Cisco Firepower Threat Defense Dynamic Access Policy 활용 사례

초판: 2021년 7월 8일

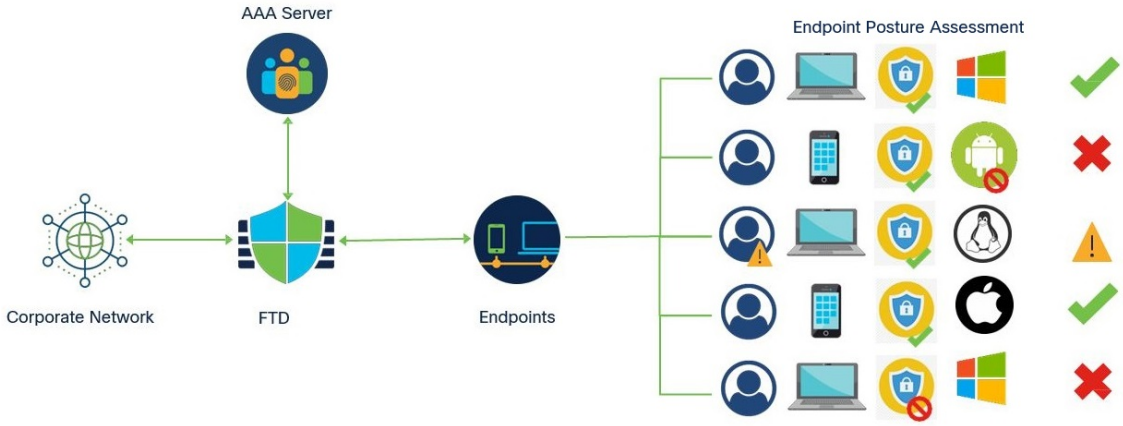
최종 변경: 2022년 9월 21일

Cisco Firepower Threat Defense Dynamic Access Policy

Firepower Threat Defense FTD에서 DAP(Dynamic Access Policy)를 사용하면 VPN 환경의 역동성을 해결하기 위한 권한 부여를 구성할 수 있습니다. Firepower Management Center FMC 웹 인터페이스를 통해 액세스 제어 속성 모음을 구성하여 DAP를 생성할 수 있습니다. 속성을 특정 사용자 터널 또는 세션과 연결할 수 있습니다. 이러한 속성은 여러 그룹 멤버십 및 엔드포인트 보안 문제를 처리합니다.

FTD은(는) DAP 구성에 따라 특정 사용자 세션에 VPN 액세스 권한을 부여합니다. FTD은(는) 하나 이상의 DAP 레코드에서 속성을 선택하고 집계한 다음 사용자 인증 중에 DAP를 생성합니다. FTD은(는) 원격 디바이스의 엔드포인트 보안 정보 및 AAA 정보를 기반으로 DAP 레코드를 선택합니다. FTD은(는) 그런 다음 DAP 레코드를 사용자 터널 또는 세션에 적용합니다.

그림 ***1: Dynamic Access Policy*** 예



DAP 구성의 요소

새 DAP 구성에서는 DAP 정책, DAP 레코드 및 DAP 기준 속성을 생성해야 합니다.

- **Dynamic Access Policy** - DAP 구성은 레코드로 이루어집니다.
- **DAP Record(DAP 레코드)** - DAP 레코드는 기준 엔드포인트 평가 및 사용자 권한 부여(AAA) 속성으로 이루어집니다. 레코드가 일치하는 경우 DAP는 VPN 세션에 적용할 작업을 정의합니다.

- **DAP Criteria and Attributes(DAP** 기준 및 속성**)** - AAA Criteria(AAA 기준), Endpoint Criteria(엔드포인트 기준) 및 Advanced Criteria(고급 기준)에는 네트워크 액세스에 대한 세분화된 구성 속성이 포함되어 있습니다.

자세한 구성 단계는 Dynamic Access Policy 구성, 4 페이지 섹션을 참조하십시오.

DAP에서 FTD 원격 액세스 VPN이 작동하는 방식

1. 원격 사용자가 엔드포인트 디바이스에서 AnyConnect Secure Mobility Client를 사용하여 VPN 연결을 시도합니다.
2. FTD는 엔드포인트에서 보안 상태 평가를 수행합니다.
3. FTD에서 AAA(인증, 권한 부여 및 계정 관리) 서버를 통해 사용자를 인증합니다. 또한 AAA 서버에서 해당 사용자에 대한 권한 부여 속성을 반환합니다.
4. FTD에서 AAA 권한 부여 속성을 세션에 적용하고 VPN 터널을 설정합니다.
5. FTD에서 사용자 AAA 권한 부여 정보 및 보안 상태 평가 정보를 기반으로 DAP 레코드를 선택합니다.
6. FTD에서 선택한 DAP 레코드로부터 DAP 속성을 집계하여 DAP 정책을 생성합니다.
7. FTD에서 DAP 정책을 원격 액세스 VPN 세션에 적용합니다.

DAP를 구현하는 이유

DAP 속성을 구성하여 연결하는 엔드포인트를 식별하고 다양한 네트워크 리소스에 대한 사용자 액세스 권한을 부여할 수 있습니다. 다음 시나리오에 대한 DAP를 생성할 수 있으며, DAP 속성으로 더 많은 작업을 수행하여 엔드포인트 및 네트워크 리소스를 보호할 수 있습니다.

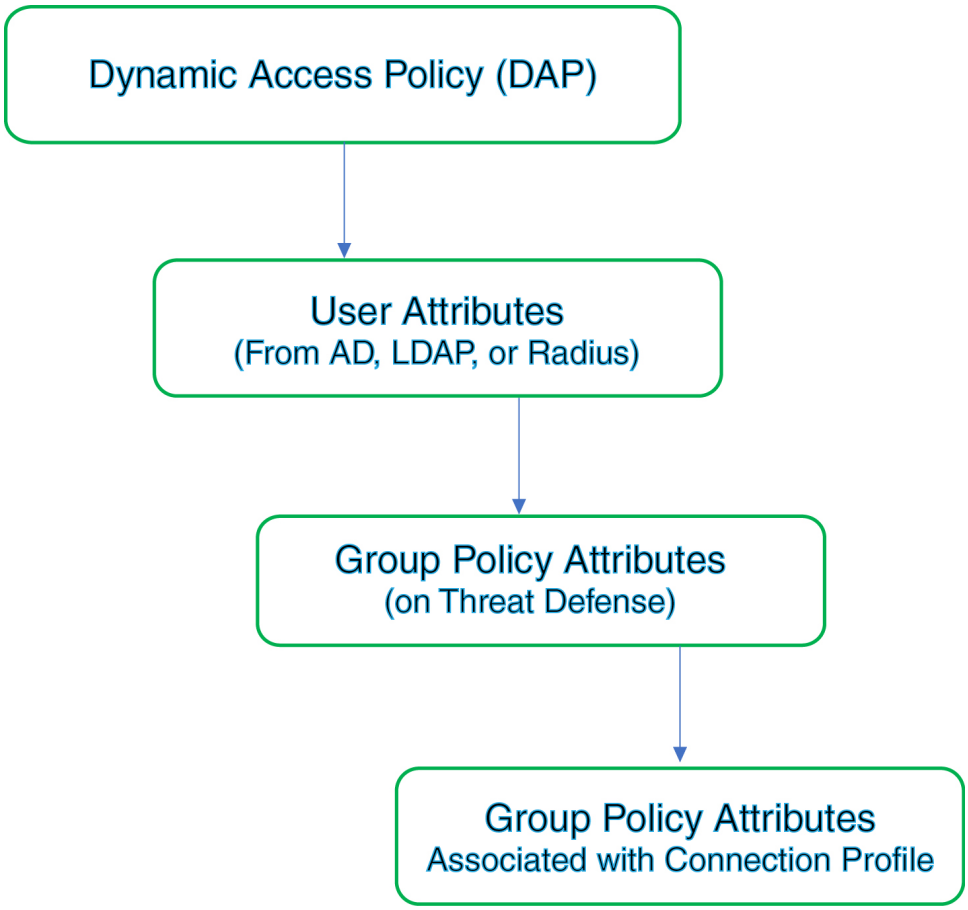
- VPN에 연결하는 엔드포인트가 엔드포인트 디바이스나 플랫폼과 상관없이 조직의 보안 정책을 준수하는지 확인합니다.
- 운영 체제, 엔드포인트에서 실행 중인 다양한 보안 소프트웨어, 레지스트리 설정, 파일 버전 및 엔드포인트에서 실행 중인 잠재적 키 입력 로거를 파악합니다.
- 회사에서 관리하는 엔드포인트에서 애플리케이션의 가용성 및 업데이트를 탐지하고 적용합니다. (예: 안티바이러스 소프트웨어)
- 권한이 있는 사용자가 액세스할 수 있는 네트워크 리소스를 결정합니다.

