JUNIPER NETWORKS | Driven by Experience™

人工智能驱动型园区

将人工智能融入未来十年的园区网络

白皮书

目录

执行摘要

未来十年的网络核心在于提供更好的用户体验和简化 IT 运维。传统的有线和无线 LAN 解决方案缺乏必要的可扩展性、可靠性、安全性、性能和敏捷性，无法应对当今的挑战和多样化的企业需求。

在云、移动和 IoT 时代，人工智能驱动型园区可以充分利用人工智能 (AI) 的力量。瞻博网络的园区解决方案将强大的硬件产品组合与 Mist AI™ 的强大功能相结合，可以简化网络运维、改善用户体验，并使 IT 团队能够专注于战略计划。本白皮书将介绍端到端人工智能驱动型园区网络的各个组成部分，所有功能皆由 Mist AI 提供强力支持。

简介

企业网络正在经历大规模转型，以期适应日益增长的云就绪网络需求，以及大量移动设备和 IoT 设备带来的需求。不幸的是，随着设备数量的增加，复杂性也在增加。基于云的应用支持新的业务模式，提供更高的业务敏捷性，并支持统一通讯、视频和其他延迟敏感型应用等核心技术的采用。此外，机器学习 (ML) 和人工智能的技术进步和广泛采用可以极大地改善 IT 团队和最终用户的运维和体验。

网络架构师正在重新设计他们的网络，以使用开放标准和软件驱动型管理平台来满足云就绪应用对数据、语音和视频的现代业务要求，进而降低运维成本。最终目标是利用更简单的自动化、遥测和人工智能功能来构建未来十年的网络。

瞻博网络人工智能驱动型园区网络

瞻博网络的云服务、软件、硬件产品组合提供端到端园区网络解决方案，可在 WAN、LAN、Wi-Fi 和安全性网域之间轻松扩展，同时还支持以太网 VPN 和虚拟可扩展 LAN (EVPN-VXLAN) 等开放标准，以提升架构的简单性、规模和性能。

瞻博网络人工智能驱动型园区解决方案由以下组件组成：

- 现代微服务云 AIOps 平台
- 人工智能驱动型 Wi-Fi 和有线交换
- 运行 EVPN-VXLAN 的园区交换矩阵
- 云就绪型园区以太网交换机
- 具有 Wi-Fi、蓝牙 LE 和 IoT 功能的企业级接入点
- Juniper Connected Security 和网络分段
- Junos® 操作系统
- Junos 遥测

现代微服务云 AIOps 平台

瞻博网络® Mist 云架构围绕微服务构建而成，具有无与伦比的敏捷性、可扩展性和弹性配置。云服务可根据需求弹性扩大或缩减规模，从而消除单体硬件的成本和复杂性。这款平台几乎每周都会提供新的增强功能和错误修复，而且不会造成网络中断。平台采用 100% 可编程的开放式 API，可实现全面自动化，并与配套的第三方产品无缝集成。瞻博网络 Mist 云架构提供新的创新方法，将人工智能、机器学习和数据科学与最新的微服务技术相结合，为企业网络提供与众不同的解决方案。

人工智能驱动型 Wi-Fi 和有线交换

瞻博网络将 Mist AI 应用于园区网络，通过统一的有线和无线解决方案优化用户体验，并简化 IT 运维。传统的解决方案已有超过 15 年的历史，但这类解决方案使用单一代码库，扩展成本高昂，容易出错，而且难以管理。正常运行时间已成为新的用户体验，这是衡量网络基础架构成功与否的一项最重要指标。瞻博网络是如何提供这种体验的？

瞻博网络 Mist Wi-Fi Assurance 以自动化无线运维取代手动故障排除任务，使 Wi-Fi 具有可预测性、可靠性和可衡量性，以及对用户服务级别的可见性。异常检测可通过自动触发机制捕获事件关联数据包，并能在客户端级别实施无线资源管理 (RRM) 来构建网络智能，针对用户的无线网络体验实现前所未有的可见性。

瞻博网络 Mist Wired Assurance（参见图 1）将人工智能驱动型自动化融入有线设备。这款产品利用来自 Juniper Networks® EX 系列以太网交换机的各种 Junos 遥测数据，可简化运维、缩短平均修复时间 (MTTR)，并提高对 IoT 设备、服务器、打印机等终端设备体验的可见性。瞻博网络 Mist Wired Assurance 简化了 EX 系列交换机的各个方面——从瞻博网络 Mist 云架构中的部署、配置到管理。

