Cisco CRS-1 的安全性

思科运营商路由系统和它的分布式、模块化 Cisco IOS XR 软件微内核架构可以通过跨越管理、控制和数据面板的内嵌检测、访问控制和流程隔离技术，支持高度安全、持续的系统运营。

服务供应商利润面临的威胁

对于服务供应商而言，网络安全与业务发展息息相关。由于病毒、入侵、操作错误和软件配置错误所导致的安全事件可能会导致广泛的相关成本提高和一系列后果，例如服务中断、经济损失、客户不满、生产率降低，甚至媒体关注。为了保护收入和利润，服务供应商必须保护他们的基础设施，为安全连接、威胁防范和终端保护提供可管理的服务。

为了在一个安全威胁（例如拒绝服务[DDoS]攻击）层出不穷和策略日益复杂的环境中保持很高的可用性，服务供应商希望采用新的路由和交换解决方案。这些解决方案应当可以提供有效、内嵌、基于硬件的安全检测，从而建立自我防御网络。这些新的不间断系统运营解决方案必须支持：

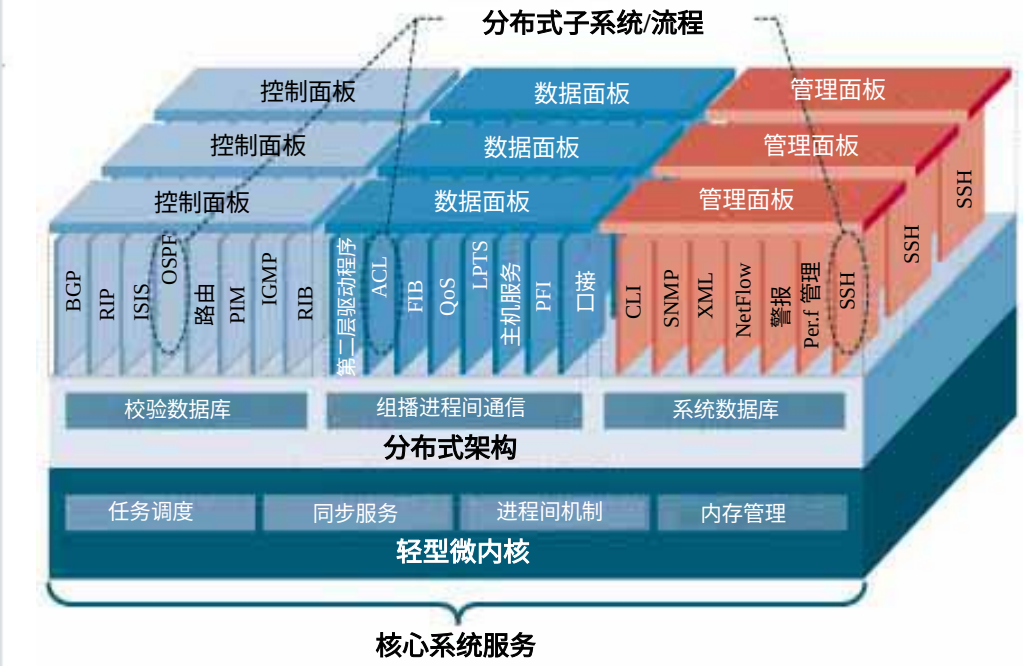
- 访问隔离、故障隔离和内存保护
- 无缝的软件和硬件恢复
- 配置和管理保护
- 主动、迅速的响应

Cisco CRS-1 的安全性

思科运营商路由系统

思科运营商路由系统（CRS-1）是一个多机架路由平台，采用了一个模块化、分布式的微内核操作系统——Cisco IOS XR（如图 1 所示）。

图1
Cisco IOS XR软件的体系结构



在设计 CRS-1 时，思科的开发人员利用了 Cisco IOS 软件的互联网安全经验。Cisco IOS XR 软件的模块化架构在逻辑上和物理上都具有分布式的特性（如图 1 所示），因而可以在创建一个高度可用的、安全的路由平台和网络方面提供巨大的优势。分散的软件组件（子系统）被部署为独立的软件流程，运行在它们自己的受保护的内存地址空间中。这可以在发生安全事件时实现真正的故障隔离和分区，防止一个子系统中发生的故障对其他的子系统造成不利影响。

