없거나 디바이스에서 인터넷에 액세스할 수 없는 경우 AnyConnect 패키지가 미리 로드된 서버를 사용하여 패키지를 업로드할 수 있습니다.

프로시저

단계 1 운영 체제에 해당하는 필드를 클릭하고 AnyConnect 패키지를 선택합니다.

단계 2 를 클릭하여 패키지를 업로드합니다. 체크섬이 일치하지 않으면 AnyConnect 패키지 업로드가 실패합니다. 장애에 대한 자세한 내용은 디바이스의 워크플로우 탭을 참조하십시오.

시작하기 전에

원하는 운영 체제에 대한 "AnyConnect 헤드엔드 구축 패키지"를 다운로드했는지 확인하십시오. 항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 수정 및 보안 패치가 있는지 확인합니다. 디바이스에서 패키지를 정기적으로 업데이트합니다.

Note 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

Procedure

단계 1 https://software.cisco.com/download/home/283000185에서 AnyConnect 패키지를 다운로드합니다.

- EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
- 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 패키지가 있습니다.

단계 2 AnyConnect 패키지를 원격 HTTP 또는 HTTPS 서버에 업로드합니다. FDM 관리 디바이스에서 HTTP 또는 HTTPS 서버로의 네트워크 경로가 있는지 확인합니다.

Note
AnyConnect 패키지를 HTTPS 서버에 업로드하는 경우 다음 단계를 수행해야 합니다.

- Firewall Device Manager에서 FDM 관리 디바이스에 있는 해당 서버의 신뢰할 수 있는 CA 인증서를 업로드합니다. 인증서를 업로드하려면 Firepower Device Manager, 버전 XY용 Cisco Firepower Threat Defense 구성 가이드의 "인증서" 장의 "신뢰할 수 있는 CA 인증서 업로드" 섹션을 참조하십시오.
- HTTPS 서버에 신뢰할 수 있는 CA 인증서를 설치합니다.

단계 3 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다. URL이 사전 인증된 경우 RA VPN 마법사의 URL을 지정하여 파일을 다운로드할 수 있습니다.

단계 4 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.

새 *AnyConnect* 패키지 업로드

다음 절차를 사용하여 버전 6.5.0을 실행하는 FDM 관리 디바이스에 새 AnyConnect 패키지를 업로드합니다.

Procedure

단계 **1** 1~4단계에서 RA VPN 구성을 생성합니다.

단계 **2** **AnyConnect Package Detected(AnyConnect** 패키지 감지됨**)**에서 Windows, Mac 및 Linux 엔드포인트용 개별 패키지를 업로드할 수 있습니다.

단계 **3** 해당하는 Platform(플랫폼) 필드에서 Windows, Mac 및 Linux와 호환되는 AnyConnect 패키지가 사전 업로드되는 서버의 경로를 지정합니다. 서버 경로의 예:
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

단계 **4** 을 클릭하여 패키지를 업로드합니다. Security Cloud Control는 경로에 연결할 수 있고 지정된 파일 이름이 유효한 패키지인지 확인합니다. 검증에 성공하면 AnyConnect 패키지의 이름이 나타납니다. RA VPN 구성에 FDM 관리 디바이스를 추가하면 AnyConnect 패키지를 해당 디바이스에 업로드할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다. AnyConnect 패키지가 RA VPN 구성에 추가됩니다.

단계 **6** 여기에서부터 원격 액세스 VPN 구성 생성 절차를 계속 수행합니다.

What to do next

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 FTD에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법을 참조하십시오.

기존 *AnyConnect* 패키지 교체

AnyConnect 패키지가 디바이스에 이미 있는 경우 RA VPN 마법사에서 확인할 수 있습니다. 드롭다운 목록에서 운영 체제에 대해 사용 가능한 모든 AnyConnect 패키지를 볼 수 있습니다. 목록에서 기존 패키지를 선택하고 새 패키지로 교체할 수 있지만 새 패키지를 목록에 추가할 수는 없습니다.

Note 기존 패키지를 새 패키지로 교체하려면 FDM 관리 디바이스가 연결할 수 있는 네트워크의 서버에 새 AnyConnect 패키지가 이미 업로드되어 있는지 확인합니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 클릭합니다.

단계 2 수정할 RA VPN 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 3 **AnyConnect Packages Detected(AnyConnect** 패키지 탐지됨**)**에서 기존 AnyConnect 패키지 옆에 나타나는 아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 교체할 패키지를 선택하고 **Edit(**편집**)**를 클릭합니다. 해당 필드에서 기존 패키지가 사라집니다.

단계 4 새 AnyConnect 패키지가 사전 로드되는 서버의 경로를 지정하고 을 클릭하여 패키지를 업로드합니다.

단계 5 **OK(**확인**)**를 클릭합니다. 새 AnyConnect 패키지가 RA VPN 구성에 추가됩니다.

단계 6 6단계부터 RA VPN 구성 생성을 계속 진행합니다.

AnyConnect 패키지 삭제

Procedure

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 클릭합니다.

단계 2 수정할 RA VPN 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 3 **AnyConnect Packages Detected(**탐지된 **AnyConnect** 패키지**)**에서 삭제할 AnyConnect 패키지 옆에 표시되는 아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 삭제할 패키지를 선택합니다. 해당 필드에서 기존 패키지가 사라집니다.

Note
삭제 작업을 중지하고 기존 패키지를 유지하려면 **Cancel(**취소**)**을 클릭합니다.

단계 4 **OK(**확인**)**를 클릭합니다.디바이스의 구성 상태가 '동기화되지 않음' 상태입니다.

Note
이 단계에서 삭제 작업을 실행 취소하려면 보안 디바이스 페이지를 클릭하고 **Discard Changes(**변경 사항 취소**)**를 클릭하여 기존 AnyConnect 패키지를 유지합니다.

단계 5 디바이스에 대한 구성 변경 사항 미리보고 구축합니다.

FDM-관리 디바이스에 대한 ID 소스 구성

Microsoft AD 영역 및 RADIUS 서버와 같은 ID 소스는 조직의 사용자에 대한 사용자 어카운트를 정의하는 AAA 서버 및 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 Security Cloud Control 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

개체를 클릭한 다음 를 클릭하고 > **RA VPN Objects (ASA & FTD)(RA VPN** 개체**(ASA** 및 **FTD))** > **Identity Source(ID** 소스**)**를 선택하여 소스를 생성합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다. 적절한 필터를 적용하여 기존 소스를 검색하고 관리할 수 있습니다.

Active Directory 영역

Active Directory에서 사용자 어카운트 및 인증 정보를 제공합니다. AD 영역을 포함하는 구성을 FDM 관리 디바이스에 구축하면 Security Cloud Control는 AD 서버에서 사용자 및 그룹을 가져옵니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 ID 소스로 사용) AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(활성 인증용으로 사용/패시브 인증에 사용되는 사용자 ID 소스로 사용)
- 사용자의 활성 인증을 위한 ID 규칙.

사용자 ID를 사용하여 액세스 제어 규칙을 생성할 수 있습니다. 자세한 내용은 ID 정책을 구현하는 방법을 참조하십시오.

Security Cloud Control는 24시간마다 한 번씩 업데이트된 사용자 그룹 목록을 요청합니다. 규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 엔지니어링 그룹의 개발 네트워크 액세스를 허용하는 규칙을 생성한 다음 네트워크에 대한 기타 모든 액세스를 거부하는 후속 규칙을 생성할 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

Security Cloud Control의 Active Directory 영역

AD ID 개체를 생성할 때 AD 영역을 구성합니다. ID 소스 개체 마법사는 AD 서버에 연결하는 방법 및 네트워크에서 AD 서버의 위치를 결정하는 데 도움이 됩니다.

Note Security Cloud Control에서 AD 영역을 생성하는 경우, Security Cloud Control는 가맹 ID 소스 개체를 생성할 때와 ID 규칙에 해당 개체를 추가할 때 AD 비밀번호를 기억합니다.

FDM의 Active Directory 영역

Security Cloud Control 개체 마법사에서 FDM에서 생성된 AD 영역 개체를 가리킬 수 있습니다. Security Cloud Control는 FDM에서 생성된 AD 영역 개체의 AD 비밀번호를 읽지 않습니다. Security Cloud Control에 올바른 AD 비밀번호를 수동으로 입력해야 합니다.

Firewall Device Manager에서 AD 영역을 구성하려면 디바이스에서 실행 중인 버전에 대한 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 재사용 가능한 개체 장의 인증서 정보 및 인증서 구성 섹션을 참조하십시오.

지원되는 디렉터리 서버

Windows Server 2008 및 2012에서 Microsoft AD(Active Directory)를 사용할 수 있습니다.

서버 구성과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 디렉터리 서버에서 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.

- 디렉터리 서버는 시스템에 대해 다음 표에 나와 있는 필드 이름을 순서대로 사용하여 해당 필드에 대한 사용자 메타데이터를 서버에서 검색해야 합니다.

메타데이터	**Active Directory Field(Active Directory** 필드**)**
LDAP user name(LDAP 사용자 이름)	samaccountname
이름	이름
성	sn
이메일 주소	mail userprincipalname(메일에 값이 없는 경우)
부서	부서 distinguishedname(부서에 값이 없는 경우)
전화 번호	telephonenumber

디렉터리 기본 *DN* 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.

Note 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우 도메인 관리자로 AD 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

이 경우 그룹 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

ADSI 편집 프로그램을 사용하여 AD 구조를 찾을 수도 있습니다(**Start(**시작**)** > **Run(**실행**)** > **adsiedit.msc**). ADSI 편집에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로 클릭하고 **Properties(**속성**)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

Procedure

단계 **1** 디렉터리 속성의 **Test Connection(**연결 테스트**)** 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.

단계 **2** 디바이스에 변경 사항을 커밋합니다.

단계 **3** 액세스 규칙을 생성하고 **Users(**사용자**)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 편집해야 합니다.

What to do next

자세한 내용은 Firepower Threat Defense Active Directory 영역 개체 생성 및 편집을 참조하십시오.

RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 관리 사용자를 인증하고 권한을 부여할 수 있습니다.

RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

자세한 내용은 Firepower Threat Defense RADIUS 서버 개체 또는 그룹 생성 및 편집을 참조하십시오.

관련 정보**:**

- 활동 디렉토리 영역 개체 생성
- RADIUS 서버 개체 또는 그룹 생성

- ID 정책 구성

Active Directory 영역 개체 생성 또는 편집

Active Directory 영역 개체 정보

AD 영역 개체와 같은 ID 소스 개체를 생성하거나 편집할 때 Security Cloud Control는 SDC를 통해 FDM 관리 디바이스에 구성 요청을 보냅니다. 그런 다음 FDM 관리 디바이스는 구성된 AD 영역과 통신합니다.

Security Cloud Control는 Firewall Device Manager 콘솔을 통해 구성된 AD 영역의 디렉터리 비밀번호를 읽지 않습니다. 원래 Firewall Device Manager에서 생성된 AD 영역 개체를 사용하는 경우 디렉터리 비밀번호를 수동으로 입력해야 합니다.

