Remote Access

서비스 검색 요구 사항 워크플로

프로시저

	명령 또는 동작	목적
단계 **1**	서비스 검색 요구 사항, 1 페이지	
단계 **2**	DNS 요구 사항, 2 페이지	
단계 **3**	인증서 요구 사항, 2 페이지	
단계 **4**	_collab-edge SRV 레코드 테스트, 2 페이지	

서비스 검색 요구 사항

서비스 검색을 통해 클라이언트는 엔터프라이즈 네트워크에서 서비스를 자동으로 감지하고 찾을 수 있습니다. 모바일 및 Remote Access를 위한 Expressway를 사용하면 엔터프라이즈 네트워크에서 서비스에 액세스할 수 있습니다. 클라이언트가 모바일 및 Remote Access 및 검색 서비스를 위한 Expressway를 통해 연결할 수 있게 하려면 다음 요구 사항을 충족해야 합니다.

- DNS 요구 사항
- 인증서 요구 사항
- 외부 SRV `_collab-edge`를 테스트합니다.

DNS 요구 사항

Remote Access를 통한 서비스 검색에 대한 DNS 요구 사항은 다음과 같습니다.

- 외부 DNS 서버에서 `_collab-edge` DNS SRV 레코드를 구성해야 합니다.
- 내부 이름 서버에 `_cisco-uds` DNS SRV 레코드를 구성해야 합니다.
- IM and Presence 서버 및 음성 서버에 대해 다른 도메인을 사용하는 하이브리드 클라우드 기반 구축의 경우에는 선택 사항으로 `_collab-edge` 레코드를 사용하여 DNS 서버를 찾도록 음성 서비스 도메인을 구성할 수 있습니다.

참고 Jabber는 DNS SRV 레코드(`_collab-edge` 및 `_cisco-uds`)가 식별하는 모든 SSO 지원 서버에서 임의로 선택되는 최대 3개의 SSO 지원 서버에 연결을 시도합니다. Jabber가 세 번 연결 되지 않으면 Edge SSO를 지원 하지 않는 것으로 간주 합니다.

인증서 요구 사항

Remote Access를 구성하기 전에 Cisco VCS Expressway 및 Cisco Expressway-E 서버 인증서를 다운로드하십시오. 이 서버 인증서는 HTTP와 XMPP 모두에 사용합니다.

Cisco VCS Expressway 인증서 구성에 대한 자세한 내용은 Cisco VCS Expressway에서 인증서 구성을 참조하십시오.

_collab-edge SRV 레코드 테스트

SRV 레코드 테스트

SRV 레코드 테스트를 생성한 후 액세스할 수 있는지 확인합니다.

팁 웹 기반 옵션을 선호한다면 협업 솔루션 분석기 사이트에서 SRV 확인 도구를 사용해도 됩니다.

프로시저

단계 **1** 명령 프롬프트를 엽니다.

단계 **2** **nslookup**을 입력합니다.

기본 DNS 서버 및 주소가 표시됩니다. 예상했던 DNS 서버인지 확인합니다.

단계 **3** **set type=SRV**를 입력합니다.

단계 **4** 각 SRV 레코드에 이름을 입력합니다.

예: _cisco-uds._tcp.*exampledomain*

- 서버 및 주소를 표시합니다 - SRV 레코드에 액세스할 수 있습니다.
- _cisco-uds_tcp.*exampledomain*: 존재하지 않는 도메인이 표시됩니다 - SRV 레코드에 문제가 있습니다.

Cisco Anyconnect 구축 워크플로

프로시저

	명령 또는 동작	목적
단계 **1**	애플리케이션 프로파일, 3 페이지	
단계 **2**	VPN 연결 자동화, 4 페이지	
단계 **3**	AnyConnect 문서 참조, 8 페이지	
단계 **4**	세션 매개변수, 8 페이지	

Cisco AnyConnect 구축

애플리케이션 프로파일

After you download the Cisco AnyConnect Secure Mobility Client to their device, the ASA must provision a configuration profile to the application.

Cisco AnyConnect Secure Mobility Client용 구성 프로파일에는 회사 ASA VPN 게이트웨이, 연결 프로토콜(IPSec 또는 SSL), 온디맨드 정책 같은 VPN 정책 정보가 포함됩니다.

다음 방법 중 하나로 iPhone 및 iPad용 Cisco Jabber의 애플리케이션 프로파일을 프로비저닝할 수 있습니다.