与像 FreeBSD UNIX 这样的单内核架构不同，网络堆栈（例如 TCP）作为一个单独的进程，在微内核之外运行。因此，即使 TCP 堆栈受到安全威胁，系统仍然可以正常运行。在需要恢复服务时，相关流程会自动重启，不需要人为干预。此外，模块化软件架构和服务中软件升级（ISSU）支持让用户可以在不关闭整个系统的情况下，迅速地安装一个补丁。

Cisco CRS-1 的安全性

在 Cisco IOS XR 软件中保持深入的故障隔离和实现安全检测的关键是，它在三个面板之间对流程进行了逻辑分配。每个面板都采用了自己的访问控制机制，以实现网络的安全运行。这三个面板分别是：

- 控制面板
- 数据面板
- 管理面板

控制面板保护

所有路由控制信息都在控制面板进行交换，这使得控制面板及其组件成为了一个攻击目标。因为控制面板的永续性取决于 CPU 的处理能力和可扩展性，所以针对 CPU 的“ 资源耗尽式 ”攻击并不少见。

为了支持可扩展性和性能，CRS-1 控制面板采用了分布式、冗余的路由处理器——对称式多处理器（SMP）CPU。在正常情况下，CRS-1 所传输的流量由它的线卡以线速进行处理。但是，在发生意外情况时，分组被转发到路由器本身。这些包括路由协议、互联网控制消息协议（ICMP）和网络管理分组在内的“ 转移分组 ”将从线卡分组处理器发送到线卡 CPU 或者路由处理器 CPU。

为了防止控制面板在一个开放的环境中遭受 DoS 攻击，CRS-1 在线卡和它的分组处理器中分配了多种层次化的安全功能。这些功能包括：

- 动态控制面板保护（DCPP）
- 自动控制面板拥塞过滤器
- 控制面板生存时间（TTL）完整性检查（RFC 3682，通用 TTL 安全机制（GTSM））
- 边界网关协议（BGP）路由协议过滤和路由策略语言（RPL）

动态控制面板保护

由于违反规定的行为（例如入侵者转移或者分析网络流量）所导致的未经授权的或者恶意的路由更新可能会威胁网络安全。部署基于报文摘要算法 5（MD5）的相邻路由器身份验证是避免伪装的一种常用方法，它实际上确保了路由器从某个可靠的来源获得可靠的信息——但是这仅仅是第一步。如果伪装的 BGP 分组开始涌向路由器，接收路径访问控制列表（ACL）和模块化 QoS CLI（MQC）速率限制能够准确地控制这些分组的传输。但是，ACL 和 MQC 控制并不是自动进行的。如果 BGP 对等主机关机或者重启，第四层端口编号就会随着每个进程的重新建立而改变。因此，网络设计人员一直在寻找一种自动、动态的方式来准许经过设置的 BGP 对等进程和丢弃未经设置的进程。

为此，CRS-1 为线卡分组处理提供了一个 DCPP 方法。利用 DCPP，经过正确设置的 BGP 对等进程会自动获得足够的资源，而未经设置的进程则会被丢弃或者获得最低限度的处理。这种准许－拒绝模式建立在静态设置的 IP 地址和动态的第四层端口号之间的关联关系的基础上。在身份验证和建立最大限度的准入控制之前，需要为初始连接设置不同的资源策略。控制面板分组必须经过是一个多层次的事先筛选流程，直到得到一个内部搜索表的授权之后，它们才会获得足够的资源。这种自动化的流程可以节约网络管理员为了其他关键任务进行手动设置所需要的时间。

自动控制面板拥塞过滤器

在严重的 DoS 或者 DDoS 攻击导致线卡超出 CRS-1 的插槽容量时，控制机制会以特定用途集成电路（ASIC）的速度执行，将超出线卡容量的分组导入第三层模块化服务卡（MSC）上的硅分组处理器，从而确保控制面板分组得到优先处理。在网络管理员利用其他安全工具安装缓解方案以解决问题时，这种功能可以保持拓扑的完整性。