FTD에서 권한 및 속성 정책 시행

FTD 디바이스는 VPN 연결에 사용자 권한 부여 속성(사용자 권한 또는 허가라고도 함)을 적용할 수 있습니다. 속성은 457903FTD, 외부 인증 서버 및/또는 권한 부여 AAA 서버(RADIUS)의 DAP 또는 FTD 디바이스의 그룹 정책에서 적용됩니다.

FTD 디바이스가 모든 소스에서 속성을 수신하면 FTD에서 평가, 병합 및 사용자 정책에 적용합니다. DAP, AAA 서버 또는 그룹 정책에서 제공하는 속성 간에 충돌이 발생하면 DAP에서 가져온 속성이 항상 우선적으로 적용됩니다.

그림 *2:* 정책 시행 흐름



1. FTD의 **DAP** 속성 — DAP 속성은 다른 모든 속성보다 우선적으로 적용됩니다.
2. **AAA** 서버의 사용자 속성 - 사용자 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이러한 속성을 반환합니다.
3. FTD에 구성된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS 클래스 속성 IETF-Class-25(OU=group-policy) 값을 반환하면 FTD 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.

4. 연결 프로파일에서 할당한 그룹 정책**(**터널 그룹으로 알려짐**)** - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다.

참고 FTD 디바이스는 기본 그룹 정책인 *DfltGrpPolicy*에서 시스템 기본 속성 상속을 지원하지 않습니다. 연결 프로파일에 할당된 그룹 정책 속성은 사용자 속성이나 AAA 서버의 그룹 정책에서 재정의하지 않는 경우 사용자 세션에 사용됩니다.

동적 액세스 정책에 대한 라이센싱

FTD에는 원격 액세스 VPN을 지원하는 AnyConnect 라이선스 중 하나가 있어야 합니다.

- AnyConnect Apex
- AnyConnect Plus
- AnyConnect VPN 전용

FMC에 내보내기 제어 기능이 활성화되어 있어야 합니다.

FTD 라이선스에 대한 자세한 내용은 *Cisco Secure Firewall Management Center* 구성 가이드의 *Firepower System* 라이선싱 장을 참조하십시오.

Dynamic Access Policy 구성

DAP(Dynamic Access Policy)는 사용자 및 엔드포인트 속성을 구성하는 여러 DAP 레코드를 포함할 수 있습니다. 사용자가 VPN 연결을 시도할 때 필수 기준이 적용되도록 DAP 레코드의 우선순위를 지정할 수 있습니다.

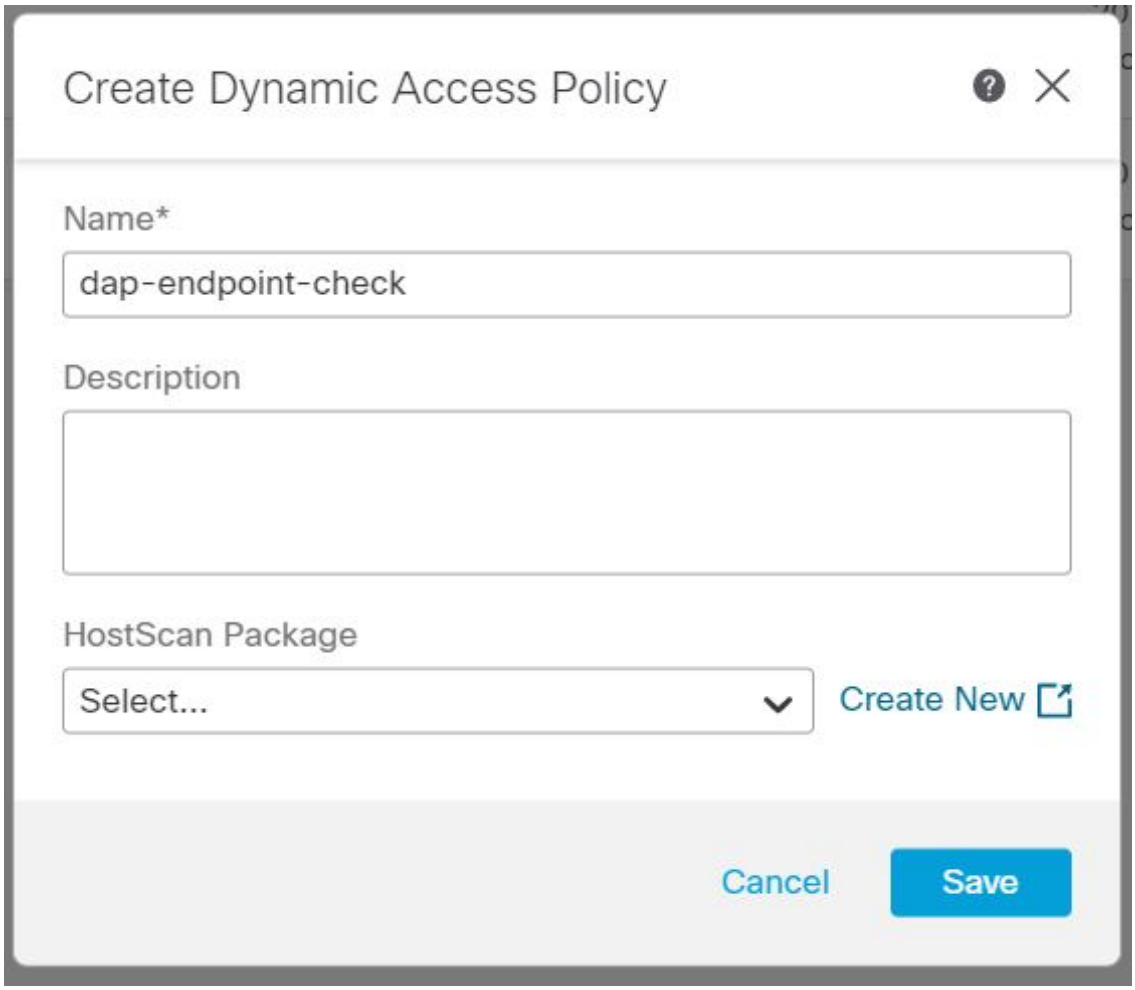
시작하기 전에

DAP(Dynamic Access Policy)를 생성하기 전에 필수 애플리케이션 및 설정을 구성해야 합니다.

- **Host Scan Package(Host Scan** 패키지**)** - Host Scan 패키지 버전 4.6 이상을 다운로드합니다.
- **AAA Server(AAA** 서버**)** - VPN 세션을 인증하거나 권한을 부여하는 동안 올바른 속성을 반환하도록 필요한 AAA 서버를 구성합니다.
- **AnyConnect Client(AnyConnect** 클라이언트**) Package(**패키지**)** - 최신 버전의 AnyConnect Secure Mobility client(AnyConnect Secure Mobility 클라이언트)를 다운로드하여 원격 액세스 VPN 구성에 추가합니다.
- **Remote Access VPN(**원격 액세스 **VPN) - Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**에서 원격 액세스 VPN 구성 마법사를 사용하여 원격 액세스 VPN 설정을 구성합니다.
- **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**에서 Host Scan 패키지를 업로드합니다.

1. 아직 지정하지 않은 경우 새 동적 정책을 구성합니다.
   a) **Devices(**디바이스**)** > **Dynamic Access Policy(**동적 액세스 정책**)** > **Create Dynamic Access Policy(**동적 액세스 정책 생성**)**를 선택합니다.

