Ivanti Connect Secure: Secure Access VPN for the Everywhere Workplace

Overview

The modern workforce is a remote workforce, and the modern workplace has spread beyond the office and the traditional data center to the cloud. With the increased number and complexity of applications users need, the many different types of devices users can connect from, and the constant threat of malicious actors, securing the Everywhere Workplace can be a daunting task.

Ivanti Connect Secure provides a seamless, cost-effective, SSL VPN solution for remote and mobile users from any web-enabled device to corporate resources — anytime, anywhere. Powerful and easy to use, Ivanti Connect Secure is the most widely deployed SSL VPN for organizations of any size, across every major industry.

Product Description

Enterprises and service providers have the difficult challenge of providing location and device independent network connectivity that is secure and capable of controlling resource access for authorized users. Breaches and threats continue to spiral out of control and increasing numbers of employees and users are connecting from outside the office as the work from home revolution continues to grow.

Ivanti Secure Access Client

Ivanti Connect Secure includes the Ivanti Secure Access Client. The Ivanti Secure Access Client is a dynamic, multiservice network client for mobile and personal computing devices. Ivanti Secure Access Clients are easy to deploy, enabling users to quickly “click and connect” from any device, anywhere.

The Ivanti Secure Access Client supports per-app VPN, on-demand VPN connectivity, always-on and lockdown modes. Ivanti Secure Access Client also supports full tunnel and FQDN or IP/network-based split tunnel connectivity.

The Ivanti Secure Access Client securely connect users to networks, both data center and cloud. Wrapped in a user-friendly package, Ivanti Secure Access Client dynamically enables the appropriate network and security services on users’ endpoints. With Ivanti, the connection just works, helping to deliver the productivity promised by mobile devices.

Ivanti Secure Access Client delivers dynamic access control, seamlessly switching between remote (SSL VPN), and local (NAC) access control services on user devices. Ivanti Client also enables comprehensive endpoint security posture assessment for mobile and desktop computing devices, and quarantine and remediate, if necessary.

Ivanti Security Appliance

Ivanti Security Appliance (ISA) is the new generation of Ivanti appliance offerings. ISA series appliances are purpose-built for speed and security and can scale to match any organizations needs, from SMB to enterprise. ISA series appliances are available as fixed-configuration rack-mounted hardware or can be deployed to the data center or cloud as virtual appliances. With massive performance increases through hardware, software and kernel optimizations, ISA series appliances boast impressive throughput speed boosts in lab testing over equivalent PSA series appliances.

Architecture and Key Components

Ivanti Connect Secure is available on Ivanti Security Appliance (ISA) and Ivanti PSA series appliances, as hardware or as a virtual appliance as noted below.

Ivanti Security Appliance (ISA) Series

- ISA 6000 Appliance: Fixed configuration, 1U rack mounted appliance, supporting up to 2,500 SSL VPN concurrent users
- ISA 8000 Appliance: Fixed configuration, 1U rack mounted appliance, supporting up to 25,000 SSL VPN concurrent users
- Virtual Appliances (ISA-V Series): VMware ESXi, KVM, Microsoft Hyper-V, Nutanix, Microsoft Azure, Amazon Web Services, and Google Cloud Platform
- Virtual Appliances (ISA-V Series) include:
  - ISA4000-V: Supporting up to 250 users
  - ISA6000-V: Supporting up to 2500 users
  - ISA8000-V: Supporting up to 25,000 users

Ivanti PSA Series

- PSA3000 Appliance: Fixed configuration, 1U rack-mount appliance, supporting up to 200 SSL VPN concurrent users
- PSA5000 Appliance: Fixed configuration 1U rack-mount appliance, supporting up to 2,500 SSL VPN concurrent users
- PSA7000 Appliance: Fixed configuration 2U appliance, supporting up to 25,000 SSL VPN concurrent users
- Virtual Appliances (PSA-V Series): VMware ESXi, KVM, Microsoft Hyper-V, Microsoft Azure, Amazon Web Services, OpenStack Fabric and Alibaba Cloud
- Virtual Appliances (PSA-V Series) include:
  - PSA3000-V: Supporting up to 200 users
  - PSA5000-V: Supporting up to 2500 users
  - PSA7000-V: Supporting up to 10,000 users