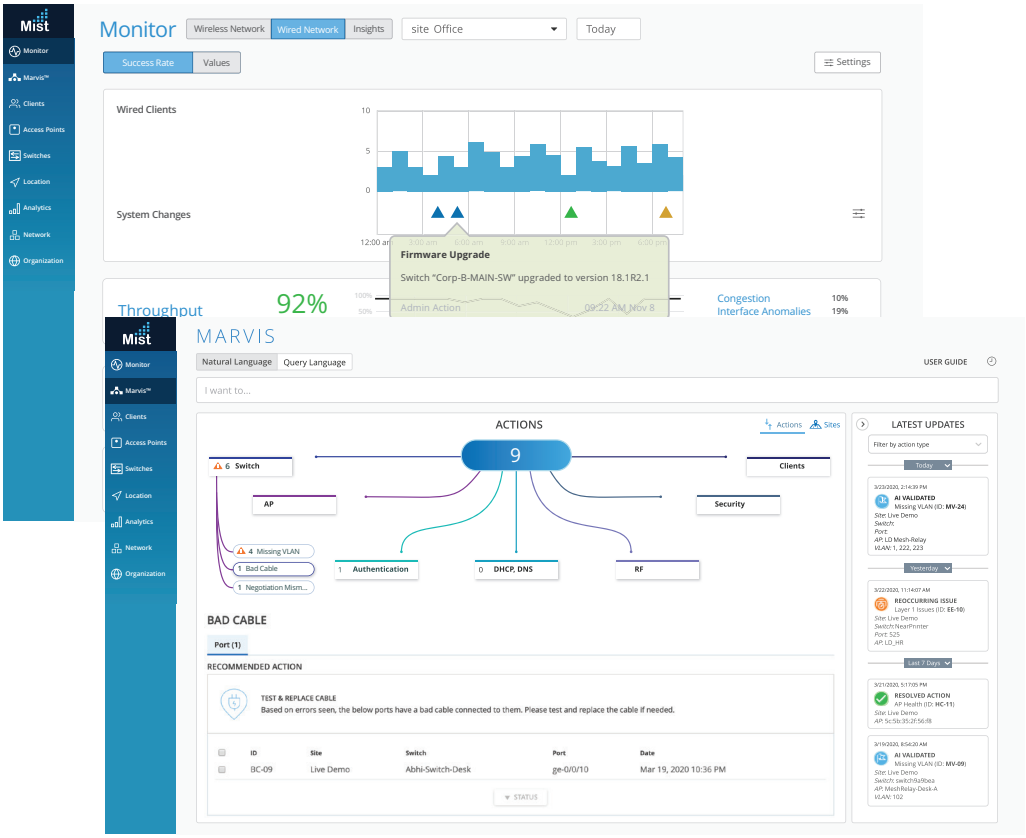

图 1：Wired Assurance 和 Marvis 虚拟网络助手

Marvis 虚拟网络助手（图 1）专门采用 Mist AI 打造而成，非常适合企业 WLAN、LAN 和 WAN 网络。这款产品采用自然语言，用户可以直接与 Mist AI 引擎进行交互，通过自我驱动型操作将网络运维从被动的故障排除转变为主动修复。Marvis 可以提高 IT 效率，最大限度减少支持工单数量，并缩短解决问题的时间。随着适用于 IT 运维的人工智能 (AIOps) 不断普及，Marvis 正在帮助各大组织高效、准确地大规模管理 IT 运维。

园区网络交换矩阵

园区内使用的 IoT 设备不断增加，决定了网络需要在不增加复杂性的情况下快速扩展。由于其中许多设备的网络功能有限，因此需要跨建筑物或园区的 L2 邻接。然而，L2 网络会导致环路、发生故障时融合速度变慢，以及数据平面泛洪造成的安全性问题。传统上，安全性问题会通过专用的私有 VLAN 来加以解决，但诸如环路和融合速度等其他问题仍然存在于 L2 网络中。而且，这种方法效率不彰且难以管理——效率不彰是因为过度消耗网络带宽，难以管理则是因为 VLAN 需要扩展到新的网络端口。

EVPN-VXLAN

人工智能驱动型园区架构采用开放标准的以太网 VPN (EVPN) 和虚拟可扩展 LAN (VXLAN) 等技术，将叠加网络与底层网络分离开来。这样便能提供融合速度更快的无环路网络，并允许网络管理员在不同的 L3 网络之间创建 L2 逻辑网络，进而满足现代企业网络的需求。EVPN-VXLAN 还能通过分离 IoT 设备之间的流量来实现微分段，从而提供额外的安全性。瞻博网络支持以下经过验证的 EVPN-VXLAN 园区交换矩阵：

