Ivanti Connect Secure
: Secure Access VPN for the Everywhere Workplace

Overview

최근 인력은 원격 근무자이며, 최근 업무 환경은 사무실과 기존 데이터 센터를 넘어 클라우드로 확장되었습니다. 사용자가 필요로 하는 애플리케이션의 수와 복잡성이 증가하고, 사용자가 연결할 수 있는 디바이스 유형이 다양해지고, 악의적인 공격자의 위협이 끊이지 않는 상황에서 어디서나 업무 환경을 보호하는 것은 어려운 일이 될 수 있습니다.

Ivanti Connect Secure는 언제 어디서나 웹 지원 장치에서 기업 리소스에 이르기까지 원격 및 모바일 사용자를 위한 원활하고 비용 효율적인 SSL VPN 솔루션을 제공합니다. 강력하고 사용하기 쉬운 Ivanti Connect Secure는 모든 주요 산업에 걸쳐 규모에 관계없이 모든 조직에 가장 널리 배포된 SSL VPN입니다.

제품 설명

기업과 서비스 제공업체는 안전하고 권한이 부여된 사용자의 리소스 액세스를 제어할 수 있는 위치 및 기기에 독립적인 네트워크 연결을 제공해야 하는 어려운 과제를 안고 있습니다. 보안 침해와 위협은 통제 불능 상태로 계속 증가하고 있으며, 재택 근무 혁명이 계속 증가함에 따라 사무실 외부에서 연결하는 직원과 사용자 수가 증가하고 있습니다.

Ivanti Secure Access Client

Ivanti Connect Secure에는 모바일 및 개인 컴퓨팅 장치를 위한 동적 멀티서비스 네트워크 클라이언트인 Ivanti Secure Access Client가 포함되어 있습니다. Ivanti Secure Access Client는 배포가 간편하여 사용자가 어디서나 모든 기기에서 빠르게 “클릭하고 연결” 할 수 있습니다.

The Ivanti Secure Access Client는 앱별 VPN, 온디맨드 VPN 연결, 상시 접속 및 잠금 모드를 지원하며, 전체 터널 및 FQDN 또는 IP/네트워크 기반 분할 터널 연결도 지원합니다.

Ivanti 보안 액세스 클라이언트는 사용자를 데이터 센터와 클라우드 네트워크에 안전하게 연결합니다. Ivanti Secure Access Client는 사용자 친화적인 패키지로 포장되어, 사용자 엔드포인트에서 적절한 네트워크 및 보안 서비스를 동적으로 활성화합니다.

Ivanti를 사용하면, 연결만 하면 모바일 디바이스가 약속하는 생산성을 제공할 수 있습니다.

Ivanti Secure Access Client는 동적 액세스 제어를 제공하여 사용자 장치에서 원격(SSL VPN) 및 로컬(NAC) 액세스 제어 서비스 간에 원활하게 전환할 수 있습니다. 또한 Ivanti Client는 모바일 및 데스크톱 컴퓨팅 디바이스에 대한 포괄적인 엔드포인트 보안 상태 평가를 수행하고, 필요한 경우 격리 및 수정할 수 있습니다.

Ivanti Security Appliance(ISA)

Ivanti Security Appliance(ISA)는 차세대 Ivanti Appliance 제품군입니다. ISA 시리즈 Appliance는 속도와 보안을 위해 특별히 설계되었으며 SMB부터 엔터프라이즈까지 모든 조직의 요구 사항에 맞게 확장할 수 있습니다. ISA 시리즈 Appliance는 고정 구성 랙 마운트 하드웨어로 제공되거나 가상 어플라이언스로 데이터센터 또는 클라우드에 배포할 수 있습니다.

아키텍처 및 주요 구성 요소

Ivanti Connect Secure는 아래 언급된 바와 같이 클라우드 또는 가상 어플라이언스인 Ivanti 보안 어플라이언스(ISA)에서 사용할 수 있습니다.

