

# Ivanti Policy Secure (IPS)

## Highlights

- Centralized visibility and policy management of all endpoints, including IoT.
- Granular assessment of endpoint security posture before allowing access.
- Dynamic network segmentation based on user role and/or device class.
- Seamless roaming between remote and local, using Connect Secure Integration.
- Granular integration with vADC for a scalable, resilient and responsive solution.
- BYOD onboarding integration with Ivanti Neurons for Workspace or 3rd party EMM.
- REST API integration with security ecosystem.
- Scales for organizations of any size.

## Total visibility and total security

Modern networks experience a proliferation of connected endpoints; BYOD connectivity is now surpassed by IoT. Every additional endpoint increases the risk to be compromised and give attackers an opportunity to gain further access into the network and to corporate resources. To limit this risk, an endpoint's security posture must always show current software security updates, virus definitions, and so on. Also, users must only be given the least amount of access necessary to perform their role.

Ivanti Policy Secure provides complete visibility and Network Access Control (NAC) for all local or remote endpoints. Its open, high-performance design helps small and large organizations easily enforce endpoint security compliance and zero trust security. The intuitive UI makes for easy administration and customizable reporting.

Policy Secure continuously enforces foundational security policies and controls network access for

managed and unmanaged endpoints, including IoT. Policy Secure uses zero trust principles to manage network access by validating the user and a device's security posture, and then connects the device with least privilege access policy.

The open platform integrates with a wide range of switching, Wi-Fi and NGFW solutions to enforce access policies. Bidirectional integration with third-party security solutions improves overall security efficacy with automated endpoint access enforcement.

Automated responses to Indicators of Compromise (IoC) reduces remediation time and streamlines administrative resources. PPS integrates with a wide range of NGFWs such as Palo Alto Networks, Checkpoint, Juniper and Fortinet, as well as SIEM solutions like IBM Qradar and Splunk. Integration with McAfee ePolicy Orchestrator (McAfee ePO) fortifies endpoint management and automated threat response. For granular OT/IoT visibility and control, PPS integrates with Nozomi Guardian.

## Benefits

- End-to-end zero trust network access security.
- Reduced threat response time.
- Reduced risk from lateral spread of threats.
- Automated policy enforcement, reduced auditing burden.
- Simple and fast deployment.

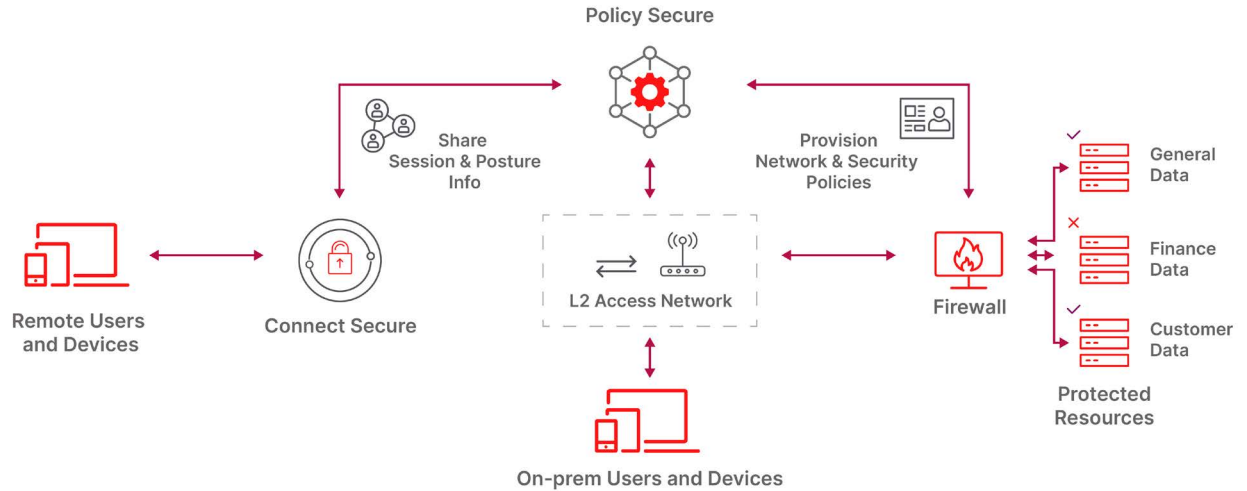


Figure 1: Access decisions for endpoints

## Key components

The Policy Secure solution includes three components:

- **Profiler** identifies and classifies endpoint devices, including IoT. It provides end-to-end visibility, reporting and behavior analytics.
- **Policy Secure** provides a high-performance policy engine that leverages contextual information from users, endpoints and applications. With a unified, open framework and policy engine, administrators can apply granular rules for dynamic monitoring, reporting and access control of all endpoints, anywhere on the network, to minimize access risks.
- **Client** offers agent and agentless options for pre- and post-admission control. The solution incorporates the host checker functionality, which verifies an endpoint's security posture. This is the same Client used for our Connect Secure VPN solution and runs on Windows, Mac, Linux, Android and IOS platforms.

