일회용 비밀번호로 AnyConnect Secure Mobility Client 구성

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>패킷 플로우</u> 구성 <u>네트워크 다이어그램</u> <u>다음을 확인합니다.</u> <u>사용자 환경</u> <u>문제 해결</u> <u>범례</u> 관련 정보

소개

이 문서에서는 ASA(Adaptive Security Appliance) Cisco AnyConnect Secure Mobility Client 액세스 를 위한 컨피그레이션 예를 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 ASA가 완전히 작동하며 Cisco ASDM(Adaptive Security Device Manager) 또는 CLI(Command Line Interface)에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA의 CLI 및 ASDM에 대한 기본 지식
- Cisco ASA 헤드 엔드의 SSLVPN 컨피그레이션
- 2단계 인증에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

Cisco Adaptive Security Appliance ASA5506

- Cisco Adaptive Security Appliance Software 버전 9.6(1)
- Adaptive Security Device Manager 버전 7.8(2)
- AnyConnect 버전 4.5.02033

참고: Cisco <u>Software Download(등록된</u> 고객만 해당)에서 AnyConnect VPN Client 패키지 (anyconnect-win*.pkg)를 다운로드합니다. ASA와의 SSL VPN 연결을 설정하기 위해 원격 사 용자 컴퓨터에 다운로드되는 ASA의 플래시 메모리에 AnyConnect VPN 클라이언트를 복사합 니다. 자세한 내용은 ASA <u>컨피그레이션 가이드</u>의 AnyConnect 클라이언트 설치 섹션을 참조 하십시오.

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

배경 정보

ASA(Adaptive Security Appliance) Cisco AnyConnect Secure Mobility Client 액세스는 OTP(One-Time Password)를 통해 2단계 인증을 사용합니다. AnyConnect 사용자가 성공적으로 연결할 수 있 도록 올바른 자격 증명과 토큰을 제공해야 합니다.

2단계 인증은 두 가지 인증 방법을 사용합니다. 이 중 두 가지 인증 방법을 사용할 수 있습니다.

- 당신이 아는 무언가
- 가지고 계신 것
- 당신이 뭔가입니다

일반적으로 사용자가 알고 있는 것(사용자 이름 및 비밀번호)과 사용자가 가지고 있는 것(예: 토큰 이나 인증서와 같이 개인만 소유한 정보의 엔티티)으로 구성됩니다. 이는 사용자가 ASA의 로컬 데 이터베이스 또는 ASA와 통합된 AD(Active Directory) 서버에 저장된 자격 증명을 통해 인증하는 기 존 인증 설계보다 안전합니다. OTP(One-Time Password)는 네트워크 액세스를 보호하기 위한 가 장 간단하고 가장 널리 사용되는 2단계 인증 형식 중 하나입니다. 예를 들어, 대기업의 경우 VPN(Virtual Private Network) 액세스를 위해 원격 사용자 인증을 위해 OTP(One-Time Password) 토큰을 사용해야 하는 경우가 많습니다.

이 시나리오에서는 ASA와 AAA 서버 간의 통신에 radius 프로토콜을 사용하는 AAA 서버로 OpenOTP 인증 서버를 사용합니다. 사용자 자격 증명은 2단계 인증을 위한 소프트 토큰으로 서비 스하는 Google Authenticator 애플리케이션과 연결된 OpenOTP 서버에서 구성됩니다.

OpenOTP 컨피그레이션은 이 문서의 범위에 속하지 않으므로 여기에서 다루지 않습니다. 추가 읽 기를 위해 이 링크를 확인할 수 있습니다.

OpenOTP 설정 https://www.rcdevs.com/docs/howtos/openotp_quick_start/openotp_quick_start/

OpenOTP 인증을 위한 ASA 구성 https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/ 이 패킷 캡처는 10.106.50.20의 AAA 서버에 연결된 ASA의 외부 인터페이스에서 수행되었습니다.

- 1. AnyConnect 사용자가 ASA를 향한 클라이언트 연결을 시작하고 구성된 group-url 및 groupalias에 따라 연결이 특정 터널 그룹(연결 프로파일)에 랜딩됩니다. 이때 사용자에게 자격 증명 을 입력하라는 프롬프트가 표시됩니다.
- 2. 사용자가 자격 증명을 입력하면 인증 요청(액세스 요청 패킷)이 ASA에서 AAA 서버로 전달됩니다.

	923 2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222	UDP	Access-Request(1) (id=9, 1=180)
+	924 2017-10-21 08:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, 1=80)
	947 2017-10-21 08:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, 1=198)
l	948 2017-10-21 08:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, 1=44)
٠		m					
D	Frame 923: 222 bytes on wire (1776)	bits), 222 bytes c	aptured (1776 bits)			
D	Ethernet II. Src: CiscoInc f0:3e:e2	(54:75:d0:f0:3e:e	2). Dst: CiscoInc	, 3c:96:7f (00:23:5e	:3c:96:7f)	
D	Internet Protocol Version 4. Src: 10	0.106.48.191. Dst:	10.106.50.20	•		· · · · · · · · · · · · · · · · · · ·	
D	User Datagram Protocol, Src Port: 1	3512 (13512), Dst	Port: 1645 (1645)				
	RADIUS Protocol	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,					
	Code: Access-Request (1)						
	Packet identifier: 0x9 (9)						
	Length: 180						
	Authenticator: She6hdha618e4fe8he	854cdc65d1522c					
	The response to this request is	in frame 9241					
	A Attribute Value Pairs	All IT DIRE SET					
	A AVP: 1=7 t=llsep_Name(1): cisco						
	lison-Name: cisco						
	A N/P: 1=18 t=llcop_Password(2):	Encounted					
	Lison Password (onstructed): 6	cherypeed	h2f27044127-0				
	oser-rassword (encrypted). o	JEJIJCJ0EJJ1J0J2220	0812194912180				

3. 인증 요청이 AAA 서버에 도달하면 자격 증명을 검증합니다. AAA 서버가 올바르면 Access-Challenge로 응답합니다. 여기서 사용자에게 일회용 비밀번호를 입력하라는 메시지가 표시됩 니다. 자격 증명이 잘못된 경우 Access-Reject 패킷이 ASA로 전송됩니다.