FTD Active Directory 영역 개체 생성

개체를 생성하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** +를 클릭한 다음, **RA VPN Objects(**개체**) (ASA & FTD)** > **Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** **Device Type(**디바이스 유형**)**을 **FTD**로 선택합니다.

단계 **5** 마법사의 첫 번째 부분에서 **ID** 소스 유형으로 **Active Directory** 영역을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 기본 영역 속성을 구성합니다.

- 디렉터리 사용자 이름**,** 디렉터리 암호- 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유한 사용자 이름과 암호입니다. AD의 경우 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

  Note
  시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환의 일부이므로 여기에서 일반 이름 "users" 폴더 아래에 지정하는 사용자를 구성해야 합니다.

- **Base Distinguished Name(**기본 고유 이름**)** - 사용자 및 그룹 정보를 검색하거나 조회하기 위한 디렉토리 트리, 즉 사용자 및 그룹의 공통 상위. cn=users,dc=example,dc=com을 예로 들 수 있습니다.

- **AD** 기본 도메인 - 디바이스가 가입해야 하는 정규화된 AD 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.

단계 **7** 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(**호스트 이름/**IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
- **Port**(포트) - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- **Encryption(**암호화**)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 **None(**없음**)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉토리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다. 원격 액세스 VPN에 영역을 사용하는 경우에는 이 옵션이 지원되지 않습니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 포트 636을 사용합니다.
- **Trusted CA Certificate(**신뢰할 수 있는 **CA** 인증서**)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

단계 **8** (선택 사항) **Test(**테스트**)** 버튼을 사용하여 구성을 확인합니다.

단계 **9** (선택 사항) AD 영역에 여러 AD 서버를 추가하려면 **Add another configuration(**다른 구성 추가**)**를 클릭합니다. 이 AD 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다. 따라서 디렉터리 이름, 디렉터리 암호 및 기본 고유 이름과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

단계 **11** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

FTD Active Directory 영역 개체 편집

ID 소스 개체를 편집할 때는 ID 소스 유형을 변경할 수 없습니다. 올바른 유형으로 새 개체를 생성해야 합니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부정보 패널의 **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **5** 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 수정합니다. 아래 나열된 구성 표시줄을 확장하여 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** Security Cloud Control에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 **8** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

RADIUS 서버 개체 또는 그룹 생성 또는 편집

RADIUS 서버 개체 또는 그룹 정보

RADIUS 서버 개체 또는 RADIUS 서버 개체 그룹과 같은 ID 소스 개체를 생성하거나 편집할 때 Security Cloud Control는 SDC를 통해 FDM 관리 디바이스에 구성 요청을 보냅니다. 그런 다음 FDM 관리 디바이스는 구성된 AD 영역과 통신합니다.

RADIUS 서버 개체 생성

RADIUS 서버는 AAA(인증, 권한 부여 및 어카운트 관리) 서비스를 제공합니다.

개체를 생성하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2**  를 클릭한 다음, **RA VPN Objects(**개체**) (ASA & FTD)** > **Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** 디바이스 유형 으로 **FTD**를 선택합니다.

단계 **5** **ID** 소스 유형으로 **RADIUS** 서버를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 다음 속성을 사용하여 ID 소스 구성을 수정합니다.

- **Server Name or IP Address(**서버 이름 또는 **IP** 주소**)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다.
- **Authentication Port(**인증 포트**)**(선택 사항) - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- **Timeout(**시간 제한**)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간(1~300초)입니다. 기본값은 10초입니다.
- 서버 비밀 키입력(선택 사항) - Firepower Threat Defense 디바이스와 RADIUS 서버 간에 데이터를 암호화하는 데 사용되는 공유 비밀입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 $ & - _ . + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀 키를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 **7** 네트워크에 대해 Cisco ISE(Identity Services Engine)가 이미 구성되어 있고 원격 액세스를 위해 서버를 사용하는 경우 VPN 인증 변경 구성, **RA VPN**전용 링크를 클릭하고 다음을 구성합니다.

- **ACL** 리디렉션 - RA VPN 리디렉션 ACL에 사용할 확장 ACL(액세스 제어 목록)을 선택합니다. 확장 ACL이 없는 경우 FDM 관리 디바이스 콘솔의 Smart CLI 템플릿에서 필요한 확장 ACL 개체를 생성해야 합니다. 디바이스가 실행 중인 버전은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 고급 구성 장에서 스마트 **CLI** 개체 구성 섹션을 참조하십시오. 리디렉션 ACL의 목적은 초기 트래픽을 USE로 보내 클라이언트 상태를 평가하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 디바이스가 실행 중인 버전은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 VPN(가상 프라이빗망) 장에서 권한 변경 구성 섹션을 참조하십시오.
- 진단 인터페이스- 이 옵션을 활성화하면 시스템이 항상 "진단" 인터페이스를 사용하여 서버와 통신할 수 있습니다. 이 기능을 비활성화된 상태로 두면 Security Cloud Control는 기본적으로 라우팅 테이블을 사용하여 사용할 인터페이스를 결정합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

RADIUS 서버 그룹 생성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없는 경우 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

개체 그룹을 생성하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2**  를 클릭한 다음 **FTD** > **Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** **Device Type(**디바이스 유형**)**을 **FTD**로 선택합니다.

단계 **5** ID 소스 유형으로 **RADIUS Server Group(RADIUS** 서버 그룹**)** 을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 다음 속성을 사용하여 ID 소스 구성을 수정합니다.

- 데드 타임 - 실패한 서버는 모든 서버가 실패한 후에만 재활성화됩니다. 데드 시간은 모든 서버를 다시 활성화하기 전에 마지막 서버가 실패한 후 대기하는 시간입니다.
- **Maximum Failed Attempts(**최대 실패 시도 횟수**)** - 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 요청(즉, 응답을 받지 못한 요청)의 수입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 Failed(장애 발생)로 표시합니다. 특정 기능에 대해 로컬 데

이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 데드 타임 동안 응답하지 않는 것으로 표시된 상태를 유지하므로 해당 기간 내의 추가 AAA 요청은 서버 그룹에 연결을 시도하지 않으며 폴백 방법이 즉시 사용됩니다.

- **Dynamic Authorization/Port(**동적 인증/포트**) (**선택사항**)** - RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 Cisco ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

단계 **7** 드롭다운 메뉴에서 RADIUS 서버를 지원하는 AD 영역을 선택합니다. AD 영역을 아직 생성하지 않은 경우 드롭다운 메뉴에서 **Create(**생성**)**를 클릭합니다.

단계 **8** 기존 RADIUS 서버 개체를 추가하려면 **Add(**추가**)** 버튼  를 클릭합니다. 선택사항으로 이 창에서 새 RADIUS 서버 개체를 만들 수 있습니다.

Note
목록의 첫 번째 서버가 응답하지 않을 때까지 사용되므로 이러한 개체를 우선 순위에 추가하십시오. FDM 관리 디바이스는 목록의 다음 서버로 기본 설정됩니다.

단계 **9** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

RADIUS 서버 개체 또는 그룹 편집

Radius 서버 개체 또는 Radius 서버 그룹을 편집하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부정보 패널의 **Actions(**작업**)** 창에서 편집 아이콘  를 클릭합니다.

단계 **5** 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다. 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트하려면 구성 표시줄을 확장합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** Security Cloud Control에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 **8** 지금 변경 사항을 검토하고 구축하거나 여러 변경 사항을 여러 변경 사항을 한 번에 구축합니다.

새 RA VPN 그룹 정책 생성

그룹 정책은 원격 액세스 VPN 연결을 위한 사용자 중심 속성/값 쌍의 집합입니다. 연결 프로파일은 터널이 설정된 이후에 사용자 연결을 위한 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사용하면 각 사용자에 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 "DfltGrpPolicy"라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

Note 일치하지 않는 그룹 정책 개체를 RA VPN 구성에 추가할 수 없습니다. RA VPN 구성 그룹 정책을 추가하기 전에 모든 불일치를 해결하십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** > **RA VPN Objects(**개체**) (ASA & FTD)** > **RA VPN Group Policy(**그룹 정책**)**을 클릭합니다.

단계 **3** 그룹 정책의 이름을 입력합니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.

단계 **4** **Device Type(**디바이스 유형**)** 드롭다운에서 **FTD**를 선택합니다.

단계 **5** 다음 중 하나를 수행합니다.

- 필요한 탭을 클릭하고 페이지에서 속성을 구성합니다.
  - 일반 속성
  - AnyConnect 클라이언트 프로파일, on page 91
  - 세션 설정 속성, on page 92
  - 주소 할당 속성, on page 93
  - 스플릿 터널링 속성, on page 93
  - AnyConnect 속성, on page 94
  - 트래픽 필터 속성, on page 96
  - Windows 브라우저 프록시 속성, on page 96

단계 **6** **Save(**저장**)**를 클릭하여 그룹 정책을 생성합니다.

RA VPN 그룹 정책 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다. Name(이름) 속성만 필수 속성입니다.

- **DNS Server(DNS 서버)**: VPN에 연결할 때 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS 서버를 정의하는 DNS 서버 그룹을 선택합니다. 필요한 그룹이 아직 정의되지 않은 경우, **Create DNS Group(DNS 그룹 생성)**을 클릭하여 바로 생성합니다.
- **Banner(배너)**: 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. AnyConnect 클라이언트에서는 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면
 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(기본 도메인)**: RA VPN의 사용자에 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다.
- **AnyConnect Client Profiles(AnyConnect 클라이언트 프로파일)**: +를 클릭하고 이 그룹에 사용할 AnyConnect 클라이언트 프로파일을 선택합니다. AnyConnect 클라이언트 프로파일 구성을 참조하십시오. 연결 프로파일에서 외부 인터페이스에 대해 FQDN(fully-qualified domain name)을 구성하는 경우, 기본 프로파일이 생성됩니다. 원하는 클라이언트 프로파일을 직접 업로드할 수도 있습니다. software.cisco.com에서 다운로드하여 설치할 수 있는 독립형 AnyConnect 프로파일 편집기를 사용하여 이러한 프로파일을 생성합니다. 클라이언트 프로파일을 선택하지 않으면 AnyConnect 클라이언트는 모든 옵션에 대해 기본값을 사용합니다. 이 목록의 항목은 프로파일 자체가 아니라 AnyConnect 클라이언트 프로파일 개체입니다. 드롭다운 목록에서 **Create New AnyConnect Client Profile(새 AnyConnect 클라이언트 프로파일 생성)**을 클릭하면 새 프로파일을 생성하고 업로드할 수 있습니다.

AnyConnect 클라이언트 프로파일

이 기능은 소프트웨어 버전 6.7 이상을 실행하는 Firewall Device Manager에서 지원됩니다.