   그림 ***3: Dynamic Access Policy*** 생성



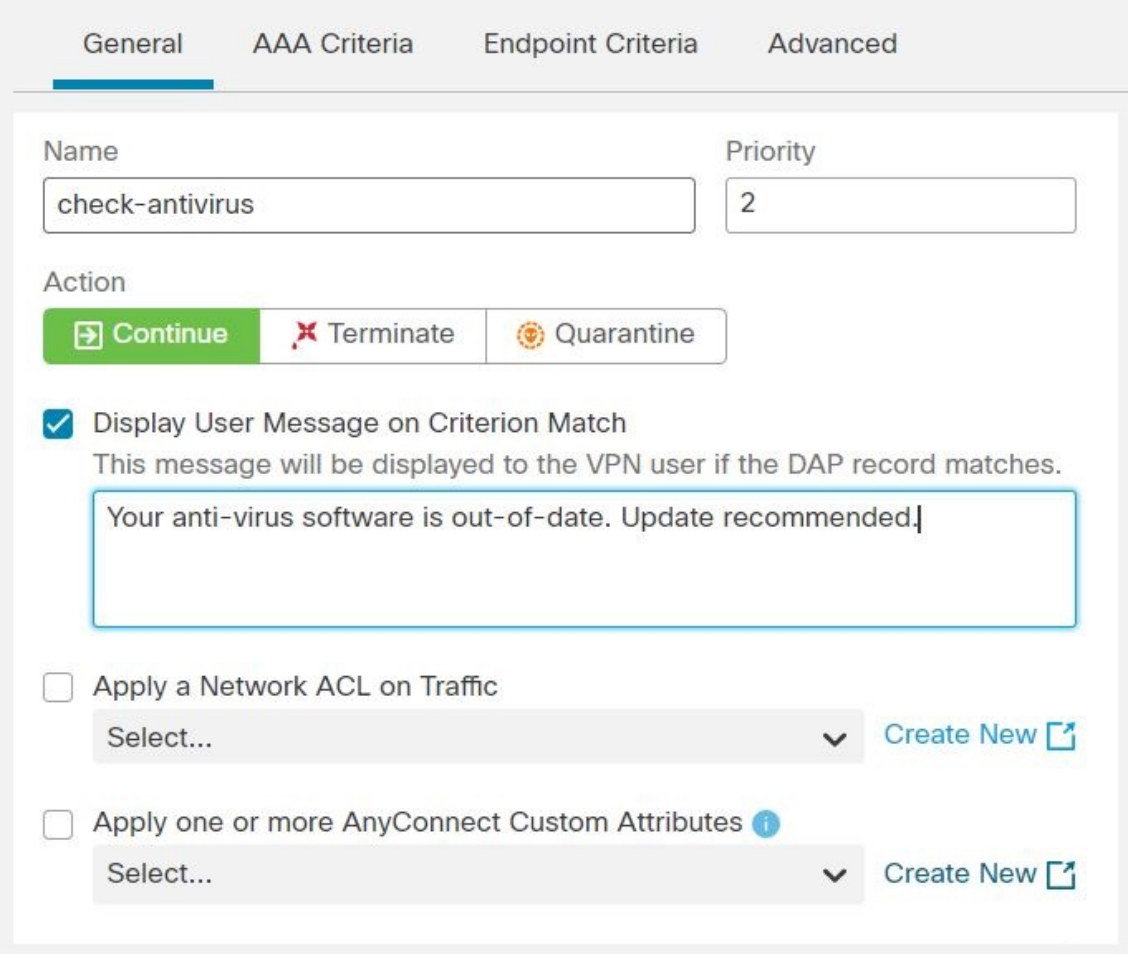
   b) DAP 정책의 **Name(**이름**)**을 지정하고 필요에 따라 **Description(**설명**)**을 입력합니다.
   c) 드롭다운에서 **Host Scan Package(Host Scan** 패키지**)**를 선택합니다. 아니면 **Create New(**새로 만들기**)**를 클릭하여 Host Scan 패키지 파일을 추가합니다.
   Dynamic Access Policy에는 기본 DAP 레코드가 포함되어 있습니다. Lua 스크립트를 사용하여 AAA Criteria(AAA 기준), Endpoint Criteria(엔드포인트 기준) 및 Advanced Criteria(고급 기준)에서 필수 속성이 있는 DAP 레코드를 추가할 수 있습니다.
   d) **Save(**저장**)**를 클릭합니다.
2. DAP 레코드를 생성하고 우선순위 번호를 할당합니다.

   DAP 레코드에는 VPN 사용자가 FTD VPN 게이트웨이로의 VPN 연결을 시도할 때 일치시키기 위한 속성이 포함되어 있습니다. DAP 레코드 설정을 사용하여 선택한 기준 속성을 기반으로 VPN 액세스를 허용, 거부 또는 제한할 수 있습니다.

우선순위 번호는 레코드가 일치하는 순서를 나타냅니다. FTD은(는) DAP 레코드의 우선순위 번호를 사용하여 레코드를 시퀀싱하고 선택합니다. 번호가 낮을수록 우선순위가 높아집니다.

참고 DAP에 대해 DAP 레코드를 구성하지 않으면 기본 **DAP** 레코드가 적용됩니다. 기본 DAP 레코드에는 우선순위가 없습니다.

a) **Devices(**디바이스**)** > **Dynamic Access Policy(**동적 액세스 정책**)**를 선택합니다.
b) 기존 DAP 정책을 편집하거나 새로 생성합니다.
c) **Create DAP Record(DAP** 레코드 생성**)**를 클릭합니다.



d) DAP 레코드의 **Name(**이름**)**을 지정합니다.
e) DAP 레코드의 **Priority(**우선순위**)** 번호를 입력합니다.
f) DAP 레코드가 일치하는 경우 수행할 **Action(**작업**)**을 선택합니다.

- **Continue(**계속**)** - 액세스 정책 속성을 세션에 적용하고 사용자를 허용하려면 클릭합니다.
- **Terminate(**종료**)** - 세션을 종료하려면 선택합니다.

- **Quarantine(**격리**)** - 연결을 격리하려면 선택합니다.

g) **Display User Message on Criterion Match(**기준 일치 시 사용자 메시지 표시**)**를 선택하고 상자에 메시지를 추가합니다.

참고 VPN 사용자는 DAP 레코드가 일치할 때 메시지를 받게 됩니다.

h) **Apply a Network ACL on Traffic(**트래픽에서 네트워크 **ACL** 적용**)** 확인란을 선택하고 목록에서 ACL을 선택합니다. ACL을 새로 생성한 다음 선택할 수도 있습니다.

해당 DAP 레코드가 일치하면 네트워크 ACL이 VPN 세션에 적용됩니다.

i) **Apply one or more AnyConnect Custom Attributes(**하나 이상의 **AnyConnect** 맞춤형 속성 적용**)**를 선택하고 드롭다운에서 맞춤형 속성 개체를 선택합니다.

j) **Save(**저장**)**를 클릭합니다.

네트워크 ACL 및 AnyConnect 맞춤형 속성에 대한 내용은 최신 Firepower Management Center 구성 가이드를 참조하십시오.

k) 사용자 및 엔드포인트가 VPN에 연결할 때 확인할 DAP 속성을 구성합니다.

- DAP에 대한 AAA 기준 설정 구성, 8 페이지
- DAP에서 엔드포인트 속성 선택 조건 구성, 10 페이지
- DAP에 대한 고급 설정 구성, 11 페이지

3. DAP를 원격 액세스 VPN 구성과 연결합니다.

VPN 세션 인증 또는 권한 부여 중에 DAP 속성을 일치시키려면 DAP를 원격 액세스 VPN 정책과 연결해야 합니다.

a) Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

b) DAP를 추가할 원격 액세스 정책을 선택하여 편집합니다.

a) Dynamic Access Policy 연결 링크를 클릭합니다.

b) 목록에서 **Dynamic Access Policy**를 선택합니다.

c) **Ok(**확인**)**를 클릭합니다.

DAP를 원격 액세스 VPN에 연결하면 FTD에서 사용자가 VPN 연결을 시도할 때 구성된 DAP 레코드 및 속성을 확인합니다. FTD에서는 일치를 기반으로 DAP를 생성하고 VPN 세션에서 적절한 작업을 수행합니다.

4. FTD 디바이스에 원격 액세스 VPN을 구축합니다.

a) FMC 메뉴 모음에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment(**구축**)**를 선택합니다.

FTD 디바이스에서 구축 보류 중인 오래된 구성 목록을 모두 볼 수 있습니다.

b) 원격 액세스 VPN 및 기타 구성 변경 사항을 구축할 디바이스를 파악하고 선택합니다.

c) **Deploy(**구축**)**를 클릭합니다.

참고 구성을 구축하기 전에 모든 오류를 수정하십시오.

DAP에 대한 AAA 기준 설정 구성

FTD는 AAA 서버에서 VPN 세션에 연결된 AAA 속성을 통해 사용자 또는 사용자 그룹을 일치시킵니다.

DAP는 AAA가 제공하는 속성을 재정의할 수 있는 제한된 권한 부여 속성 집합을 제공하여 AAA 서비스를 보완합니다. FTD은(는) VPN 세션에 대한 AAA 권한 부여 정보 및 보안 상태 평가 정보를 기반으로 DAP 레코드를 선택합니다. FTD는 평가에 따라 여러 DAP 레코드를 선택한 다음 집계하여 DAP 권한 부여 속성을 생성할 수 있습니다.

시작하기 전에

VPN 사용자 인증, 권한 부여 및 계정 지정에 필요한 AAA 서버를 구성했는지 확인합니다. 원격 액세스 VPN을 구축하려는 FTD 디바이스에서 AAA 서버에 연결할 수 있어야 합니다.