	923 2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222	UDP	Access-Request(1) (id=9, 1=180)							
	924 2017-10-21 08:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, 1=80)							
	947 2017-10-21 08:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, 1=198)							
l	948 2017-10-21 08:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, 1=44)							
		m												
-	Frame 924: 122 bytes on wire (976 b)	its). 122 bytes car	ptured (976 bits)											
	Ethernet II. Src: CiscoInc 3c:96:7f	(00:23:5e:3c:96:7	f). Dst: CiscoInc	f0:3e:e2 (54:75:de):f0:3e:e2)								
	Internet Protocol Version 4, Src: 10	0.106.50.20, Dst:	10.106.48.191			,								
1	User Datagram Protocol, Src Port: 10	645 (1645), Dst Por	rt: 13512 (13512)											
	ADDIS Protocol													
	Code: Access-Challenge (11)													
	Packet identifier: 0x9 (9)													
	Length: 80													
	Authenticator: 291ef37118c398ae35	5187b27252dcc74												
	[This is a response to a request	in frame 923]												
	[Time from request: 0.079479000 s	seconds]												
	Attribute Value Pairs													
	AVP: 1=18 t=State(24): 6a65573	57a6d625a674932653	1664134											
	AVP: 1=36 t=Reply-Message(18):	Enter your TOKEN	one-time password	1										
	Reply-Message: Enter your TO	KEN one-time passw	lord	-										
	AVP: 1=6 t=Session-Timeout(27)	: 90												