## Use case overview

Policy Secure helps to adapt zero trust network access security for small and large organizations in the Everywhere Workplace. Enterprises use Policy Secure to enforce endpoint policy compliance for employees, guests and contractors regardless of location, device type or device ownership. Users enjoy greater productivity and the freedom to work anywhere without limiting access to authorized network resources and applications. BYOD onboarding optimizes the user experience by allowing workers to use their preferred device. Policy Secure provides complete visibility of managed and unmanaged network devices.

## Visibility

To protect your network endpoints, you need to see what endpoints are connected. Complete visibility means having the insights to identify and classify all managed and unmanaged endpoints.

CHALLENGES	POLICY SECURE SOLUTION
Profiling	Profiler dynamically identifies and enables automatic and custom classification of both managed and unmanaged endpoint devices. This provides operational visibility, reporting and policy-based controlled access to networks and resources based on the user, device, applications and other attributes.
Behavioral analytics	Profiler continuously performs behavioral analytics and builds baseline behavior profiles for IoT devices by collecting and correlating NetFlow, user, and device data. This is used to detect anomalous device activity, anomalous user access, domain generation attacks and MAC spoofing.
Numerous device types	Profiler can automatically classify devices against a growing database of more than 2.3M unique fingerprints. The solution profiles endpoints' static or dynamic IP addresses and actively scans open ports to detect MAC spoofing.

## The Internet of Things (IoT)

Enterprises today merge IoT devices with the IT environment to improve business. Policy Secure offers enterprises the ability to discover and secure these devices.

CHALLENGES	POLICY SECURE SOLUTION
Discovery, profiling and segmentation of IoT devices	Profiler discovers managed and unmanaged IoT devices. It profiles them so they can be matched to specific access policies. Dynamic segmentation limits the risk of threats spreading laterally and helps with regulatory compliance.

## Device onboarding and policy compliance

Policy Secure prevents unauthorized network, application or data access by dynamically assessing and remediating device security before the device connects to the enterprise for both VPN and Wi-Fi access. This protects the corporate network from infected devices and enforces consistent, cross-network access policies. It also ensures only authorized workers have access to enterprise resources based on their role, location and time of day.

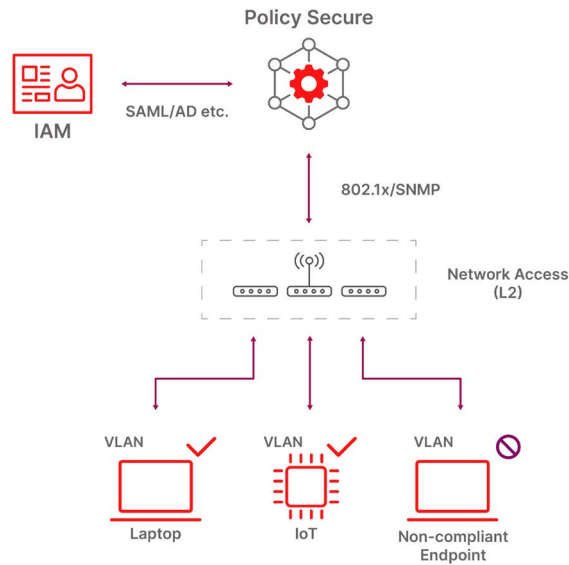


Figure 2: Dynamic access control and network segmentation (L2)

## Ivanti Policy Secure (IPS) Security Standards and Certifications

Ivanti Policy Secure (IPS) adheres to National Institute of Standards and Technology (NIST) [Federal Information Processing Standards \(FIPS\)](#) and [National Information Assurance Partnership \(NIAP\)](#) standards to ensure the security and interoperability of systems and products, and to protect the confidentiality, integrity and availability of data.

Ivanti Policy Secure (IPS)	NIST / FIPS: <a href="#">Certified by using openssl.org FIPS provider/module in IPS 22.7R1 release or later.</a>
	NIAP: <a href="#">Certified as Compliant Product</a> , IPS 22.2 or later.