Cisco AnyConnect VPN 클라이언트는 다양한 내장 모듈을 통해 향상된 보안을 제공합니다. 이러한 모듈은 웹 보안, 엔드 포인트 플로우에 대한 네트워크 가시성, 네트워크 외부 로밍 보호와 같은 서비스를 제공합니다. 각 클라이언트 모듈에는 요구 사항에 따라 사용자 지정 구성 그룹이 포함된 클라이언트 프로파일이 포함되어 있습니다.

VPN 사용자가 VPN AnyConnect 클라이언트 소프트웨어를 다운로드할 때 클라이언트에 다운로드할 AnyConnect VPN 프로파일 개체 및 AnyConnect 모듈을 선택할 수 있습니다.

1. AnyConnect VPN 프로파일 개체를 선택하거나 생성합니다. RA VPN AnyConnect 클라이언트 프로파일 업로드, on page 109의 내용을 참조하십시오. DART 및 Start Before Login(로그인 전 시작) 모듈을 제외하고 AnyConnect VPN 프로파일 개체를 선택해야 합니다.
2. **Add Any Connect Client Module(모든 연결 클라이언트 모듈 추가)**을 클릭합니다.

   다음 AnyConnect 모듈은 선택 사항이며 이러한 모듈을 VPN AnyConnect 클라이언트 소프트웨어와 함께 다운로드하도록 구성할 수 있습니다.

   - **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
   - **DART** — 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
   - **Feedback(피드백)** - 고객이 활성화하고 사용한 기능 및 모듈에 대한 정보를 제공합니다.

- **ISE Posture**: OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다.
- **Network Access Manager** - 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
- **Network Visibility(**네트워크 가시성**)** — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다.
- **Start Before Login(**로그인 전 시작**)** - Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그인하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
- **Umbrella** 로밍 보안 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다.
- 웹 보안 - 정의된 보안 정책에 따라 웹 페이지의 요소를 분석하고 허용되는 콘텐츠를 허용하며 악성 또는 허용되지 않는 콘텐츠를 차단합니다.

3. 클라이언트 모듈 목록에서 **AnyConnect** 모듈을 선택합니다.
4. **Profile(**프로파일**)** 목록에서 AnyConnect 클라이언트 프로파일을 포함하는 프로파일 개체를 선택하거나 생성합니다.
5. 프로파일과 함께 클라이언트 모듈을 다운로드하려면 **Enable Module Download(**모듈 다운로드 활성화**)**를 선택하여 엔드포인트를 활성화합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time(**최대 연결 시간**)**: 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유휴 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval(**연결 시간 알림 간격**)**: 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Idle Time(**유휴 시간**)**: VPN 연결이 자동으로 종료될 때까지 유휴 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval(**유휴 시간 알림 간격**)**: 유휴 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유휴 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.

- **Simultaneous Login Per User(**사용자당 동시 로그인 수**)**: 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool(IPv4** 주소 풀**), IPv6 Address Pool(IPv6** 주소 풀**)**: 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하는 네트워크 개체를 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다. 로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다.

- **DHCP Scope(DHCP** 범위**)**: 연결 프로파일에서 주소 풀에 대한 DHCP 서버를 구성하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 풀에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다. 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다. 범위를 지정하려면 네트워크 번호 호스트 주소를 포함하는 네트워크 개체를 선택합니다. 개체가 아직 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다. 예를 들어 192.168.5.0/24 서브넷 풀에서 주소를 사용하도록 DHCP 서버에 지시하려면 192.168.5.0을 호스트 주소로 지정하는 네트워크 개체를 선택하십시오. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다.

스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 일반 텍스트 형식)로 보냅니다.

- **IPv4 Split Tunneling(IPv4** 스플릿 터널링**)**, **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)**: 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의 경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.

  - **Allow all traffic over tunnel(**터널을 지나는 모든 트래픽 허용**)**: 스플릿 터널링은 실행하지 마십시오. 사용자가 RA VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.

  - **Allow specified traffic over tunnel(**터널을 지나는 지정된 트래픽 허용**)**: 대상 네트워크 및 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 이러한 대상으로 가는 모든 트래픽은

보호된 터널을 통과합니다. 클라이언트는 다른 대상으로 가는 트래픽을 터널 외부의 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.

- **Exclude networks specified below(**아래에 지정된 네트워크 제외**)**: 대상 네트워크 또는 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 클라이언트는 이러한 대상으로 가는 모든 트래픽을 터널 외부 연결로 라우팅합니다. 기타 대상으로 가는 트래픽은 터널을 통과합니다.

- **Split DNS(**스플릿 **DNS)**: 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 구성함과 동시에 클라이언트가 클라이언트에 구성된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 구성할 수 있습니다.

  - **Send DNS Request as per split tunnel policy(**스플릿 터널 정책에 따라 **DNS** 요청 전송**)**: 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.

  - **Always send DNS requests over tunnel(**항상 터널을 통해 **DNS** 요청 전송**)**: 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.

  - **Send only specified domains over tunnel(**지정된 도메인만 터널을 통해 전송**)**: 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

AnyConnect 속성

그룹 정책의 AnyConnect 속성에서는 원격 액세스 VPN 연결에 대해 AnyConnect 클라이언트에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

- **SSL** 설정

  - **Enable Datagram Transport Layer Security (DTLS)(DTLS(Datagram Transport Layer Security)** 활성화**)**: AnyConnect 클라이언트에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다. DTLS를 활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 AnyConnect 클라이언트 사용자가 SSL 터널만 사용하여 연결합니다.

  - **DTLS Compression(DTLS** 압축**)**: LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.

  - **SSL** 압축: 데이터 압축 활성화 여부를 선택하고, 활성화하는 경우 압축 해제 또는 **LZS** 중 사용할 데이터 압축 방법을 선택합니다. SSL 압축은 기본적으로 **Disabled(**비활성화**)** 상태입니

다. 데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.

- **SSL Rekey Method(SSL** 키 재입력 방법**)**, **SSL Rekey Interval(SSL** 키 재입력 간격**)**: 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None(**없음**)**을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel(**새 터널**)**을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel(**기존 터널**)** 옵션을 선택하면 **New Tunnle(**새 터널**)**과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

- **Connection Settings(**연결 설정**)**
  - **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment)** 비트 무시**)**: 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
  - **Client Bypass Protocol(**클라이언트 우회 프로토콜**)**: 이 옵션을 선택하면 보안 게이트웨이에서 IPv6 트래픽만 예상할 때 IPv4 트래픽을 관리하는 방법 또는 IPv4 트래픽만 예상할 때 IPv6 트래픽을 관리하는 방법을 구성할 수 있습니다.

    AnyConnect 클라이언트에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 "일반 텍스트" 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 구성할 수 있습니다.

    예를 들어 보안 게이트웨이에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.

  - **MTU**: Cisco AnyConnect VPN 클라이언트에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.
    - **Keepalive Messages Between AnyConnect and VPN Gateway(AnyConnect**와 **VPN** 게이트웨이 간의 연결 유지 메시지**)**: 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.
    - **DPD on Gateway Side Interval(**게이트웨이 측 간격의 **DPD)**, **DPD on Client Side Interval(**클라이언트 측 간격의 **DPD)**: DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 RA VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다. 기본적으로 그룹 정책에 따라 RA VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter(**액세스 목록 필터**)**: 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. Smart CLI 확장 ACL 개체를 선택합니다. 확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암묵적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. 확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 Firewall Device Manager에 로그인하고 **Device(**디바이스**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**로 이동하여 개체를 생성하고 **Extended Access List(**확장 액세스 목록**)**를 개체 유형으로 선택합니다.
- **Restrict VPN to VLAN(VPN**을 **VLAN**으로 제한**)**: “VLAN 매핑”이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

Windows 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

Browser Proxy During VPN Session(VPN 세션 중 브라우저 프록시**)**에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings(**엔드포인트 설정에 변경 사항 없음**)**: 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 구성하거나 구성하지 않을 수 있으며 구성되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy(**브라우저 프록시 비활성화**)**: 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.
- **Auto detect settings(**설정 자동 탐지**)**: 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings(**사용자 정의 설정 사용**)**: HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.

- **Proxy Server IP or Hostname(**프록시 서버 **IP** 또는 호스트네임**)**, **Port(**포트**)**: 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
- **Browser Exemption List(**브라우저 면제 목록**)**: 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. www.example.com port 80을 예로 들 수 있습니다. 목록에 항목을 추가하려면 **Add Proxy Exemption(**프록시 예외 추가**)**을 클릭합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

RA VPN 구성 생성

Security Cloud Control를 사용하면 원격 액세스 VPN 구성 마법사에 하나 이상의 FDM 관리 디바이스를 추가하고 디바이스와 연결된 VPN 인터페이스, 액세스 제어 및 NAT 면제 설정을 구성할 수 있습니다. 따라서 각 RA VPN 구성에는 RA VPN 구성과 연결된 여러 FDM 관리 디바이스에서 공유되는 연결 프로파일 및 그룹 정책이 있을 수 있습니다. 또한 연결 프로파일 및 그룹 정책을 생성하여 구성을 개선할 수 있습니다.

RA VPN 설정으로 이미 구성된 FDM 관리 디바이스 또는 RA VPN 설정이 없는 새 디바이스를 온보딩할 수 있습니다. 이미 RA VPN 설정이 있는 FDM 관리 디바이스를 온보딩하는 경우 Security Cloud Control는 자동으로 "기본 RA VPN 구성"을 생성하고 FDM 관리 디바이스를 이 구성과 연결합니다. 또한 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다.

Important

- 동일한 원격 액세스 VPN 구성에서 ASA 및 FDM 관리 디바이스를 추가할 수 없습니다.
- FDM 관리 디바이스는 두 개 이상의 RA VPN 구성을 가질 수 없습니다.

사전 요구 사항

RA VPN 구성에 FDM 관리 디바이스를 추가하기 전에 다음 사전 요구 사항을 충족해야 합니다.

- FDM 관리 디바이스에 다음이 있는지 확인합니다.
  - 유효한 라이선스. 자세한 내용은 원격 액세스 VPN에 대한 라이선싱 요건을 참조하십시오.
  - FDM 버전 6.4.0의 경우, 최소 하나의 AnyConnect 소프트웨어 패키지가 디바이스에 사전 업로드되었는지 확인합니다. 자세한 내용은 Firepower Threat Defense 디바이스 버전 6.4.0에 AnyConnect 소프트웨어 패키지 업로드를 참조하십시오.
  - FDM 버전 6.5.0+의 경우 Security Cloud Control를 사용하여 AnyConnect 패키지를 업로드할 수 있습니다. 자세한 내용은 Firepower Threat Defense 디바이스 버전 6.5.0에 AnyConnect 소프트웨어 패키지 업로드를 참조하십시오.
  - 보류 중인 구성 구축이 없습니다.
- FDM 변경 사항은 Security Cloud Control에 동기화됩니다.