4. 사용자가 일회용 비밀번호를 입력하면 액세스 요청 패킷 형태의 인증 요청이 ASA에서 AAA 서버로 전송됩니다

	923 2017-10-21 08	:20:07.184621	10.106.48.191	10.106.50.20	KADIUS	222	UDP	Access-Kequest(1) (1d=9, 1=180)
	924 2017-10-21 08	:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, 1=80)
	947 2017-10-21 08	:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, 1=198)
+	948 2017-10-21 08	:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, 1=44)
٠ -			m					
⊳ Fr	rame 947: 240 bytes	on wire (1920 b	its), 240 bytes c	aptured (1920 bits)			
> Et	thernet II. Src: Ci	scoInc f0:3e:e2	(54:75:d0:f0:3e:e)	2). Dst: CiscoInc	, 3c:96:7f (00:23:5e:	3c:96:7f)	
⊳ In	nternet Protocol Ve	rsion 4. Src: 10	.106.48.191, Dst:	10.106.50.20			/	
⊳ Us	ser Datagram Protoc	ol, Src Port: 13	512 (13512), Dst	Port: 1645 (1645)				
A RA	ADIUS Protocol							
	Code: Access-Reque	est (1)						
	Packet identifier:	0xa (10)						
	Length: 198							
	Authenticator: 8be	6bdba618e4fe0be	854cdc65d1522c					
	[The response to t	his request is	in frame 948]					
4	 Attribute Value Pa 	airs						
	AVP: 1=7 t=User	-Name(1): cisco						
	User-Name: ci	sco						
	AVP: 1=18 t=Use	r-Password(2): E	ncrvpted					
	User-Password	(encrypted): 3	06+1e69bd063832226	b3+3/94412/a0				
		101-10			~	고고디		
AA	AA 서버에서	너 일회용	비밀번호	가 성공적의	으로 검	증되	면 Access-	Accept 패킷이 서버에서
AA	AA 서버에서	서 일회용	비밀번호	가 성공적의	으로 걷	승되	면 Access-	Accept 패킷이 서버에서
AA AS	AA 서버에서 SA로 전송되	너 일회용 티며, 사용	비밀번호: ·자가 성공	가 성공적의 적으로 인종	으로 검 증되고	념중되 1.2단	면 Access- 계 인증 프로	Accept 패킷이 서버에서 르세스가 완료됩니다.
AA AS	AA 서버에서 SA로 전송되	너 일회용 티며, 사용	비밀번호: ·자가 성공	가 성공적의 적으로 인종	으로 걷 증되고	්증되 2 2 단	면 Access- 계 인증 프로	Accept 패킷이 서버에서 르세스가 완료됩니다.
AA AS	AA 서버에서 SA로 전송5	너 일회용 티며, 사용	비밀번호: ·자가 성공	가 성공적의 적으로 인종	으로 검 증되고	념증되 1 2단	면 Access- 계 인증 프릐	Accept 패킷이 서버에서 르세스가 완료됩니다.
AA AS	AA 서버에서 SA로 전송5	너 일회용 티며, 사용	비밀번호: 자가 성공	가 성공적의 적으로 인종	으로 검 증되고 RADIUS	성증되 2 2단 222	면 Access- 계 인증 프로	Accept 패킷이 서버에서 E세스가 완료됩니다.
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08	서 일회용 티며, 사용 ::20:07.184621 ::20:07.264100	비밀번호: 자가 성공 ^{10.106.48.191} ^{10.106.59.20}	가 성공적의 적으로 인종 ^{10.106.59.20} ^{10.106.48.191}	으로 검 증되고 RADIUS RADIUS	성증되 2 2단	면 Access- 계 인증 프트	Accept 패킷이 서버에서 리세스가 완료됩니다.
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08	서 일회용 티며, 사용 ::20:07.184621 ::20:07.264100 ::20:13.996393	비밀번호: 자가 성공 ^{10.106.48.191} ^{10.106.59.20} ^{10.106.48.191}	가 성공적의 적으로 인종 ^{10.106.59.20} ^{10.106.48.191} ^{10.106.59.20}	으로 검 증되고 RADIUS RADIUS RADIUS	성종되 2 2단 ²²² ²²² ²⁴⁰	면 Access-, 계 인증 프로	Accept 패킷이 서버에서 2세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198)
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08	서 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258	비밀번호 자가 성공 ^{10.106.48.191} ^{10.106.50.20} ^{10.106.50.20}	가 성공적의 적으로 인종 ^{10.106.59.20} ^{10.106.48.191} ^{10.106.48.191}	으로 검 증되고 RADIUS RADIUS RADIUS RADIUS	남중되 2 2단 ²²² 122 240 86	면 Access-, 계 인증 프로 ^{UDP} UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=19, 1=38) Access-Accept(2) (id=10, 1=44)
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08	서 일회용 티며, 사용 ^{1:20:07.184621} ^{1:20:07.264100} ^{1:20:13.996393} ^{1:20:14.065258}	비밀번호 자가 성공 ^{10.106.48.191} ^{10.106.50.20} ^{10.106.50.20}	가 성공적의 적으로 인종 ^{10.106.59.20} ^{10.106.48.191} ^{10.106.48.191}	으로 검 증되고 RADIUS RADIUS RADIUS RADIUS	김종되 2 2단 ²²² 122 240 86	면 Access-, 계 인증 프로 ^{UDP} UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08	서 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258	비밀번호 자가 성공 ^{10.106.48.191} ^{10.106.50.20} ¹⁰	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.59.20 10.106.48.191	으로 검 중되고 RADIUS RADIUS RADIUS RADIUS	김종되 2 2단 ²²² 122 240 86	면 Access- 계 인증 프로 ^{UDP} UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)
	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08	서 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " s), 86 bytes capt((%):31:56:30:96:7	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 ured (688 bits) (). Dst: (iscolor of	으로 건 중되고 RADIUS RADIUS RADIUS RADIUS	김종되 2 2단 ²²² ¹²² ²⁴⁰ 86	면 Access-, 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=88) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 rame 948: 86 bytes thernet II, Src: Ci thernet II, Src: Ci	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " s), 86 bytes cept (@0:23:58:3c:96:7 106.50.20 btt:	가 성공적으 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 10.106.48.191 ured (688 bits) f), Dst: Ciscolinc.	으로 검 증되고 RADIUS RADIUS RADIUS RADIUS RADIUS	남중되 2 2단 ²²² ¹²² ²⁴⁰ ⁸⁶	면 Access-, 계 인증 프로 UDP UDP UDP UDP UDP	Accept 패킷이 서버에서 2세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08	서 일회용 리며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst Po	가 성공적의 적으로 인종 10.106.59.20 10.106.48.191 10.106.48.191 10.106.48.191 ured (688 bits) f), Dst: CiscoInc_ 10.106.48.191 10.106.48.191	으로 검 중되고 RADIUS RADIUS RADIUS RADIUS RADIUS	222 122 240 86	면 Access- 계 인증 프로 ^{UDP} UDP UDP UDP (DP) (DP) (DP) (DP) (DP)	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 withernet II, Src: Ci internet Protocol Ve Iser Datagram Protoc ADIUS Protocol	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 18 ol, Src Port: 16	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 10.106.50.20 " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst: 3 45 (1645), Dst Po	가 성공적으 적으로 인종 10.106.50.20 10.106.48.191 10.106.50.20 10.106.48.191 ured (688 bits) f), Dst: CiscoInc 10.106.48.191 rt: 13512 (13512)	으로 건 중되고 RADIUS RADIUS RADIUS RADIUS f0:3e:e2 (222 122 122 240 86	면 Access- 계 인증 프로 ^{UDP} UDP UDP UDP UDP (DP) (DP) (DP) (DP) (DP) (DP) (DP) (D	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)
AA AS	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 rame 948: 86 bytes thernet II, Src: Ci nternet Protocol Ve lser Datagram Protocol ADIUS Protocol Code: Access-Acce	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10 ol, Src Port: 16 ol, Src Port: 16	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 " " s), 86 bytes capti (00:23:56:3c:96:7 .106.59.20, Dst Poi	가 성공적으 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 ured (688 bits) f), 0st: CiscoInc_1 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS F0:3e:e2 (1	222 122 122 240 86 54:75:d0:	면 Access- 계 인증 프로 UDP UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
AA AS • Fr • Et • Us • RA	AA 서버에서 SA로 전송5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 rame 948: 86 bytes thernet II, Src: Ci internet Protocol Ve Iser Datagram Protoco (ADIUS Protocol Code: Access-Acceg Packet identifier:	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10 ol, Src Port: 16 ott (2) : Øxa (10)	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " \$), 86 bytes capt (@0.23.56:3c:96:7 .106.58.20, Dst: 45 (1645), Dst Po	가 성공적으 적으로 인종 10.106.59.20 10.106.48.191 10.106.48.191 10.106.48.191 (f), Dst: CiscoInc_1 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS RADIUS F0:3e:e2 (· · · · · · · · · · · · · · · · · · ·	면 Access-, 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 2세스가 완료됩니다. Access-Request(1) (id=9, 1-180) Access-Challenge(11) (id=9, 1-80) Access-Request(1) (id=10, 1-198) Access-Accept(2) (id=10, 1=44)