Ivanti Security Appliance(ISA) 시리즈

- ISA 6000 Appliance: 고정 구성, 1U 랙 마운트 어플라이언스, 최대 2,500명의 SSL VPN 동시 사용자 지원
- ISA 8000 Appliance: 고정 구성, 1U 랙 마운트 어플라이언스, 최대 25,000명의 SSL VPN 동시 사용자 지원
- 가상 어플라이언스(ISA-V 시리즈): VMware ESXi, KVM, Microsoft Hyper-V, Nutanix, Microsoft Azure, Amazon Web Services, Google Cloud Platform.
- 가상 어플라이언스(ISA-V 시리즈) 포함 내역
  - ISA4000-V: 최대 250명의 사용자 지원
  - ISA6000-V: 최대 2,500명의 사용자 지원
  - ISA8000-V: 최대 25,000명의 사용자 지원

Ivanti Connect Secure (ICS) 보안 표준 및 인증

Ivanti Connect Secure (ICS)는 미국 국립표준기술연구소(NIST)의 연방 정보 처리 표준(FIPS) 및 국가 정보 보증 파트너십(NIAP) 표준을 준수하여 시스템 및 제품의 보안과 상호 운용성을 보장하고 데이터의 기밀성, 무결성 및 가용성을 보호합니다.

Ivanti Connect Secure (ICS)	NIST / FIPS: Certified by using openSSL.org's FIPS provider/ module in ICS 22.6R2 or later
	NIAP: Certified as Compliant Product, ICS 22.2 or later.
Ivanti Secure Access Client (ISAC) for Windows	NIST / FIPS: 22.7R2 or later based on openSSL.org Cert #4282.
ISAC for macOS	NIST / FIPS: 22.7R2 or later based on openSSL.org Cert #4282.
ISAC Mobile – iOS, Android	NIST / FIPS: SafeLogic based Cert #1938

Features and Benefits

Feature	Description
Layer 3 SSL VPN	▪ 이중 전송(SSL + 보안 페이로드 캡슐화) 전체 레이어 3 VPN 연결과 세분화된 액세스 제어 ▪ 규정 준수를 위한 '잠금 모드가 있는 상시 접속 VPN' 및 'VPN 전용 액세스' 모드(사용자 위치에 따라 VPN 연결이 자동으로 연결/연결 해제됨) ▪ 사용자 로그인 후 사용자 기반 인증까지 단계적으로 강화할 수 있는 머신 기반 VPN ▪ 온디맨드 VPN" 및 '앱별 VPN'을 통해 원활하고 안전한 최종 사용자 경험 제공
Layer 4 VPN	▪ 특정 애플리케이션에서 특정 대상으로 트래픽을 터널링하는 클라이언트/서버 프록시 애플리케이션 ▪ 보안 애플리케이션 관리자(PSAM)의 Windows 버전은 개별 클라이언트/서버 애플리케이션 및 애플리케이션 서버에 대한 보안 트래픽 활성화 ▪ 보안 애플리케이션 관리자(JSAM)의 Java 버전은 정적 TCP 포트 클라이언트/서버 애플리케이션 지원
조건부 액세스	▪ 네트워크와 데이터를 보호하기 위해 일련의 자동화된 정책을 통해 디바이스와 사용자를 검증하고 확인. 각 액세스 시도는 동적으로 평가되고 유효한 정책에 따라 실시간으로 제어
SAML을 통한 Layer 7 웹 싱글 사인온 (SSO)	▪ 최종 사용자가 레이어 3 터널을 통해 네트워크에 인증하는 동시에 SAML SSO 지원을 통해 브라우저를 통해 액세스하는 웹 애플리케이션에 대한 SSO를 사용 가능
고급 사용자 포털 (Layer 7/클라이언트 VPN)	▪ HTML5 지원 브라우저에서 게시되거나 사용자가 추가한 애플리케이션 및 링크에 대한 클라이언트리스 보안 ▪ 사용자 역할에 따른 동적 생성 ▪ 고급 HTML5를 통한 RDP/텔넷/VNC/SSH 액세스 ▪ 웹 리라이터 및 웹 프록시 내장 ▪ 다중 포털 지원(예: 직원용 SSO 포털, 계약업체용 2FA 포털) ▪ Windows 터미널 서비스, VDI(Citrix, VMware) 및 파일 브라우징 지원
최적화된 최종 사용자 경험	▪ 원격 접속에서 Local LAN 접속까지 원활한 로밍(Ivanti Policy Secure) ▪ 원격 또는 현장 위치에서 빠르고 안전하게 액세스할 수 있는 Single Sign On(SSO) 제공 (Ivanti Cloud Secure 및 Ivanti Policy Secure와의 통합으로)
상태 기반 엔드포인트 무결성 및 평가	▪ 간편한 정책 정의로 인증 전에 최종 사용자 디바이스를 평가하고 수정 ▪ Windows, MacOS, Apple iOS and Android