ASDM

ASDM(ASA 장치 관리자)에서 프로파일 편집기를 이용해 Cisco AnyConnect Secure Mobility Client의 VPN 프로파일을 정의하는 방법을 권장합니다.

이 방법을 사용하면 클라이언트가 VPN 연결을 처음 설정한 후 VPN 프로파일이 Cisco AnyConnect Secure Mobility Client로 자동 다운로드됩니다. 이 방법은 모든 장치 및 OS 유형에서 사용할 수 있으며, ASA에서 VPN 프로파일을 중앙집중식으로 관리할 수 있습니다.

자세한 내용은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 프로파일 생성 및 편집 항목을 참조하십시오.

iPCU

IPCU(iPhone 구성 유틸리티)로 생성하는 Apple 구성 프로파일을 사용하여 iOS 장치를 프로비저닝할 수 있습니다. Apple 구성 프로파일은 장치 보안 정책, VPN 구성 정보, Wi-Fi, 메일 및 캘린더 설정 등의 정보가 포함된 XML 파일입니다.

고수준 절차는 다음과 같습니다.

1. IPCU를 사용하여 Apple 구성 프로파일을 생성합니다.

   자세한 내용은 iPCU 설명서를 참조하십시오.

2. XML 프로파일을 .mobileconfig 파일로 내보냅니다.
3. 사용자에게 .mobileconfig 파일을 이메일로 전송합니다.

   사용자가 파일을 열면 AnyConnect VPN 프로파일 및 기타 프로파일 설정이 클라이언트 애플리케이션에 설치됩니다.

MDM

타사 MDM(모바일 장치 관리) 소프트웨어로 만든 Apple 구성 프로파일을 사용하여 iOS 장치를 프로비저닝할 수 있습니다. Apple 구성 프로파일은 장치 보안 정책, VPN 구성 정보, Wi-Fi, 메일 및 캘린더 설정 등의 정보가 포함된 XML 파일입니다.

고수준 절차는 다음과 같습니다.

1. MDM을 사용하여 Apple 구성 프로파일을 만듭니다.

   MDM 사용에 관한 자세한 내용은 Apple 설명서를 참조하십시오.

2. Apple 구성 프로파일을 등록된 장치로 푸시합니다.

Android용 Cisco Jabber의 애플리케이션 프로파일을 프로비저닝하려면, ASDM(ASA 장치 관리자)에서 프로파일 편집기를 이용해 Cisco AnyConnect Secure Mobility Client의 VPN 프로파일을 정의하십시오. 클라이언트가 VPN 연결을 처음 설정한 후 VPN 프로파일이 Cisco AnyConnect Secure Mobility Client로 자동 다운로드됩니다. 이 방법은 모든 장치 및 OS 유형에서 사용할 수 있으며, ASA에서 VPN 프로파일을 중앙집중식으로 관리할 수 있습니다. 자세한 내용은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 프로파일 생성 및 편집 항목을 참조하십시오.

VPN 연결 자동화

사용자가 회사 Wi-Fi 네트워크 외부에서 Cisco Jabber를 열면, Cisco Jabber는 Cisco UC 애플리케이션 서버에 액세스하기 위해 VPN 연결을 요구합니다. Cisco AnyConnect Secure Mobility Client가 백그라운드에 자동으로 VPN 연결을 설정하도록 시스템을 설정할 수도 있습니다. 이렇게 하면 원활한 사용자 경험을 보장하는 데 도움이 됩니다.

참고 VPN을 자동 연결로 설정하더라도, 연결 우선순위가 높은 Expressway Mobile 및 Remote Access를 수행해야 VPN을 시작할 수 있습니다.

신뢰할 수 있는 네트워크 연결 설정

Trusted Network Detection 기능을 이용하면 사용자의 위치를 기반으로 VPN 연결을 자동화하여 사용자 환경을 개선할 수 있습니다. 사용자가 회사 Wi-Fi 네트워크 내부에 있다면 Cisco Jabber는 Cisco UC 인프라에 직접 연결할 수 있습니다. 사용자가 회사 Wi-Fi 네트워크에서 나가면, Cisco Jabber는 사용자가 신뢰할 수 있는 네트워크 외부에 있음을 자동으로 감지합니다. 이 현상이 발생하면, Cisco AnyConnect Secure Mobility Client는 VPN을 시작하여 UC 인프라에 대한 연결을 보장합니다.