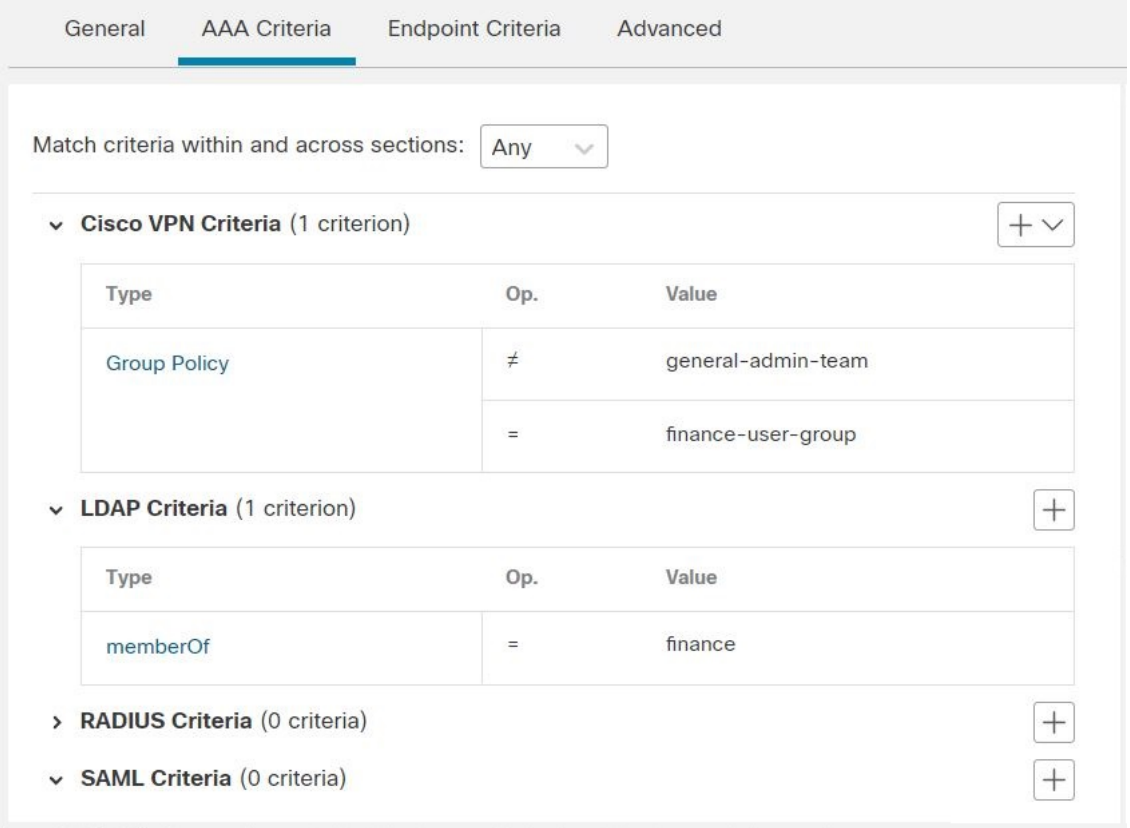
프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy(**동적 액세스 정책**)**를 선택합니다.

단계 **2** 기존 DAP 정책을 편집하거나 새 정책을 생성한 다음 편집합니다.

단계 **3** DAP 레코드를 선택하거나 새 레코드를 생성하고 DAP 레코드를 수정합니다.

단계 **4** **AAA Criteria(AAA** 기준**)**를 클릭합니다.



단계 **5** 다음의 **Match criteria between sections(**섹션 간 일치 기준**)** 중에서 하나를 선택합니다.

- **Any(**일부**)** - 일부 기준과 일치합니다.
- **All(**모두**)** - 설정된 모든 기준과 일치합니다.
- **None(**없음**)** - 설정된 기준과 일치하지 않습니다.

단계 **6** **Add(**추가**)**를 클릭하여 필요한 **Cisco VPN Criteria(Cisco VPN** 기준**)**를 추가합니다.

Cisco VPN 기준에는 그룹 정책, 할당된 IPv4 주소, 할당된 IPv6 주소, 연결 프로파일, 사용자 이름, 사용자 이름 2 및 필수 SCEP에 대한 사전 정의된 속성이 포함됩니다.

a) **Attribute ID(**속성 **ID)** 및 연산자를 선택한 다음 일치시킬 **Value(**값**)**를 지정합니다.
b) AAA 기준을 더 추가하려면 **Add another criteria(**다른 기준 추가**)**를 클릭합니다.
c) **Save(**저장**)**를 클릭합니다.

단계 **7** **LDAP Criteria(LDAP** 기준**)**, **RADIUS Criteria(RADIUS** 기준**)** 또는 **SAML Criteria(SAML** 기준**)**를 선택합니다. **Attribute ID(**속성 **ID)** 및 **Value(**값**)**를 지정합니다.

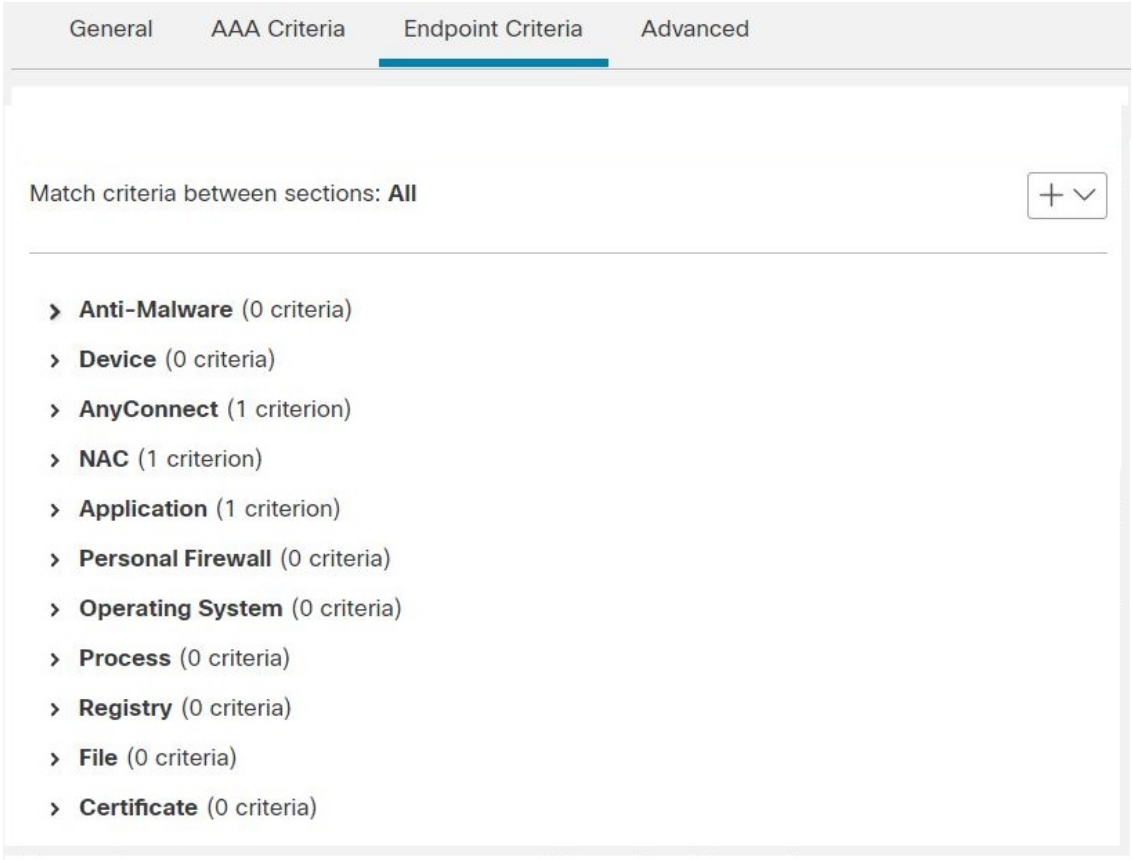
이러한 속성을 입력한 값과 같음(=) 또는 같지 않음(≠)으로 설정할 수 있습니다. 각 DAP 레코드에 대해 AAA 속성을 원하는 만큼 추가할 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

DAP에서 엔드포인트 속성 선택 조건 구성

엔드포인트 속성은 엔드포인트 시스템 환경, 상태 진단 결과 및 애플리케이션에 대한 정보를 포함합니다. FTD에서는 세션을 설정하는 동안 엔드포인트 속성 모음을 생성하고 이러한 속성을 해당 세션과 연계된 데이터베이스에 저장합니다. 각 DAP 레코드는 FTD에서 세션에 대해 선택하기 위해 충족해야 하는 엔드포인트 선택 속성을 지정합니다. FTD에서는 구성된 모든 조건을 충족하는 DAP 레코드만 선택합니다.