1. 왼쪽 창에서 보안 디바이스를 클릭하고 동기화할 하나 이상의 FDM 관리 디바이스를 검색합니다.
2. 디바이스를 하나 이상 선택한 다음 **Check for changes(**변경 사항 확인)를 클릭합니다. Security Cloud Control는 하나 이상의 FDM 관리 디바이스와 통신하여 변경 사항을 동기화 합니다.

- RA VPN 구성 그룹 정책 개체가 일치합니다.
  - 일치하지 않는 모든 그룹 정책 개체는 RA VPN 구성에 추가할 수 없으므로 확인해야 합니다. 문제를 해결하거나 **Objects(**개체**)** 페이지에서 일치하지 않는 그룹 정책 개체를 제거합니다. 자세한 내용은 중복 개체 문제 해결 및 불일치 개체 문제 해결을 참조하십시오.
- FDM 관리 디바이스의 RA VPN 그룹 정책이 RA VPN 구성 그룹 정책과 일치합니다.

절차

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 클릭합니다.

단계 **2** 파란색 플러스  버튼을 클릭하여새 RA VPN 구성을 생성합니다.

단계 **3** 원격 액세스 VPN 구성의 이름을 입력합니다.

단계 **4** 파란색 플러스  버튼을 클릭하여 FDM 관리 디바이스를 구성에 추가합니다. 디바이스 세부 정보를 추가하고 디바이스와 연결된 네트워크 트래픽 관련 권한을 구성할 수 있습니다.

a. 다음 디바이스 세부 사항을 입력합니다.

- 디바이스**:** 추가할 FDM 관리 디바이스를 선택하고 **Select(**선택**)**를 클릭합니다.

  Important
  동일한 원격 액세스 VPN 구성에서 ASA 및 FDM 관리 디바이스를 추가할 수 없습니다.

- **Certificate of Device Identity(**디바이스 **ID**의 인증서**)**: 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 그러면 AnyConnect 클라이언트가 디바이스에 연결할 때 디바이스 ID를 설정합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다. 인증서가 아직 없는 경우 드롭다운 목록에서 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭합니다. 자체 서명 내부 및 내부 CA 인증서 생성를 참조하십시오.
- **Outside Interface(**외부 인터페이스**)**: 사용자가 원격 액세스 VPN 연결을 설정할 때 연결하는 인터페이스입니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

  새 하위 인터페이스를 생성하려면 Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성을 참조하십시오.

- 외부 인터페이스의 **FQDN(Fully-Qualified Domain Name)** 또는 **IP**: ravpn.example.com과 같은 인터페이스의 이름 또는 IP 주소를 제공해야 합니다. 이름을 지정하는 경우 시스템이 클라이언트 프로파일을 자동으로 생성할 수 있습니다. 참고:VPN과 클라이언트에 사용되는 DNS 서버가 외부 인터페이스 IP 주소에 대해 이 이름을 확인할 수 있도록 해야 합니다. 관련 DNS 서버에 FQDN을 추가합니다.

b. Continue(계속**)**를 클릭하여 트래픽 권한을 구성합니다.

- **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)**: 암호 해독된 트래픽은 기본적으로 액세스 제어 정책 검사를 받습니다. 이 옵션을 활성화하면 암호 해독된 트래픽 옵션이 액세스 제어 정책 검사를 무시하지만, VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다. 이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 sysopt connection permit-vpn 명령을 구성한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다. 이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스푸핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다. 이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.
- **NAT Exempt(NAT** 제외**)**: NAT 변환에서 원격 액세스 VPN 엔드포인트와 주고받는 트래픽을 제외하려면 NAT 제외를 활성화합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 RA VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.
  - 내부 인터페이스: 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
  - 내부 네트워크: 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

- Firewall Device Manager 버전 6.4.0 디바이스를 온보딩한 경우, 탐지된 **AnyConnect** 패키지에 디바이스에서 사용 가능한 AnyConnect 패키지가 표시됩니다.
- Firewall Device Manager 버전 6.5.0 이상 디바이스를 온보딩한 경우 AnyConnect 패키지가 사전 업로드된 서버에서 AnyConnect 패키지를 추가해야 합니다. 지침은 버전 6.5.0을 실행하는 FDM 매니지드 디바이스에 AnyConnect 소프트웨어 패키지 업로드를 참조하십시오.

단계 6 **OK(확인)**를 클릭합니다. 디바이스가 구성에 추가됩니다.

What to do next

Note 구성을 선택하고 **Actions(작업)** 아래에서 적절한 작업을 클릭합니다.

- **Group Policies(그룹 정책)** - 그룹 정책을 추가하거나 제거합니다.
  - +를 클릭하여 필요한 그룹 정책을 선택합니다. 새 RA VPN 그룹 정책을 만들려면 새 FTD RA VPN 그룹 정책 생성을 참조하십시오.
- **Remove(제거)**- 선택한 RA VPN 구성을 삭제합니다.

RA VPN 구성 수정

기존 RA VPN 구성의 이름 및 디바이스 세부 정보를 수정할 수 있습니다.

Procedure

수정할 구성을 선택하고 **Actions(작업)** 아래에서 **Edit(편집)**를 클릭합니다.

- 필요한 경우 이름을 수정합니다.
- 디바이스를 추가하려면 파란색 플러스 버튼  을 클릭합니다.
- 를 클릭하여 FDM 관리 디바이스에서 다음을 수행합니다.
  - **Edit(편집)**를 클릭하여 기존 RA VPN 구성을 수정합니다.
  - **Remove(제거)**를 클릭하여 RA VPN 구성에서 FDM 관리 디바이스를 제거합니다. 그룹 정책을 제외하고 해당 디바이스와 연결된 모든 연결 프로파일 및 RA VPN 설정이 삭제됩니다. 개체 페이지에서 그룹 정책을 명시적으로 제거할 수 있습니다. 참고: 구성을 사용하는 유일한 디바이스인 경우 FDM 관리 디바이스를 제거할 수 없습니다. 이 경우 대신 RA VPN 구성을 제거할 수 있습니다.

구성 또는 디바이스의 이름을 입력하여 Remote Access VPN 구성을 검색할 수도 있습니다.

관련 정보**:**

- FTD RA VPN 연결 프로파일 구성
- 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

- 원격 액세스 VPN을 통한 트래픽을 허용합니다.

RA VPN 연결 프로파일 구성

RA VPN 연결 프로파일은 외부 사용자가 AnyConnect 클라이언트를 사용하여 시스템에 대한 VPN 연결을 생성할 수 있도록 허용하는 특성을 정의합니다. 각 프로파일은 사용자 인증에 사용되는 AAA 서버 및 인증서, 사용자 IP 주소 할당을 위한 주소 풀, 다양한 사용자 지향 속성을 정의하는 그룹 정책을 정의합니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 다양한 인증 소스가 있는 경우, RA VPN구성 내에 프로파일을 여러 개 생성합니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.

RA VPN 연결 프로파일을 사용하면 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

시작하기 전에

RA(원격 액세스) VPN 연결을 구성하기 전에 다음 작업을 수행합니다.

- 원격 액세스 VPN 연결을 종료하는 외부 인터페이스가 HTTPS 연결을 허용하는 관리 액세스 목록도 포함할 수는 없습니다. RA VPN을 구성하기 전에 외부 인터페이스에서 HTTPS 규칙을 삭제하십시오. Firepower Device Manager 버전 X.Y용 Cisco Firepower Threat Defense 구성 가이드의 "시스템 설정" 장에서 "관리 액세스 목록 구성" 섹션을 참조하십시오.
- RA VPN 구성을 생성합니다. RA VPN 구성 생성을 참조하십시오.

절차

Procedure

단계 **1**

단계 **2** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 클릭합니다. VPN 구성을 클릭하여 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지에 대한 요약 정보를 볼 수 있습니다.

단계 **3** 연결 프로파일을 클릭하고 오른쪽 사이드바의 **Actions(**작업**)** 아래에서 **Add Connection Profile(**연결 프로파일 추가**)**를 클릭합니다.

단계 **4** 기본 연결 속성을 구성합니다.

- **Connection Profile Name(**연결 프로파일 이름**)**: 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다.

  Note
  여기서 입력하는 이름이 AnyConnect 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(그룹 별칭), Group URL(그룹 URL)**: 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. FDM 관리 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 AnyConnect 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 구성할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 AnyConnect 클라이언트가 아직 없는 클라이언트에서 사용됩니다. 그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.
- 예를 들어 별칭 계약자 및 그룹 URL https://ravpn.example.com/contractor가 있을 수 있습니다. AnyConnect 클라이언트가 설치된 후 사용자는 연결의 AnyConnect VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

단계 **5** 기본 ID 소스를 구성하고, 선택적으로 보조 ID 소스를 구성합니다. 이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD 영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(인증 유형)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA만)**: 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 연결 프로파일에 대해 AAA 구성을 참조하십시오.
- **Client Certificate Only(클라이언트 인증서만)**: 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 연결 프로파일에 대한 인증서 인증 구성을 참조하십시오.
- **AAA and ClientCertificate(AAA 및 ClientCertificate)**: 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.

단계 **6** 클라이언트에 대해 주소 풀을 구성합니다. 주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 클라이언트 주소 풀 할당 구성을 참조하십시오.

단계 **7** **Continue(계속)**를 클릭합니다.

단계 **8** 목록에서 이 프로파일에 사용할 **Group Policy(그룹 정책)**를 선택하고 **Select(선택)**를 클릭합니다. 그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 DfltGrpPolicy라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

Note
필요한 그룹 정책이 아직 없는 경우 **Objects(개체)** 페이지에서 그룹 정책을 생성한 다음 해당 정책을 RA VPN 구성에 연결합니다. 그룹 정책에 대한 세부 정보는 새 RA VPN 그룹 정책 생성을 참조하십시오.

단계 **9** **Continue(계속)**를 클릭합니다.

단계 **10** 요약을 검토합니다. 먼저 요약이 정확한지 확인합니다. AnyConnect 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악할 수 있습니다.  를 클릭하여 지침을 클립보드에 복사한 다음 사용자에게 구축합니다.

단계 **11** **Done(**완료**)**을 클릭합니다.

What to do next

원격 액세스 VPN을 통한 트래픽 허용에 설명된 대로 VPN 터널에서 트래픽이 허용되는지 확인합니다.

연결 프로파일에 대해 *AAA* 구성

인증, 권한 부여, 어카운트 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 어카운트 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 구성하는 경우, 기본 ID 소스를 구성해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 2단계 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용합니다.

