# 利用安全情报保护传统和云数据中心

## 通过动态情报提高安全效力

### 挑战

日益复杂化的威胁可能导致云停机、中断数据中心的运营，致使关键数据被窃。尽管多种安全情报源能够提供实时威胁的可见性，但要将这些数据转化为切实可行的情报以便通过防火墙策略执行，过程将极度复杂。

### 解决方案

SRX 系列服务网关提供适应性安全情报服务，可帮助您优化安全策略并防范网络攻击。这些防火墙有助于确保合理调整安全势态以便抵御面对的威胁。

### 优势

- 获取有效的威胁情报可以提供针对最新威胁的及时保护
- 轻松应用各种威胁情报源以提高灵活性，实现高度定制化的防火墙策略
- 将安全情报动态整合到防火墙策略之中，从而降低运营负担
- 通过智能服务链维护高性能、可扩展的数据中心保护

数据中心、边缘和云环境的保护是一项持续挑战。您的对手（网络犯罪者、国家攻击者、黑客分子）不断开发出更先进的入侵技术，导致威胁格局不断演化。专注于第 3 层和第 4 层检测的传统防火墙不足以满足当今威胁环境的需要。新一代防火墙极其强大，但其保护措施的设计并未考虑到新型攻击的速度和种类。当今环境中，防火墙必须能根据已知或新出现的情报立即采取措施。它必须能准确识别攻击并迅速采取行动。

分布式安全性极度复杂，因此朝着云架构过渡的趋势使得传统防火墙管理成为一种繁琐不堪的方法且易于出现人为错误。急需一种能以自动化、动态化的的方式接近实时地适应新型威胁的防火墙。

## 面临的挑战

构建和管理传统或云数据中心时，安全性是基本要素。在用户访问应用程序的需求与保护数字资产的需求之间找到平衡并不容易。试想以下几项挑战：

- **专有、刻板的安全平台**—某些防火墙解决方案利用基于云的威胁情报[1]，但其中的数据往往是在防火墙上进行预先配置的专有数据且灵活性较差，不允许选择或运用所提供信息的控制权。
- **无效的安全性**—市场上充斥着宣称提供威胁情报的来源，但大多数可用数据源并非可立即投入使用。因此，您的防火墙无法直接在策略内利用这些数据源，也就无法提供最优保护。
- **静态地址组**—管理员通常依靠静态地址列表应用检测或是拦截，这些列表每次发生更改时都必须手动更新防火墙策略。这不但非常繁琐，而且维护难度也很大。
- **防火墙性能**—防火墙服务（例如 IPS 和应用程序检测）往往会导致性能大幅下降。具体来说，一个防火墙设备中的情报数据源条目可以迅速增加到数千条甚至更多，从而造成性能问题并且最终可能导致不必要的升级。您的防火墙可能无法以最大限度发挥防火墙资源作用的方式利用威胁情报。
- **分散化的策略管理**—随着网络中防火墙数量的增加，您需要跨防火墙资产应用一致的策略，因此可靠、集中且基于 Web 的管理解决方案至关重要。

[1] 这篇文章中，我们认为除了提及 GeoIP（表示地址组）的地方之外，“威胁情报”可与“安全情报”交换使用。

## Juniper Networks SRX 系列防火墙及安全情报

瞻博提供完善的可扩展安全解决方案产品组合，我们基于 Juniper SRX 系列服务网关保护客户免受最严重的威胁所扰。SRX 系列提供坚实基础，允许企业和服务提供商实施各类服务，包括 UTM 服务、新一代防火墙服务和动态情报服务。

这些动态情报服务支持聚合、规范化、分析多种情报源（无论是原始还是辅助情报源），并将其动态分布到在防火墙实施点执行的安全策略。这些服务由作为 SRX 环境完整组成部分的开放、可扩展框架提供支持。这种开放框架的设计是基于这样一个假设：威胁将不断发展，情报源将不断演进，安全管理员希望利用所需大数据保证可靠的安全势态。