그림 ***4: DAP*** 엔드포인트 속성



프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy(**동적 액세스 정책**)** > **Create Dynamic Access Policy(**동적 액세스 정책 생성**)**를 선택합니다.

단계 **2** DAP 정책을 수정한 다음 DAP 레코드를 수정합니다.

참고 아직 수행하지 않은 경우 DAP 정책 및 DAP 레코드를 생성합니다.

단계 **3** **Endpoint Criteria(**엔드포인트 기준**)**를 클릭하고 다음 속성 유형에서 필요한 엔드포인트 기준 속성을 구성합니다.

- 안티맬웨어
- 디바이스
- AnyConnect
- NAC
- 애플리케이션
- 방화벽
- 운영 체제
- 프로세스
- 레지스트리
- 파일
- 인증서

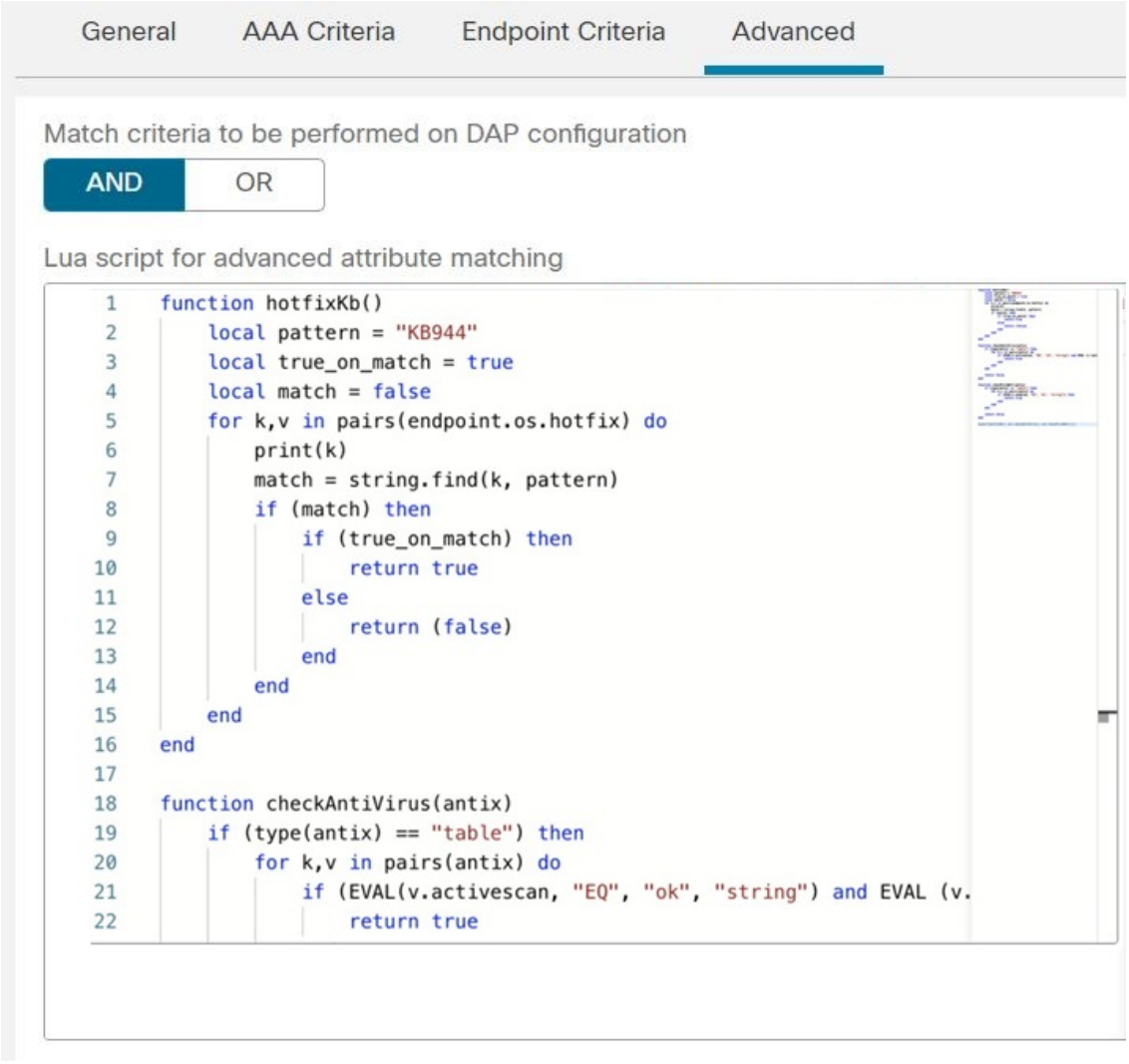
참고 각 엔드포인트 속성 유형의 여러 인스턴스를 만들 수 있습니다. 각 DAP 레코드에 대해 엔드포인트 속성을 원하는 만큼 추가할 수도 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

DAP에 대한 고급 설정 구성

Advanced(고급) 탭을 사용하여 AAA 및 엔드포인트 속성 영역에서 지정할 수 없는 선택 기준을 추가할 수 있습니다. Lua에서 적절한 논리식을 생성하여 여기에 입력합니다.

그림 ***5: Lua*** 스크립트를 사용한 고급 기준 일치



프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy(**동적 액세스 정책**)**를 선택합니다.

단계 **2** DAP 정책을 편집한 다음 DAP 레코드를 변경합니다.

참고 아직 수행하지 않은 경우 DAP 정책 및 DAP 레코드를 생성합니다.

단계 **3** DAP 구성에서 일치시킬 일치 기준으로 **AND** 또는 **OR**를 선택합니다.

단계 **4** **Lua script for advanced attribute matching(**고급 속성 일치를 위한 **Lua** 스크립트**)**을 추가합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Dynamic Access Policy 문제 해결

DAP 문제를 해결하기 전에 다음 작업을 수행합니다.

- 플랫폼 설정 정책에서 VPN 시스템 로그를 활성화합니다.
- **Devices(**디바이스**)** > **VPN** > **Troubleshooting(**문제 해결**)** > 에서 **DAP** 관련 로그를 확인합니다**.**

문제 **1: DAP** 구성을 저장할 수 없음

해결책

FMC 웹 인터페이스에서 DAP 구성을 저장할 수 없는 경우 해당 로그를 검토하여 실패 사유를 확인합니다.

- `/var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log.*`
- `/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log.*`

`vpn` 또는 `sso` 키워드를 사용하여 관련 로그를 필터링할 수 있습니다.

문제 **2: DAP** 구축 실패

해결 방법**:**

DAP 구축에 실패하면 구축 기록 세부 정보를 확인한 다음 로그 파일 (`/var/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log*`)을 확인합니다.

Dynamic Access Policy 예

이 섹션에서는 VPN 사용자 및 해당 엔드포인트에 대한 VPN 액세스를 허용하거나 차단하는 DAP(Dynamic Access Policy) 구성의 예를 보여 줍니다.

참고 이 문서에서 제공하는 지침은 구성 예시입니다. 다양한 DAP 설정을 사용하여 요구 사항에 따라 단일 DAP 레코드 또는 여러 DAP 레코드를 구성할 수 있습니다. DAP 설정에는 Lua 스크립트를 사용하는 AAA Criteria(AAA 기준), Endpoint Criteria(엔드포인트 기준) 및 Advanced(고급) 설정에 속성이 포함되어 있습니다.

보안 요구 사항에 따라 여러 기준 일치에 대해 단일 DAP 레코드를 구성하거나, 여러 DAP 레코드를 생성하고 필요에 따라 우선순위를 지정할 수 있습니다.

운영 체제에 따라 VPN 액세스 허용 또는 차단

운영 체제에 따라 엔드포인트에 대한 VPN 액세스 권한을 결정할 수 있습니다. 여기에 나와 있는 예를 참조하여 Windows 운영 체제 버전 7을 실행하고 서비스 팩키지 SP1 Convenience Rollup을 사용하지 않는 엔드포인트를 차단합니다.