- **EVPN 多宿主（在折叠式核心层或分布层上）**：网络分布层上的 EVPN 多宿主允许接入交换机跨分布层中的一对设备进行 LAG。通过提供从接入层到分布层的多宿主功能，消除了对跨园区网络生成树协议 (STP) 的需求。这也使得分布层和核心层可以折叠起来。
- **园区交换矩阵核心分布**：一对互连的 EX 系列核心或分布交换机可提供 L2 EVPN 和 L3 VXLAN 网关支持。分布层和核心层之间的 IP Clos 网络提供两种模式：集中或边缘路由桥接叠加。
- **园区交换矩阵 IP Clos**：园区交换矩阵 IP Clos 架构将 VXLAN L2 网关功能推送到接入层，能够支持使用基于标准、基于组的策略进行微分段。

端到端 EVPN-VXLAN 架构可让您将园区和数据中心作为单个 IP 交换矩阵进行管理，只需借助瞻博网络提供的 Over-The-Top (OTT) 策略和控制，即可完成这一操作。该架构还使用基于组的策略简化了整个网络的策略实施。在 Clos 网络或 IP 交换矩阵中，可以连接任意数量的交换机。其中，EVPN-VLAN 可以扩展交换矩阵并连接多栋企业大楼，VXLAN 则可在整个网络中扩展 L2。

有关更多信息，请访问：www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510643-en.pdf。

除了基于 EVPN-VXLAN 的架构外，瞻博网络还支持虚拟机箱技术，允许多达 10 台互连的交换机以具有单一 IP 地址的单个逻辑设备进行运作。借助虚拟机箱技术，企业可以将物理拓扑与端点的逻辑分组分离开来，从而提高资源利用效率。

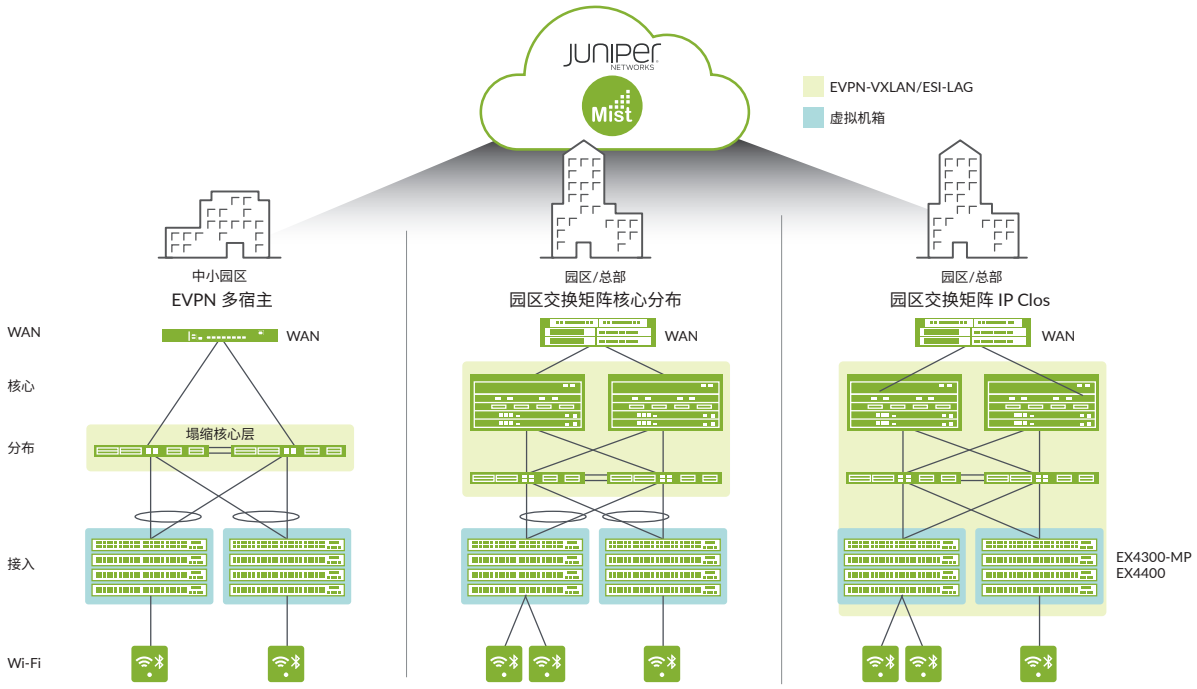

图 2：园区交换矩阵虚拟机箱和基于 EVPN-VXLAN 的架构展示图。

云就绪型园区以太网交换机

瞻博网络为企业园区网络提供人工智能驱动的可编程、开放式接入和核心/分布式交换机产品组合。云就绪型接入交换机支持瞻博网络 Mist Wired Assurance，可将 AIOps 引入接入层交换。这些交换机可以满足园区的诸多需求，例如：