기본 **ID** 소스 옵션

- **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)**: 원격 사용자 인증에 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.
  - AD(Active Directory) ID 영역. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭합니다.
  - Radius 서버 그룹.
  - LocalIdentitySource(로컬 사용자 데이터베이스): 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.
- **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)**: 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.
- **Strip options(**제거 옵션**)**: 영역은 관리 도메인입니다. 다음 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.
  - **Strip Identity Source Server from Username(**사용자 이름에서 **ID** 소스 서버 제거**)**: AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들어 이 옵션을 선택하고 사용자가 도메인\사용자 이름을 사용자 이름으로 입력하는 경우, 도

메인은 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

- **Strip Group from Username(**사용자 이름에서 그룹 제거**)**: AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거할지 여부. 이 옵션은 username@domain 형식에서 지정된 이름에 적용되며, 도메인 및 @ 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

보조 **ID** 소스

- **Secondary Identity Source for User Authorization(**사용자 권한 부여를 위한 보조 **ID** 소스**)**: 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options(**고급 옵션**)**: **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.
  - **Fallback Local Identity Source for Secondary(**보조용 대체 시스템 로컬 **ID** 소스**)**: 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, LocalIdentitySource를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
  - **Use Primary Username for Secondary Login(**보조 로그인에 기본 사용자 이름 사용**)**: 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 구성하는 경우, 이 옵션을 선택합니다.
    - **Username for Session Server(**세션 서버의 사용자 이름**)**: 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 어카운트를 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
    - **Password Type(**암호 유형**)**: 보조 서버의 암호를 가져오는 방법. 기본값은 **Prompt(**프롬프트**)**입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다. 사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password(**기본 **ID** 소스 암호**)**를 선택합니다. 모든 사용자에 대해 동일한 암호를 사용하려면 **Common Password(**공통 암호**)**를 선택한 다음, **Common Password(**공통 암호**)** 필드에 해당 암호를 입력합니다.
  - **Authorization Server(**권한 부여 서버**)**: 원격 액세스 VPN 사용자를 인증하도록 구성된 RADIUS 서버 그룹. 인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을 결합함으로써 작동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게

동일한 액세스 권한을 제공합니다. 권한 부여를 위해 RADIUS를 구성하는 방법에 대한 자세한 내용은 RADIUS 및 그룹 정책을 사용하여 사용자 권한 및 속성 제어를 참조하십시오. 시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 재정의한다는 점에 유의하십시오.

- **Accounting Server(**과금 서버**)**: (선택 사항) 원격 액세스 VPN 세션에 대한 어카운트 관리에 사용할 RADIUS 서버 그룹입니다. 어카운트 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 수까지도 추적합니다. FTD 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 어카운트 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대한 데이터를 분석할 수 있습니다. 관리 어카운트 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

연결 프로파일에 대한 인증서 인증 구성

Note 이 섹션은 **Authentication Type(**인증 유형**)**이 **AAA Only(AAA**만**)**인 경우에는 적용되지 않습니다.

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 구성할 수 있습니다. 이는 AAA 옵션입니다. 자세한 내용은 RA VPN 연결 프로파일 구성을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 구성할 수 있습니다. 보조 소스 구성은 선택 사항입니다.

- **Username from Certificate(**인증서의 사용자 이름**)**: 다음 중 하나를 선택합니다.
  - **Map Specific Field(**특정 필드 매핑**)**: **Primary Field(**기본 필드**)** 및 **Secondary Field(**보조 필드**)**의 순서대로 인증서 요소를 사용합니다. 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.
  - **Use entire DN (distinguished name) as username(**전체 **DN(**고유 이름**)**을 사용자 이름으로 사용**)**: 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다. •
- 고급 옵션(**Authentication Type(**인증 유형**)**이 **Client Certificate Only(**클라이언트 인증서 전용**)**인 경우에는 해당되지 않음): **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.
  - **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)**: 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
  - **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**)**: **Prefill(**미리 채우기**)** 옵션을 선택하면 사용자 이름을 숨길 수 있습니다. 따라서 사용자는 암호 프롬프트에서 사용자 이름을 편집할 수 없습니다.

클라이언트 주소 풀 할당 구성

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. AAA 서버는 이러한 주소, DHCP 서버, 그룹 정책에 구성된 IP 주소 풀 또는 연결 프로파일에 구성된 IP 주소 풀을 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 페일세이프를 생성할 수 있는 여러 가지 옵션을 구성할 수 있습니다.

연결 프로파일에 대한 주소 풀을 구성하려면 다음 방법 중 한 가지 이상을 사용합니다.

- **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv4 Address Pool(IPv4** 주소 풀**)**: 먼저 서브넷을 지정하는 최대 6개의 네트워크 개체를 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 구성할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv6 Address Pool(IPv6** 주소 풀**)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 구성할 필요는 없고 지원하려는 주소 체계를 구성하면 됩니다. 또한 그룹 정책 및 연결 프로파일 모두에서 풀을 구성할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 재정의하므로 그룹 정책에서 풀을 구성하는 경우, 연결 프로파일에서 옵션을 비워두십시오. 풀은 나열한 순서대로 사용된다는 점에 유의하십시오.

- **DHCP Servers(DHCP** 서버**)**: 먼저 RA VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 구성합니다(DHCP를 사용하여 IPv6 풀을 구성할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP** 서버**)** 속성에서 이 개체를 선택할 수 있습니다. 두 개 이상의 DHCP 서버를 구성할 수 있습니다. DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 그룹 정책에서 **DHCP Scope(DHCP** 범위**)** 속성을 사용해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.

원격 액세스 VPN을 통한 트래픽 허용

다음 기법 중 하나를 사용해 원격 액세스 VPN 터널에서 트래픽 플로우을 활성화할 수 있습니다.

- **sysopt connection permit-vpn** 명령을 구성합니다. 이 명령에서는 VPN 연결과 일치하는 트래픽을 액세스 제어 정책에서 제외합니다. 이 명령의 기본값은 **no sysopt connection permit-vpn**입니다. 이는 액세스 제어 정책에서도 VPN 트래픽을 허용해야 한다는 의미입니다. 이 방법은 외부 사용자가 원격 액세스 VPN 주소 풀에서 IP 주소를 스푸핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 즉, 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다. 이 명령을 구성하려면 RA VPN 구성에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택합니다. RA VPN 구성 생성을 참조하십시오.

- 원격 액세스 VPN 주소 풀에서 연결을 허용하는 액세스 제어 규칙을 생성합니다. 이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스푸핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다.

  FDM 액세스 제어 정책 구성을 참조하십시오.

버전 6.4.0을 실행하는 FDM-관리 디바이스에서 AnyConnect 패키지 업그레이드

Security Cloud Control을 사용하여 FDM 관리 디바이스에서 사용 가능한 AnyConnect 패키지를 업그레이드하여 RA VPN 사용자에게 구축할 수 있습니다.

다음은 AnyConnect 패키지 업그레이드와 관련된 주요 단계입니다.

Procedure

단계 1 Firewall Device Manager을 사용하여 AnyConnect 패키지를 제거하고 최신 버전의 패키지를 업로드합니다. 이 작업을 수행하려면 다음 방법 중 하나를 사용합니다.

- 이전 패키지를 제거하고 Firewall Device Manager UI에서 새 패키지를 업로드합니다.
- 이전 패키지를 제거하고 Firewall Device Manager API 탐색기에서 새 패키지를 업로드합니다.

단계 2 디바이스에 Firewall Device Manager 변경 사항을 구축합니다.

단계 3 새 구성 정보를 Security Cloud Control로 읽습니다.

단계 4 RA VPN 연결 프로파일에서 새 패키지를 확인합니다.

사전 요구 사항

- 연결 프로파일이 있는 하나 이상의 RA VPN 구성이 이미 FDM 관리 디바이스에 구축되어 있습니다.
- https://software.cisco.com/download/home/283000185에서 원하는 AnyConnect 패키지를 다운로드합니다. Cisco에서는 사용 가능한 최신 패키지로 업그레이드할 것을 권장합니다.

*Firewall Device Manager*을 사용하여 *Secure Firewall Threat Defense*에 원하는 *AnyConnect* 패키지 업로드

Procedure

단계 1 브라우저를 사용하여 시스템의 홈페이지를 엽니다. 예를 들면 `https://ftd.example.com`입니다.

단계 2 Firewall Device Manager에 로그인합니다.

단계 3 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**구성 보기**)**을 클릭합니다. 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 4 보기(버튼) (구성 **View(**보기**)** 버튼)을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다.

Note

연결 프로파일 중 하나를 수정하여 AnyConnect 패키지를 FDM 관리 디바이스에 업로드할 수 있습니다.

단계 **5** **Edit(**편집**)** 버튼을 클릭하여 변경합니다.

단계 **6** **Global Settings(**전역 설정**)** 화면이 나타날 때까지 **Next(**다음**)**를 클릭합니다. **AnyConnect Package(AnyConnect** 패키지**)**에는 FDM 관리 디바이스에서 사용 가능한 AnyConnect 패키지가 표시됩니다.

단계 **7** 'X' 버튼을 클릭하여 교체할 AnyConnect 패키지를 제거합니다.

단계 **8** **Upload Package(**패키지 업로드**)**를 클릭한 다음 호환되는 패키지를 업로드할 OS를 클릭합니다.

단계 **9** 패키지를 선택하고 **Open(**열기**)**을 클릭합니다. Firewall Device Manager UI에서 업로드 중인 패키지를 확인할 수 있습니다.

단계 **10** **Finish(**마침**)**를 클릭합니다. 구성이 저장됩니다.

Note
또는 Firewall Device Manager API 탐색기를 사용하여 새 AnyConnect 패키지를 제거하고 업로드할 수 있습니다.

a. /#/api-explorer를 가리키도록 URL을 수정합니다(예: `https://ftd.example.com/#/api-explorer`).

b. FDM 관리디바이스에서 패키지를 삭제하려면, **AnyConnectPackageFile** > **Delete(**삭제**)** 를 클릭합니다. **objID** 필드에 패키지 ID를 입력하고 **TRY IT OUT!**을 클릭합니다.

c. Firepower Threat Defense 디바이스에 AnyConnect 소프트웨어 패키지 업로드 섹션에 설명된 단계를 수행하여 새 패키지를 업로드합니다.

단계 **11** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다. 구축되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

단계 **12** 변경 사항에 만족하는 경우 **Deploy Now(**지금 구축**)**를 클릭하여 작업을 즉시 시작할 수 있습니다. 창에는 구축이 진행 중임이 표시됩니다. 창을 닫을 수도 있고 구축이 완료될 때까지 기다릴 수도 있습니다.

RA VPN 연결 프로파일에서 새 패키지 참조 확인

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **FTD** 탭을 클릭하고 업그레이드된 AnyConnect 패키지가 있는 FDM 관리 디바이스를 선택합니다. 이 디바이스에서 충돌을 보고합니다.

단계 **4** 디바이스의 실행 중인 구성으로 Security Cloud Control에 저장된 구성 및 보류 중인 변경 사항을 덮어쓰려면 OOB(Out of Band) 변경 사항을 수락합니다. 자세한 내용은 "충돌 탐지 상태" 해결을 참조하십시오.

단계 **5** 다음을 수행하여 새 AnyConnect 패키지를 확인합니다.

- **VPN** > **Remote Access VPN(**원격 액세스 **VPN)**을 클릭합니다.
- 이 FDM 관리 디바이스와 연결된 RA VPN 구성을 클릭합니다.
- **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다. 새 패키지가 **Devices(**디바이스**)** 아래에 표시됩니다.

RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

Security Cloud Control는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 — AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. Security Cloud Control은 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드포인트로 푸시됩니다. Security Cloud Control는 XML 및 ASP 파일 형식을 지원합니다.
- 피드백 프로파일 - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. Security Cloud Control는 FSP 파일 형식을 지원합니다.

- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. Security Cloud Control는 XML 및 ISP 파일 형식을 지원합니다.
- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. Security Cloud Control은 NSP 파일 형식을 지원합니다.
- 네트워크 가시성 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. Security Cloud Control은 XML 및 NVMSP 파일 형식을 지원합니다.
- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. Security Cloud Control는 XML 및 JSON 파일 형식을 지원합니다.
- 웹 보안 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. Security Cloud Control는 XML, WSO 및 WSP 파일 형식을 지원합니다.

Before you begin

적합한 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 해당 릴리스의 *AnyConnect* 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 Cisco Umbrella 사용 가이드의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로파일 다운로드" 섹션을 참조하십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 선택합니다.

단계 **2** 파란색 플러스  버튼을 클릭합니다.

단계 **3** **RA VPN Objects (ASA & FDM)(RA VPN** 개체**(ASA** 및 **FDM))** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**를 클릭합니다.

단계 **4** **Object Name(**개체 이름**)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 **6** **Open(**열기**)**을 클릭하여 프로파일을 업로드합니다.

단계 7 **Add(추가)**를 클릭하여 개체를 추가합니다.

관련 정보:

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. 새 FTD RA VPN 그룹 정책 생성을 참조하십시오.

Note 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

FDM-관리 디바이스용 원격 액세스 VPN의 지침 및 제한 사항

RA VPN을 구성할 때 다음 지침 및 제한 사항을 염두에 두십시오.

- Firewall Device Manager을 사용하여 버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 패키지를 사전 로드해야 합니다.

Note Security Cloud Control의 원격 액세스 VPN 구성 마법사를 사용하여 버전 6.5.0을 실행하는 FDM-관리 디바이스에 AnyConnect 패키지를 별도로 업로드합니다.

- Security Cloud Control에서 RA VPN을 구성하기 전에,
  - Firewall Device Manager에서 FDM 관리 디바이스에 대한 라이선스를 등록합니다.
  - 내보내기 제어 기능이 있는 Firewall Device Manager에서 라이선스를 활성화합니다.
- Security Cloud Control는 확장 액세스 목록 개체를 지원하지 않습니다. Firewall Device Manager에서 Smart CLI를 사용하여 개체를 구성한 다음 VPN 필터 및 CoA(Change of Authorization) 리디렉션 ACL에서 사용합니다.
- FDM 관리 디바이스에서 생성한 템플릿에는 RA VPN 구성이 포함되지 않습니다.
- IP 풀 개체 및 RADIUS ID 소스에는 디바이스별 재정의가 필요합니다.
- 동일한 TCP 포트에 대해 동일한 인터페이스에서 Firewall Device Manager 액세스(관리 액세스 목록의 HTTPS 액세스)와 AnyConnect 원격 액세스 SSL VPN을 모두 구성할 수 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. Firewall Device Manager의 이러한 기능에서 사용되는 포트를 구성할 수 없으므로 동일한 인터페이스에서 두 가지 기능을 모두 구성할 수는 없습니다.
- RADIUS 및 RSA 토큰을 사용하여 2단계 인증을 구성하는 경우, 기본 인증 시간 제한 값인 12초는 너무 짧아 대부분의 경우 성공적인 인증을 허용하기 어렵습니다. RA VPN AnyConnect 클라이언트 프로파일 업로드, on page 109에 설명된 대로 사용자 지정 AnyConnect 클라이언트 프로파일을 생성하고 RA VPN 연결 프로파일에 적용하여 인증 제한 시간 값을 늘리십시오. 사용자가 RSA

토큰을 인증한 다음 붙여넣고 토큰의 왕복 확인에 충분한 시간을 가질 수 있도록 최소 60초의 인증 제한 시간을 권장합니다.

FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법

Firewall Device Manager API를 사용하여 AnyConnect 클라이언트 소프트웨어 패키지를 FDM 관리 디바이스에 업로드하여 사용자에게 구축합니다. Firepower Threat Defense 디바이스에 AnyConnect 소프트웨어 패키지 업로드를 참조하십시오.

VPN 연결을 완료하려면 사용자가 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 기존 소프트웨어 구축 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 FDM 관리 디바이스에서 AnyConnect 클라이언트를 직접 설치하게 할 수도 있습니다.

Note 소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

사용자가 FDM 관리 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.

Note Android 및 iOS 사용자는 해당 앱 스토어에서 AnyConnect를 다운로드해야 합니다.

Procedure

단계 **1** 웹 브라우저를 사용하여 **https://** *ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.

단계 **2** 사이트에 로그인합니다. 사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인이 성공해야 설치를 계속할 수 있습니다. 로그인이 성공하면 시스템은 사용자에게 필요한 AnyConnect 클라이언트 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 AnyConnect 클라이언트가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 AnyConnect 소프트웨어 설치를 자동으로 시작합니다. 설치가 완료되면, AnyConnect에서 원격 액세스 VPN 연결을 완료합니다.

새 AnyConnect 클라이언트 소프트웨어 버전 구축

이전 버전을 제거하지 않고 새 버전의 AnyConnect 클라이언트 소프트웨어를 FDM 관리 디바이스에 업로드하여 사용자에게 구축할 수 있습니다. AnyConnect 클라이언트가 성공적으로 업로드되면 이전 버전을 제거할 수 있습니다.

AnyConnect 클라이언트는 사용자가 다음 VPN 연결에서 새 버전을 탐지합니다. 그러면 시스템에서 업데이트된 클라이언트 소프트웨어를 다운로드하여 설치하라는 메시지를 사용자에게 자동으로 표시합니다. 이러한 자동화로 인해 개발자와 고객을 위한 소프트웨어 구축를 간소화할 수 있습니다.

다음 그림에는 Windows OS용 AnyConnect 클라이언트 소프트웨어의 두 가지 버전(**AnyConnectWindows_3.2_BGL** 및 **AnyConnectWindows_4.2_BGL**)이 포함된 FDM 관리 디바이스의 예가 나와 있습니다.

RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

Security Cloud Control는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 — AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. Security Cloud Control은 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드포인트로 푸시됩니다. Security Cloud Control는 XML 및 ASP 파일 형식을 지원합니다.
- 피드백 프로파일 - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. Security Cloud Control는 FSP 파일 형식을 지원합니다.
- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. Security Cloud Control는 XML 및 ISP 파일 형식을 지원합니다.

- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. Security Cloud Control은 NSP 파일 형식을 지원합니다.
- 네트워크 가시성 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. Security Cloud Control은 XML 및 NVMSP 파일 형식을 지원합니다.
- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. Security Cloud Control는 XML 및 JSON 파일 형식을 지원합니다.
- 웹 보안 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. Security Cloud Control는 XML, WSO 및 WSP 파일 형식을 지원합니다.

Before you begin

적합한 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 해당 릴리스의 *AnyConnect* 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 Cisco Umbrella 사용 가이드의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로파일 다운로드" 섹션을 참조하십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 선택합니다.

단계 **2** 파란색 플러스  버튼을 클릭합니다.

단계 **3** **RA VPN Objects (ASA & FDM)(RA VPN** 개체**(ASA** 및 **FDM))** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**를 클릭합니다.

단계 **4** **Object Name(**개체 이름**)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 **6** **Open(**열기**)**을 클릭하여 프로파일을 업로드합니다.

단계 **7** **Add(**추가**)**를 클릭하여 개체를 추가합니다.

관련 정보**:**

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. 새 FTD RA VPN 그룹 정책 생성을 참조하십시오.

Note 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

원격 액세스 VPN에 대한 라이선싱 요구 사항

Firewall Device Manager에서 FDM 관리 디바이스에 대한 라이선스를 활성화(등록)하여 RA VPN 연결을 구성합니다. 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager(SSM) 어카운트를 사용하여 등록을 수행해야 합니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다.

또한 라이선스를 구매하여 활성화해야 합니다. 중 하나일 수 있습니다. 이러한 라이선스는 FDM 관리 디바이스에 대해 동일하게 처리되지만, ASA 소프트웨어 기반 헤드엔드와 함께 사용할 때는 각기 다른 기능 집합을 허용하도록 설계되었습니다.

Firewall Device Manager에서 라이선스 활성화에 대한 자세한 내용은 디바이스가 실행 중인 버전에 대한 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 원격 액세스 VPN 장의 원격 액세스 **VPN** 라이선스 요구 사항 섹션을 참조하십시오.

자세한 내용은 *Cisco AnyConnect* 주문 가이드를 참조하십시오. 다른 데이터 시트도 http://www.cisco.com/c/en/us/product...t-listing.html에서 확인할 수 있습니다.

라이선스 상태를 보려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 디바이스를 클릭합니다.

단계 **3** **FTD** 탭을 클릭하고 원하는 디바이스를 선택합니다.

단계 **4** 오른쪽의 **Device Actions(**디바이스 작업**)** 창에서 **Manage Licenses(**라이선스 관리**)**를 클릭합니다. 라이선스가 유효한 경우 **Status(**상태**)**에 **Enabled(**활성화됨**)**가 표시됩니다.

디바이스 모델별 최대 동시 VPN 세션

디바이스 모델에 따라 디바이스에서 허용되는 동시 원격 액세스 VPN 세션 수에는 최대 제한이 적용됩니다. 이 제한은 시스템 성능이 허용할 수 없는 수준으로 저하되지 않도록 설계되었습니다. 용량 계획 시에 이러한 제한을 사용하십시오.

디바이스 모델	최대 동시 원격 액세스 VPN 세션
Firepower 2110	1,500

디바이스 모델	최대 동시 원격 액세스 **VPN** 세션
Firepower 2120	3,500
Firepower 2130	7,500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250

RADIUS COA(Change of Authorization)

RADIUS CoA(Change of Authorization: 권한 부여 변경) 기능은 인증 후 AAA(인증, 권한 부여 및 어카운트 관리) 세션의 특성을 변경하는 메커니즘을 제공합니다. RA VPN의 주요 당면 과제는 감염된 엔드포인트로부터 내부 네트워크를 보호하는 것입니다. 또한 엔드포인트에 대한 공격을 해결하여 바이러스 또는 멀웨어의 침해를 받을 때 엔드포인트 자체를 보호하는 것입니다. RA VPN 세션 전, 중, 후 모든 단계에서 엔드포인트와 내부 네트워크를 보호해야 합니다. RADIUS CoA 기능을 통해 이 목표를 달성할 수 있습니다.