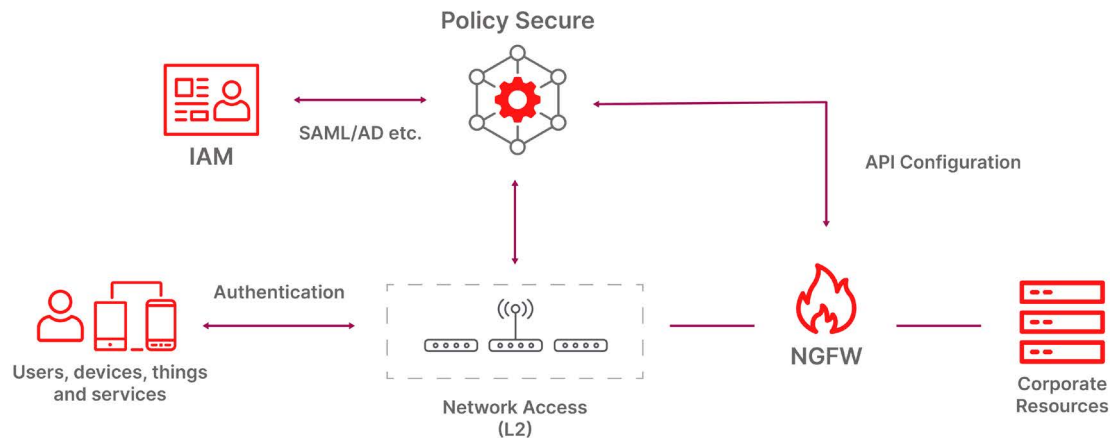


Figure 3: Dynamic access control at perimeter (L3)

CHALLENGES	POLICY SECURE SOLUTION
Guest user support	Policy Secure provides a self-service portal with a customizable interface. It is a highly scalable enterprise guest access platform that supports thousands of guest users. For additional control, secure guest access can be enabled by an admin (e.g. a receptionist), or by a sponsor who approves the guest's access request. Policy Secure integrates with wireless controllers like Aruba, Cisco, Huawei, Juniper Mist, Meraki and Ruckus.
BYOD onboarding	Policy Secure empowers employees to use their personal devices for work with self-service onboarding of personal laptops and mobile devices.


KEY FEATURES	
Profiler	Identifies and classifies endpoint devices, including IoT. It provides end-to-end visibility, reporting and behavior analytics.
RADIUS/802.1X support	An integrated, high-performance RADIUS authenticates users and devices that are forwarded from industry-standard 802.1X functions on network switches and wireless controllers.
TACACS+ support	Use the TACACS+ authentication system to distribute policies to the access infrastructure. Supports two-factor authentication with smart cards.
Host checker	Identifies the security posture of the device. Options include OS or software patch status and active apps.
Session federation	Active VPN sessions seamlessly migrate to the local network without the need to re-authenticate.
UEBA Analytics	Correlation of user access, device data and system logs in a new analytics engine integrates with the Ivanti One management solution.
Identity-based admission control	Shares identity context with NGFWs from vendors such as Fortinet, Palo Alto Networks, Checkpoint and Juniper SRX, enabling each to be employed as policy enforcement points on the network perimeter.
Automated threat response	Leverages external threat intelligence alerts from NGFW or SIEM solutions to take automated actions at the device connection level. Policy engine leverages rich contextual information to allow various mitigating actions based on threat severity.
Captive portal	Provides user-friendly access control for guests and contractors.

## KEY FEATURES

Self-service guest access support	Provides secure, simple and differentiated guest access.
Wizard-based configuration	Simplifies configuration tasks for administrators to avoid mistakes and faster deployment.
Granular auditing and logging	Granular logging capabilities of system, user and device events in a clear, easy-to-understand format. Can be analyzed locally or shared with external syslog solutions or SIEMs such as IBM Qradar and Splunk. Supports WELF format and WELF-SRC-2.0-Access Report.
Centralized policy management	Saves administrative time and cost and delivers a superior user experience with common remote and local access control policy implementation and enforcement across a distributed enterprise.
REST API	Standardized interface for third-party systems such as NGFWs and SIEMs to integrate with Policy Secure and limit an endpoint's access on the local network.
Flexible deployment options	Policy Secure runs on physical, virtual and cloud platforms. See the Supported Platforms Guide for details.

## About Ivanti

Ivanti breaks down barriers between IT and security so that Everywhere Work can thrive. Ivanti has created the first purpose-built technology platform for CIOs and CISOs – giving IT and security teams comprehensive software solutions that scale with their organizations' needs to enable, secure and elevate employees' experiences. The Ivanti platform is powered by Ivanti Neurons - a cloud-scale, intelligent hyperautomation layer that enables proactive healing, user-friendly security across the organization, and provides an employee experience that delights users. Over 40,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com) and follow @Golvanti.

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the left side of the text block, featuring a red-to-orange gradient.

For more information,  
or to contact Ivanti,  
please visit [ivanti.com](https://www.ivanti.com)