Ivanti Policy Secure (NAC)

功能特色

- 集中化的可视性和策略管理，覆盖所有端点，包括物联网。
- 细化评估端点安全态势，然后允许访问。
- 基于用户角色和/或设备类别的动态网络分段。
- 使用Connect Secure Integration，在远程和本地之间无缝漫游。
- 与vADC细化整合，打造可扩展、有弹性、响应迅速的解决方案。
- 自带设备入网可整合Ivanti Neurons 神经元工作空间或第三方EMM。
- 与安全生态系统REST API集成。
- 适用于任何规模的企业组织。

全面的可见性和安全性

在现代网络中，联网端点如雨后春笋般增加，而自带设备的联网规模正在被物联网所超越。每增加一个端点，泄漏的风险也增加了一分，攻击者也获得更多机会深入网络和企业资源。为了抵御这种风险，一个端点的安全态势必须始终显示当前的软件安全更新、病毒定义等。此外，用户必须只被授予履行职责所需的最低限度的访问权限。

Ivanti Policy Secure为所有本地和远程端点提供全面可视性和网络访问控制（NAC）。它的高性能开放式设计有助于大小企业轻松执行端点安全合规策略和零信任安全。直观的用户界面带来轻松管理和可定制报告。

Policy Secure针对所有受管理和不受管理的端点持续执行基础安全策略，同时控制网络访问，包括物联网端点。Policy Secure采用零信任原则，通过验证用户和设备的安全状况来管理网络访问，然后根据最低权限访问策略连接设备。

开放式的平台可与各种交换、Wi-Fi和NGFW解决方案集成，以执行访问策略。自动化的端点访问执行以及与第三方安全解决方案双向集成，提高整体安全效能。

通过对失陷指标（IoC）作出自动响应，减少了修复时间，并精简了管理资源。PPS还可与多种NGFW（如Palo Alto Networks、Checkpoint、Juniper和Fortinet）以及SIEM集成。

优势

- 端到端的零信任网络访问安全。
- 缩短威胁响应时间。
- 降低威胁横向传播的风险。
- 自动策略执行，减轻审计负担。
- 简单而快速的部署。

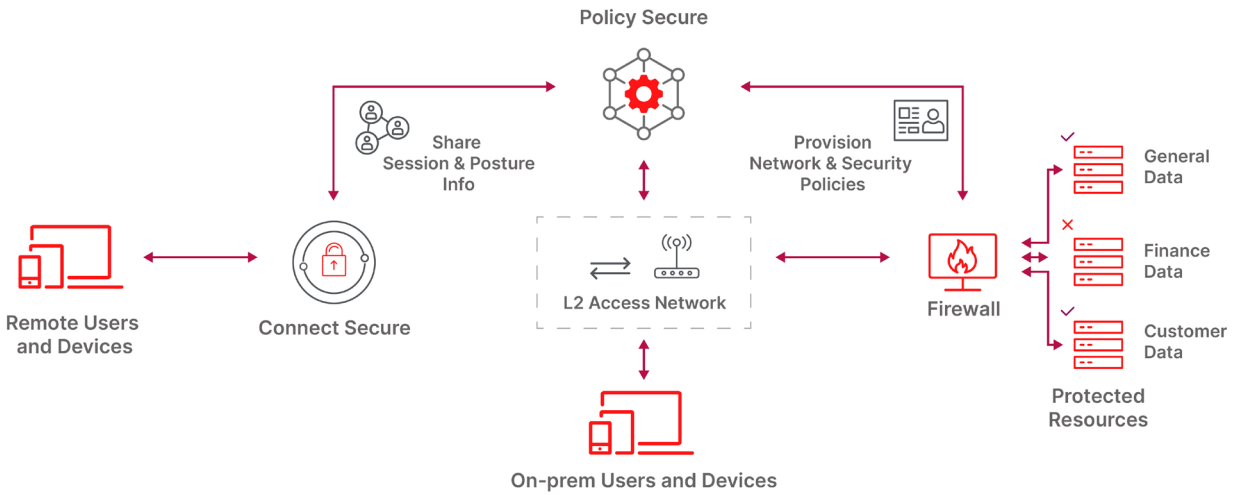

图1: 为端点作出访问决定

主要构成

Policy Secure 解决方案由三大部分构成：

- **Profiler** 对端点设备进行识别和分类，包括物联网。它提供端到端的可视性、报告和行为分析数据。
- **Policy Secure** 提供的高性能策略引擎可充分运用来自用户、端点和应用程序的上下文信息。有了统一、开放的框架和策略引擎，管理员可以应用细化规则，对网络上任何位置的所有端点进行动态监控、报告和访问控制，最大限度地减少访问风险。
- **支持客户端或无客户端模式** 提供代理和无代理选项，用于准入前和准入后控制。这款解决方案融合了主机安全检查功能，可验证端点的安全态势。该客户端同样用于我们的Connect Secure VPN解决方案，可在Windows、Mac、Linux、Android和IOS平台上运行。