- 由瞻博网络 Mist 云架构管理的云就绪功能
- 多千兆支持
- 媒体访问控制安全性 (MACsec) AES256
- 以太网供电 (PoE/PoE+/PoE++)
- 通过虚拟机箱和 EVPN-VXLAN 实现可扩展的交换矩阵架构
- 多供应商支持
- 使用基于组的策略 (GBP) 进行基于标准的微分段
- 基于流的遥测

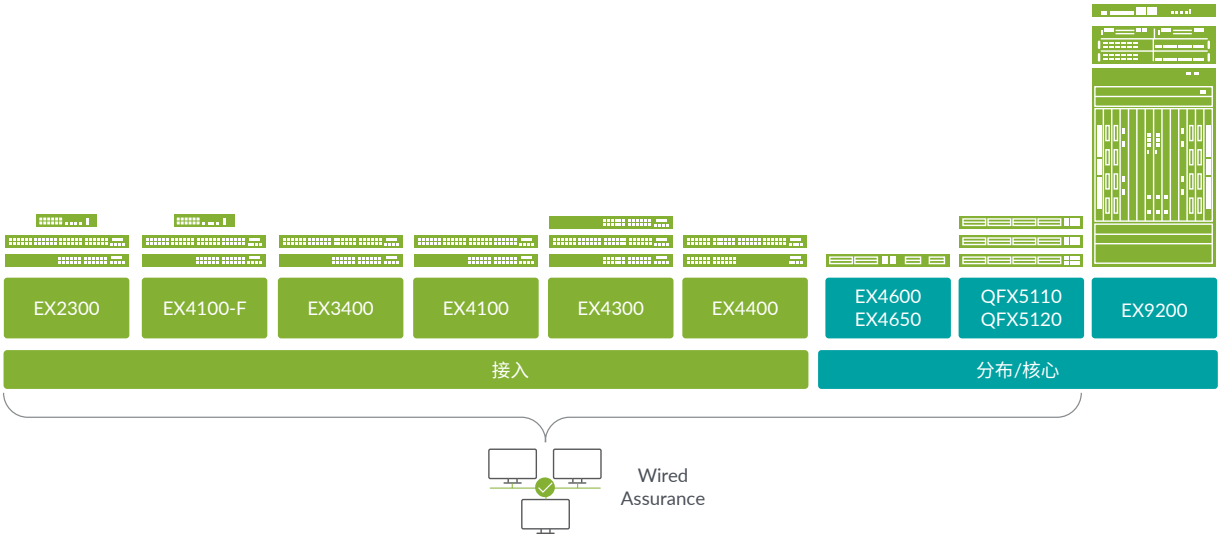

图 3：EX 系列和 QFX 系列园区交换机产品组合。

部署人工智能驱动型园区交换矩阵

手动配置园区交换矩阵会导致部署时出现不一致和非受迫性错误。瞻博网络通过将 EVPN-VXLAN 园区交换矩阵交由瞻博网络 Mist 云来管理，轻松解决了这一运维负担。具体来说，管理员可以选择一种拓扑结构（EVPN 多宿主、分布-核心或 IP CLOS），然后让软件完成其余的工作（参见图 4）。这种人工智能驱动的方法统一了对园区和分支机构的 LAN、WLAN 和 WAN 环境的管理，同时确保有线和无线园区网络能够提供良好的用户体验。