Juniper SRX 及安全情报解决方案：三阶段方法

1. 安全情报数据与 Spotlight Secure Connector 共享。
   a. Spotlight Secure 收集、优化最新情报数据源并将其发送到 Spotlight Secure Connector。目前支持的源如下：命令和控制（C&C）、GeoIP 地址源。
   b. 本地情报数据（客户提供的源或第三方源）发送到 Spotlight Secure Connector。
2. Spotlight Secure Connector 动态聚合安全情报，确保仅将最新数据分发到 SRX 系列网关。通过在内部聚合威胁情报，即可从各种来源获取情报，包括 Spotlight Secure、您自己的本地源甚至是第三方源。随后，所有这些数据均可用于 SRX 系列设备的策略设施。这与市面上的其他产品不同，其他产品要求防火墙本身承担访问云服务以获取数据源的重任，要求防火墙管理员负责管理各使用安全情报的防火墙。此外，Junos Space Security Director 和 Log Director 集中管理威胁情报策略，为 SRX 系列设备提供安全事件日志。
3. SRX 系列网关将安全情报作为安全策略的一部分。SRX 系列可以利用数据源为特定用例实施策略，例如阻止遭遇入侵的系统访问 C&C 服务器。SRX 系列使用的地址组将通过管理员提供的定制源或者来自 Spotlight Secure 的 GeoIP 数据动态更新，因此这能显著提高运营效率，迅速实现保护。所有动态地址组均动态更新 — 不需要更改任何提交或配置，因此您可以更改在 SRX 系列上应用安全策略时所用的地址而不需要占用维护时段。