참고 Trusted Network Detection 기능인 인증서 및 암호 기반 인증 모두에서 작동합니다. 그러나 인증서 기반 인증이 가장 원활한 사용자 환경을 제공합니다.

프로시저

단계 **1** ASDM을 사용하여 Cisco AnyConnect 클라이언트 프로파일을 엽니다.

단계 **2** 클라이언트가 회사 Wi-Fi 네트워크 내에 있을 때 인터페이스가 수신할 수 있는, 신뢰할 수 있는 DNS 서버 및 신뢰할 수 있는 DNS 도메인 접미사 목록을 입력합니다. Cisco AnyConnect 클라이언트는 현재 인터페이스 DNS 서버와 도메인 접미사를 이 프로파일의 설정과 비교합니다.

참고 Trusted Network Detection 기능이 올바르게 작동하려면 모든 DNS 서버를 지정해야 합니다. TrustedDNSDomains와 TrustedDNSServers를 모두 설정했다면, 세션은 두 설정을 일치시켜 신뢰할 수 있는 네트워크로 정의되게 해야 합니다.

Trusted Network Detection을 설정하는 자세한 방법은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 기능 구성 장(릴리스 2.5) 또는 *VPN* 액세스 구성(릴리스 3.0 또는 3.1)에 있는 *Trusted Network Detection* 섹션을 참조하십시오.

온디맨드 **VPN** 연결 설정

Apple iOS Connect On Demand 기능을 이용하면 사용자의 도메인을 기반으로 VPN 연결을 자동화하여 사용자 환경을 개선할 수 있습니다.

사용자가 회사 Wi-Fi 네트워크 내부에 있다면 Cisco Jabber는 Cisco UC 인프라에 직접 연결할 수 있습니다. AnyConnect 클라이언트 프로파일에 지정한 도메인에 연결된 Cisco AnyConnect는 사용자가 회사 Wi-Fi 네트워크에서 나갈 때 이를 자동으로 감지합니다. 이 경우 애플리케이션은 VPN을 시작하여 UC 인프라와의 연결을 보장합니다. Cisco Jabber를 포함한 장치의 모든 애플리케이션이 이 기능을 활용할 수 있습니다.

참고 Connect On Demand는 인증서 인증 연결만 지원합니다.

이 기능은 다음 옵션을 지원합니다.

- 항상 연결 — Apple iOS는 항상 이 목록에 있는 도메인과의 VPN 연결을 시작합니다.
- 필요한 경우 연결 — Apple iOS는 DNS를 이용해 주소를 확인할 수 없을 때만 목록에 있는 도메인과의 VPN 연결을 시작합니다.
- 연결 안함 — Apple iOS는 이 목록에 있는 도메인과의 VPN 연결을 시작하지 않습니다.

주의 Apple은 조만간 항상 연결 옵션을 제거할 예정입니다. [항상 연결] 옵션이 제거되면 사용자는 [필요한 경우 연결] 옵션을 선택하면 됩니다. [필요한 경우 연결] 옵션을 사용할 때 Cisco Jabber 사용자에게 문제가 발생하기도 합니다. 예를 들어 Cisco Unified Communications Manager의 호스트 이름을 회사 네트워크 회부에서 확인할 수 있다면, iOS는 VPN 연결을 트리거하지 않습니다. 사용자는 전화를 걸기 전에 Cisco AnyConnect Secure Mobility Client를 수동으로 시작하여 이러한 문제를 해결할 수 있습니다.

프로시저

단계 **1** ASDM 프로파일 편집기, iPCU 또는 MDM 소프트웨어를 사용하여 AnyConnect 클라이언트 프로파일을 엽니다.

단계 **2** AnyConnect 클라이언트 프로파일의 [필요한 경우 연결] 섹션에서 온디맨드 도메인 목록을 입력합니다.

도메인 목록에는 와일드 카드 옵션(예: cucm.cisco.com, cisco.com 및 *. webex.com)이 포함될 수 있습니다.