Cisco Identity Services Engine(ISE) RADIUS 서버를 사용하는 경우, CoA(Change of Authorization) 정책 시행을 구성할 수 있습니다. 정책에서 AAA의 사용자 또는 사용자 그룹을 변경하는 경우, ISE에서는 FTD 디바이스로 CoA 메시지를 전송하여 인증을 다시 시작하고 새 정책을 적용합니다. IPEP(Inline Posture Enforcement Point: 인라인 보안 상태 시행 지점)에는 FTD 디바이스로 설정된 각 VPN 세션에 대한 ACL(Access Control List: 액세스 제어 목록)이 필요하지 않습니다.

관련 정보:

- FTD 디바이스에서 COA(Change of Authorization) 구성

FTD 디바이스에서 COA(Change of Authorization) 구성

CoA(Change of Authorization) 정책의 대부분은 ISE 서버에서 구성됩니다. 그러나 ISE에 올바르게 연결하려면 FTD 디바이스를 구성해야 합니다.

시작하기 전에

개체에서 호스트 이름을 사용하는 경우 디바이스가 실행 중인 버전에 대한 Firepower Device Manager용 Cisco Firepower Threat Defense 설정 가이드, 시스템 설정 장의 데이터 및 관리 인터페이스용 **DNS** 구성에 설명된 대로 데이터 인터페이스에 사용할 DNS 서버를 구성해야 합니다. 일반적으로 시스템이 완전히 작동하려면 DNS를 구성해야 합니다.

절차

Procedure

단계 **1** FDM 관리 디바이스에 대해 Firewall Device Manager에 로그인합니다.

단계 **2** 초기 연결을 ISE로 리디렉션하기 위한 확장 ACL(Access Control List)을 구성합니다. 리디렉션 ACL의 목적은 초기 트래픽을 ISE로 전송하여 ISE에서 클라이언트 보안 상태를 평가할 수 있게 하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는

이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 샘플 리디렉션 ACL은 다음과 같이 표시될 수 있습니다.

access-list redirect extended deny ip any host<ISE server IP>

access-list redirect extended deny ip any host<DNS server IP>

access-list redirect extended deny icmp any any

access-list redirect extended permit tcp any any eq www

하지만 ACL에는 마지막 ACE(액세스 제어 항목)인 암시적 "deny any any"가 있다는 점에 유의하십시오. 이 예에서는 TCP 포트 www(즉 포트 80)와 일치하는 마지막 ACE가 첫 ACE 3개와 일치하는 모든 트래픽과 일치하지 않습니다. 따라서 이 ACE 3개는 이중화됩니다. 마지막 ACE로 ACL을 생성하기만 해도 동일한 결과를 얻을 수 있습니다. 리디렉션 ACL의 허용 및 거부 작업에서는 일치하는 것은 허용하고 일치하지 않는 것은 거부하여 ACL과 일치하는 트래픽을 확인할 뿐이라는 점에 유의하십시오. 트래픽이 실제로 차단되는 경우는 없으며, 거부된 트래픽은 ISE로 리디렉션되지 않을 뿐입니다. 리디렉션 ACL을 생성하려면 스마트 CLI 개체를 구성해야 합니다.

a. **Device(**디바이스**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

b. **+**를 클릭하여 새 개체를 생성합니다.

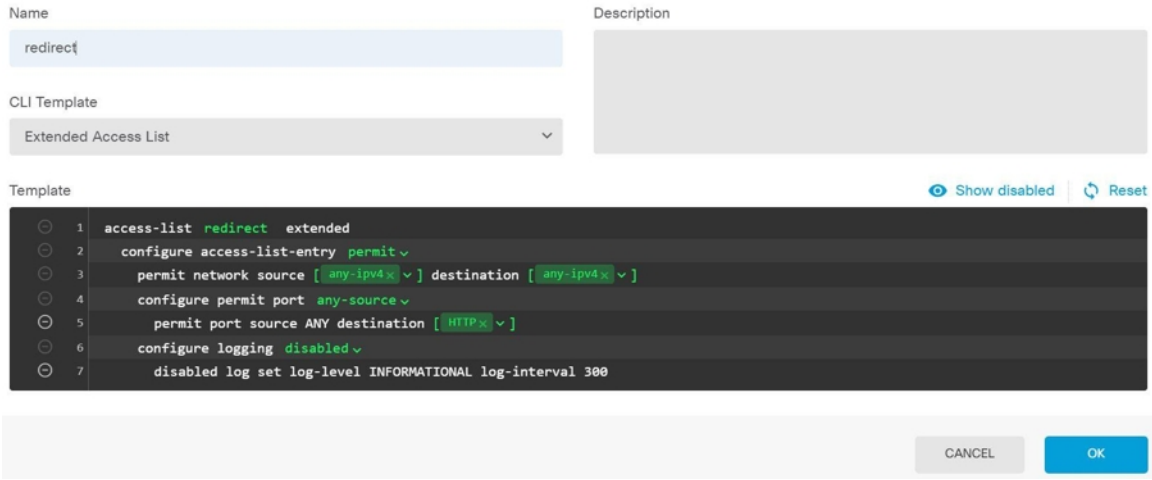
c. ACL의 이름을 입력합니다. 예: **redirect(**리디렉션**)**.

d. **CLI Template(CLI** 템플릿**)**에서 **Extended Access List(**확장 액세스 목록**)**를 선택합니다.

e. **Template(**템플릿**)** 본문에서 다음과 같이 구성합니다.

   - configure access-list-entry action = permit
   - source-network = any-ipv4
   - destination-network = any-ipv4
   - configure permit port = any-source
   - destination-port = HTTP
   - configure logging = disabled

   ACE는 다음과 같이 표시되어야 합니다.



f. **OK(**확인**)**를 클릭합니다.

이 ACL은 다음번에 변경 사항을 구축할 때 구성됩니다. 다른 정책에서 개체를 사용하여 구축을 강제 적용할 필요가 없습니다.

Note
이 ACL은 IPv4에만 적용됩니다. IPv6도 지원하려면 속성이 모두 동일한 두 번째 ACE를 추가하기만 하면 됩니다. 단, 소스 및 대상 네트워크용으로 선택된 any-ipv6은 제외합니다. 트래픽이 ISE 또는 DNS 서버로 리디렉션되지 않도록 다른 ACE를 추가할 수도 있습니다. 먼저 해당 서버의 IP 주소를 보유할 호스트 네트워크 개체를 생성해야 합니다.

단계 **3** 동적 권한 부여를 위해 RADIUS 서버 그룹을 구성합니다.

Firepower Threat Defense RADIUS 서버 개체나 그룹 생성 또는 편집 섹션에 제공된 지침에 따라 아래 단계를 수행합니다.

a. RADIUS 서버 개체 생성

b. RADIUS 서버 그룹 생성

단계 **4** 이 RADIUS 서버 그룹을 사용하는 연결 프로파일을 생성합니다. RA VPN 연결 프로파일 구성을 참조하십시오. **AAA Authentication(AAA** 인증**)**을 사용하고(이것만 사용하거나 인증서와 함께 사용), **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)**, **Authorization(**권한 부여**)** 및 **Accounting(**어카운트 관리**)** 옵션에서 서버 그룹을 선택합니다.

FDM-관리 디바이스의 원격 액세스 VPN 구성 확인

원격 액세스 VPN을 구성하고 디바이스에 구성을 구축한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

Procedure

단계 **1** 외부 네트워크에서 AnyConnect 클라이언트를 사용하여 VPN 연결을 설정합니다. 웹 브라우저를 사용하여 **https://** *ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. 사용자가 FTD에 AnyConnect 클라이언트 소프트웨어를 설치하는 방법을 참조하십시오. 그룹 URL을 구성한 경우, 그룹 URL도 시도해 보십시오.

단계 **2** **Security Devices(**보안 디바이스**)** 페이지에서 확인하려는 디바이스를 선택하고 **Device Actions(**디바이스 작업**)**에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **3** **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 봅니다.

단계 **4** 통계에는 활성 AnyConnect 클라이언트 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야 합니다. 다음은 명령의 샘플 출력입니다.

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                           Active : Cumulative : Peak Concur : Inactive
                          ------------------------------------------------
AnyConnect Client         :      1 :         49 :           3 :        0
  SSL/TLS/DTLS            :      1 :         49 :           3 :        0
Clientless VPN            :      0 :          1 :           1
  Browser                 :      0 :          1 :           1
----------------------------------------------------------------------------


