



원격 액세스 VPN을 사용하여 사용자 제어

다음 주제는 Remote Access VPN을 이용해 사용자 인식 및 사용자 제어를 수행하는 방법을 설명합니다.

- [Remote Access VPN ID 소스, 1 페이지](#)
- [사용자 제어에 대한 RA VPN 설정, 2 페이지](#)
- [원격 액세스 VPN ID 소스 문제 해결, 3 페이지](#)

Remote Access VPN ID 소스

AnyConnect는 threat defense 디바이스에 원격 VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

새 [Remote Access VPN 정책 생성](#)에 설명된 대로 안전한 VPN 게이트웨이를 설정할 때, 사용자가 Active Directory 저장소에 있다면 이러한 사용자에 대한 ID 정책을 설정하고 ID 정책을 액세스 컨트롤 정책과 연결할 수 있습니다.



참고 사용자 ID 및 RADIUS를 ID 소스로 사용하는 원격 액세스 VPN을 사용하는 경우 영역을 구성해야 합니다(**Objects(개체) > Object Management(개체 관리) > AAA Server(AAA 서버) > RADIUS Server Group(RADIUS 서버 그룹)**).

원격 사용자가 제공한 로그인 정보는 LDAP 또는 AD 영역 또는 RADIUS 서버 그룹에서 검증합니다. 이러한 엔터티는 Secure Firewall Threat Defense 보안 게이트웨이와 통합됩니다.



참고 사용자가 Active Directory를 인증 소스로 사용하여 원격 액세스 VPN으로 인증하는 경우 사용자 이름을 사용하여 로그인해야 합니다. domain\username 또는 username@domain 형식은 실패하게 됩니다. (Active Directory는 이 사용자 이름을 로그인 이름 또는 경우에 따라 sAMAccountName으로 참조합니다.) 자세한 내용은 MSDN의 [User Naming Attributes](#)를 참조하십시오.

RADIUS를 사용하여 인증하는 경우 사용자는 위의 형식 중 하나로 로그인할 수 있습니다.

VPN 연결을 통해 인증되면 원격 사용자는 VPN ID를 사용합니다. Secure Firewall Threat Defense 보안 게이트웨이의 ID 정책에서 이 VPN ID를 사용하여 해당 원격 사용자에게 속하는 네트워크 트래픽을 인식하고 필터링합니다.

ID 정책은 네트워크 리소스에 대한 액세스 권한을 가진 사용자를 확인하는 액세스 제어 정책과 연결됩니다. 이러한 방식으로 원격 사용자는 네트워크 리소스에 대한 액세스가 차단되거나 허용됩니다.

관련 항목

[VPN 개요](#)

[Secure Firewall Threat Defense 원격 액세스 VPN 개요](#)

[VPN 기본 사항](#)

[Remote Access VPN 기능](#)

[Remote Access VPN에 대한 지침 및 제한 사항](#)

[새 Remote Access VPN 정책 생성](#)

사용자 제어에 대한 RA VPN 설정

시작하기 전에

- [Active Directory 영역 및 영역 디렉터리 생성](#)에 설명된 대로 영역을 생성합니다.
- 인증, 권한 부여 및 감사(AAA)를 사용하려면, [RADIUS 서버 그룹 추가](#)에 설명된 대로 RADIUS 서버 그룹을 설정합니다.

프로시저

단계 1 management center에 로그인합니다.

단계 2 **Devices**(디바이스) > **VPN** > **Remote Access**(원격 액세스)를 클릭합니다.

단계 3 새 [Remote Access VPN 정책 생성](#)의 내용을 참조하십시오.

다음에 수행할 작업

- [ID 정책 생성](#)에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- [액세스 제어에 다른 정책 연결](#)에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- [구성 변경 사항 구축](#)에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- [VPN 세션 및 사용자 정보](#)에 설명된 대로 VPN 사용자 트래픽을 모니터링합니다.

원격 액세스 VPN ID 소스 문제 해결

- 기타 관련 문제 해결 정보를 보려면 [영역 및 사용자 다운로드 문제 해결](#), [사용자 제어 문제 해결](#), [VPN 문제 해결](#)을 참조하십시오.
- Remote Access VPN 관련 문제가 발생한다면, management center 및 매니지드 디바이스 간의 연결을 확인하십시오. 연결에 실패했을 때, 사용자가 이전에 확인된 적이 있고 management center에 다운로드된 경우가 아니라면 다운타임 동안에는 디바이스에서 보고된 모든 원격 액세스 VPN 로그인을 식별할 수 없습니다.
식별되지 않은 사용자는 management center에서 알 수 없는 사용자로 로그인됩니다. 다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.
- Kerberos 인증에 성공하려면 매니지드 디바이스의 호스트 이름이 15자 미만이어야 합니다.
- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 [RFC 959](#)를 참조하십시오.

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.