Cisco Unified Communications Manager에서 자동 VPN 액세스 설정

시작하기 전에

- 모바일 장치는 인증서 기반 인증을 이용한 VPN 온디맨드 액세스를 설정해야 합니다. VPN 액세스를 설정 관련 도움이 필요하다면, VPN 클라이언트 및 헤드 엔드 공급업체에 문의하십시오.
- Cisco AnyConnect Secure Mobility Client 및 Cisco Adaptive Security Appliance의 요구 사항은 소프트웨어 요구 사항 항목을 참조하십시오.
- Cisco AnyConnect 설정에 관한 자세한 내용은 *Cisco AnyConnect VPN Client* 유지 관리 및 작동 설명서를 참조하십시오.

프로시저

단계 **1** 클라이언트가 VPN을 요청 시 시작하게 하는 URL을 식별합니다.

a) 다음 방법 중 하나를 사용하여 클라이언트가 VPN을 요청 시 시작하게 하는 URL을 식별합니다.

- 필요한 경우 연결
  - (IP 주소가 아닌) 도메인 이름을 통해 액세스하도록 Cisco Unified Communications Manager를 구성하고, 이 도메인 이름이 방화벽 외부에서 확인할 수 없는지 확인합니다.
  - 이 도메인을 Cisco AnyConnect 클라이언트 연결의 요청 시 연결 도메인 목록의 "필요한 경우 연결" 목록에 포함합니다.
- 항상 연결
  - 4단계에서 매개변수를 존재하지 않는 도메인으로 설정합니다. 존재하지 않는 도메인을 이용하면 사용자가 방화벽 내부 또는 외부에 있을 때 DNS 쿼리가 실패하게 됩니다.
  - 이 도메인을 Cisco AnyConnect 클라이언트 연결의 요청 시 연결 도메인 목록의 "항상 연결" 목록에 포함합니다.

    URL은 도메인 이름만 포함해야 합니다. 프로토콜이나 경로는 포함하지 마십시오(예: "https://cm8ondemand.company.com/vpn" 대신 "cm8ondemand.company.com" 사용).

b) Cisco AnyConnect에 URL을 입력하고 이 도메인에서 DNS 쿼리가 실패하는지 확인합니다.

단계 **2** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **3** 사용자의 장치 페이지로 이동합니다.

단계 **4** 온디맨드 **VPN URL** 필드의 제품별 구성 레이아웃 섹션에, 1단계에서 Cisco AnyConnect에서 식별하고 사용한 URL을 입력합니다.

URL에는 프로토콜이나 경로가 없는 도메인 이름만 사용해야 합니다.

단계 **5** 저장을 선택합니다.

Cisco Jabber가 열리면 URL에 대한 DNS 쿼리를 시작합니다. 이 URL이 이번 절차에서 정의한 온디맨드 도메인 목록 항목(예: cisco.com)과 일치한다면, Cisco Jabber는 AnyConnect VPN 연결을 간접적으로 시작합니다.

다음에 수행할 작업

- 이 기능을 테스트합니다.
  - IOS 장치의 인터넷 브라우저에 URL을 입력하고 VPN이 자동으로 시작되는지 확인합니다. 상태 표시줄에 VPN 아이콘이 표시되어야 합니다.
  - IOS 장치에서 VPN을 사용하여 회사 네트워크에 연결할 수 있는지 확인합니다. 예를 들어 회사 인트라넷에서 웹 페이지에 액세스합니다. IOS 장치를 연결할 수 없다면, VPN 기술 공급업체에 문의하십시오.
  - IT 부서와 함께 VPN이 특정 트래픽 유형에 대한 액세스를 차단하지 않는지 확인합니다(예: 관리자가 이메일과 캘린더 트래픽만 허용하도록 시스템을 설정).
- 회사 네트워크에 직접 연결되도록 클라이언트를 설정했는지 확인합니다.

AnyConnect 문서 참조

AnyConnect 요구 사항 및 구축에 대한 자세한 내용은 아래의 릴리스 설명서를 참조하십시오.
https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

세션 매개변수

ASA 세션 매개변수를 구성하여 보안 연결 성능을 향상할 수 있습니다. 최상의 사용자 경험을 위해서는 다음과 같은 ASA 세션 매개변수를 구성해야 합니다.