用例一览

Policy Secure 协助处于“无处不在的工作空间”的大小企业采纳零信任网络接入安全。企业可使用Policy Secure确保员工、访客和承包商的政策合规性，无论他们在任何地点、使用任何类型的设备，或这些设备由谁所有。用户将享有更高的工作效率和在任何地方工作的自由，无需对他们限制授权网络资源和应用程序的访问权限。自带设备入网允许员工使用最得心应手的设备，从而改善用户体验。Policy Secure针对受管理和不受管理的设备提供全面可视性。

可视性

只有能够看到哪些端点连入了网络，您才能保护您的网络端点。全面可视性意味着拥有充分的洞察力，可识别和分类所有受管理和不受管理的端点。

问题	POLICY SECURE 解决方案
可视性	Profiler能够针对受管理和不受管理的端点设备进行动态识别，并实现自动、自定义分类，从而根据用户、设备、应用程序和其他属性提供运营可视性、报告和基于策略的网络和资源受控访问。
行为分析	Profiler收集和关联NetFlow、用户和设备数据，持续进行行为分析，为物联网设备建立基线行为档案。该功能用于检测异常的设备活动、异常的用户访问、域名生成攻击和MAC欺骗。
众多的设备类型	Profiler根据拥有超过230万个唯一指纹、且在不断扩展的数据库，对设备进行自动分类。这款解决方案对端点的静态或动态IP地址进行分析，并主动扫描开放的端口，以侦测MAC欺骗行为。

物联网（IoT）

今天的企业通过合并物联网设备与IT环境来优化业务。Policy Secure 为企业赋予发现和保护这些设备的能力。

问题	POLICY SECURE 解决方案
发现、剖析和细分物联网设备	Profiler能发现受管理和不受管理的物联网设备，对它们进行剖析，把它们与指定访问策略相匹配。动态分段减小了威胁横向传播的风险，并有助于确保监管合规。

设备入网和策略合规

Policy Secure在设备连接到企业的VPN和Wi-Fi访问之前动态评估和修正设备安全，防止未经授权的网络、应用程序或数据访问。这可以保护企业网络不受感染设备访问，同时执行一致的跨网络访问策略，并确保只有经授权的员工才能在符合其角色、地理位置和时间的情况下访问企业资源。

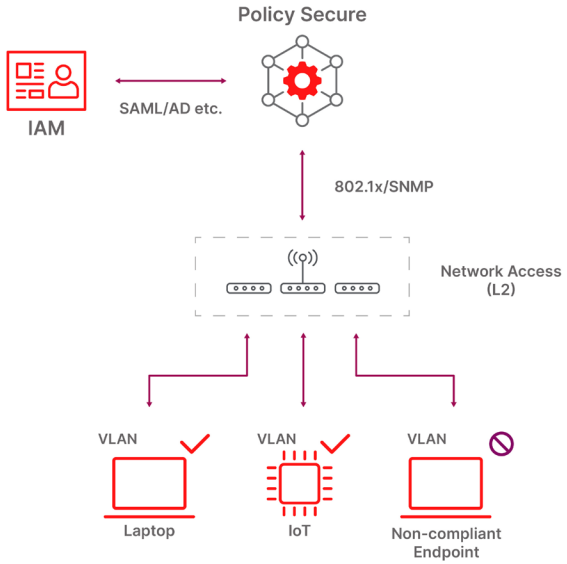

图 2：动态访问控制和网络分段 (L2)