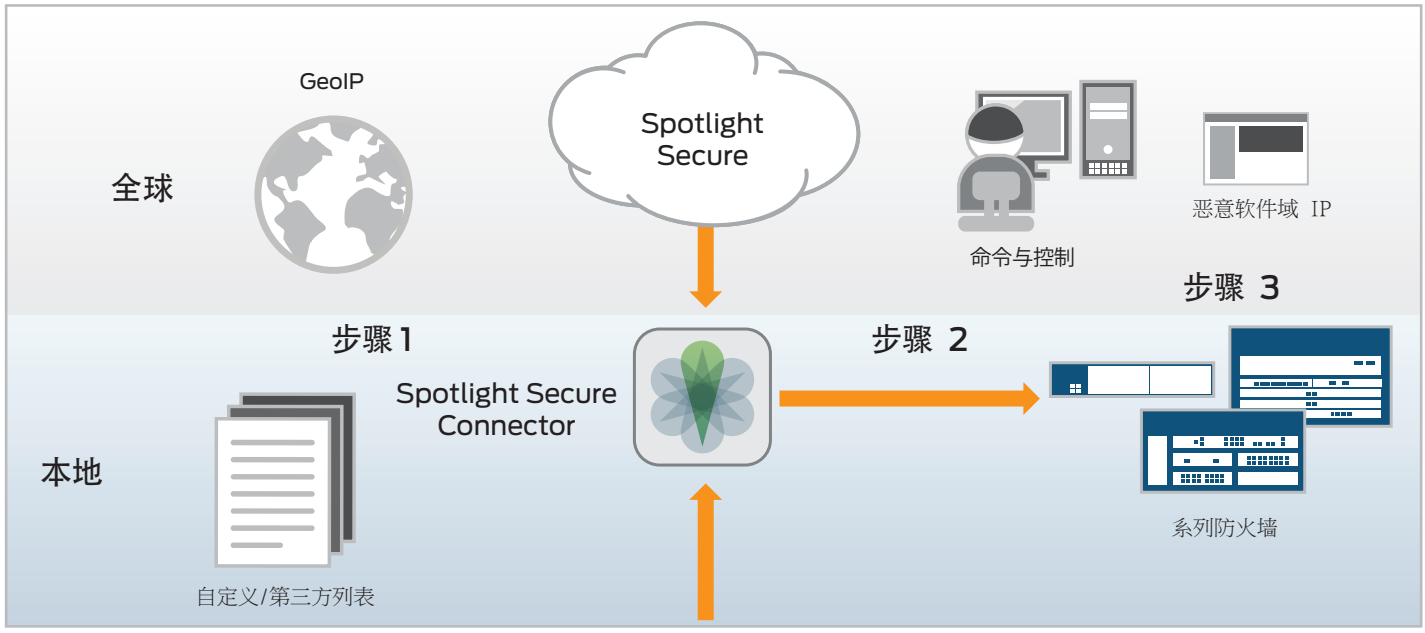


图 1： SRX 系列基于与 Spotlight Secure 和 Spotlight Secure Connector 的集成提供安全情报

## 瞻博解决方案的功能与优势

| 瞻博安全情报解决方案功能 | 说明 | 优势 |
|---|---|---|
| 可扩展、开放的安全情报框架 | • 威胁情报的内部聚合和控制。<br>• 可扩展的框架支持添加新威胁情报源，包括定制源和其他类型的数据，可加强针对新威胁的保护。<br>• 客户可控制数据源刷新率。<br>• 顺应未来的设计支持“插入”式新技术。 | • 适应您的需求和定制用例情况，提供更高的安全性和运营灵活性<br>• 允许您轻松、灵活地应用数据源，实现定制程度更高的策略 |
| 切实可行的安全情报可动态整合到 SRX 系列防火墙策略之中 | • 由于威胁情报数据实现了聚合，因此威胁情报源随时可供 SRX 系列设备使用。<br>• 误报更少，与市面上的其他解决方案相比更可靠。<br>• 提供威胁严重度评分，因此切实可行。<br>• 专门针对 SRX 系列防火墙设备应用进行了优化。 | • 客户无须先手动聚合和清理威胁情报即可将情报用于实施<br>• 支持有效、即时地防范最新威胁，以支持您独特的需求和网络环境 |
| 动态更新的地址组 | • 不需要依靠静态地址列表应用检测或拦截。<br>• SRX 系列使用的地址组将通过管理员提供的定制源或者来自 Spotlight Secure 的 GeoIP 数据动态更新。 | • 降低安全管理员的工作负担<br>• 提高运营效率 |
| 优化实施以最大限度利用资源并提供切实的客户价值 | • SRX 系列可支持超大数量的数据源条目（一个防火墙上多达 1 百万条数据源条目）。<br>• 客户可借助 Spotlight Secure Connector 划分威胁优先级，最大限度地利用防火墙资源。 | • 实现现代威胁保护所需的性能 |
| 灵活、集中化的防火墙策略配置与管理 | • 瞻博防火墙、IPsec VPN、IPS、UTM、NAT 和安全情报策略可通过 Junos Space Security Director 轻松实现集中化管理。 | • 允许支持和管理大规模部署<br>• 可实现跨所有 SRX 系列防火墙应用一致策略 |

### 有效的安全性是云和数据中心的关键所在

为帮助您随时了解最新威胁，瞻博为分布式威胁情报源添加了重要、持续的价值。具体而言，瞻博威胁源具有以下特征：

- 高度关注与恶意软件和僵尸网络相关的命令与控制（C&C）流量，包括 IP 地址、域和 URL 形式的威胁情报
- 基于多种第三方数据源的组合以及瞻博自有反恶意软件研究团队提供的原创情报
- Spotlight Secure 每个小时刷新一次，确保提供最新信息并且仅拦截最新威胁
- 包含每个源条目的威胁严重度评分，因此您可以根据威胁严重度编写策略，根据自己的部署调优解决方案以减少误报、加强效力

我们的集成化解决方案基于可用内存和资源支持各种 SRX 系列设备，以确定其能够使用多少数据。Spotlight Secure Connector 将确定最活跃、最危险的威胁，从而确保防火墙资源的最高利用率，带来最佳威胁覆盖。

## 解决方案组件

SRX 系列服务网关：瞻博防火墙，基于 Spotlight Secure 源（例如，C&C、GeoIP）和/或 Spotlight Secure Connector（例如客户或第三方）源实施防火墙、IPsec VPN、IPS、AppSecure、UTM、NAT 和威胁情报策略。最重要的是，这些功能彼此关联，允许您根据业务需求选择重要的安全服务，并将其作为分层式安全方法的一部分加以应用。