Features and Benefits(Continue)

Feature	Description
유연한 실행 옵션 (Standalone 클라이언트, 브라우저 기반 실행)	▪ 사용자는 웹 브라우저를 통해 또는 데스크톱에서 직접 SSL VPN을 쉽게 실행 가능 ▪ 자동 연결 기능을 통해 기기가 시작되거나 사용자가 로그온할 때 자동으로 VPN에 연결 가능 ▪ 주문형 VPN 기능은 승인된 애플리케이션에 기업 접속이 필요할 때 백그라운드에서 원활하게 VPN을 자동 트리거하기 위해 OS 기능 활용
클라우드 보안 솔루션 지원	▪ 클라우드 및 데이터센터 액세스를 차세대 작업자를 위한 원활한 사용자 환경으로 통합 ▪ 하이브리드 DC 액세스에 대한 규정 준수 규칙 추가
사전 구성 옵션(Windows 및 Mac만 해당)	▪ 관리자는 최종 사용자가 선택할 수 있는 게이트웨이 목록으로 배포를 사전 구성 가능
인증 옵션	▪ 여러 사용자 속성을 사용하는 동적 다단계 인증을 사용하는 적응형 인증 ▪ 관리자는 비즈니스용 Windows Hello를 통한 생체 인증 지원, 하드웨어 토큰, 스마트 카드, 소프트 토큰, 스마트 카드, 소프트 토큰, 구글 인증기, 일회용 비밀번호, 인증서 인증 등 다양한 인증 메커니즘을 사용하여 원격 사용자 인증을 위해 Ivanti 배포 가능 ▪ 관리자는 원하는 인터페이스(내부/외부/관리)를 통해 AAA 트래픽을 전송하도록 선택하여 ID 공급자에게 사용자 인증 위임 가능 ▪ OAuth/OpenID Connect 지원으로 연결 보안(신뢰 당사자 역할)에 연결하는 동안 Google, OKTA, Azure AD 등과 같은 모든 표준 OpenID 공급자와 통합 가능
VMware Horizon 및 Citrix XenApp/ XenDesktop VPN	▪ Ivanti는 최신 버전의 VMware Horizon and Citrix XenApp / XenDesktop 지원
세분화된 SSL 암호 구성	▪ 관리자가 보안 규정 준수를 위해 사전 구성된 암호 대신 특정 암호 선택 가능
REST API	▪ 어플라이언스에 대한 프로그래밍 방식의 액세스를 위한 포괄적인 REST 기반 API

