Cisco IOS 防火墙特性集

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION

Fact Sheet

Cisco IOS 防火墙特性集

当人们寻求利用 Internet 无与伦比性能的同时，他们需要安全的解决方案来:

- 保护内部网络，防止黑客入侵。
- 提供安全的 Internet 和远程访问连接。
- 通过 World Wide Web 启动网络贸易。

今天，Internet 成为功能强大的新技术焦点，极大地增强了企业与客户、供应商、合作伙伴及远程雇员的通信。用户必须确信网络业务，尤其是公共网络上的业务是安全的。

Cisco IOS 软件运行于 80% 以上的 Internet 骨干网路由器中。Cisco IOS 软件提供全面的网络服务，并启动网络化的应用程序。Cisco IOS 安全服务为建立 Internet、内部网及远程访问网络的提供安全解决方案，进而提供端到端网络安全。

整个安全解决方案的一个关键部分是网络防火墙，负责监视穿过网络周边的通信及根据安全策略加以限制。周边路由器可见于任何网络边界，例如专用网络、内部网、外部网或 Internet 之间。防火墙分离内部(专用)和外部(公共)网络。Cisco IOS 防火墙特性集作为 Cisco IOS 软件的一个选项上市，提供一个先进的安全解决方案，保护网络，防止安全违规。这种集成化路由器安全解决方案提供 Cisco Systems 安全解决方案系统中的一个部件。

Cisco IOS 防火墙特性集是三个 Cisco 防火墙解决方案之一，这些解决方案被设计用来满足一个网络内的不同防火墙要求，无论是专用设备(PIX 防火墙)、基于 NT 的解决方案(Centri 防火墙)还是集成在网络基础机构(Cisco IOS 防火墙特性集)之中。Cisco 防火墙家族全面的安全特性，可以满足边界政策加强、扩展到更加复杂的虚拟专用网络(VPN)、内容过滤以及服务否决(Denial of Service)检测和预防的需求。如果结合部署，Cisco 防火墙允许网络管理人员通过实现一个分层的安全策略，实现功能更加强大的安全体系结构。没有其他网络供应商能够在其安全解决方案中提供这样的灵活性。Cisco IOS防火墙特性集通过在网络基础机构本身内提供访问目录政策加强，完善了 Cisco 的端到端安全产品，从而实现了独立设备不能提供的灵活性和控制水准。

Cisco IOS 防火墙特性集的一些好处包括:

- 灵活性——一揽子解决方案可以执行路由，提供安全的 Internet 连接，在每用户或每应用的基础上，根据一个用户定义的政策，针对每一个接口采用不同的安全特征。
- 投资保护——将防火墙功能性集成进一个多协议路由器可以利用现有的路由器投资。路由器通常被部署用于分离敏感的网络区段和管理专用 / 公共网络接口。增量变化可以节省与学习新平台相关的成本和管理培训。
- 更加容易的管理——通过利用远程管理功能，网络管理员可以从网络上的一个中央控制台实现安全特性。
- 无缝的互操作性——与其他 Cisco IOS 软件特性一起使用，优化广域网使用，提供稳健、可伸缩的路由，并与现有的基于 Cisco IOS 的网络(例如 Internet)互操作。

新的防火墙特性和优点

Cisco IOS 安全服务包括一系列特性，能使管理人员将一台 Cisco 路由器配置为一个防火墙。Cisco IOS 防火墙特性集给现有的 Cisco IOS 安全解决方案增加了更大的深度和灵活性。表 1 提供新特性的一个概览，这些新特性给可能已经作为防火墙运行的路由器带来新增的灵活性和保护。目前，这些特性可用于 Cisco 1600 和 2500 系列路由器，并将从 1998 年第三季度开始可用于 Cisco 2600 和 3600 系列路由器。