AA AS • Fr • Et • Ir • Us	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2000000000000000000000000000000000000	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10 ol, Src Port: 16 ol, Src Port: 16 st (2) : @xa (10)	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 10.106.50.20 " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst: 5 .45 (1645), Dst Po	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 10.106.48.191 ured (688 bits) f), Dst: (iscoInc_ 10.106.48.191 rt: 13512 (13512)	으로 걷 중되고 RADIUS RADIUS RADIUS RADIUS RADIUS	· · · · · · · · · · · · · · · · · · ·	면 Access- 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
AA AS • Fr • Et • Us • R	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 ser Datagram Protoc ADIUS Protocol Code: Access-Accep Packet identifier: Length: 44 Authenticator: d86	너 일회용 리며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10 ol, Src Port: 16 ot (2) : 0xa (10)	비밀번호: 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst: 45 (1645), Dst Poo	가 성공적으 적으로 인종 10.106.50.20 10.106.48.191 10.106.50.20 10.106.48.191 ured (688 bits) f), Dst: CiscoInc. 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS RADIUS f0:3e:e2 (1	222 122 122 240 86 54:75:d0:	면 Access- 계 인증 프로 UDP UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)
AA AS • Fr • Et • Us • R	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 ithernet II, Src: Ci nternet Protocol V loser Datagram Protocol ADIUS Protocol Code: Access-Accep Packet identifier: Length: 44 Authenticator: d86 [This is a response	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10 ol, Src Port: 16 ol, Src Port: 16 vt (2) : 0xa (10)	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 " s), 86 bytes capt (00:23:5e:3c:96:7 .106.59.20, Dstr 45 (1645), Dst Po	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 10.106.48.191 f), Dst: CiscoInc_1 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS F0:3e:e2 (1	김종되 222 122 240 86 54:75:d0:	면 Access-, 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)
	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 rame 948: 86 bytes thernet II, Src: Ci internet Protocol Ve Iser Datagram Protocol ADIUS Protocol Code: Access-Acceg Packet identifier: Length: 44 Authenticator: d86 [This is a response] [Time from request	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bif rsion 4, Src: 18 ol, Src Port: 16 ol, Src Port: 16 ot (2) : 0xa (10) Sb54ccaf531e9efc: : 0.068865600 s	비밀번호: 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst: 45 (1645), Dst Po 116cfb11d91d75 116 fname 947] seconds]	가 성공적으 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 10.106.48.191 ured (688 bits) f), Dst: CiscoInc_1 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS RADIUS	· · · · · · · · · · ·	면 Access-, 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id-9, 1-180) Access-Challenge(11) (id-9, 1-88) Access-Request(1) (id-10, 1-198) Access-Accept(2) (id-10, 1-44)
AA AS • Fr • Et • Us • RA	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 947 2017-10-21 08 948 200-100-100-100-100-100-100-100-100-100-	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:13.996393 :20:14.065258 :20:13.996393 :20:14.065258 :20:13.996393 :20:14.065258 :20:14.065258 :00, Src Port: 16 ol, Src Port: 16 ol, Src Port: 16 ot (2) : 0xa (10) Sb54ccaf531e9efc: : 0.068865000 spains	비밀번호 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 10.106.50.20 " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst : 45 (1645), Dst Po 116cfb11d91d75 in frame 947] accords]	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 10.106.48.191 ^(f) , Dst: Ciscolle 10.106.48.191 ^(f) , Dst: Ciscolle 10.106.48.191 ^(f) , 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS RADIUS F0:3e:e2 (· · · · · · · ·	면 Access- 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=198) Access-Accept(2) (id=10, 1=44)
AA AS • Fr • Et • Us • RA	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 947 2017-10-21 08 948 2000000000000000000000000000000000000	너 일회용 티며, 사용 리며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 :20:14.05526 :20:14.06526 :20:14.0658 :20:14.05526 :20:14.	비밀번호: 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " s), 86 bytes capt (00:23:55:3c:96:7 .106.50.20, Dst: 45 (1645), Dst Pool 116cfb11d91d75 in frame 947] aconds] Authentication su	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.50.20 10.106.48.191 ured (688 bits) f), Dst: CiscoInc_ 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS RADIUS f0:3e:e2 (1	222 122 240 86 54:75:d0:	면 Access- 계 인증 프로 UDP UDP UDP UDP UDP	Accept 패킷이 서버에서 E세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)
AA AS > Fr > Et > Ir	AA 서버에서 SA로 전송 5 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 947 2017-10-21 08 948 2017-10-21 08 948 2017-10-21 08 ithernet II, Src: Ci nternet Protocol Velser Datagram Protoc ADIUS Protocol Code: Access-Accep Packet identifier: Length: 44 Authenticator: d86 [This 1s a respons [Time from request • Attribute Value Pa • AVP: 1-24 t=Rep Reply-Message	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:13.996393 :20:14.065258 on wire (688 bit scoInc_3c:96:7f rsion 4, Src: 10 ol, Src Port: 16 ol, Src Port: 16 ol, Src Port: 16 it (2) : 0xa (10) Sb54ccaf531e9efc: t: 0.068865000 sp sirs ly-Message(18): :2 Authentication	비밀번호: 자가 성공 10.106.48.191 10.106.50.20 10.106.48.191 10.106.50.20 " s), 86 bytes capture (00:23:56:36:76:77 .106.59.20, Dstr 45 (1645), Dst Pol 116cfb11d91d75 in frame 947] econds] Authentication suu	가 성공적의 적으로 인종 10.106.50.20 10.106.48.191 10.106.50.20 10.106.48.191 wred (688 bits) f), Dst: CiscoInc_1 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS F0:3e:e2 (1	· · · · · · · ·	면 Access- 계 인증 프로 UDP UDP UDP UDP	Accept 패킷이 서버에서 로세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)
AA AS Fr Et Ir Us R	AA 서버에서 SA로 전송도 923 2017-10-21 08 924 2017-10-21 08 947 2017-10-21 08 948 2017-10-2	너 일회용 티며, 사용 :20:07.184621 :20:07.264100 :20:07.264100 :20:13.996393 :20:14.065258 :20:14.05258 :20:14.065258 :20:14.0558	비밀번호: 자가 성공 10.106.48.191 10.106.50.20 10.106.50.20 " " s), 86 bytes capt (00:23:5e:3c:96:7 .106.50.20, Dst: 45 (1645), Dst Po 116cfb11d91d75 in frame 947] acconds] Authentication su	가 성공적으 적으로 인종 10.106.50.20 10.106.48.191 10.106.48.191 ured (688 bits) f), Dst: CiscoInc_1 10.106.48.191 rt: 13512 (13512)	으로 2 중되고 RADIUS RADIUS RADIUS RADIUS	· · · · · ·	면 Access-, 계 인증 프로 UDP UDP UDP UDP UDP	Accept 패킷이 서버에서 로세스가 완료됩니다. Access-Request(1) (id=9, 1=180) Access-Challenge(11) (id=9, 1=80) Access-Request(1) (id=10, 1=80) Access-Accept(2) (id=10, 1=44)