Junos Space Security Director：集中化管理平台，可用以管理 SRX 系列策略。

注意：您必须部署 Junos Space 网络管理平台才能使用 Security Director 进行安全策略管理。

Juniper Spotlight Secure：为了与不断变化的威胁格局保持同步，动态安全情报必不可少。目前，通过基于 Spotlight Secure 云的情报服务和相关威胁情报系统，瞻博支持一组威胁情报源且可针对各类威胁提供保护：

- 命令与控制（C&C）源—保护网络免受僵尸网络所扰
- GeoIP 数据(一组与地理位置相关的 IP 地址)—出于业务理由，限制发送到特定位置的流量或者不发送此类流量
- 定制威胁数据源（客户或第三方提供）—针对对于客户/用例情景至关重要的特定威胁提供保护；例如，可以黑名单/白名单的形式作为 SRX 系列防火性策略一部分使用的 IP/URL 列表

动态地址组： 可用作 SRX 系列规则中的“源”或“目标”对象的 IP 列表。所有动态地址组均动态更新—不需要更改任何提交或配置，因此您可以更改应用安全策略时所用的地址而不需要占用维护时段。动态地址组支持以下源：

- 定制 IP 列表源
- GeoIP 源（来自 Spotlight Secure）

Spotlight Secure Connector：作为 Spotlight Secure 连接到您的内部环境的扩展，Spotlight Secure Connector 利用 Spotlight Secure 和本地来源提供的源，为解决方案提供随后与 SRX 系列网关共享的控制和情报。Spotlight Secure 提供的安全情报源包括：

- 恶意 C&C 活动或僵尸网络活动的已知 IP、域和 URL；例如，如果受感染的设备尝试连接到互联网上的 C&C 服务器，SRX 系列可以根据通过 Spotlight Secure 提供的 C&C 目标的实时源拦截流量。源数据频繁更新、动态加载，并且不需要执行任何提交或配置更改。
- GeoIP（国家与 IP 的映射）数据

通过 Spotlight Secure Connector 在本地收集到的安全情报，其中包括：

- 来自客户提供的数据或第三方数据（例如，各种联盟）的定制 IP 列表源 — 形式可能是手动上载的定制文件，您也可以通过 Web 服务器配置定期更新

## 总结 — 有效的网络防护等同于更好的客户体验

所有组织都会认同，客户体验是一项重要的业务需要，安全措施必须正常运作，即便在新威胁刚刚浮现且不断增长的情况下也是如此。

瞻博为 SRX 系列服务网关提供的安全情报最根本的目的就是响应迅速变化的威胁格局。瞻博还能利用 Junos Space 网络管理平台集中管理所有 SRX 系列策略，从而帮您节省时间并最大程度降低复杂性。

最后，我们提供了一种开放的安全情报解决方案，让您可以根据业务需求进行构建和扩展。Spotlight Secure 提供切实可行的安全情报且可直接在策略中使用，而且随着需求的变化，您还可以选择添加资源的威胁情报源。

### 后续步骤

访问 www.juniper.net/security 或联系瞻博代表，获取有关 SRX 系列服务网关和集成安全情报的更多信息。

## 关于瞻博网络

瞻博网络引领网络创新。从设备到数据中心，从消费者到云提供商，瞻博网络均提供全方位改善网络体验和经济效益的软件、硬件和系统。瞻博网络公司为全球客户和合作伙伴竭诚服务。如需了解更多信息，请访问 www.juniper.net。

公司和销售总部

Juniper Networks, Inc.
1194 North Mathilda Avenue
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

APAC 和 EMEA 总部

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话： +31.0.207.125.700
传真： +31.0.207.125.701

若要购买瞻博网络解决方案，请联系瞻博网络销售代表（致电 +1-866-298-6428）或授权经销商。



3510517-001-CN 2014 年 8 月