Features and Benefits

Feature	Description
Layer 3 SSL VPN	■ Dual-transport (SSL + Encapsulating Security Payload) full Layer 3 VPN connectivity with granular access control. ■ “Always-on VPN with Lockdown Mode” & “VPN Only Access” modes for Compliance (VPN connection automatically connects/disconnects based on user’s location). ■ Machine based VPN with ability to step up to user-based authentication after user log-in
Application VPN	■ Client/server proxy application that tunnels traffic from specific applications to specific destinations ■ “On Demand VPN” and “Per App VPN” for a seamless and secure end user experience
Layer 7 Web single sign-on (SSO) via SAML	■ Allows end users to authenticate to the network through a Layer 3 tunnel, while simultaneously enjoying SSO to Web applications accessed through their browser via SAML SSO support
Conditional Access	■ Validate and verify devices and users via a set of automated policies to protect networks and data. Each access attempt is evaluated dynamically and controlled in real-time based on the policies in effect. Enables granular control and Zero Trust enforcement for application access
Advanced User Portal	■ Secure clientless access from any HTML5 capable browser to published and/or user added applications and links ■ Dynamically generated based on user role ■ RDP/Telnet/VNC/SSH access with Advanced HTML5 ■ Web rewriter and web proxy built in ■ Multi-portal support (e.g., SSO portal for employees, 2FA portal for contractors)
Optimized end-user experience	■ Smooth roaming from remote access to local LAN access (Ivanti Policy Secure) ■ Single Sign On (SSO) for rapid, secure access from remote or on-site locations (via integration with Ivanti Cloud Secure and Ivanti Policy Secure)
Stateful endpoint integrity and assessment	■ Assess and remediate end user devices prior to authentication with easy policy definitions ■ Windows (Desktop & Mobile), MacOS, Apple iOS, and Android

Features and Benefits (continued)

Flexible launch options (standalone client, browser-based launch)	■ Users can easily launch SSL VPN via their Web browser, or directly from their desktop ■ Auto Connect feature allows devices to automatically connect to VPN, either at the time when the machine starts or user logs on ■ VPN on demand feature leverages OS capabilities for auto triggering VPN, seamlessly in the background, when an approved application needs corporate access
Supports Cloud Secure Solution	■ Blend cloud and data center access into a seamless user experience for next generation workers ■ Ability to add compliance rules for hybrid DC access
Pre-configuration options (Windows and Mac only)	■ Administrators can preconfigure a deployment with a list of gateways for end users to choose from
Authentication Options	■ Adaptive Authentication using dynamic, multi-factor authentication using several user attributes. ■ Administrators can deploy Ivanti for remote user authentication using a wide array of authentication mechanisms, including biometric authentication support with Windows Hello for Business, hardware token, smart card, soft token, smart card, soft token, Google Authenticator, one-time passwords and certificate authentication. ■ Administrators can choose to send AAA traffic via a desired interface (internal / external / management), for delegating user authentication to an Identity Provider. ■ OAuth/OpenID Connect support allows integration with any standard OpenID Providers like Google, OKTA, Azure AD, etc. while connecting to Connect Secure (acting as Relying Party)
VMware Horizon and Citrix XenApp/ XenDesktop VPN	■ Ivanti supports the latest versions of VMware and Citrix.
Granular SSL Cipher Configuration	■ Enables the administrator to select specific ciphers over those pre-configured for highly secure compliance.
REST API	■ A comprehensive REST-based API for programmatic access to the appliances.