  Total Active and Inactive    :      1            Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  Tunnels Summary
  ----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
  Clientless                :      0 :          1 :               1
  AnyConnect-Parent         :      1 :         49 :               3
  SSL-Tunnel                :      1 :         46 :               3
  DTLS-Tunnel               :      1 :         46 :               3
  ----------------------------------------------------------------------------
  Totals                    :      3 :        142
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  IPv6 Usage Summary
  ----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
  AnyConnect SSL/TLS/DTLS   :        :            :
    Tunneled IPv6           :      1 :         20 :               2
  ----------------------------------------------------------------------------
```

단계 **5** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

FDM-관리 디바이스의 원격 액세스 VPN 구성 세부 정보 보기

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **End User Connections(**엔드 유저 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **ASA & FDM**를 선택합니다.

단계 **2** 존재하는 VPN 구성 개체를 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

- RA VPN 구성을 확장하여 연결된 모든 연결 프로파일을 확인합니다.
  - 추가 + 버튼을 클릭하여 새 연결 프로파일을 추가합니다.
  - 보기 버튼( )을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭하여 변경 사항을 편집할 수 있습니다.
- **Actions(**작업**)** 아래의 다음 옵션 중 하나를 클릭하여 추가 작업을 수행할 수 있습니다.
  - 그룹 정책을 할당/추가하려면 **Group Policies(**그룹 정책**)**를 클릭합니다.
  - 더 이상 필요하지 않은 구성 개체 또는 연결 프로파일을 클릭하고 **Remove(**제거**)**를 클릭하여 삭제합니다.

원격 액세스 가상 프라이빗 네트워크 세션

원격 액세스 가상 프라이빗 네트워크는 모바일 사용자 또는 재택 근무자와 같은 원격 사용자에게 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요한 지표를 한눈에 확인할 수 있습니다. Security Cloud Control 원격 액세스 VPN 모니터링 기능을 사용하면 원격 액세스 VPN 문제의 존재 여부와 그 위치를 신속하게 파악할 수 있습니다. 그런 다음 이 정보를 적용하고 네트워크 관리 도구를 사용하여 네트워크 및 사용자의 문제를 줄이거나 없앨 수 있습니다. 필요에 따라 원격 액세스 VPN 세션의 연결을 끊을 수도 있습니다.

Remote Access Virtual Private Monitoring(원격 액세스 가상 프라이빗 모니터링) 페이지는 다음 정보를 제공합니다.

- 최대 1년 동안의 활성 및 기록 세션 목록입니다.
- Security Cloud Control에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 Security Cloud Control 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 디바이스 유형, 디바이스 이름, 세션 길이, 전송 및 수신된 데이터의 양과 같은 기준을 기반으로 검색 범위를 좁힐 수 있는 필터링 기능입니다.

관련 정보:

- 라이브 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 121
- 기록 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 123
- RA VPN 세션 검색 및 필터링
- RA VPN 모니터링 보기 사용자 지정
- RA VPN 세션을 CSV 파일로 내보내기
- FTD에서 활성 RA VPN 세션 연결 끊기

라이브 **AnyConnect** 원격 액세스 **VPN** 세션 모니터링

디바이스의 활성 AnyConnect 원격 액세스 VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 이 데이터는 10분마다 자동으로 새로 고쳐집니다. 언제든지 최신 세션 목록을 검색하려면 화면 오른쪽 모서리에 나타나는 다시 로드 아이콘 을 클릭하십시오.

시작하기 전에

- 원격 액세스 VPN 헤드 엔드를 Security Cloud Control에 온보딩합니다.

- 라이브 데이터를 모니터링하려는 디바이스의 연결 상태는 **Security Devices(**보안 디바이스**)** 페이지에서 "Online(온라인)"인지 확인합니다.

프로시저

단계 **1** 왼쪽 창에서 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **Reports & Analytics(**보고서 및 애널리틱스**)** > **Remote Access Monitoring(**원격 액세스 모니터링**)**을 클릭합니다.

단계 **2** **RA VPN**을 클릭합니다.

단계 **3** **Live(**라이브**)**를 클릭합니다.

RA VPN 세션을 검색 및 필터링하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

참고
데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

라이브 원격 액세스 VPN 데이터 보기

라이브 데이터는 대시보드 및 테이블 형식으로 표시됩니다.

Dashboard(대시보드**)** 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭해야 합니다.

대시보드는 Security Cloud Control에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다.

- **Breakdown (All Devices)(**애널리틱스 데이터**(**모든 디바이스**))**: 총 라이브 세션 수를 표시합니다. 4개의 호 길이로 구분된 원도표도 표시됩니다. 세션 수가 가장 많은 상위 3개 디바이스의 VPN 세션 비율을 보여줍니다. 나머지 호 길이는 다른 디바이스의 어그리게이션를 나타냅니다.
- Security Cloud Control 테넌트에서 가장 많이 사용되는 운영 체제 및 연결 프로파일이 표시됩니다.
- 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- **Active Sessions by Country(**국가별 활성 세션**)**: RA VPN 헤드엔드에 연결된 사용자 위치의 인터랙티브 히트맵을 표시합니다.
  - 사용자가 연결한 국가는 해당 국가에서 설정된 세션의 상대적 비율에 따라 점점 더 짙은 파란색 음영으로 표시됩니다. 파란색이 어두울수록 해당 국가에서 더 많은 세션이 설정되었음을 의미합니다.
  - 맵의 맨 아래에 있는 범례는 국가의 세션 수와 국가를 표시하는 데 사용되는 파란색 음영 간의 상관관계를 나타내는 척도를 제공합니다.

- 맵에 마우스 포인터를 올려놓으면 해당 국가의 이름 및 해당 국가에서 설정된 총 활성 사용자 세션 수를 확인할 수 있습니다.
- 테이블 위에 마우스 포인터를 올려놓으면 해당 국가의 위치와 맵의 총 활성 사용자 세션 수를 확인할 수 있습니다.

테이블 형식 보기

데이터를 테이블 형식으로 보려면 화면의 오른쪽 상단 모서리에 있는 **Show Tabular View(**테이블 형식 보기 표시**)** 아이콘을 클릭합니다.

테이블 형식은 현재 연결된 VPN 사용자의 전체 목록을 제공합니다.

- **Location(**위치**)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.

중요 Security Cloud Control는 라이브 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 사용자 지정 필터는 시각적 대시보드 보기에서 지원되지 않으므로, 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 적용한 모든 필터를 제거하려면 **Clear(**지우기**)**를 클릭합니다. 표준 필터는 제거할 수 없습니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(**활성**)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

기록 AnyConnect 원격 액세스 VPN 세션 모니터링

지난 1년 동안 기록된 AnyConnect 원격 액세스 VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

시작하기 전에

- RA VPN 헤드 엔드를 Security Cloud Control에 온보딩합니다.

프로시저

단계 **1** 왼쪽 창에서 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **Reports & Analytics(**보고서 및 애널리틱스**)** > **Remote Access Monitoring(**원격 액세스 모니터링**)**을 클릭합니다.

단계 **2** **RA VPN**을 클릭합니다.

단계 **3** **Historical(**기록**)**을 클릭합니다.

- 원격 액세스 VPN 세션 데이터는 저장되며 1년간 조회할 수 있습니다.
- RA VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.
- 데이터 **TX** 및 데이터 **RX** 정보는 Secure Firewall Threat Defense에서 사용할 수 없습니다.

원격 액세스 VPN 데이터 기록 보기

이력 데이터는 대시보드 및 표 형식으로 표시됩니다.

Dashboard(대시보드**)** 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭해야 합니다. 테이블 보기와 함께 대시보드 보기가 표시됩니다.

대시보드는 Security Cloud Control에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다. 지난 24시간, 7일 및 30일 동안 모든 디바이스에 대해 기록된 VPN 세션을 보여주는 막대 그래프를 제공합니다. 드롭다운에서 기간을 선택할 수 있습니다. 개별 막대에 마우스 커서를 대면 해당 날짜의 총 세션 수와 날짜를 확인할 수 있습니다.

테이블 형식 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Tabular View(**테이블 형식 보기 표시**)** 아이콘을 클릭하여 테이블 형식 보기만 표시해야 합니다. 테이블 형식은 지난 1년 동안 연결된 VPN 사용자의 전체 목록을 제공합니다.

Location(위치**)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.

중요 Security Cloud Control는 기록 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 대시보드는 맞춤형 필터를 지원하지 않으므로 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 새로 적용된 필터를 지우면 대시보드가 다시 실행됩니다. 화면에서 **Clear(**지우기**)**를 클릭하여 수동으로 적용된 필터를 제거합니다. 표준 필터는 제거할 수 없습니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 세션 날짜와 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(**활성**)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

원격 액세스 VPN 세션 검색 및 필터링

검색

검색 창 기능을 사용하여 원격 액세스 VPN 세션을 찾습니다. 검색 창에 디바이스 이름, IP 주소 또는 일련 번호를 입력하기 시작합니다. 그러면 검색 기준에 맞는 원격 액세스 VPN 세션이 표시됩니다. 검색은 대/소문자를 구분하지 않습니다.

필터

필터 사이드바를 사용하여 세션 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 원격 액세스 VPN 세션을 찾습니다. 필터 기능은 라이브 보기와 기록 보기 모두에서 사용할 수 있습니다.

- **Filter by Devices(**디바이스별 필터링**)**: **All Types(**모든 유형**)** 탭에서 하나 또는 모든 디바이스를 선택하여 선택한 디바이스의 세션을 봅니다. 창은 또한 유형에 따라 디바이스를 분류하고 해당 탭 아래에 표시합니다.
- **Sessions Time Range(**세션 시간 범위**)(**기록 데이터에만 적용 가능): 지정된 날짜 및 시간 범위의 기록 세션을 표시합니다. 지난 3개월 동안 기록된 데이터를 볼 수 있습니다.
- **Sessions Length(**세션 길이**)**: 지정된 세션의 기간 길이를 기준으로 세션을 표시합니다. 시간 단위(시간, 분 또는 초)를 설정하고 슬라이더를 이동하여 최소 및 최대 기간 길이를 지정합니다. 제공된 필드에 길이를 지정할 수도 있습니다.
- **Upload (TX)(**업로드**(TX))**: 보안 네트워크에 업로드되거나 전송된 데이터의 지정된 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.
- **Download (RX)(**다운로드**(RX))**: 보안 네트워크에서 다운로드하거나 수신한 지정된 데이터 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.

원격 액세스 VPN 모니터링 보기 사용자 지정

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 모드에서 원격 액세스 VPN 모니터링 보기를 편집할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘  을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.

Security Cloud Control는 다음에 Security Cloud Control에 로그인할 때 선택 항목을 기억합니다.

원격 액세스 VPN 세션을 CSV 파일로 내보내기

하나 이상의 디바이스의 원격 액세스 VPN 세션을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. Microsoft Excel과 같은 스프레드시트 애플리케이션에서 .csv 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다. 이 정보는 원격 액세스 VPN 세션을 분석하는 데 도움이 됩니다. 세션을 내보낼

때마다 Security Cloud Control는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.

Security Cloud Control는 최대 100,000개의 활성 세션을 CSV 파일로 내보낼 수 있습니다. 모든 디바이스의 총 세션 수가 최대 제한을 초과하는 경우 **View By Device(**디바이스별 보기**)** 필터를 사용하여 개별 디바이스에 대한 보고서를 생성할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **Reports & Analytics(**보고서 및 애널리틱스**)** > **Remote Access Monitoring(**원격 액세스 모니터링**)**을 클릭합니다.

단계 **2** **View By Devices(**디바이스별 보기**)** 영역에서 다음 중 하나를 선택합니다.

- **All Devices(**모든 디바이스**)** - 그 아래에 나열된 모든 디바이스에서 활성 세션을 내보냅니다.
- 해당 디바이스의 세션을 내보낼 디바이스를 클릭합니다.

단계 **3** 오른쪽 상단에 있는 아이콘을 클릭하면 Security Cloud Control는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.

단계 **4** 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

원격 액세스 VPN 대시보드

Security Cloud Control는 ASA , 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense및 FDM 관리 디바이스의 원격 액세스 VPN 연결에 대한 통합 정보를 제공합니다.

1. 왼쪽 창 에서 **Secure Connections(**보안 연결**)** > **Remote Access VPN(**원격 액세스 **VPN)**을 클릭합니다.

   - **VPN Tunnel Status(VPN** 터널 상태**)**: 활성 및 유휴 VPN 터널을 각각 적절한 색상으로 나타내는 원형 차트가 표시됩니다. 이 차트는 헤드엔드별 상위 10개의 원격 액세스 VPN 세션 수를 보여줍니다.
   - **Statistics(**통계**)**: 평균 세션 기간과 업로드 및 다운로드한 데이터를 표시합니다.

FDM-관리 디바이스에서 원격 액세스 VPN 세션 연결 끊기

현재 Security Cloud Control 인터페이스를 사용하는 FDM 관리 디바이스에서 원격 액세스 VPN 세션을 종료하는 것은 불가능합니다. 대신 SSH를 사용하여 Firewall Threat Defense CLI에 연결하고 원하는 사용자의 연결을 끊을 수 있습니다. Security Cloud Control에 온보딩된 온라인 FDM 관리 디바이스에서 이 작업을 수행할 수 있습니다.

Procedure

단계 1 Firewall Device Manager에 로그인하고 디바이스에서 실행 중인 버전에 맞는 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 "시작하기" 장의 명령줄 인터페이스(CLI)에 로그인 섹션에 설명된 대로 디바이스 CLI를 사용합니다.

단계 2 `vpn-sessionsdb logoff {name}` 명령을 실행하고 **name**을 사용자 이름으로 대체합니다. 이 명령은 지정한 사용자 이름에 대한 모든 세션을 종료합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.