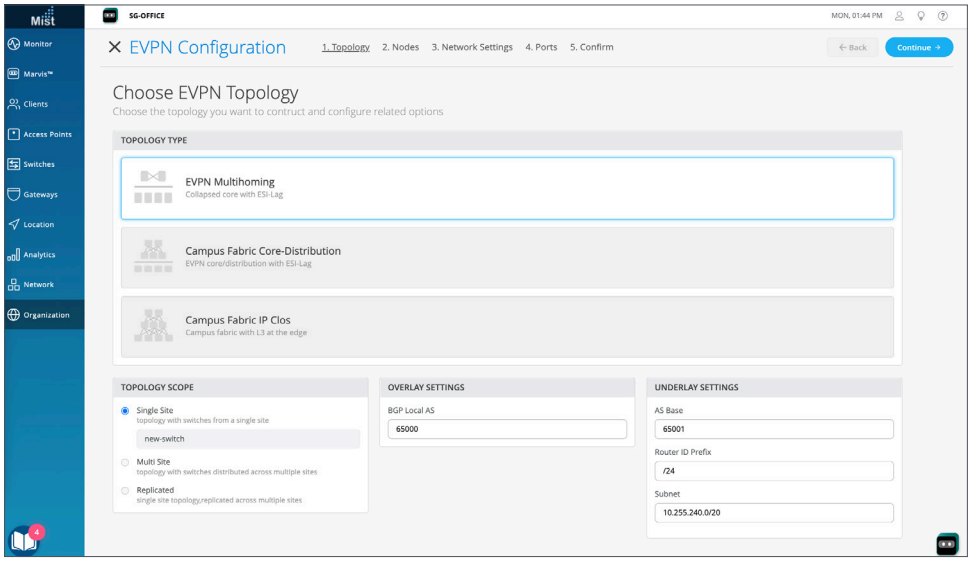

图 4：瞻博网络 Mist Wired Assurance 园区交换矩阵设计

*初始支持 EVPN 多宿主，将在未来的版本中支持其他架构。

人工智能驱动型园区交换矩阵运维

瞻博网络 Mist™ Wired Assurance 会对云托管 EX 系列以太网交换机进行声明、配置、管理和故障排除。基于云的服务提供人工智能驱动的自动化和服务级别，能够确保为连接的设备提供更好的体验。瞻博网络 Mist Wired Assurance 利用丰富的 Junos® 操作系统交换机遥测数据来简化运维，减少平均修复时间并提高可见性。第 0 天到第 2 天运维的主要功能包括：

- **第 0 天运维** —— 通过声明全新交换机或采用现有交换机来无缝部署交换机，只需使用一个激活码，真正实现即插即用的简单性。
- **第 1 天运维** —— 实施基于模板的配置模型，以便批量部署传统和园区交换矩阵，同时保留应用自定义、特定于站点或交换机的属性所需的灵活性和控制力。通过动态端口配置文件自动配置端口。
- **第 2 天运维** —— 利用瞻博网络 Mist Wired Assurance 中的人工智能，通过关键的连接前和连接后指标，满足服务级别预期，如吞吐量、成功连接数和交换机运行状况等（参见图 5）。只需在 Marvis Actions 中添加自我驱动型功能，即可检测环路、添加缺失的 VLAN、修复配置错误的端口、识别有问题的电缆、隔离发生抖动的端口，以及发现持续出现故障的客户端（参见图 6）。您还可以通过瞻博网络 Mist 云轻松执行软件升级。

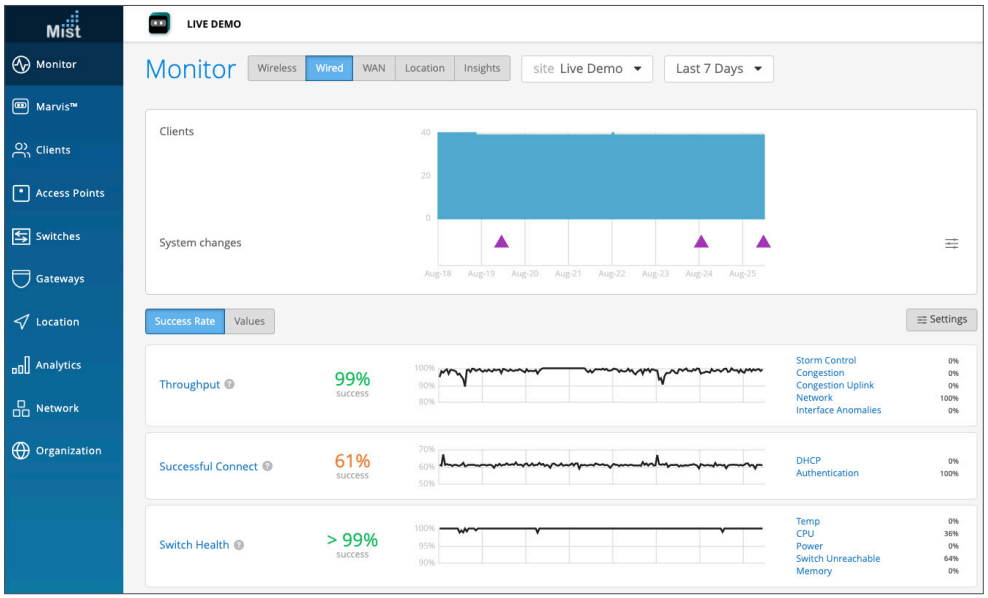

图 5：瞻博网络 Mist Wired Assurance 服务级别预期

图 6：适用于有线交换机的 Marvis Actions

了解有关 Juniper Mist™ Wired Assurance 的更多信息。

企业级 Wi-Fi 接入点

瞻博网络通过企业级接入点引领了 Wi-Fi、蓝牙低功耗 (BLE) 和 IoT 的融合。这些产品可利用机器学习和事件关联来提供数据收集、分析和策略实施等功能。瞻博网络 AP43 和 AP45 系列高性能接入点拥有获得专利的动态 vBLE 16 单元天线阵列，可提供业界领先的高精度、可扩展定位服务。瞻博网络接入点专为收集 150 多种状态的元数据构建而成，这些元数据将流入 Mist AI 引擎。