Rich Access Privilege Management Capabilities

Feature	Description	Benefit
Dynamic role mapping with custom expressions	■ Combines network, device, and session attributes to determine which types of access are allowed. ■ A dynamic combination of attributes on a per- session basis can be used to make the role mapping decision. ■ Through MDM integration, fetch device attributes and apply policy decisions appropriately before granting access	■ Enables the administrator to provision by purpose for each unique session.
SSL VPN federation with NAC (Ivanti Policy Secure)	■ Seamlessly provision SSL VPN user sessions into NAC sessions upon login. ■ Since session data is shared between the Ivanti Appliances for SSL VPN and NAC, users need to authenticate only one time to get access in these types of environments. ■ Policy and access decisions can also be controlled by device attributes discovered by NAC Profiler	■ Provides users, whether remote or local, seamless access with a single login to corporate resources that are protected by access control policies. ■ Simplifies the end user experience.
Support for RSA Authentication Manager	■ RSA Authentications Manager 8.1 enables Risk Based Authentication.	■ Offer another authentication layer option via email account.
Standards based built-in Time- based One-Time Password (TOTP)	■ Enables multi-factor authentication using smartphones	■ Leverage ubiquitous smart phones to roll out a cost-effective and self-serve two-factor authentication mechanism, where one-time passcodes are generated by a mobile app. Implemented based on RFC6238
Multiple sessions per user	■ Allows remote users to launch multiple remote access sessions.	■ Enables remote users to have multiple authenticated sessions open at the same time, such as when accessing VPN from a laptop and from a smartphone simultaneously.
User record synchronization	■ Supports synchronization of user records such as user bookmarks across different Ivanti Appliances.	■ Ensures a consistent experience for users who often travel from one region to another and therefore need to connect to different Ivanti Appliances running Ivanti Connect Secure.
Mobile-friendly SSL VPN login pages	■ Provides predefined HTML pages that are customized for mobile devices, including Apple iPhone and iPad, Google Android, and Nokia Symbian devices.	■ Provides mobile device users with a simplified and enhanced user experience and webpages customized for their device types.
Integration with strong authentication and identity and access management (IAM) platforms	■ Ability to support SecurID, Security Assertion Markup Language ■ (SAML) including standards based SAML v2.0 support, and public key infrastructure (PKI)/digital certificates. ■ OAuth/OpenID Connect Support	■ Leverages existing corporate authentication methods to simplify administration.

Ease of Administration

Feature	Description	Benefit
Mobile Device Management (MDM) integration	■ Enables consolidated reporting and dashboards for simplified management. ■ Leverages MDM attributes for more intelligent and centralized policy creation. ■ Facilitates transparent "no touch" MDM-based deployment of Ivanti Clients to iOS and Android devices.	■ Extend MDM investments to gain comprehensive endpoint visibility and support additional mobile use cases.
Secure Browser	■ A mobile browser for securely accessing corporate web applications, without the need of installing / managing / launching a VPN client.	■ IT does not have to worry about deploying and managing VPN on mobile devices. End user does not have to worry about launching VPN. Seamless end user experience where a user launches browser and accesses his resources, as he would normally expect to.
Bridge Certification Authority (BCA) support	■ Supports federated PKI deployments with client certificate authentication. Bridge CA is a PKI extension (as specified in RFC 5280) to cross-certify client certificates that are issued by different trust anchors (Root CAs). ■ Also, enables customers to configure policy extensions in the admin UI, to be enforced during certificate validation.	■ Enables customers who use advanced PKI deployments to deploy the Ivanti Appliances to perform strict standards-compliant certificate validation—before allowing data and applications to be shared between organizations and users.
Multiple hostname support	■ Ability to host different virtual extranet websites from a single appliance.	■ Saves the cost of incremental servers. ■ Provides a transparent user experience with differentiated entry URLs ■ Eases management overhead.
Intuitive Dashboard Design	■ View and control enterprise access to the data center and cloud from one console.	■ Quick access to dynamic information and reports. ■ Customizable layouts via drag and drop functionality.
Customizable user interface	■ Creation of completely customized sign-on pages.	■ Provides an individualized look for specified roles, streamlining the user experience.
Application Launcher (AL)	■ Enhanced support for non-JAVA based browsers.	■ Support for latest generation browsers (Apple, Microsoft, Google, Firefox, etc) that do not support Java and Active X.
Neurons for Secure Access	■ Optional centralized management, analytics and reporting platform for Ivanti Connect Secure Deployments ■ Full Configuration management, one-click upgrades, centralized logging, custom reporting and troubleshooting ■ "Lift and shift" configurations through configuration templates and multi-node configuration management	■ Centralized configuration and gateway lifestyle management saves time and money ■ Enhanced behavioral analytics identify and automatically act on risky user behavior before it becomes a problem ■ Simplify management of multi-node or global deployments