풍부한 액세스 권한 관리 기능

Feature	Description	Benefits
사용자 지정 표현식을 사용한 동적 역할 매핑	▪ 네트워크, 장치 및 세션 속성을 결합하여 허용되는 액세스 유형 결정 ▪ 세션별로 속성을 동적으로 조합하여 역할 매핑 가능 ▪ MDM 통합을 통해 기기 속성을 가져오고, 접근 권한을 부여하기 전에 적절한 정책 적용	▪ 관리자가 각 고유 세션에 대해 목적별 프로비저닝 가능
RSA 인증 관리자 지원	▪ RSA 인증 관리자 위험 기반 인증	▪ 다른 인증 계층 옵션 제공
표준 기반 내장형 시간 기반 일회성 비밀번호(TOTP)	▪ 스마트폰을 사용하여 다단계 인증 활성화	▪ 스마트폰을 활용하여 모바일 앱으로 일회용 비밀번호를 생성하는 비용 효율적인 셀프 서비스 2단계 인증 메커니즘 배포
사용자 다중 세션 지원	▪ 원격 사용자가 여러 원격 액세스 세션 시작 가능	▪ 원격 사용자가 노트북과 스마트폰에서 동시에 VPN에 액세스할 때와 같이 여러 개의 인증된 세션을 동시에 오픈 가능
사용자 기록 동기화	▪ 여러 Ivanti Appliance에서 사용자 북마크와 같은 사용자 기록의 동기화 지원	▪ 한 지역에서 다른 지역으로 자주 이동하는 사용자에게 일관된 경험 보장. 이를 위해 Ivanti Connect Secure를 실행하는 다른 Ivanti Appliance에 연결
모바일 친화적인 SSL VPN 로그인 페이지	▪ 애플 아이폰, 아이패드, 구글 안드로이드 등 모바일 기기에 맞게 미리 정의된 HTML 페이지 제공	▪ 모바일 디바이스 사용자에게 간소화되고 향상된 사용자 경험과 디바이스 유형에 맞게 맞춤화된 웹 페이지 제공
강력한 인증 및 ID 및 액세스 관리(IAM) 플랫폼과의 통합	▪ 표준 기반 SAML v2.0 지원 및 공개 키 인프라(PKI)/디지털 인증서를 포함한 보안 어설션 마크업 언어(SAML), SecurID 지원. OAuth/OpenID Connect 지원	▪ 기존 기업 인증 방법을 활용하여 관리 간소화

관리 용이성

Feature	Description	Benefits
Neurons for Secure Access(nSA)	▪ Ivanti Connect Secure 배포를 위한 중앙 집중식 관리, 분석 및 보고 플랫폼(옵션) ▪ 전체 구성 관리, 원클릭 업그레이드, 중앙 집중식 로깅, 사용자 지정 보고 및 문제 해결 ▪ 구성 템플릿 및 멀티노드 구성 관리를 통한 구성 '리프트 앤 시프트'	▪ 중앙 집중식 구성 및 게이트웨이 라이프스타일 관리로 시간과 비용 절약 가능 ▪ 향상된 행동 분석으로 위험한 사용자 행동을 식별하고 문제가 발생하기 전 자동 조치 ▪ 멀티노드 또는 글로벌 배포 관리 간소화
모바일 디바이스 관리 (MDM) 통합	▪ 통합 보고 및 대시보드를 통해 관리 가소화 ▪ 보다 지능적이고 중앙 집중화된 정책 생성을 위해 MDM 속성 활용 ▪ 투명한 '노터치' MDM 기반 Ivanti Client를 iOS 및 Android 디바이스에 배포	▪ 포괄적인 엔드포인트 가시성을 확보하고 추가적인 모바일 사용 사례를 지원하기 위해 MDM 투자 확장
Bridge Certification Authority (BCA) 지원	▪ Bridge CA는 루트 인증 기관(Root CAs)을 교차 인증하는 PKI 확장 ▪ 클라이언트 인증서 인증을 사용하는 연합된 PKI 배치 지원 ▪ 고객이 관리 UI에서 정책 확장을 구성하고, 이를 인증서 검증 중에 적용되도록 함	▪ 고급 PKI 배포를 사용하는 고객이 Ivanti Appliance를 배포하여 조직과 사용자 간에 데이터와 애플리케이션을 공유하기 전에 엄격한 표준을 준수하는 인증서 유효성 검사 수행 가능
다중 호스트 이름 지원	▪ 단일 어플라이언스에서 다양한 가상 엑스트라넷 웹사이트를 호스팅할 수 있는 기능	▪ 서버 증설에 따른 비용 제거 ▪ 차별화된 엔트리 URL을 통해 투명한 사용자 경험 제공 ▪ 관리 오버헤드 완화
커스터마이징 가능한 사용자 인터페이스	▪ 완전히 사용자 정의된 로그인 페이지 생성	▪ 지정된 역할에 대한 개별화된 보기를 제공하여 사용자 경험 간소화