功能	AP45	AP34	AP43	AP63	AP33	AP32	AP12
Wi-Fi 标准	Wi-Fi 6E 802.11ax (Wi-Fi 6) 4x4:4SS	Wi-Fi 6E 802.11ax (Wi-Fi 6) 2x2:2SS	802.11ax (Wi-Fi 6) 4x4:4SS	802.11ax (Wi-Fi 6) 4x4:4SS	802.11ax (Wi-Fi 6) 5GHz: 4x4:4SS 2.4GHz: 2x2:2SS	802.11ax (Wi-Fi 6) 5GHz:4x4:4SS 2.4GHz: 2x2:2SS	802.11ax (Wi-Fi 6) 2x2:2SS
天线选项	内部/外部	内部	内部/外部	内部/外部	内部	内部/外部	内部
虚拟 BLE	✓	—	✓	✓	✓	—	—

Juniper Connected Security

ZDNet 在 2020 年报告称，美国联邦调查局收到的网络攻击投诉同比增长了 69%。现在，不论组织规模如何，制定有效的安全战略比以往任何时候都更加重要。为了保护网络，组织需要纵观全局，无论是从保护还是防御的角度，都难以承受巨大的可见性差异。即便在过去十年里网络安全创新有了长足的进步，网络攻击得逞的新闻仍屡见报端。很明显，组织需要为整个园区网络的所有连接点提供安全保障。这样，网络就可以利用人工智能构筑安全防线，从而更快、更成功地进行自我防御。

Juniper® Connected Security 可以将安全可见性、智能和实施扩展到网络上的每个连接点（从客户端到工作负载）。通过利用所有连接点来深入了解园区网络中的人员和活动，以及利用人工智能判断当时的风险，组织可以减轻风险并平衡园区网络安全，同时确保对园区网络资源的访问。

数据至关重要。安全防护应从两个方面着手：数据中心内的数据和对边缘数据的访问。虽然零信任的所有其他元素都是为了保护和访问数据而设计，但保护数据需要进行传输中加密、静态加密和安全连接。

- 安全矢量路由允许基于路由矢量进行分段，以增加攻击者拦截传输中数据的难度。
- Secure Connect 为来自任何地方的网络连接提供零信任网络访问 (ZTNA)，并将其封装在专用隧道中。
- 基于意图的安全控件可以通过 Junos 自动化在公共云环境中自动实施数据安全策略。例如，新创建的 Amazon S3 存储桶中的任何数据都会进行静态加密，并且强制执行授权数据访问，无需手动配置规则。

网络

在网络上进行点到点传输的数据包应当是合法的，不能包含漏洞或恶意软件，并且被授权从 A 点传输到 B 点。因此，必须对流量进行监测或恶意内容分析。

新一代防火墙 (NGFW) 已成为流量监测的理想解决方案。虽然签名通常应用于数据包标头、数据包主体和数据包组来判断流量是否包含恶意内容，但人工智能可以通过快速评估未知文件、系统行为和流量模式来确定是否存在攻击意图。

瞻博网络 SRX 系列服务网关提供对网络流量以及其他安全功能的可见性和控制力，可通过人工智能驱动型安全服务来应对已知和未知的威胁，其中包括：

- 针对新恶意软件的威胁防范。瞻博网络 ATP 云使用机器学习快速评估未知文件，并通过了解运行时的文件行为来判断它们是否为恶意软件或灰色软件
- 无需解密即可实现可见性和控制力。ATP 云还能了解所用证书的关键组件和流量行为，从而评估加密网络流量和连接设备（包括物联网）的风险。

人员/用户

园区网络上的用户可以访问内部资源和面向互联网的资源。用户是潜在的攻击矢量，必须通过对其进行访问控制和身份验证来限制风险。

SRX 系列网关提供基于用户的策略，可以对任何内部或外部资源进行精细化访问控制。SRX 系列可与任何身份识别服务提供商集成，并可通过安全接入和安全策略跟踪用户。此外，ATP 云可评估用户帐户是否遭到入侵，可动态调整到适当的安全策略和/或 VLAN，并在必要时应用多层身份验证。

工作负载

工作负载是构成应用的瞬时组件。保护工作负载，预防应用攻击，并将其与其他工作负载和应用分隔开来，是为数据中心内的宝贵资源提供最后一道防线的绝佳方法。

- 云工作负载保护会在发生零日攻击时，自动为任何云或本地环境中的应用工作负载提供防御。它将确保生产应用始终拥有可防御漏洞利用的安全网，保持关键业务服务的连接性和弹性。这项功能无需手动干预，即可利用微分段来保护单个数据库、数据收集器和所有单个资源，例如运行时应用保护。
- 瞻博网络 cSRX 容器防火墙可以分割和控制各应用之间的流量，进而通过容器化防火墙来保护应用。