控制面板 TTL 完整性检查（RFC 3682，GTSM）

大部分控制协议对等进程都建立在相邻或者直连的路由器之间。在 GTSM（过去被称为 BGP TTL 安全破解[BTSH]）出现之前，从非定向对等节点发往路由器的 BGP 分组必须由路由器 CPU 进行处理。在生成大量这类分组时，它会导致一个严重的 DDoS 攻击，从而耗尽 CPU 资源。现在，管理员可以利用 GTSM 对 BGP 对等分组进行 TTL 检查，从而在 MSC SPP 中有效地阻止所有非定向 BGP 伪装分组。

这些技术还可用于很多其他的应用，例如标签分发协议（LDP）和资源预留协议（RSVP）。RSVP 可以利用通用 GTSM 的功能。由于 CRS-1 采用了完全可编程的 MSC 架构，GTSM 对于其他应用协议的支持可以被方便地添加到 MSC。

BGP 路由协议过滤和 RPL

BGP 是互联网上最基础的路由协议之一。不幸的是，如果 BGP 在没有采用适当的前缀过滤措施的情况下遭受攻击，互联网上将会出现大量的“ 垃圾 ”流量。因此，前缀过滤多年以来一直是互联网服务供应商（ISP）行业的最佳实践之一。（如需了解更多信息，请访问 http://www.ispbook.com。）

但是，随着路由策略的日益复杂和每台对等路由器必须交互的对等主机的不断增多，服务供应商在如何成功地部署前缀过滤方面面临着艰巨的挑战。为此，思科推出了 RPL，并将其集成到了 Cisco IOS XR 软件中。针对大规模路由配置而开发的 RPL 具有一些重要的功能，可以改进传统路由图中的设置，以及 ACL 或者面向前缀列表的配置。

第一项改进是模块化的策略组件。这样，通用的策略模块可以独立地定义和维护。这些通用模块可用于其他策略模块，以构成完整的策略，从而减少需要维护的配置信息。另外，可以为这些通用策略模块设置参数。这使得网络管理员可以将那些具有相同结构，但是特定参数不同的策略作为独立的策略模块进行维护。例如，三个除了本地优先值以外完全相同的策略可以表示为一个统一的策略，并使用不同的本地优先值作为策略的参数。

RPL 还采用了集合的概念。它是可以被用于路由属性匹配和设置操作中的类似数据的容器。有多种不同的集合类型，例如前缀集合、公共集合、as-path 集合和扩展公共集合，它们包含了相应的群组。这些集合分别类似于传统的 Cisco IOS 软件配置中的前缀列表、公共列表、as-path 列表和扩展公共列表，但是两者之间存在一个重要的区别。集合并不包括 Cisco IOS 软件配置中的“ 接受 ”和“ 拒绝 ”的概念。集合仅仅是数据的容器。大部分集合还拥有一个内嵌变量，它允许在完全在内部指定的数据值，而不需要引用某个只包含部分数据的特定集合。

决策——例如接受还是丢弃路由——完全取决于所制定的策略。RPL 让用户可以将匹配的操作符（可能使用集合数据）和传统布尔逻辑操作符（“ 与 ”、“ 或 ”和“ 非 ”）集成到复杂的条件表达式中。所有匹配操作符都会返回一个“ 真 ”或“ 伪 ”结果。这些条件表达式的执行和相关操作都可以由用户所指定的、简单的“ if-then，else-if，else ”结构控制。这使得策略的评估路径可以完全由用户设置。

随着 RPL 的采用，对等策略预计将会比现有的、基于路由图的对等语句更加模块化和更有效率。RPL 可以提供必要的可扩展性，使得用户能够通过一个多机架路由系统（例如 CRS-1）与数千个对等主机进行对等通信。