프로시저

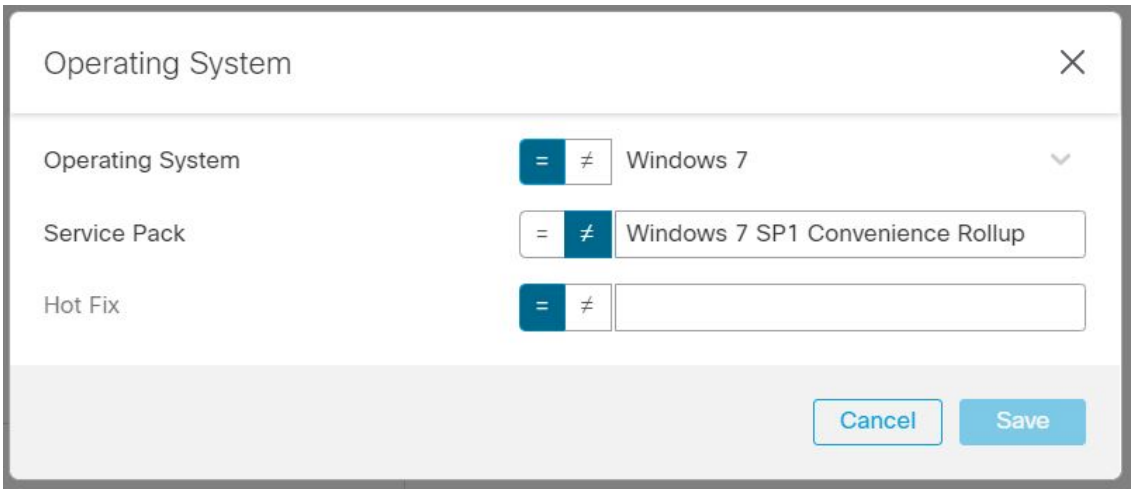
단계 **1** **Terminate(**종료**)** 작업을 사용하여 DAP 레코드를 생성하거나 기존 레코드를 편집합니다.

단계 **2** **Endpoint Criteria(**엔드포인트 기준**)** > **Operating System(**운영 체제**)**을 선택합니다.

단계 **3** 구성된 모든 속성이 일치하는 경우에만 기준을 선택하려면 **All(**모두**)** 일치 기준을 선택합니다.

단계 **4** **Add(**추가**)**를 클릭하여 운영 체제 속성을 추가합니다.

그림 ***6: DAP*** 운영 체제 엔드포인트 기준



단계 **5** **Operating System(**운영 체제**)**에 대해 같음(=) 연산자를 선택한 다음 *Windows 7*을 선택합니다.

단계 **6** **Service Pack(**서비스 팩키지**)**에 대해 같지 않음(≠) 연산자를 선택한 다음 *SP1 Convenience Rollup*을 지정합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

엔드포인트에서 악성코드 차단 속성을 기반으로 트래픽 차단

여기에 나와 있는 단계를 수행하면 엔드포인트가 VPN에 연결을 시도할 때 확인할 악성코드 차단 속성을 구성할 수 있습니다. DAP 레코드 속성을 사용하여 다음을 확인할 수 있습니다.

- 엔드포인트에 Cisco AMP for Endpoints가 설치되어 있고 실시간 검사가 활성화되어 있는지 여부
- Cisco AMP for Endpoints 버전이 1.1 이상이고 악성코드 차단이 15일 안에 업데이트되는 경우

FTD에서 DAP를 구성하는 방법에 대한 자세한 지침은 Dynamic Access Policy 구성, 4 페이지 섹션을 참조하십시오.

프로시저

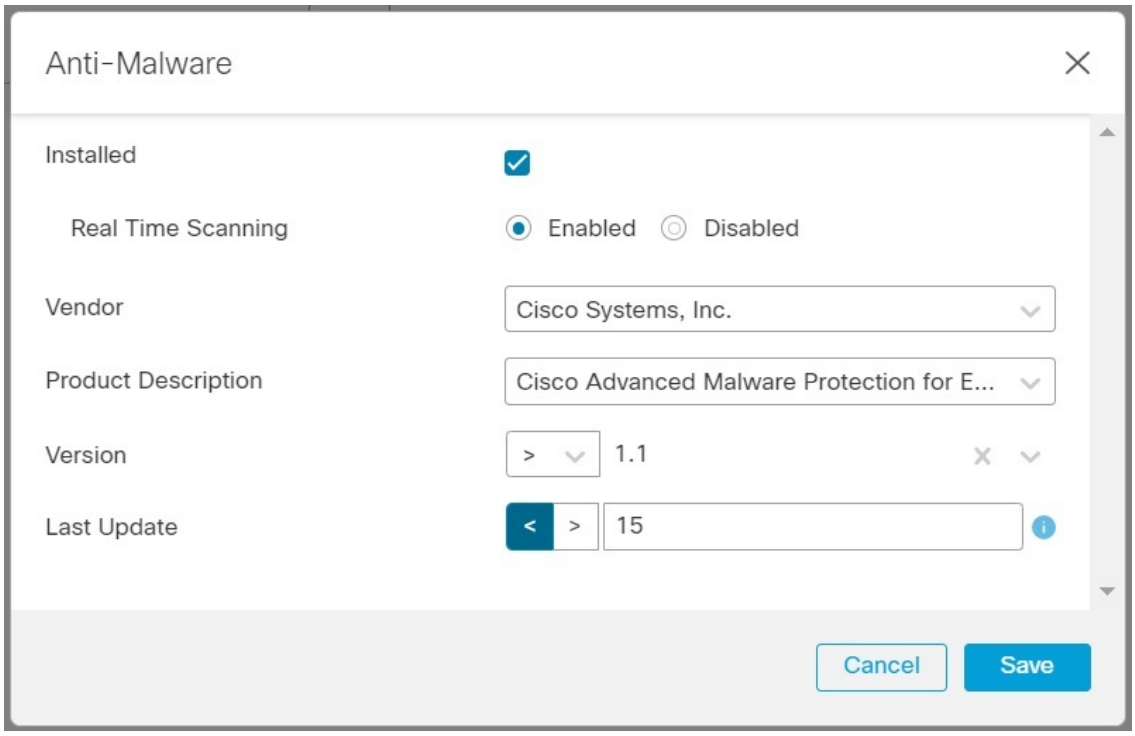
단계 **1** **Terminate(**종료**)** 작업을 사용하여 DAP 레코드를 생성하거나 기존 DAP 레코드를 편집합니다.

단계 **2** DAP 레코드에서 **Endpoint Criteria(**엔드포인트 기준**)** > **Anti-Malware(**악성코드 차단**)**를 선택합니다.

단계 **3** 구성된 모든 속성이 일치하는 경우에만 기준을 선택하려면 **All(**모두**)** 일치 기준을 선택하고, 속성 중 하나와 일치하는 경우에도 기준을 선택하려면 **Any(**일부**)**를 선택합니다.

단계 **4** **Add(**추가**)**를 클릭하여 악성코드 차단 속성을 추가합니다.

그림 ***7: DAP*** 악성코드 차단 엔드포인트 기준



단계 **5** **Installed(**설치됨**)**를 클릭하여 악성코드 차단 제품의 설치 여부를 확인합니다.

단계 **6** **Enabled(**활성화됨**)**를 선택하여 실시간 악성코드 검사가 활성 상태인지 확인합니다.

단계 **7** 목록에서 악성코드 차단 **Vendor(**벤더**)**의 이름을 선택합니다.

이 예에서는 *Cisco Systems, Inc.*를 Cisco AMP for Endpoints의 벤더로 선택합니다. 원하는 벤더를 선택합니다.

단계 **8** 악성코드 차단 **Product Description(**제품 설명**)**, *Cisco AMP for Endpoints*을 선택합니다.

참고 VPN에 연결하는 엔드포인트에서 실행 중인 악성코드 차단 제품을 기준으로 원하는 다른 벤더 및 제품을 선택합니다.

단계 **9** **Version(**버전**)**에는 버전이 1.1 이상인 악성코드 차단 제품을 선택합니다.

단계 **10** **Last Update(**마지막 업데이트**)**에는 마지막 업데이트 이후로 경과한 일 수를 지정합니다.

이미지는 15일 안에(<) 악성코드 차단 업데이트가 이루어져야 함을 나타냅니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

원격 액세스 애플리케이션에 대한 **VPN** 액세스 허용 또는 차단

사용자의 VPN 액세스를 허용하거나 거부하는 원격 액세스 연결 유형을 확인하려면 DAP 레코드에서 애플리케이션 엔드포인트 기준을 사용합니다.

프로시저

단계 **1** 필요에 따라 **Continue(**계속**)** 또는 **Terminate(**종료**)** 작업을 사용하여 DAP 레코드를 생성하거나 기존 레코드를 편집합니다.

단계 **2** **Endpoint Criteria(**엔드포인트 기준**)** > **Application(**애플리케이션**)**을 선택합니다.

단계 **3** 구성된 모든 속성이 일치하는 경우에만 기준을 선택하려면 **All(**모두**)** 일치 기준을 선택하고, 속성 중 하나와 일치하는 경우에도 기준을 선택하려면 **Any(**일부**)**를 선택합니다.