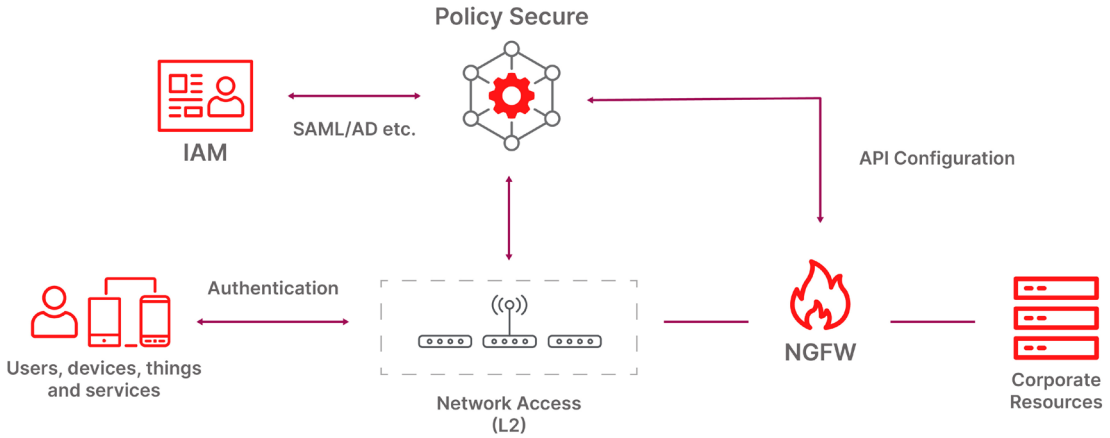

图3：周界上的动态访问控制 (L3)

问题	POLICY SECURE 解决方案
访客用户支持	Policy Secure提供了一个拥有可定制界面的自助服务门户。它是一个高度可扩展的企业访客访问平台，支持成千上万的访客用户。为了加强控制，安全访客访问可以由管理员（如前台）或担保人在批准访客请求后启用。Policy Secure可与Aruba、Cisco、思科、Juniper Mist、Meraki和Ruckus等无线控制器集成。
自带设备入网	Policy Secure允许员工为个人笔记本电脑和移动设备办理自助入网，从而能够使用个人设备工作。

主要功能	
Profiler	对端点设备进行识别和分类，包括物联网设备。它提供端到端的可视性、报告和行为分析数据。
RADIUS/802.1X支持	A集成的高性能远程认证拨号用户服务（RADIUS）可验证从网络交换机和无线控制器通过行业标准802.1X功能转发的用户和设备。
TTACACS+ 支持	使用TACACS+验证系统把策略分配到访问架构。支持使用智能卡的双因素验证。
主机检查器	识别设备的安全态势。提供OS或软件补丁状态和活跃应用程序等选择。
会话联盟	A活跃的VPN会话无缝迁移到本地网络，无需重新验证。
UEBA分析数据	全新的分析引擎显示用户访问、设备数据和系统日志相关性，可整合于Ivanti One管理解决方案。
基于身份的准入控制	与Fortinet、Palo Alto Networks、Checkpoint和Juniper SRX等供应商的NGFW共享身份背景，使每个NGFW都能成为网络周界上的策略执行点。
自动威胁响应	L从NGFW或SIEM解决方案获取外部威胁信息警报，在设备连接层面自动采取行动。策略引擎利用丰富的上下文信息，可根据威胁的严重程度采取各种缓解行动。
强制门户	提供用户友好的访客和承包商访问控制。

主要功能	
自助访客访问支持	提供安全、简单和区别化的访客访问。
基于向导的配置	简化管理员的配置任务，避免错误，加快部署。
细化的审计和日志	以清晰易懂的格式对系统、用户和设备事件进行细化记录。可以在本地分析或与外部系统日志解决方案或SIEM（如IBM Qradar和Splunk）共享。支持WELF格式和WELF-SRC- 2.0-访问报告。
集中化的策略管理	节省管理时间和成本，在分布式企业中实施和执行共同的远程和本地访问控制策略，提供卓越的用户体验。
REST API	为NGFW和SIEM等第三方系统提供标准化接口，便于与Policy Secure整合，限制终端在本地网络的访问。
灵活的部署选项	Policy Secure可在物理、虚拟和云平台上运行。详情见《支持平台指南》。

关于Ivanti

Ivanti让无处不在的工作空间成为可能。在“无 处不在的工作空间”，员工可能会在任何地方 工作，并使用多种设备来访问IT网络、应用 程序和数据，以保证工作效率。Ivanti自动化 平台集成了业内领先的统一端点管理、零信 任安全和企业服务管理解决方案，通过一站 式平台实现为企业实现自我修复和自我安全，并为终端用户提供自我服务。已经有4万多位 客户，包括78家《财富》百强企业，选择了 Ivanti为他们检测、管理、保护和维护从云端 到边缘的IT资产，同时为员工提供卓越的终 端用户体验，无论他们在哪里、使用何种方 式工作。更多信息请访问ivanti.com.cn

ivanti.com.cn
+86 (0)10 85412999
ContactChina@ivanti.com