设备

掌控从园区接入网络的设备是一项挑战，因为这会涉及到用户设备、临时服务器和物联网设备等。物联网设备遍布园区的各个角落，从联网的自动售货机到咖啡壶再到打印机。与基于用户的设备不同，由于物联网设备并不总是配备端点代理，因此识别适当的网络访问级别和当前设备状况可能比较困难。

- ATP 云是瞻博网络的网络威胁情报中心，可以评估连接设备的风险、识别不同的设备类型（包括物联网），以及在连接设备受到威胁时协调适当的行动。

ATP 云中的以下功能有助于保护零信任网络中的设备：

Mist AI 驱动的风险分析

此功能可为分布式接入网络边缘提供网络安全。它可提供深入的网络可见性并在网络的各连接点实施策略，从而支持 IT 团队保护其基础架构。作为威胁感知网络的一部分，园区网络会积极参与网络防御。

适用于 Mist 的安全智能

SRX 系列和 ATP 云的威胁告警可以在用户和设备连接到无线网络时迅速评估安全风险，并采取适当的措施，例如隔离或实施策略。

适用于 EX 系列的 SecIntel

ATP 会云向 EX 交换机发送设备危害信息，以便交换机可以阻止或隔离受感染的设备，即使在没有端点代理的情况下也可提供设备控制。

分析与自动化

掌控网络活动只完成了一半任务；善用可见性和收集的情报，并利用这些能力和信息实施零信任策略，将进一步降低风险，同时能让网络和安全团队获得扩展能力。组织可以通过以下途径获得可见性：

- Security Director 云。从单一用户界面管理本地安全控制、基于云的安全控制和云交付的安全控制。使用 Security Director 云来确保安全策略始终跟随用户、设备和应用，无论位于何处，永远不会破坏可见性或威胁防范措施。您可以一次性创建好安全策略，然后将其扩展到任何用户、设备和应用，而无需考虑位置变化。
- Security Director 洞察。Security Director 的这项功能可以从任何第三方安全工具获取情报和检测结果，利用这一特性突出显示正在进行的攻击，并将检测结果映射到 Mitre ATT&CK 框架。然后，Security Director 可以直接或通过 Ansible 自动化定义适当的操作，为网络中的其他工具提供编排。
- Junos 自动化。使用瞻博网络的 Junos 操作系统增强自动化功能。该系统拥有一组强大的 API 和其他本地自动化元素。组织将拥有独特的能力来控制、配置和审核瞻博网络平台上几乎所有流程或功能的表现。这种程序化访问 Junos 功能的能力可简化操作，通过自动处理工单和客户变更请求来降低 CapEx 和 OpEx，同时保障整个架构的总体运行状况。

园区网络分段

网络架构师可以采用微分段和宏分段等技术的组合来确保数据和资产的安全性。通用 EVPN-VXLAN 架构可以跨园区和数据中心进行扩展，对端点和应用进行一致的端到端网络分段。该架构还有助于最大限度地减少第 2 层泛洪，从而减少安全威胁并简化网络。

- 宏分段是共享网络设备内部和共享链路网络之间的逻辑分离。在 EVPN-VXLAN 网络中，这种分段是通过在第 2 层使用 VLAN 和在第 3 层使用虚拟路由和转发 (VRF) 来实现的。VRF 通过将两个 VRF 设备之间的 IP 流量相互隔离来实现隔离。
- 微分段通过降低风险和适应安全性需求来解决关键的网络保护问题。瞻博网络可帮助实施基于访问控制列表 (ACL) 或防火墙过滤器的微分段，从而控制虚拟网络内的流量。