表 1: Cisco IOS 防火墙特性集概览

新特性	说明
基于上下文的访问控制(CBAC)	针对通过周边(例如专用企业网和 Internet 之间)的所有通信流量，给内部用户提供安全的、基于每应用的访问控制。
Java 阻断	提供针对未识别的恶意 Java 小程序的保护。
Denial of Service(服务拒绝)检测 / 预防	防御和保护路由器资源免受常见攻击；检查数据包包头和丢掉可疑的数据包。
审计踪迹	详细说明事务；记录事件印迹、源主机、目的主机、端口、持续时间和传输的总字节数。
实时告警	记录在发生服务拒决攻击或出现其他预配置条件时的告警。
支持 ConfigMaker	一种基于 Win95/WinNT 向导的网络配置工具，为网络设计、寻址和防火墙特性集实现提供逐步的指导。

以前发布的 Cisco IOS 防火墙功能包括:

- 基本的和高级的通信过滤
  - 标准和扩展的访问控制列表(ACL)：将访问控制用于特定的网段，并定义那些通信可以通过一个网段。
  - 锁定和密钥动态的 ACL：根据用户身份(用户名 / 口令)授予通过防火墙的暂时访问。

- 基于策略的多端口支持：根据由安全策略决定的 IP 地址和端口，提供控制用户访问的能力。
- 网络地址转换(NAT)：通过对外界隐藏内部地址增强网络保密性；通过启动注册 IP 地址的保护，降低 Internet 访问的成本。
- 同级路由器验证：确保路由器从可 靠的来源收到路由信息。
- 事件日志记录：通过将系统错误消息输出到一个控制台终端或系统日志服务器、设置严重级以及记录其他参数，允许管理员实时跟踪潜在的违法或其他非标准活动。
- 虚拟专用网络(VPN)：利用下列任何协议，通过公共线路(例如 Internet)提供安全的数据传输；降低远程分支办事处和外部网的实现及管理成本；增强服务质量和可靠性；提供基于标准的互操作性。
  - 一般路由密封(GRE)隧穿
  - 第二层转发(L2F)
  - 第二层隧穿协议(L2TP)
  - 服务质量(QoS)控制：排定应用程序优先顺序和分配网络资源，进而确保关键任务应用程序通信的交付。
- Cisco 加密技术：网络层加密功能，在传输期间防止通过网络窃取或窜改数据。
- IPSec：基于标准的网络层加密，提供数据保密性和验证。

关于新特性的详细资料

基于上下文的访问控制

基于上下文的访问控制(CBAC)是 Cisco IOS 防火墙特性集最显著的新增特性。CBAC 技术的重要性在于，它第一次使管理员能够将防火墙智能实现为一个集成化单框解决方案的一部分。现在，紧密安全的网络不仅允许今天的应用通信，而且为未来先进的应用(例如多媒体和电视会议)作好了准备。CBAC 通过严格审查源和目的地址，增强了使用众所周知端口(例如 ftp 和电子邮件通信)的 TCP 和 UDP 应用程序的安全。

CBAC 的工作原理

CBAC 是一个适用于 IP 通信的基于每个应用的控制机制，包括标准 TCP 和 UDP Internet 应用程序、多媒体应用程序(包括 H.323 应用程序、CU-SeeME、VDOLive、Streamworks 及其他应用程序)以及 Oracle 数据库。CBAC 检查 TCP 和 UDP 包，并跟踪它们的“状态”或连接状态。

TCP 是一个面向连接的协议。在传输数据之前，源主机与一个目的主机洽谈连接，通常被称为“三向握手”。这种握手过程确保有效的 TCP 连接和无错的传输。在连接建立期间，TCP 穿过几个 " 状态 " 或阶段(由数据包头标识的)。标准和扩展的访问控制列肯(ACL)从包头状态来决定是否允许通信通过一个连接。

CBAC 通过检查整个(数据)包了解应用程序状态信息，给 ACL 功能增加了检查智能。CBAC 利用这种信息创建一个暂时的、对话期特定的ACL 入口，从而允许回返通信进入可靠网络。这种暂时的ACL 有效地在防火墙中打开了一个大门。当一个对话期结束时，ACL入口被删除，大门关闭。标准和扩展的ACL不能创建暂时的ACL入口，因此直至目前，管理员一直被迫针对信息访问要求衡量安全风险。利用标准或扩展的 ACL，难以确保为回返通信流量选择通道的先进应用程序的安全。