- 데이터그램 전송 계층 보안(DTLS) - DTLS는 지연 및 데이터 손실을 방지하는 데이터 경로를 제공하는 SSL 프로토콜입니다.
- 자동 재연결 - 자동 재연결 또는 세션 지속성을 사용하여 CiscoAnyConnect Secure Mobility Client에서 세션 중단을 복구하고 세션을 다시 설정할 수 있습니다.
- 세션 지속성 - 이 매개변수를 사용하면 VPN 세션에서 서비스 중단을 복구하고 연결을 다시 설정할 수 있습니다.
- 유휴 시간 제한 - 유휴 시간 제한은 통신 활동이 전혀 없는 경우, ASA가 보안 연결을 종료한 이후의 시간을 정의합니다.
- 데드 피어 감지(DTD) - DTD는 ASA 및 Cisco AnyConnect Secure Mobility Client가 실패한 연결을 신속하게 감지할 수 있도록 보장합니다.

ASA 세션 매개변수 설정

Cisco AnyConnect Secure Mobility Client에 대한 최종 사용자 경험을 최적화하려면 ASA 세션 매개변수를 다음과 같이 설정하는 것이 좋습니다.

프로시저

단계 **1** DTLS를 사용하도록 Cisco AnyConnect를 설정합니다.

자세한 내용은 *Cisco AnyConnect VPN Client* 관리자 설명서 버전 *2.0*, *ASDM*을 이용한 *AnyConnect* 기능 구성 장의 *AnyConnect(SSL)* 연결을 이용한 *DTLS(Datagram Transport Layer Security)* 활성화를 참조하십시오.

단계 **2** 세션 지속성(자동 재연결)을 설정합니다.

a) ASDM을 사용하여 VPN 클라이언트 프로파일을 엽니다.
b) 자동 재연결 동작 매개변수를 재개 후 재연결로 설정합니다.

자세한 내용은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 기능 구성 장(릴리스 2.5) 또는 *VPN* 액세스 구성 장(릴리스 3.0 또는 3.1)에 있는 자동 재연결 구성 항목을 참조하십시오.

단계 **3** 유휴 시간 초과 값을 설정합니다.

a) Cisco Jabber 클라이언트와 관련된 그룹 정책을 만듭니다.
b) 유휴 시간 초과 값을 30분으로 설정합니다.

자세한 내용은 사용자 릴리스의 *Cisco ASA 5580* 적응형 보안 어플라이언스 명령 참조의 *vpn-idle-timeout* 섹션을 참조하십시오.

단계 **4** DPD(비활성 피어 감지)를 설정합니다.

a) 서버측 DPD를 비활성화합니다.
b) 클라이언트측 DPD를 활성화합니다.

자세한 내용은 *CLI, 8.4, 8.6*를 이용한 *Cisco ASA 5500* 시리즈 구성 설명서*VPN* 구성 장의 비활성 피어 감지 활성화 및 조정 항목을 참조하십시오.

사용자 프로파일에 대해 모바일 및 **Remote Access** 정책 정의

사용자가 회사 네트워크 외부에서 작업 중인 경우, Cisco Unified Communications Manager에서 MRA(Mobile and Remote Access) 액세스 정책을 추가하고 Cisco Jabber에서 액세스할 수 있는 서비스를 제어할 수 있습니다. MRA 액세스 정책은 사용자 프로파일에 할당되며, 조직의 사용자에게 다른 MRA 액세스 정책을 할당할 수 있습니다.

시작하기 전에

모바일 및 Remote Access 정책은 Cisco Unified Communications Manager 릴리스 12.0 이상, Cisco Expressway X8.10 이상, OAuth 활성화 환경에서 지원됩니다.

프로시저

단계 **1** **Cisco Unified CM** 관리에서 사용자 관리로 이동하여 최종 사용자를 선택합니다.
단계 **2** 찾기를 클릭해 최종 사용자를 검색하여 선택합니다.
단계 **3** 최종 사용자 구성 창에서 사용자 프로파일의 세부 정보 보기를 클릭합니다.
단계 **4** 모바일 및 **Remote Access** 정책 섹션에서 모바일 및 **Remote Access** 활성화를 선택합니다.
단계 **5** **Jabber** 정책 드롭다운에서 정책을 선택합니다.

- 서비스 없음 - 사용자는 Cisco Jabber 서비스에 액세스할 수 없습니다.
- **IM & Presence** 전용 - 사용자는 IM, 프레즌스, 음성 메일 및 연락처 검색에만 액세스할 수 있습니다.
- **IM & Presence,** 음성 및 영상 통화 - 사용자는 모든 Cisco Jabber 서비스에 액세스할 수 있습니다.

단계 **6** 저장을 선택합니다.