단계 **4** **Add(**추가**)**를 클릭하여 운영 체제 속성을 추가합니다.

그림 ***8: DAP*** 애플리케이션 엔드포인트 기준

참고 이 예를 사용하여 AnyConnect 애플리케이션을 통해 연결하는 VPN 사용자를 허용하거나 차단할 수 있습니다.

확인할 항목만 선택한 후 필요한 값을 입력할 수 있습니다. 디바이스 확인을 여러 엔드포인트나 AAA 기준이 있는 다른 DAP 레코드와 결합하도록 선택할 수도 있습니다.

단계 **5** 같음(=) 또는 같지 않음(≠) 연산자를 선택하고 원격 액세스 **Client Type(**클라이언트 유형**)**을 선택합니다.

나열된 클라이언트 유형은 Clientless, Cut-Through-Proxy, AnyConnect, IPsec, L2TP 및 IPsec-IKEv2-Generic-RA입니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

엔드포인트 디바이스를 확인하여 **VPN** 액세스를 허용 또는 차단

DAP 기준을 설정하여 특정 디바이스에 대한 VPN 액세스를 허용하거나 차단할 수 있습니다. 사용자가 VPN 연결을 시도할 때 확인할 디바이스 세부 정보를 구성합니다.

프로시저

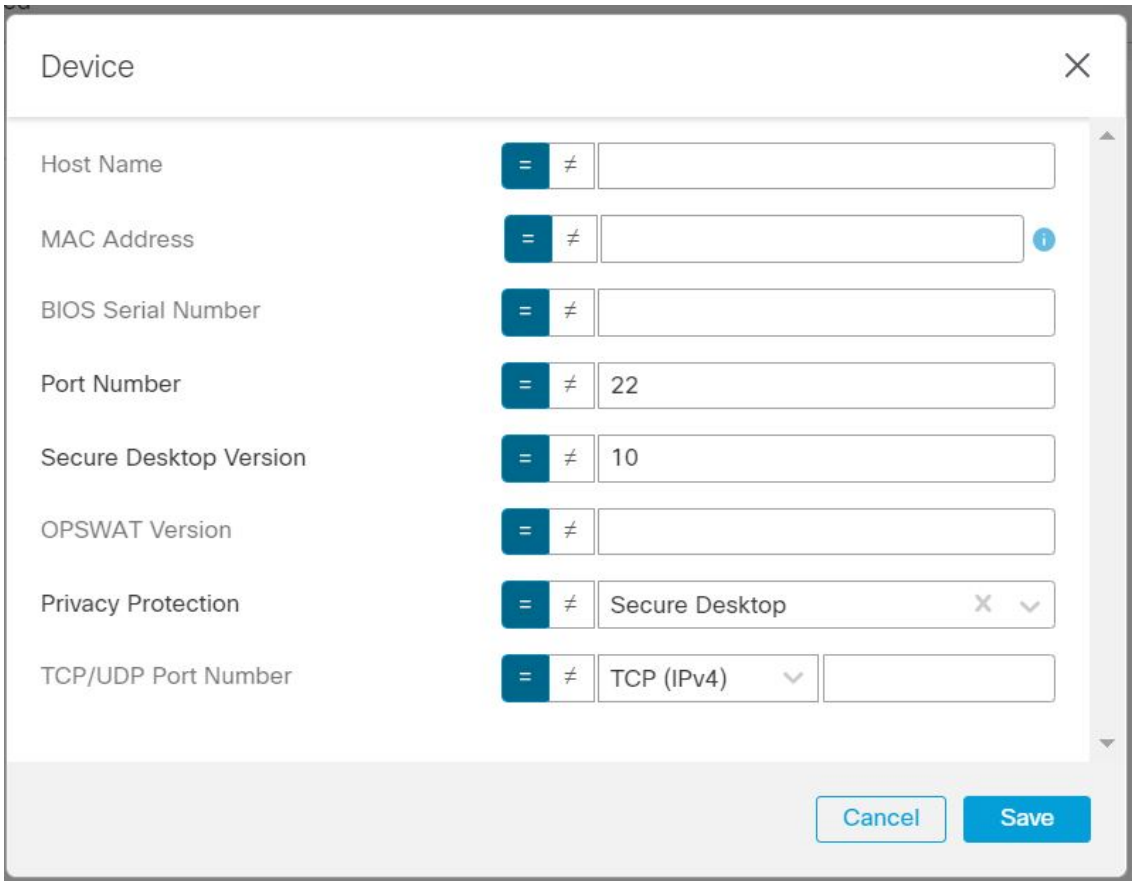
단계 **1** 필요에 따라 **Continue(**계속**)** 또는 **Terminate(**종료**)** 작업을 사용하여 DAP 레코드를 생성하거나 기존 레코드를 편집합니다.

단계 **2** **Endpoint Criteria(**엔드포인트 기준**)** > **Device(**디바이스**)**를 선택합니다.

단계 **3** 구성된 모든 속성이 일치하는 경우에만 기준을 선택하려면 **All(**모두**)** 일치 기준을 선택하고, 속성 중 하나와 일치하는 경우에도 기준을 선택하려면 **Any(**일부**)**를 선택합니다.

단계 **4** **Add(**추가**)**를 클릭하여 운영 체제 속성을 추가합니다.

그림 ***9: DAP*** 디바이스 엔드포인트 기준 예



참고 이 예를 사용하여 포트 번호 22, 보안 데스크톱 버전 10 및 개인정보 보호 Secure Desktop을 통한 엔드포인트 연결을 허용하거나 차단할 수 있습니다.

확인할 항목만 선택한 다음 필요한 값을 입력할 수 있습니다. 디바이스 확인을 여러 엔드포인트나 AAA 기준이 있는 다른 DAP 레코드와 결합하도록 선택할 수도 있습니다.

단계 **5** 같음(=) 또는 같지 않음(≠) 연산자를 선택한 다음 디바이스 정보를 지정합니다. 필수 필드를 선택하고 Host Name(호스트 이름), MAC Address(MAC 주소), BIOS Serial Number(BIOS 일련 번호), Port Number(포트 번호), Secure Desktop Version(Secure Desktop 버전) 및 OPSWAT Version(OPSWAT 버전)에 대한 값을 입력합니다.

단계 **6** 같음(=) 또는 같지 않음(≠) 연산자를 선택하고 Privacy Protection(개인정보 보호) 및 TCP/UDP Port Number(TCP/UDP 포트 번호)를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

Lua 스크립트를 사용하여 엔드포인트에서 악성코드 차단 확인

이 섹션에 나와 있는 구성 예에서는 엔드포인트에 악성코드 차단 제품이 있는지 확인하는 데 필요한 Lua 스크립트를 제공합니다.

Lua 스크립트를 사용하여 논리식을 구성하려면 Lua에 대해 알고 있어야 합니다. Lua 프로그래밍에 대한 자세한 내용은 http://www.lua.org/manual/5.1/manual.html에서 확인할 수 있습니다.

자세한 내용은 *Cisco Secure Firewall Management Center* 구성 가이드의 *Cisco Secure Firewall Threat Defense Dynamic Access Policies* 섹션을 참조하십시오.

프로시저

단계 **1** DAP 레코드를 생성하거나 기존 레코드를 편집합니다.

단계 **2** DAP 레코드에서 **Advanced(**고급**)**를 클릭합니다.

단계 **3** 일치 기준으로 **AND** 또는 **OR**를 선택합니다.

단계 **4** 다음 스크립트를 Lua 스크립트 영역에 복사합니다.

```
assert(function()
local am_count = 0;
CheckAndMsg( true, "endpoint.av="..type(endpoint.am), nil)
for k,v in pairs(endpoint.am) do
am_count = am_count + 1
-- CheckAndMsg( true, "v.exists"..v.exists, nil)
-- CheckAndMsg( true, "v.description"..v.description, nil)
-- CheckAndMsg( true, "v.version"..v.version, nil)
-- CheckAndMsg( true, "v.activescan"..v.activescan, nil)
end
CheckAndMsg( true, "Your request has "..am_count.." Ams", nil)
return true
end)()
```

단계 **5** **Save(**저장**)**를 클릭합니다.

DAP에서 지원되는 AAA 및 엔드포인트 속성

FTD 디바이스에서는 사용자 속성이 구성된 AAA 및 엔드포인트 속성과 일치하는 경우 DAP 정책을 사용합니다. Cisco AnyConnect Secure Mobility Client 의 Host Scan 모듈은 구성된 엔드포인트 속성에 대한 정보를 디바이스에 반환합니다. DAP 하위 시스템은 이 정보를 사용하여 해당 속성의 값과 일치하는 DAP 레코드를 선택합니다.