CBAC比目前的ACL 解决方案更加安全，因为它根据应用类型决定是否允许一个对话通过防火墙，并决定是否为回返通信流量从多个通道进行选择。在 CBAC 之前，管理员仅通过编写基本上使防火墙大门洞开的永久性ACL，就能够许可先进的应用通信，因此大多数管理员选择否决所有这类应用通信。现在，有了CBAC，通过在需要时打开防火墙大门和其他时候关闭大门，他们能够安全地许可多媒体和其他应用通信。例如，如果CBAC被配置成允许 Microsoft NetMeeting，那么当一个内部用户初始化一次连接时，防火墙允许回返通信。但是，如果一个外部 NetMeeting 来源与一个内部用户出始化连接时，CBAC 将否决进入，并撤消数据包。

从一个更加技术的观点来看，CBAC 使用几个加强机制:

1. 数据包检查监视数据包控制通道，识别控制通道中的应用专用指令，检测和预防应用级攻击。
2. 通过检查的包将被转发，而 CBAC 创建一个状态表来维护对话状态信息。如果状态表存在，表明(数据)包属于一个有效对话，回返通信流量将仅被许可通过集成化的防火墙。这种可配置的特性负责监视定义的对话。
3. 当对话结束时，状态表被删除。在 UDP(一种非连接的服务)情况下，CBAC 通过根据地址 / 端口配对检查包来决定 UDP 对话，相应地中止 UDP“对话”访问。
4. CBAC根据状态表中的信息，动态地创建和删除每一个路由器接口的访问控制列入口。这些入口在集成的防火墙中创建暂时的“开口”，允许有效的回返通信流量进入网络。与状态表相似，动态 ACL 在对话结束时不被保存。

CBAC 适用于何处

CBAC 是根据每个接口配置的。CBAC 可能被配置用于控制源于防火墙另一方的通信(双向)；但是，大多数客户将 CBAC 用于仅源于一方的通信(单向)。

将CBAC配置为一个单向控制，其中客户对话是在内部网内启动的，必须穿过防火墙才能访问一个主机。例如，一个分支办事处可能需要跨一个广域网连接或 Internet 访问企业服务器。CBAC 根据需要打开连接，并监视回返通信流量。

当一个防火墙双方都需要保护时，CBAC适合作为一个双向解决方案。这种配置的一个例子是在两个合作伙伴公司的网络之间，其中某些应用程序通信被限制在一个方向，其他应用程序在另一个方向。

有关 CBAC 的其他说明

- 对于每一个连接，CBAC 都为状态表和动态 ACL 跟踪及分配内存。如果只有一个 ACL 组被配置在某一给定的方向，那么 CBAC 的内存消耗少于每连接 600 字节(跨所有平台)。一个应用程序对话可能包括多个 TCP/UDP 连接。例如，一个 NetMeeting 对话包括多达 7 个 TCP/UDP 连接。
- CBAC 和加密可以在同一接口上使用。但是，CBAC 不能检查加密的数据包的内容。当路由器也是加密点时，CBAC 和加密可以协同工作 – CBAC 可以在加密以前检查数据包。
- CBAC 可以与快速交换和过程交换一同工作，在 Cisco 1600 和 2500 系列路由器平台上提供一流的性能。

Java 阻断

随着大量 Java 小程序可用于 Internet，保护网络免受恶意小程序的攻击已经成为网络管理人员的一个主要课题。可以配置 Java 阻断来过滤或完全拒绝对没有嵌入在一个文档或压缩文件中的 Java 小程序的访问。

服务拒绝检测和预防

新近增强的服务拒绝检测和预防针对syn泛滥、端口扫瞄和包注入提供网络防御。服务拒绝检测和预防检查TCP连接中的包顺序号。如果这些号码不在预期的范围内，路由器将撤消可疑的包。当路由器检测出新建，它就发出一条告警信息。它还撤消半开的 TCP 连接状态表，以防止系统资源耗尽。