Flexible Single Sign-On (SSO) Capabilities

Feature	Description	Benefit
SAML single sign- on for cloud and Web applications access	■ SAML 2.0-based SSO to a variety of Web applications, including many of today's most popular Software as a Service (SaaS) applications such as Salesforce.com and Google Apps. ■ Includes SSO functionality, even when connecting via a Ivanti Connect Secure Layer 3 VPN tunnel, which is unique in the industry. ■ Ivanti Connect Secure supports deployments as both an SAML Identity Provider (IdP) and as a SAML Service Provider (SP).	■ Single sign-on to a user's Web and cloud-based applications, simplifying the user's connectivity experience.
Kerberos Constrained Delegation	■ Support for Kerberos Constrained Delegation protocol. ■ When a user logs into Ivanti Connect Secure with a credential that cannot be proxied through to the backend server, the gateway will retrieve a Kerberos ticket on behalf of the user from the Active Directory infrastructure. ■ The ticket will be cached on Ivanti Connect Secure throughout the session. ■ When the user accesses Kerberos-protected applications, the Appliance will use the cached Kerberos credentials to log the user into the application without prompting for a password.	■ Eliminates the need for companies to manage static passwords resulting in reduced administration time and costs.
Kerberos SSO and NT LAN Manager (NTLMv2) support	■ Ivanti Connect Secure will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	■ Simplifies the user experience by eliminating users entering credentials multiple times to access different applications.
Password management integration	■ Standards-based interface for extensive integration with password policies in directory stores (LDAP, AD, and others).	■ Leverages existing servers to authenticate users. ■ Users can manage their passwords directly through the Ivanti Connect Secure interface.
Web-based SSO basic authentication and NTLM	■ Allows users to access other applications or resources that are protected by another access management system without reentering login credentials.	■ Alleviates the need for users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.
Web-based SSO forms-based, header variable- based, SAML- based	■ Ability to pass user name, credentials, and other customer defined attributes to the authentication forms of other products and as header variables.	■ Enhances user productivity and provides a customized experience.
OAuth/OpenID Connect	■ OAuth/OpenID Connect support allows integration with any standard OpenID Providers like Google, OKTA, Azure AD, etc. while connecting to Connect Secure (acting as Relying Party)	■ Integrate into existing OAuth deployments for easy user ID federation

Provision by Purpose

Feature	Description	Benefit
Ivanti Secure Access Client	■ Single, integrated, remote access client that can also provide LAN access control, and dynamic VPN features to remote users.	■ Ivanti Secure Access Client replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN and LAN access control. The end user simply "clicks and connects" the connection they need.
Clientless core Web access	■ Secure access to many different types of web- based applications, including many of today's most common Web applications such as Outlook Web Access, SharePoint, and many others. ■ Remote Desktop Protocol (RDP) access in Ivanti Connect Secure can be delivered over HTML5, via third-party RDP, through a WebSockets translator such as Ericom.	■ Provides the most easily accessible form of application and resource access from a variety of end user devices with extremely granular security control options. ■ Completely clientless approach using only a web browser.
IPsec/IKEv2 support for mobile devices	■ Allows remote users to connect from any mobile device that supports Internet Key Exchange (IKEv2) VPN connectivity. ■ Administrator can enable strict certificate or username/password authentication for access via IPsec/IKEv2.	■ Full L3 VPN support for new devices that support IKEv2 but for which a client is not yet available.
Virtual Desktop Infrastructure (VDI) support	■ Allows interoperability with VMware View Manager to enable administrators to deploy virtual desktops with Ivanti Connect Secure.	■ Provides remote users seamless access to their virtual desktops hosted on VMware servers ■ Provides dynamic delivery of the VMware View client, including dynamic client fallback options, to allow users to connect to their virtual desktops.
Zero Touch Provisioning	■ Deploy PCS using OpenStack centralized orchestration. ■ Obtain initial configuration from local DHCP server without manual data entry. ■ Configure and manage via REST API.	■ Enables customers to allow a large number of users (including employees, contractors, and partners) to access corporate resources through mobile phones via ActiveSync.
ActiveSync Proxy	■ Provides secure access connectivity (strong encryption + certificate authentication) from mobile devices (such as iOS or Android devices) to the Exchange Server via proxy, with no client software installation. Enables up to 5,000 simultaneous sessions.	■ Enhances user productivity and provides a customized experience.
Secure Application Manager (SAM)	■ A lightweight application download enabling access to client/server applications.	■ Enables access to client/server applications using just a Web browser. Also provides native access to terminal server applications without the need for a preinstalled client.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti

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