Anyconnect 라이센스 정보

다음은 Cisco AnyConnect Secure Mobility Client 라이센스에 대한 유용한 정보로 연결되는 링크입니다.

- 자주 묻는 <u>AnyConnect</u> 라이센싱 관련 질문은 이 문서를 참조하십시오.
- AnyConnect Apex 및 Plus <u>라이센스</u>에 대한 자세한 내용은 Cisco AnyConnect 주문 가이드를 참조하십시오.

구성

이 섹션에서는 ASA에서 Cisco AnyConnect Secure Mobility Client를 구성하는 방법에 대해 설명합니다.

참고: 이 섹션에서 사용된 <u>명령에</u> 대한 자세한 내용을 보려면<u>Command Lookup Tool(등록된</u> 고객만 해당)을 사용하십시오.

네트워크 다이어그램



ASDM AnyConnect 컨피그레이션 마법사

AnyConnect Secure Mobility Client를 구성하기 위해 AnyConnect 컨피그레이션 마법사를 사용할 수 있습니다. 계속하기 전에 AnyConnect 클라이언트 패키지가 ASA 방화벽의 플래시/디스크에 업 로드되었는지 확인합니다.

컨피그레이션 마법사를 통해 Anyconnect Secure Mobility Client를 구성하려면 다음 단계를 완료하 십시오.

ASDM을 통한 스플릿 터널 컨피그레이션의 경우 AnyConnect를 다운로드하고 설치하려면 이 문서 를 참조하십시오.

<u>AnyConnect Secure Mobility 클라이언트</u>

ASA CLI 컨피그레이션

이 섹션에서는 참조를 위해 Cisco anyConnect Secure Mobility Client에 대한 CLI 컨피그레이션을 제공합니다.

!-----Client pool configuration-----

ip local pool ANYCONNECT-POOL 192.168.100.1-192.168.100.254 mask 255.255.255.0

!

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address dhcp setroute

!

!-----Split ACL configuration-----

access-list SPLIT-TUNNEL standard permit 10.0.0.0 255.255.255.0

pager lines 24 logging enable logging timestamp mtu tftp 1500 mtu outside 1500 icmp unreachable rate-limit 1 burst-size 1 icmp permit any outside asdm image disk0:/asdm-782.bin no asdm history enable arp timeout 14400 no arp permit-nonconnected route outside 0.0.0.0 0.0.0.0 10.106.56.1 1 !-----Configure AAA server ----aaa-server RADIUS_OTP protocol radius aaa-server RADIUS_OTP (outside) host 10.106.50.20 key *****

!-----Configure Trustpoint containing ASA Identity Certificate -----

crypto ca trustpoint ASDM_Trustpoint 0

enrollment self

subject-name CN=bglanyconnect.cisco.com

!-----Apply trustpoint on outside interface-----

ssl trust-point ASDM_Trustpoint0 outside

!-----Enable AnyConnect and configuring AnyConnect Image-----

webvpn

enable outside

anyconnect image disk0:/anyconnect-win-4.5.02033-webdeploy-k9.pkg 1

anyconnect enable

tunnel-group-list enable

!-----Group Policy configuration-----

group-policy GroupPolicy_ANYCONNECT-PROFILE internal group-policy GroupPolicy_ANYCONNECT-PROFILE attributes dns-server value 10.10.10.99 vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelspecified split-tunnel-network-list value SPLIT-TUNNEL default-domain value cisco.com !-----Tunnel-Group (Connection Profile) Configuration------

```
tunnel-group ANYCONNECT_PROFILE type remote-access
tunnel-group ANYCONNECT_PROFILE general-attributes
address-pool ANYCONNECT-POOL
authentication-server-group RADIUS_OTP
default-group-policy GroupPolicy_ANYCONNECT-PROFILE
```

tunnel-group ANYCONNECT_PROFILE webvpn-attributes

group-alias ANYCONNECT-PROFILE enable

: end

AnyConnect 클라이언트 연결을 위해 ASA에 서드파티 인증서를 구성하고 설치하려면 이 문서를 참 조하십시오.