유연한 싱글 사인온(SSO) 기능

Feature	Description	Benefits
클라우드 및 웹용 SAML 싱글 사인온 애플리케이션 액세스	▪ 최근 가장 인기 있는 SaaS(서비스형 소프트웨어) 애플리케이션을 비롯한 다양한 웹 애플리케이션에 대한 SAML 2.0 기반 SSO 제공 ▪ Ivanti Connect Secure Layer 3 VPN 터널을 통해 연결할 때도 SSO 기능 포함 ▪ Ivanti Connect Secure는 SAML ID 공급자(IdP)와 SAML 서비스 공급자(SP) 배포 모두 지원	▪ 사용자의 웹 및 클라우드 기반 애플리케이션에 대한 싱글 사인온으로 사용자 연결 환경 간소화
Kerberos Constrained Delegation	▪ KCD(Kerberos 제한 위임) 프로토콜 지원 ▪ 클라이언트 인증서, 신뢰할 수 있는 CA 인증서 및 인증을 위한 적절한 위임 정책을 요구하는 Exchange Active Sync 트래픽에 대해 KCD 적용	▪ 회사에서 정적 암호를 관리할 필요가 없으므로 관리 시간과 비용 절감
Kerberos SSO 및 NT LAN 관리자(NTLMv2) 지원	▪ Ivanti Connect Secure는 사용자 자격 증명을 사용하여 Kerberos 또는 NTLMv2를 통해 원격 사용자를 자동 인증	▪ 여러 애플리케이션에 액세스하기 위해 자격 증명을 여러번 입력할 필요가 없어 사용자 환경 간소화
패스워드 관리 통합	▪ 디렉토리 저장소(LDAP, AD 등)의 비밀번호 정책과 광범위한 통합을 위한 표준 기반 인터페이스	▪ 기존 서버를 활용하여 사용자 인증 ▪ 사용자가 Ivanti Connect Secure 인터페이스를 통해 직접 비밀번호를 관리 가능
웹 기반 SSO 기본 인증 및 NTLM	▪ 사용자가 로그인 자격 증명을 다시 입력하지 않고도 다른 액세스 관리 시스템으로 보호되는 다른 애플리케이션이나 리소스에 액세스 가능	▪ 사용자가 웹 기반 및 Microsoft 애플리케이션을 위해 여러 개의 웹 기반 및 Microsoft 애플리케이션에 대한 자격 증명을 입력하고 관리할 필요 없음
웹 기반 SSO - 폼 기반, 헤더 변수 기반, SAML 기반	▪ 사용자 이름, 자격 증명 및 기타 고객 정의 속성을 다른 제품의 인증 양식과 헤더 변수로 전달 가능	▪ 사용자 생산성 향상 및 맞춤형 경험 제공
OAuth/OpenID 연결	▪ OAuth/OpenID Connect 지원으로, Connect Secure(신뢰 당사자 역할)에 연결하면서 Google, Okta, Azure AD 등과 같은 모든 표준 OpenID 공급자와 통합	▪ 기존 OAuth 배포에 통합하여 손쉬운 사용자 ID 페더레이션 가능