数据面板保护

数据面板可以接收、处理和传输网络组件之间的网络数据，控制进出路由器的大量网络流量。为了防止数据面板流量遭受已知的攻击，CRS-1 的转发引擎中内置了一些缺省的完整性检查（基于互联网行业积累的知识）。此外，CRS-1 还提供了多种功能和工具，例如 ACL、单播反向路径转发（uRPF）和 NetFlow 记帐，并在 MSC 上进行专门的输入和输出处理。

- **ACL**——ACL（包括 IPv4 和 IPv6）是很多路由器数据面板应用——例如分组分类、速率限制、统计和审核——的一个重要组成部分。它实际上是一个针对分组的准许－拒绝操作符。

  Cisco CRS-1 的设计目的是满足最严格的性能和可扩展性要求，因而它能够在网络负载繁重的情况下以线速处理 ACL。例如，在处理 200 万个路由和 500 个 BGP 对等主机的同时，CRS-1 可以在不影响性能的情况下处理数千个 ACL 及其条目。

Cisco CRS-1 的安全性

- **uRPF**——Cisco CRS-1 支持 uRPF（严格和松散模式）。它使得 Cisco CRS-1 可以通过丢弃缺乏可验证的 IP 源地址的 IP 分组，解决因为在网络中引入错误的或者伪装的 IP 源地址所导致的问题。当某个接口启用 uRPF 严格模式时，路由器会检查接收到的所有分组，验证源地址和接口是否出现在路由表中，以及与收到分组的接口是否匹配。

  uRPF 松散模式是在 ISP 行业广泛使用的触发式黑洞过滤技术的基础。在松散模式下，uRPF 可以根据源 IP 地址有效地丢弃 DoS 和 DDoS 攻击分组，并在很短的时间内将该方案发送到数百台路由器。
- **NetFlow——**记帐是网络管理在流量工程、网络监控和计费领域的一个不可或缺的组成部分。NetFlow 最初是一个记帐应用，可以为查看单个分组报头的内部信息、按照不同的流量等级汇总分组，以及搜集每个流量等级的统计数据和详细路由信息提供一个有效的机制。部署于 Cisco IOS XR 软件中的 NetFlow 统计数据构成了一个重要的数据库。它可以精确地发现流量的细微行为，从而为流量工程和安全分析提供支持。
- **静态 NetFlow 和分组监听——**Cisco IOS XR 软件还支持功能超过 NetFlow 的静态 NetFlow。与动态的 NetFlow 不同，静态 NetFlow 对待分组流的方式与 ACL 处理数据的方式很类似，但是它具有一些扩展字段，例如源或者目的地自治系统号和多协议标签交换（MPLS）标签。利用静态 NetFlow，管理员可以定义一个带有扩展 ACL 的数据流过滤器，以跟踪某个特定数据流的分组或者字节计数器。大量的 NetFlow 数据能够与某个扩展 ACL 关联，从而让操作人员可以过滤其他数据，直接找到他们所感兴趣的数据流，从而为防御 DoS 和 DDoS 攻击创造了又一个有效的工具。

  从 Cisco IOS XR 静态 NetFlow 功能中衍生出来的带内分组监听采用了与静态 NetFlow 相同的功能，例如类似于 ACL 的过滤，且还可以搜集样本，并将它们转发到某个指定的目的地。

管理面板保护

管理面板是所有与路由平台的系统管理有关的流量的逻辑路径。在一个分布式、模块化的环境中，管理面板可以提供新的复杂度等级，因而提高了对于确保安全访问的要求。这种安全访问最好通过下列手段实现：

- **拒绝缺省访问**——一个已知的、常见的系统漏洞是在缺省情况下启用某些协议。这些开放的端口导致了一些让入侵者有可乘之机的安全漏洞。为了满足服务供应商的要求，CRS-1 采用了专门的设计，即在缺省配置下关闭所有这些服务，直到由操作人员手动启用这些服务。
- **身份验证、授权和记帐（AAA）和加密协议**——所有对路由器的访问和路由器对外的访问都应当被加密和控制。Cisco CRS-1 支持 AAA 身份验证和加密协议 SSH、SSL、IPSec 和 SNMPv3。利用 ACL，还可以使用其他的控制功能，将访问权限只限制于特定的源主机。每个用户都可以被明确归于某个 AAA 区域，以反映用户的访问权限。
- **隔离管理端口**——核心路由器和交换机通常都带有专用的管理以太网端口，它们可能会导致对设备的不安全访问。Cisco CRS-1 以太网管理端口都是可以路由的，因而可以通过 AAA 访问控制和加密进行控制。隔离数据和控制面板流量可以防止它们不会“干扰”。ACL 可以被用于阻塞干扰，而且管理员利用 Cisco Craft Works 界面（CWI），只需点击几下鼠标就可以在多个端口之间有效地部署 ACL。CWI 是一个专门为多机架路由器管理而设计的增值 GUI 工具。