<u>ASA SSL 디지털 인증서 구성</u>

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

참고: Output <u>Interpreter Tool(등록된</u> 고객만 해당)은 특정 **show** 명령을 지원합니다. **show** 명 령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

이러한 show 명령을 실행하여 AnyConnect 클라이언트의 상태와 해당 통계를 확인할 수 있습니다.

ASA(config) # show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 1 Assigned IP : 192.168.100.1 Public IP : 10.106.49.111 Protocol : AnyConnect-Parent DTLS-Tunnel : AnyConnect Premium License Encryption : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)AES256 Hashing : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)SHA1 Bytes Tx : 15122 Bytes Rx : 5897 Group Policy : GroupPolicy_ANYCONNECT-PROFILE Tunnel Group : ANYCONNECT_PROFILE Login Time : 14:47:09 UTC Wed Nov 1 2017 Duration : 1h:04m:52s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000000059f9de6d

ASA(config) # show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

```
Username : cisco
                                  Index : 1
Assigned IP : 192.168.100.1
                                  Public IP : 10.106.49.111
          : AnyConnect-Parent DTLS-Tunnel
Protocol
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)SHA1
Bytes Tx
          : 15122
                                 Bytes Rx : 5897
Pkts Tx : 10
                                  Pkts Rx : 90
Pkts Tx Drop : 0
                                  Pkts Rx Drop : 0
Group Policy : GroupPolicy_ANYCONNECT-PROFILE
Tunnel Group : ANYCONNECT_PROFILE
Login Time : 14:47:09 UTC Wed Nov 1 2017
Duration : 1h:04m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                  VLAN
                                            : none
Audt Sess ID : 0000000000000059f9de6d
Security Grp : none
AnyConnect-Parent Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 1.1
Public IP : 10.106.49.111
Encryption : none
                                   Hashing : none
TCP Src Port : 53113
                                   TCP Dst Port : 443
```

Auth Mode	:	userPassword			
Idle Time Out	:	30 Minutes	Idle TO Left	:	1 Minutes
Client OS	:	win			
Client OS Ver	:	6.1.7601 Service Pack 2	L		
Client Type	:	AnyConnect			
Client Ver	:	Cisco AnyConnect VPN Ag	gent for Windo	SWS	s 4.5.02033
Bytes Tx	:	7561	Bytes Rx	:	0
Pkts Tx	:	5	Pkts Rx	:	0
Pkts Tx Drop	:	0	Pkts Rx Drop	:	0
DTLS-Tunnel:					
Tunnel ID	:	1.3			
Assigned IP	:	192.168.100.1	Public IP	:	10.106.49.111
Encryption	:	AES256	Hashing	:	SHA1
Ciphersute :	I	AES256-SHA			
Encapsulation	:	DTLSv1.0	UDP Src Port	:	63257
UDP Dst Port	:	443	Auth Mode	:	userPassword
Idle Time Out	:	30 Minutes	Idle TO Left	:	0 Minutes
Client OS	:	Windows			
Client Type	:	DTLS VPN Client			
Client Ver	:	Cisco AnyConnect VPN Ag	gent for Windo	SWS	s 4.5.02033
Bytes Tx	:	0	Bytes Rx	:	5801
Pkts Tx	:	0	Pkts Rx	:	88
Pkts Tx Drop	:	0	Pkts Rx Drop	:	0

사용자 환경



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고: debug 명령<u>을</u> 사용하기<u>전에 Debug 명령</u>에 대한 중요 정보**를** 참조하십시오.

주의: ASA에서는 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니 다. 디버그 수준을 변경하면 디버그의 세부 정도가 증가할 수 있습니다. 특히 프로덕션 환경에 서는 이 작업을 신중하게 수행해야 합니다.

들어오는 AnyConnect 클라이언트 연결에 대한 전체 인증 프로세스 문제를 해결하려면 다음 디버그 를 사용할 수 있습니다.

- 모두 RADIUS 디버그
- aaa 인증 디버그
- wrbvpn anyconnect 디버그

이 명령은 사용자 자격 증명이 올바른지 확인합니다.

테스트 aaa-server 인증 <aaa_server_group> [<host_ip>] 사용자 이름 <user> 암호 <password>

올바른 사용자 이름과 비밀번호의 경우

ASA(config) # test aaa authentication RADIUS_OTP host 10.106.50.20

Username: cisco

Password: *****

INFO: Attempting Authentication test to IP address <10.106.50.20> (timeout: 12 seconds)

ERROR: Authentication Challenged: No error

마지막 오류는 AAA 서버가 사용자 이름 및 암호의 인증 성공 후 사용자가 일회용 비밀번호를 입력 할 것으로 예상하며, 이 테스트에는 사용자가 OTP에 적극적으로 입력하는 것이 포함되지 않으므로 ASA에 오류가 표시되지 않는 응답으로 AAA 서버가 보낸 Access-Challenge가 표시됩니다.

사용자 이름 및/또는 비밀번호가 잘못된 경우

ASA(config)# test aaa authentication RADIUS_OTP host 10.106.50.20

Username: cisco

Password: ***

INFO: Attempting Authentication test to IP address <10.106.50.20> (timeout: 12 seconds)

ERROR: Authentication Rejected: AAA failure 작업 설정에서 디버깅하는 내용은 다음과 같습니다.

범례

AnyConnect 클라이언트 실제 IP: 10.106.49.111

ASA IP: 10.106.48.191

ASA(config) # debug radius all

ASA(config)# debug aaa authentication debug aaa authentication enabled at level 1 radius mkreq: 0x8 alloc_rip 0x74251058 new request 0x8 --> 7 (0x74251058) got user 'cisco' got password add_req 0x74251058 session 0x8 id 7 RADIUS_REQUEST radius.c: rad_mkpkt rad_mkpkt: ip:source-ip=10.106.49.111 RADIUS packet decode (authentication request)

Raw packet data (length = 180).....