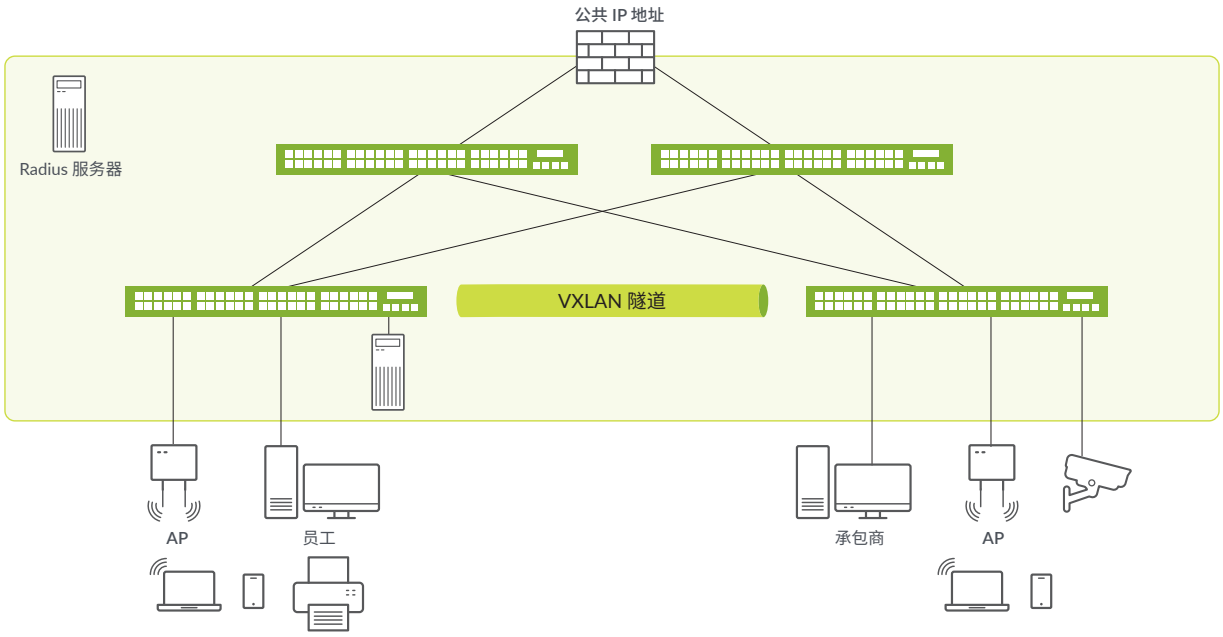

图 7：基于员工或 IoT 设备的网络分段

Junos OS：高性能网络的基础

Junos® 操作系统为瞻博网络的路由、交换和安全性设备提供通用语言。一套 Junos OS 提供的强大功能足以降低高性能网络的复杂性，使企业能够以更低的总拥有成本提高可用性并加速部署服务。Junos OS 提供一致的用户体验和自动化工具集，可让规划和培训变得更加简单，提高日常运维的效率，并允许在整个网络中加速实施变更。

Junos OS 与其他网络操作系统的不同之处在于其构建方式——Junos 是在单一软件发布轨道上进行交付，并且采用单一模块化架构，其主要优势包括：

- 在所有类型和规模的平台上使用同一操作系统，可减少规划、部署及运维网络和安全性基础架构的时间和工作量。
- 单一发布轨道可以满足不断变化的软件需求，以稳定、经过时间检验的节奏交付新功能。
- 单个模块化的软件架构可提供高度可用、安全、可扩展的软件，并为自动化和合作伙伴创新做好了准备。

Junos 遥测

在网络规模和效率方面，收集运维状况统计数据的传统数据模型已达到极限。Junos 遥测接口克服了这些限制，采用推送模式来异步提供数据，从而消除了轮询。因此，Junos 遥测接口具有高度的可扩展性，可以监测网络中成千上万的对象。

通过 Junos 遥测接口，您可以配置传感器来收集和导出各种系统资源的数据，如物理接口和防火墙过滤器。支持两种数据模型：

- 瞻博网络定义的开放和可扩展式数据模型。由于此模型采用分布式架构，因此可以轻松扩展。
- OpenConfig 数据模型，以通用的键/值格式将数据生成为 Google Protocol Buffe (gpb) 结构化消息。gRPC 远程过程调用基于 TCP，并支持 SSL 加密，因此被认为是安全可靠的。

总结

瞻博网络的人工智能驱动型园区旨在为客户提供灵活的、基于标准的现代架构，以迎接云就绪的未来。它能满足当今严苛的要求，而不影响可靠性、安全性和敏捷性。通用构建块、预先打包的自动化工作流程以及自定义的自动化工具包将预测性分析的优势从数据中心扩展到了园区内外。

更多资源

- 园区设计中心
- EX 系列网页
- 瞻博网络 Mist 云服务
- Juniper Connected Security
- 直播演示：Wired Wednesday 和 Wirelesss Wednesday
- 直播演示：人工智能驱动型企业
- Juniper Connected Security

关于瞻博网络

瞻博网络致力于大幅简化网络运维，并为最终用户提供卓越的网络体验。我们的解决方案可提供业界领先的洞察、自动化、安全性和人工智能技术，促进实现真正的业务成果。我们相信，增强连接将使我们更加紧密地联系在一起，同时解决所有人在实现全球福祉、可持续发展和自由平等方面的最严峻挑战。

JUNIPER NETWORKS | Driven by Experience™

亚太地区及欧洲、中东和非洲地区总部
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.207.125.700
传真：+31.207.125.701

公司和销售总部
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737)
或 +1.408.745.2000 | 传真：+1.408.745.2100
www.juniper.net

2000752-006-CN 2022 年 7 月