- **基于角色的权限模式**——因为未经授权的或者缺乏经验的网络操作人员可能会对系统的可用性造成威胁，服务供应商需要用灵活的方法，根据用户所设定的标准分配操作人员的权限。

  Cisco IOS XR 软件可以通过一种方便、灵活的方法，向特定的操作人员或团队分配适当的访问权限，从而实现一种基于角色的权限模式。它可以将各项操作业务设置为不同的任务。例如，BGP 配置是一项任务，而开放最短路径优先（OSPF）是另外一项任务。系统重启也是另外一项任务。每项任务都具有一个与众不同的标识号——任务 ID，并且具有指定的读取或者写入权限。用户可以与任务组关联，以继承相应的访问权限。为了确保安全，任务 ID 可以与 AAA 服务器配合，为访问路由器提供最大限度的集中控制。

总结

DoS 和 DDoS 攻击是互联网现状的重要组成部分，也是服务供应商的盈利能力面临的最严重的威胁之一。为了保护利润，服务供应商必须在具有嵌入式安全检测功能的下一代路由系统的基础上建设一个自我防御网络。服务供应商应当确保该系统的成功，并在整个网络中采用最佳实践。

Cisco CRS-1 的分布式、模块化架构通过内存保护，逻辑路由器内部的服务隔离，以及管理、控制和数据面板之间的流程隔离，支持高度安全的、不间断的系统运营。

除了 CRS-1 的内嵌功能和推荐的最佳实践以外，思科产品安全事件响应团队（PSIRT）是一个全球性的专家小组，每天 24 小时待命。他们能够迅速地解决涉及到思科产品的客户安全事件和消除产品的安全漏洞。借助于思科在网络市场上的领先优势，思科客户可以获得业界独一无二的、主动、迅速的响应服务。

如需了解更多关于 Cisco CRS-1 安全功能的信息，请联络您的思科客户团队，或者访问 http://www.cisco.com。如需了解关于思科 PSIRT 和现有建议的最新信息，请访问：http://www.cisco.com/go/psirt。

参考资料

“ CRS-1 系统概述”

http://www.cisco.com/

Barry Greene 和 Philip Smith, “ISP Essentials,”

http://www.ispbook.com

vijay Gill、John Heasley 和 David Meyer, “RFC 3682—通用 TTL 安全机制 (GTSM)”

http://www.ietf.org/rfc/rfc3682.txt

Vijay Gill, “缺少优先级排序功能，路由处理器会对系统的安全性造成不利影响”

http://www.nanog.org/mtg-0302/gill.html

“ 加强思科路由器的安全性”

http://www.cisco.com/warp/public/707/21.html

P. Ferguson 和 D. Senie, “RFC 2827—网络输入过滤：阻止利用 IP 源地址伪装发动的拒绝服务攻击”

http://www.ietf.org/rfc/rfc2827.txt

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街一号东方广场东一办公楼 19-21 层

邮政编码：100738
电话：(8610) 65267777
传真：(8610) 85181881

上海
上海市淮海中路 222 号力宝广场 32-33 层

邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

广州
广州市天河北路 233 号中信广场 43 楼

邮政编码：510620
电话：(8620) 87007000
传真：(8620) 38770077

成都
成都市顺城大街 308 号冠城广场 23 层

邮政编码：610017
电话：(8628) 86758000
传真：(8628) 86528999

如需了解思科公司的更多信息，请浏览 http://www.cisco.com /cn