목적별 프로비저닝

Feature	Description	Benefits
Ivanti Secure Access Client	▪ 원격 사용자에게 LAN 액세스 제어 및 동적 VPN 기능을 제공할 수 있는 통합된 원격 액세스 클라이언트	▪ Ivanti Secure Access Client는 VPN 및 LAN 액세스 제어와 같은 다양한 기능을 위해 여러 개의 개별 클라이언트를 배포하고 유지 관리할 필요성을 대체. 최종 사용자는 필요한 연결을 '클릭하고 연결'하기만 하면 됨
클라이언트 없는 핵심 웹 액세스	▪ Outlook 웹 액세스, SharePoint 등을 포함한 다양한 유형의 웹 기반 애플리케이션에 안전하게 액세스 지원 ▪ Ivanti Connect Secure의 원격 데스크톱 프로토콜(RDP) 액세스는 HTML5, 타사 RDP, Ericom과 같은 웹소켓 번역기를 통해 제공	▪ 매우 세분화된 보안 제어 옵션으로 다양한 최종 사용자 기기에서 가장 쉽게 액세스할 수 있는 형태의 애플리케이션 및 리소스 액세스 제공 ▪ 웹 브라우저만을 사용하는 완전한 클라이언트리스 접근방식
모바일 장치에 대한 IKEv2 지원	▪ 원격 사용자가 IKEv2(인터넷 키 교환) VPN 연결을 지원하는 모든 모바일 장치에서 연결 ▪ 관리자는 엄격한 인증서 또는 사용자 이름/암호 인증을 활성화하여 IKEv2를 통한 액세스를 허용	▪ IKEv2를 지원하지만 아직 클라이언트를 사용할 수 없는 새로운 장치에 대한 완전한 L3 VPN 지원
가상 데스크톱 인프라 (VDI) 지원	▪ VMware View Manager 및 Citrix Xen Desktop과의 상호 운용성을 지원하여 관리자가 Ivanti Connect Secure와 함께 가상 데스크톱을 배포할 수 있도록 지원	▪ 원격 사용자가 VMware 서버에 호스팅된 가상 데스크톱에 원활하게 액세스 가능 ▪ 사용자가 가상 데스크톱에 연결할 수 있도록 동적 클라이언트 폴백 옵션을 포함하여 Vmware View 클라이언트 및 Citrix Workspace 클라이언트의 동적 딜리버리 제공
제로 터치 프로비저닝	▪ OpenStack, VMWare, Hyper V 및 클라우드(GCP, Azure, AWS)를 사용하여 ICS 배포 ▪ 수동 입력 없이 로컬 DHCP 서버에서 초기 구성을 가져옴 ▪ REST API로 구성 및 관리	▪ 관리자의 생산성 향상 및 맞춤형 환경 제공
액티브싱크 프록시	▪ 클라이언트 소프트웨어를 설치하지 않고도 프록시를 통해 모바일 장치(예: iOS 또는 Android)에서 Exchange Server에 대한 보안 액세스 연결(강력한 암호화 + 인증서 인증) 제공 ▪ 최대 5,000개의 동시 세션 지원.	▪ 많은 사용자(직원, 계약자 및 파트너 포함)가 ActiveSync로 휴대폰을 통해 회사 리소스에 액세스하도록 허용
보안 어플리케이션 매니저 (SAM)	▪ 클라이언트/서버 애플리케이션에 액세스할 수 있는 경량 애플리케이션 다운로드	▪ 웹 브라우저만으로 클라이언트/서버 애플리케이션에 액세스 ▪ 사전 설치된 클라이언트 없이도 터미널 서버 애플리케이션에 대한 기본 액세스 제공

Ivanti 소개

Ivanti는 IT와 보안 사이의 장벽을 허물어 Everywhere Work가 성공할 수 있도록 지원합니다. Ivanti는 CIO와 CISO를 위해 특별히 설계된 최초의 기술 플랫폼을 개발하여 IT 및 보안 팀이 조직의 필요에 따라 확장할 수 있는 포괄적인 소프트웨어 솔루션을 제공하여 직원의 경험을 지원하고 보호하며 향상시킬 수 있도록 지원합니다. Ivanti 플랫폼은 클라우드 규모의 지능형 하이퍼자동화 레이어인 Ivanti Neurons를 기반으로 하며, 조직 전체에서 사전 예방적 치유와 사용자 친화적인 보안을 지원하고 사용자에게 만족스러운 직원 경험을 제공합니다. 포춘 100대 기업 중 85개 기업을 포함한 40,000개 이상의 고객이 Ivanti의 엔드투엔드 솔루션으로 문제를 정면으로 해결하기 위해 Ivanti를 선택했습니다. Ivanti는 모든 관점을 경청하고 존중하며 가치를 인정하는 환경을 조성하기 위해 노력하며 고객, 파트너, 직원, 지구를 위해 보다 지속 가능한 미래를 위해 최선을 다하고 있습니다. 자세한 내용은 ivanti.com을 방문하거나 @GoIvanti를 팔로우하세요.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

이반티 총판 에쓰티케이
No1. AI &Security Solution Company

홈페이지: stkcorp.co.kr
영업문의: ivanti.sales@stkcorp.co.kr
마케팅문의: ivnati.mkt@stkcorp.co.kr
기술문의: ivanti.tech@stkcorp.co.kr