

VPN 3000 Concentrator의 Cisco VPN 클라이언트 사용자 및 그룹 특성 처리

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[VPN 클라이언트가 VPN 3000 Concentrator에 연결](#)

[RADIUS를 통해 외부에서 그룹 및 사용자 인증](#)

[VPN 3000 Concentrator에서 사용자 및 그룹 특성을 사용하는 방법](#)

[관련 정보](#)

소개

이 문서에서는 Cisco VPN Client가 VPN Concentrator에서 인증되는 방법과 Cisco VPN 3000 Concentrator에서 사용자 및 그룹 특성을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN 3000 Concentrator를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

VPN 클라이언트가 VPN 3000 Concentrator에 연결

VPN 클라이언트가 VPN 3000 Concentrator에 연결되면 최대 4개의 인증이 발생할 수 있습니다.

1. 그룹이 인증됩니다.(종종 "터널 그룹"이라고 합니다.)
2. 사용자가 인증됩니다.
3. (선택 사항) 사용자가 다른 그룹의 일부인 경우 이 그룹이 다음에 인증됩니다.사용자가 다른 그룹 또는 터널 그룹에 속하지 않은 경우 기본 그룹이 기본값으로 설정되며 이 단계는 발생하지 않습니다.
4. 1단계의 "터널 그룹"이 다시 인증됩니다.이 작업은 "그룹 잠금" 기능이 사용되는 경우에 수행됩니다.이 기능은 버전 2.1 이상에서 사용할 수 있습니다.)

내부 데이터베이스를 통해 인증된 VPN 클라이언트에 대한 이벤트 로그에 표시되는 이벤트의 예입니다("testuser"는 "Engineering" 그룹의 일부입니다).

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

참고: 이러한 이벤트를 보려면 Configuration(컨피그레이션) > System(시스템) > Events(이벤트) > Classes(클래스)에서 Auth Event Class(인증 이벤트 클래스)를 심각도 1-6으로 구성해야 합니다.

그룹 잠금 기능 - 그룹 - Tunnel_Group에서 그룹 잠금 기능이 활성화된 경우 사용자는 Tunnel_Group의 일부여야 연결할 수 있습니다.앞의 예에서는 모든 동일한 이벤트를 볼 수 있지만 "testuser"는 Group - Tunnel_Group의 일부가 아니라 Group - Engineering의 일부이므로 연결되지 않습니다.다음 이벤트도 표시됩니다.

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

그룹 잠금 기능 및 샘플 컨피그레이션에 대한 자세한 내용은 [RADIUS 서버를 사용하여 VPN 3000 Concentrator 그룹에 사용자 잠금을 참조하십시오.](#)

RADIUS를 통해 외부에서 그룹 및 사용자 인증

RADIUS 서버를 통해 외부 사용자 및 그룹을 인증하도록 VPN 3000 Concentrator를 구성할 수도 있습니다.이렇게 하려면 VPN Concentrator에 그룹 이름을 구성해야 하지만 그룹 유형은 "외부"로 구성됩니다.

- 외부 그룹은 RADIUS 서버가 VSA(Vendor Specific Attributes)를 지원하는 경우 Cisco/Altiga 특성을 반환할 수 있습니다.
- RADIUS에 의해 반환되지 않는 모든 Cisco/Altiga 특성은 기본 그룹의 값으로 기본 설정됩니다.
- RADIUS 서버가 VSA를 지원하지 않는 경우 ALL 특성은 Base Group 특성에 기본값으로 설정됩니다.

참고: RADIUS 서버는 그룹 이름을 사용자 이름과 다르게 취급합니다.RADIUS 서버의 그룹은 표준 사용자와 마찬가지로 구성됩니다.

이 단계는 사용자와 그룹이 모두 외부에서 인증된 경우 IPsec 클라이언트가 VPN 3000 Concentrator에 연결할 때 발생하는 상황을 간략하게 설명합니다.내부 사례와 마찬가지로 최대 4개의 인증이 발생할 수 있습니다.

1. 그룹은 RADIUS를 통해 인증됩니다.RADIUS 서버는 그룹에 대해 많은 특성을 반환하거나 전혀 반환하지 않을 수 있습니다.최소한 RADIUS 서버는 Cisco/Altiqa 특성 "IPSec 인증 = RADIUS"를 반환하여 VPN Concentrator에 사용자를 인증하는 방법을 알려 주어야 합니다.그렇지 않은 경우 기본 그룹의 IPSec 인증 방법을 "RADIUS"로 설정해야 합니다.
2. 사용자는 RADIUS를 통해 인증됩니다.RADIUS 서버는 사용자에 대해 많은 특성을 반환하거나 전혀 반환하지 않을 수 있습니다.RADIUS 서버가 CLASS(표준 RADIUS 특성 #25) 특성을 반환하는 경우 VPN 3000 Concentrator는 해당 특성을 그룹 이름으로 사용하고 3단계로 이동하거나 4단계로 이동합니다.
3. 사용자의 그룹은 RADIUS를 통해 다음에 인증됩니다.RADIUS 서버는 그룹에 대해 많은 특성을 반환하거나 전혀 반환하지 않을 수 있습니다.
4. 1단계의 "터널 그룹"이 RADIUS를 통해 다시 인증됩니다.인증 하위 시스템은 1단계의 인증에서 특성(있는 경우)을 저장하지 않았으므로 터널 그룹을 다시 인증해야 합니다. 이는 "그룹 잠금" 기능이 사용된 경우에 수행됩니다.

VPN 3000 Concentrator에서 사용자 및 그룹 특성을 사용하는 방법

VPN 3000 Concentrator가 사용자 및 그룹을 인증한 후 수신한 특성을 구성해야 합니다.VPN Concentrator는 이 기본 설정 순서로 특성을 사용합니다.인증이 내부 또는 외부에서 수행되었는지 여부는 중요하지 않습니다.

1. **User attributes(사용자 특성)** - 다른 모든 특성보다 우선합니다.
2. **Group attributes(그룹 특성)** - User 속성에서 누락된 모든 특성은 Group(그룹) 특성으로 채워집니다.동일한 모든 속성은 사용자 속성에 의해 재정의됩니다.
3. **Tunnel Group attributes(터널 그룹 특성)** - User(사용자) 또는 Group(그룹) 특성에서 누락된 모든 특성은 Tunnel Group(터널 그룹) 특성으로 채워집니다.동일한 모든 속성은 사용자 속성에 의해 재정의됩니다.
4. **Base Group attributes(기본 그룹 특성)** - User(사용자), Group(그룹) 또는 Tunnel Group(터널 그룹) 특성에서 누락된 모든 특성은 Base Group(기본 그룹) 특성으로 채워집니다.

관련 정보

- [Cisco VPN 3000 Series Concentrator 지원 페이지](#)
- [Cisco VPN 클라이언트 지원 페이지](#)
- [IPSec 지원 페이지](#)
- [RADIUS 지원 페이지](#)
- [RFC\(Request for Comments\)](#)
- [Technical Support - Cisco Systems](#)