01	07	00	b4	b6	c2	bf	25	cf	80	53	a9	a2	3d	с8	са			%S=	
74	05	27	5c	01	07	63	69	73	63	6f	02	12	d7	99	45		t	E	
6e	0f	46	71	bc	52	47	b0	81	b4	18	ae	34	05	06	00		n	n.Fq.RG4	
00	40	00	1e	0f	31	30	2e	31	30	36	2e	34	38	2e	31			@10.106.48.1	
39	31	1f	0f	31	30	2e	31	30	36	2e	34	39	2e	31	31		9	9110.106.49.11	
31	3d	06	00	00	00	05	42	0f	31	30	2e	31	30	36	2e		1	=B.10.106.	
34	39	2e	31	31	31	04	06	0a	бa	30	bf	1a	22	00	00		4	9.111j0"	
00	09	01	1c	69	70	3a	73	6f	75	72	63	65	2d	69	70			ip:source-ip	
3d	31	30	2e	31	30	36	2e	34	39	2e	31	31	31	1a	1a		=	10.106.49.111	
00	00	0c	04	92	14	41	4e	59	43	4f	4e	4e	45	43	54			ANYCONNECT	
2d	50	52	4f	46	49	4c	45	1a	0c	00	00	0c	04	96	06		_	PROFILE	
00	00	00	02													1			

Parsed packet data.... Radius: Code = 1 (0x01) Radius: Identifier = 7 (0x07) Radius: Length = 180 (0x00B4) Radius: Vector: B6C2BF25CF8053A9A23DC8CA7405275C Radius: Type = 1 (0x01) User-Name Radius: Length = 7 (0x07) Radius: Value (String) = 63 69 73 63 6f | cisco Radius: Type = 2 (0x02) User-Password Radius: Length = 18 (0x12) Radius: Value (String) = d7 99 45 6e 0f 46 71 bc 52 47 b0 81 b4 18 ae 34 | ..En.Fq.RG....4 Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x4000Radius: Type = 30 (0x1E) Called-Station-Id Radius: Length = 15 (0x0F)Radius: Value (String) = 31 30 2e 31 30 36 2e 34 38 2e 31 39 31 | 10.106.48.191 Radius: Type = 31 (0x1F) Calling-Station-Id Radius: Length = 15 (0x0F)Radius: Value (String) = 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 10.106.49.111 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x5 Radius: Type = 66 (0x42) Tunnel-Client-Endpoint Radius: Length = 15 (0x0F)Radius: Value (String) = 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | 10.106.49.111 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)Radius: Value (IP Address) = 10.106.48.191 (0x0A6A30BF) Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 34 (0x22)Radius: Vendor ID = 9 (0x0000009) Radius: Type = 1 (0x01) Cisco-AV-pair Radius: Length = 28 (0x1C) Radius: Value (String) = 69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=10. 31 30 36 2e 34 39 2e 31 31 31 106.49.111 Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 26 (0x1A)Radius: Vendor ID = 3076 (0x00000C04) Radius: Type = 146 (0x92) Tunnel-Group-Name

```
Radius: Length = 20 (0x14)
Radius: Value (String) =
41 4e 59 43 4f 4e 4e 45 43 54 2d 50 52 4f 46 49 ANYCONNECT-PROFI
4c 45
                                                   LE
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
send pkt 10.106.50.20/1645
rip 0x74251058 state 7 id 7
rad_vrfy() : response message verified
rip 0x74251058
 : chall_state ''
 : state 0x7
 : regauth:
   b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca 74 05 27 5c
 : info 0x74251190
    session_id 0x8
    request_id 0x7
   user 'cisco'
   response '***'
   app 0
    reason 0
    skey 'testing123'
    sip 10.106.50.20
    type 1
RADIUS packet decode (response)
```

Raw packet data (length = 80)....

0b 07 00 50 ed 7a 06 92 f7 18 16 6b 97 d4 83 5f | ...P.z....k..._ be 9b d7 29 18 12 75 6b 35 36 58 49 4f 6e 35 31 ...)..uk56XIOn51 58 36 4b 75 4c 74 12 24 45 6e 74 65 72 20 79 6f X6KuLt.\$Enter yo 75 72 20 54 4f 4b 45 4e 20 6f 6e 65 2d 74 69 6d | ur TOKEN one-tim 65 20 70 61 73 73 77 6f 72 64 1b 06 00 00 00 5a e password....Z Parsed packet data..... Radius: Code = 11 (0x0B)Radius: Identifier = 7 (0x07)Radius: Length = 80 (0x0050)Radius: Vector: ED7A0692F718166B97D4835FBE9BD729 Radius: Type = 24 (0x18) State Radius: Length = 18 (0x12)Radius: Value (String) = 75 6b 35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74 | uk56XIOn51X6KuLt Radius: Type = 18 (0x12) Reply-Message Radius: Length = 36 (0x24)Radius: Value (String) = 45 6e 74 65 72 20 79 6f 75 72 20 54 4f 4b 45 4e | Enter your TOKEN 20 6f 6e 65 2d 74 69 6d 65 20 70 61 73 73 77 6f one-time passwo 72 64 rd Radius: Type = 27 (0x1B) Session-Timeout Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x5Arad_procpkt: CHALLENGE radius mkreq: 0x8 old request 0x8 --> 8 (0x74251058), state 3 wait pass - pass '***'. make request RADIUS_REQUEST radius.c: rad_mkpkt

rad_mkpkt: ip:source-ip=10.106.49.111

RADIUS packet decode (authentication request)

Raw packet data (length = 198).....