审计跟踪

增强的审计跟踪利用系统日志来跟踪所有事务；记录时间印迹、来源主机、目的地主机、所用的端口、对话以及传输的总字节数。

实时告警

一旦查出可疑的活动，实时告警将向中央管理控制台发送系统日志错误信息。网络管理人员有能力立即对入侵作出反应。

支持 ConfigMaker

通过使用ConfigMaker(一种基于Win95/WinNT向导的管理工具，它能使你将网络上支持的任何路由器配置为一个防火墙)，Cisco IOS防火墙特性集非常容易安装。ConfigMaker是现有Cisco命令行接口工具的一个配置替换。它指导分销商和网络管理员完成网络设计及路由器安装过程。ConfigMaker允许从一台单一PC配置整个路由器网络，而不是将每一个路由器以独立的设备方式配置。

应用程序

分支办事处与总部和 Internet 的连接

作为分支办事处一个关键的安全部件，Cisco IOS防火墙特性集不占用布线柜中的额外空间。例如:使用Cisco 2514利用一个端口连接Internet网,另一个端口通过专线访问总部资源。通过防火墙特性集，管理员可以远程配置路由器，从而在一个接口拒绝某些应用通信和从Internet下载的Java小程序，并允许SNA通信和Java小程序通过另一个广域网进入总部网络。这一解决方案授权访问要求的应用程序，例如SNA主机和客户机/服务器应用程序，并拒绝对意外应用通信的访问。

小型企业 Web 服务器

在另一种情况中,一家小企业老板正通过一个现场Internet Web服务器与客户和供应商通信。通过使用一个Cisco 1605路由器，客户和供应商可以随时登录Web服务器，而内部以太网在另一个接口上仍然受到保护。防火墙特性集在每一个端口提供CBAC检查，密切监视通信，并保护Web服务器和内部网免受攻击。

Cisco 端到端网络

一项稳健的安全策略不仅需要周边控制，或防火墙安装和管理。Cisco IOS软件是实现一项全球安全策略的理想工具。建立一个端到端Cisco解决方案可以给管理人员提供随网络发展在整个网络加强安全策略的能力。

Cisco 支持

根据现有的一项支持计划，你可以从Cisco获奖的Web站点－Cisco Connection Online随时获得Cisco IOS安全软件的升级版本。为了补充其业界领先的网络解决方案，Cisco开发了全面的支持解决方案。Cisco以寿命周期为重点的支持产品提供启动、维护、市场以及先进的服务和定制服务，来保护和实现你的投资的最大化。这些服务一起提供根据特定应用程序和环境定制解决方案的覆盖面、广度以及灵活性。现在，通过世界级的Cisco支持服务，网络管理人员可以端到端地支持他们的局域和广域Cisco网络。

表 2：Cisco IOS 防火墙特性集规范

特性	说明
基于上下文的访问控制(CBAC)	
包状态检查	维护穿过路由器的每一个连接的状态和上下文；检查入站和出站通信，加强安全策略
智能检查过滤器	了解控制通道中应用程序特定的指令；检测应用程序攻击；在动态分配(根据需要)的基础上打开端口
CBAC 支持的应用程序(可以模块化安装)	
TCP/UDP 应用程序	Telnet、http、tftp、SNMP
文件传输协议(FTP)	包括积极和被动模式
多媒体应用程序	检查控制通道流，确保在每一次对话期间打开视频和音频通道；支持 H.323 应用程序、CU-SeeMe、RealAudio、StreamWorks 和 VDOLive
电子邮件服务(SMTP 协议检查)	查出无效的 SMTP 指令；消除对“非军事化区域”中外部邮件中继的需求
远程过程呼叫(RPC)服务	检查端口映象程序请求，在需要时打开通道支持 RPC 通信流量
伯克莱标准分布(BSD)-Rcmds	检查服务器回答，打开任何辅助通道
Oracle 数据库应用程序支持	检查来自 Oracle 收听者过程的转向信息；为客户连接到服务器打开端口
基于 T.323 的电视会议应用程序	检查 Q931 和 H.245 控制消息，为视频和音频数据打开增加的 UDP 通道。
服务拒绝检测和预防	
防御流行的攻击模式	防御 syn 泛滥、端口扫瞄和包注入；防止路由器资源耗尽
包撤消	暂时撤消始自攻击者的包；基于 IP 地址
顺序号检查	检查 TCP 连接中的包顺序号，确保它们是在预期的范围之内
事务记录	详细说明事务；记录终止时间印迹、源主机、目的主机、端口和传输的总字节数
推荐的缺省选项(请参见全面的推荐缺省选项目录)	允许 / 否决推荐的启动设置；来源路由关 / 开；废止 / 使能代理 arp；仅启动所需的应用程序 / 所有应用程序；通过 Message Digest 5(MD5)散列算法加密路由器口令；将访问目录和口令用于虚拟终端端口；在所支持的路由协议中，使能 / 废止路径验证
增强的 TCP/UDP 事务日志	根据来源 / 目的地地址和端口配对跟踪用户访问
Java 阻断	
设置保护级	可以配置用于过滤或完全否决对没有嵌入在任何文档或压缩文件中的 Java 小程序的访问
实时报警	
先进的日志记录特性	通过一个系统日志机制，生成报警
与 Cisco IOS 特性兼容	与 ACL、NAT、TCP Intercept 和 Reflexive Access Lists 兼容；Cisco 加密技术
网络管理	
支持 ConfigMaker	一种基于 Win95/WinNT 向导的网络管理工具，为网络设计、寻址和防火墙特性集实现提供逐步的指导