대부분의 안티바이러스, 안티스파이웨어 및 개인 방화벽 프로그램은 액티브 검사를 지원합니다. 따라서 메모리에 상주하므로 항상 실행됩니다. Host Scan에서는 다음과 같이 엔드포인트에 설치된 프로그램이 있는지, 그리고 해당 프로그램이 메모리에 상주하는지 검사합니다.

- 설치된 프로그램이 액티브 검사를 지원하지 않는 경우 Host Scan에서 해당 소프트웨어의 존재를 보고합니다. 그러면 DAP 시스템에서 해당 프로그램을 지정하는 DAP 레코드를 선택합니다.
- 설치된 프로그램이 액티브 검사를 지원하고 해당 프로그램에 대해 액티브 검사가 활성화된 경우 Host Scan에서 해당 소프트웨어의 존재를 보고합니다. 그러면 보안 어플라이언스에서 해당 프로그램을 지정하는 DAP 레코드를 선택합니다.
- 설치된 프로그램이 액티브 검사를 지원하고 해당 프로그램에 대해 액티브 검사가 비활성화된 경우 Host Scan에서 해당 소프트웨어의 존재를 무시합니다. 그러면 보안 어플라이언스에서 해당 프로그램을 지정하는 DAP 레코드를 선택하지 않습니다.

DAP에서 지원되는 AAA 속성

AAA 속성을 DAP 레코드의 선택 조건으로 구성하려면 Add/Edit AAA Attributes(AAA 속성 추가/수정) 대화 상자에서 사용할 Cisco, LDAP 또는 RADIUS 속성을 설정합니다. 이러한 속성을 입력한 값과 같음(=) 또는 같지 않음(!=)으로 설정할 수 있습니다. 각 DAP 레코드의 AAA 속성 수에 대한 제한은 없습니다.

Cisco VPN 기준

Cisco VPN 기준은 AAA 계층 모델에 저장된 사용자 권한 부여 속성을 참조합니다. DAP 레코드의 AAA 선택 속성에 대해 이러한 속성의 작은 하위 집합을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- **Group Policy(**그룹 정책**)** - VPN 사용자 세션과 연계된 그룹 정책 이름입니다. 보안 어플라이언스에 로컬로 설정되거나, RADIUS/LDAP 서버에서 IETF-Class(25) 속성으로 전송될 수 있습니다. 최대 64자입니다.
- **Assigned IPv4 Address(**할당된 **IPv4** 주소**)** - 정책에 대해 지정할 IPv4 주소를 입력합니다. 전체 터널 VPN 클라이언트(IPsec, L2TP/IPsec, SSL VPN AnyConnect)에 할당된 IP 주소입니다.
- **Assigned IPv6 Address(**할당된 **IPv6** 주소**)** - 정책에 대해 지정할 IPv6 주소를 입력합니다.
- Connection Profile(연결 프로파일) - 원격 액세스 VPN 연결 프로파일 이름입니다. 최대 64자입니다.

- Username(사용자 이름) - 인증된 사용자의 기본 사용자 이름입니다. 최대 64자입니다. 로컬, RADIUS, LDAP 인증/권한 부여 또는 기타 인증 유형(예: RSA/SDI), NT 도메인 등)을 사용하는 경우에 적용됩니다.
- Username2(사용자 이름 2) - 인증된 사용자의 보조 사용자 이름입니다. 최대 64자입니다.

LDAP 기준

LDAP 클라이언트(보안 어플라이언스)는 모든 네이티브 LDAP 응답 속성 값 쌍을 사용자의 AAA 세션과 연계된 데이터베이스에 저장합니다. LDAP 클라이언트는 검색한 순서대로 응답 속성을 데이터베이스에 기록합니다. 해당 이름을 가진 후속 속성은 모두 제거됩니다. 이 시나리오는 사용자 레코드 및 그룹 레코드를 모두 LDAP 서버에서 읽을 때 발생할 수 있습니다. 사용자 레코드 속성을 먼저 읽으며, 항상 사용자 레코드 속성이 그룹 레코드 속성에 우선합니다.

Active Directory(AD) 그룹 멤버십을 지원하기 위해 AAA LDAP 클라이언트에서는 LDAP memberOf 응답 속성을 특수한 방식으로 처리합니다. AD memberOf 속성은 AD에서 그룹 레코드의 DN 문자열을 지정합니다. 그룹 이름은 DN 문자열의 첫 번째 CN 값입니다. LDAP 클라이언트는 DN 문자열에서 그룹 이름을 추출하여 AAA memberOf 속성으로 저장하며, 응답 속성 데이터베이스에는 LDAP memberOf 속성으로 저장합니다. LDAP 응답 메시지에 추가 memberOf 속성이 있는 경우 그룹 이름은 이러한 속성에서 추출되며, 이전의 AAA memberOf 속성과 결합되어 쉼표로 구분된 그룹 이름 문자열을 구성합니다. 이는 응답 속성 데이터베이스에서도 업데이트됩니다.

LDAP 인증/권한 부여 서버에 대한 VPN 원격 액세스 세션이 다음 세 가지 Active Directory 그룹(memberOf 열거형)을 반환하면 Threat Defense Device는 세 개의 Active Directory 그룹을 처리합니다.

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

이러한 그룹은 aaa.ldap 선택 기준으로 어떤 조합에나 사용할 수 있습니다.

LDAP 속성은 DAP 레코드의 속성 이름 및 속성 값 쌍으로 구성됩니다. LDAP 속성 이름은 대/소문자를 구분하는 구문입니다. 예를 들어 AD 서버에서 department로 반환하는 항목 대신 LDAP 속성 Department를 지정한 경우에는 이 속성 설정을 기반으로 DAP 레코드가 일치하지 않게 됩니다.

참고 Value(값) 필드에 여러 값을 입력하려면 세미콜론(;)을 구분 기호로 사용합니다. 예를 들면 다음과 같습니다.

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

RADIUS 기준

RADIUS 클라이언트는 모든 네이티브 RADIUS 응답 속성 값 쌍을 사용자의 AAA 세션과 연계된 데이터베이스에 저장합니다. RADIUS 클라이언트는 검색한 순서대로 응답 속성을 데이터베이스에 기록합니다. 해당 이름을 가진 후속 속성은 모두 제거됩니다. 이 시나리오는 사용자 레코드 및 그룹 레코드를 모두 RADIUS 서버에서 읽을 때 발생할 수 있습니다. 사용자 레코드 속성을 먼저 읽으며, 항상 사용자 레코드 속성이 그룹 레코드 속성에 우선합니다.

RADIUS 속성은 DAP 레코드의 속성 번호 및 속성 값 쌍으로 구성됩니다.

참고 RADIUS 속성의 경우 DAP는 속성 ID = 4096 + RADIUS ID를 정의합니다.

예를 들어 RADIUS 속성 "Access Hours"의 Radius ID가 1이므로, DAP 속성 값이 4,096 + 1 = 4,097입니다.

RADIUS 속성 "Member Of"의 Radius ID = 146이므로 DAP 속성 값 = 4,096 + 146 = 4,242입니다.

SAML 기준

권한 부여 속성을 검색하기 위해 외부 서버(RADIUS 또는 LDAP)를 사용할 필요 없이 DAP를 통해 SAML 권한 부여 및 그룹 정책 선택을 구성할 수 있습니다.

인증 어설션 외에 권한 부여 속성을 전송하도록 SAML ID 제공자를 구성할 수 있습니다. 위협 방어 디바이스의 SAML 통신 사업자 구성 요소는 SAML 어설션을 해석하고 수신된 어설션을 기반으로 권한 부여 또는 그룹 정책을 선택합니다. 어설션 속성은 관리 센터에 구성된 DAP 규칙을 사용하여 처리됩니다.

그룹 정책 속성은 속성 이름 **cisco_group_policy**를 사용해야 합니다. 이 속성은 구성 중인 DAP에 종속되지 않습니다. 그러나 DAP가 구성된 경우 DAP 정책의 일부로 사용할 수 있습니다.

cisco_group_policy라는 이름의 속성이 수신되면 해당 값이 연결 그룹 정책을 선택하는 데 사용됩니다.

연결이 설정되면 여러 소스에서 그룹 정책 정보를 가져와 결합하여 연결에 적용되는 효과적인 그룹 정책을 구성할 수 있습니다.

DAP에서 지원되는 엔드포인트 속성

악성코드 차단 및 방화벽 벤더, Host Scan 애플리케이션이 탐지할 수 있는 애플리케이션 목록과 지원되는 벤더의 보안 상태 속성에 대해 알아보려면 Host Scan 악성코드 차단 및 방화벽 지원 차트를 참조하십시오.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. 모든 권리 보유.

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.