01	08	00	сб	b6	c2	bf	25	cf	80	53	a9	a2	3d	с8	са		%S=
74	05	27	5c	01	07	63	69	73	63	6f	02	12	83	c4	00		t.'\cisco
3e	56	73	71	bc	52	47	b0	81	b4	18	ae	34	05	06	00		>Vsq.RG4
00	40	00	1e	0£	31	30	2e	31	30	36	2e	34	38	2e	31		.@10.106.48.1
39	31	1f	0f	31	30	2e	31	30	36	2e	34	39	2e	31	31		9110.106.49.11
31	3d	06	00	00	00	05	42	0f	31	30	2e	31	30	36	2e		1=B.10.106.
34	39	2e	31	31	31	04	06	0a	бa	30	bf	18	12	75	6b		49.111j0uk
35	36	58	49	4f	бе	35	31	58	36	4b	75	4c	74	1a	22		56XIOn51X6KuLt."
00	00	00	09	01	1c	69	70	3a	73	6f	75	72	63	65	2d		ip:source-
69	70	3d	31	30	2e	31	30	36	2e	34	39	2e	31	31	31		ip=10.106.49.111
1a	1a	00	00	0c	04	92	14	41	4e	59	43	4f	4e	4e	45		ANYCONNE
43	54	2d	50	52	4f	46	49	4c	45	1a	0c	00	00	0c	04		CT-PROFILE
96	06	00	00	00	02												

Parsed packet data.... Radius: Code = 1 (0x01) Radius: Identifier = 8 (0x08) Radius: Length = 198 (0x00C6) Radius: Vector: B6C2BF25CF8053A9A23DC8CA7405275C Radius: Type = 1 (0x01) User-Name Radius: Length = 7 (0x07) Radius: Value (String) = 63 69 73 63 6f | cisco Radius: Type = 2 (0x02) User-Password Radius: Length = 18 (0x12) Radius: Value (String) = 83 c4 00 3e 56 73 71 bc 52 47 b0 81 b4 18 ae 34 | ...>Vsq.RG....4

Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x4000 Radius: Type = 30 (0x1E) Called-Station-Id Radius: Length = 15 (0x0F)Radius: Value (String) = 31 30 2e 31 30 36 2e 34 38 2e 31 39 31 | 10.106.48.191 Radius: Type = 31 (0x1F) Calling-Station-Id Radius: Length = 15 (0x0F)Radius: Value (String) = 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | 10.106.49.111 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x5 Radius: Type = 66 (0x42) Tunnel-Client-Endpoint Radius: Length = 15 (0x0F)Radius: Value (String) = 10.106.49.111 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)Radius: Value (IP Address) = 10.106.48.191 (0x0A6A30BF) Radius: Type = 24 (0x18) State Radius: Length = 18 (0x12)Radius: Value (String) = 75 6b 35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74 | uk56XIOn51X6KuLt Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 34 (0x22)Radius: Vendor ID = 9 (0x0000009)Radius: Type = 1 (0x01) Cisco-AV-pair Radius: Length = 28 (0x1C) Radius: Value (String) = 69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=10.

31 30 36 2e 34 39 2e 31 31 31 106.49.111 Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 26 (0x1A)Radius: Vendor ID = 3076 (0x00000C04) Radius: Type = 146 (0x92) Tunnel-Group-Name Radius: Length = 20 (0x14)Radius: Value (String) = 41 4e 59 43 4f 4e 4e 45 43 54 2d 50 52 4f 46 49 | ANYCONNECT-PROFI 4c 45 LE Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 12 (0x0C)Radius: Vendor ID = 3076 (0x0000C04) Radius: Type = 150 (0x96) Client-Type Radius: Length = 6 (0x06)Radius: Value (Integer) = 2 (0x0002)send pkt 10.106.50.20/1645 rip 0x74251058 state 7 id 8 rad_vrfy() : response message verified rip 0x74251058 : chall_state 'uk56XIOn51X6KuLt' : state 0x7 : reqauth: b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca 74 05 27 5c : info 0x74251190 session_id 0x8 request_id 0x8 user 'cisco' response '***' app 0 reason 0 skey 'testing123' sip 10.106.50.20

```
RADIUS packet decode (response)
_____
Raw packet data (length = 44).....
02 08 00 2c c0 80 63 1c 3e 43 a4 bd 46 78 bd 68 | ...,.c.>C..Fx.h
49 29 23 bd 12 18 41 75 74 68 65 6e 74 69 63 61 | I)#...Authentica
74 69 6f 6e 20 73 75 63 63 65 73 73
                                               | tion success
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 8 (0x08)
Radius: Length = 44 (0 \times 002C)
Radius: Vector: C080631C3E43A4BD4678BD68492923BD
Radius: Type = 18 (0x12) Reply-Message
Radius: Length = 24 (0x18)
Radius: Value (String) =
41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 20 73 | Authentication s
75 63 63 65 73 73
                                                 uccess
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_reg 0x74251058 session 0x8 id 8
free_rip 0x74251058
radius: send queue empty
```

관련 정보

type 1

• <u>ASA에서 스플릿 터널링으로 AnyConnect Secure Mobility Client 설정</u>

- <u>Cisco IOS Headend 컨피그레이션의 AnyConnect 클라이언트에 대한 RSA SecurID 인증</u>
- <u>ASA 및 ACS의 RSA 토큰 서버 및 SDI 프로토콜 사용량</u>
- <u>ASA AnyConnect Double Authentication with Certificate Validation, Mapping, Pre-Fill 컨피그레</u> 이션 가이드
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.