定购信息和内存要求

产品编号	说明	内存要求
SF160CH-11.2.13P	Cisco IOS 1601-1604 IP/FIREWALL(包括 NAT)	闪存: 4MB DRAM: 2MB
SF160BHP-11.2.13P	Cisco IOS 1601-1604 IP/IPX/FIREWALL Plus	闪存: 6MB DRAM: 4MB
SF160QHY-11.2.13P	Cisco IOS 1601-1604 IP/IPX/AT/IBM/FIREWALL Plus 56	闪存: 8MB DRAM: 6MB
SF16RCH-11.2.13P	Cisco IOS 1605 IP/FIREWALL(包括 NAT)	闪存: 2MB DRAM: 8MB
SF16RBHP-11.2.13P	Cisco IOS 1605 IP/IPX/FIREWALL Plus	闪存: 4MB DRAM: 10MB
SF16RQHY-11.2.13P	Cisco IOS 1605 IP/IPX/AT/IBM/FIREWALL Plus 56	闪存: 4MB DRAM: 12MB
SF25CH-11.2.13P	Cisco IOS 2500 系列 IP/FIREWALL(包括 NAT)	闪存: 8MB DRAM: 4MB
SF25BHP-11.2.13P	Cisco IOS 2500 系列 IP/IPX/AT/DEC/FIREWALL Plus	闪存: 16MB DRAM: 4MB
SF25AHY-11.2.13P	Cisco IOS 2500 系列 Enterprise/Firewall Plus 56	闪存: 16MB DRAM: 6MB

可用性和价格

现在，客户可以将 Cisco IOS 防火墙特性集作为 Cisco 1600 和 2500 系列路由器的一个额外选项来定购。你可以从 Cisco 的 Web 站点作为一个软件下载防火墙特性集，或者申请一个 CD-ROM。有关价格信息，请与你的本地 Cisco 销售办事处、Cisco 代理商联系，或者访问 Cisco Web 站点，网址为 www.cisco.com。

进一步信息

如需了解Cisco IOS软件和Cisco IOS安全服务的更多信息，请访问Cisco Web站点，网址为http://www.cisco.com/security 或 http://www.cisco.com/iosfirewall。

从交换到路由，

从 Intranet 到 Internet，

从计算机网络到电信基础，

. . . . . .

Cisco 都给您

端到端的真实享受!

思科系统(中国)网络技术有限公司

北京
北京南礼士路 66 号
建威大厦 18~19 层
邮政编码:100045
电话:(8610)68023355
传真:(8610)68038348

广州
广州市环市东路 362-366 号
好世界广场 3106-3107 室
邮政编码:510060
电话:(8620)83870097
传真:(8620)83870070

上海
上海市遵义南路 88 号
协泰中心 2205 室
邮政编码:200335
电话:(8621)62198668
传真:(8621)62753431

成都
成都市西御街 77 号
四川国信大厦 8 楼 A 座
邮政编码:610015
电话:(8628)6198198
传真:(8628)6198305

重庆
重庆市南坪北路 15 号
扬子江假日饭店 415 房
邮政编码:400060
电话:(8623)62918749
62918750
传真:(8623)62918746