



中华人民共和国通信行业标准

YD/T 1906-2009

IPv6 网络设备安全技术要求 ——核心路由器

Security Requirements of Core Router Equipment Supporting IPv6

2009-06-15 发布

2009-09-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

4 概述.....5

5 数据转发平面安全.....6

6 控制平面安全.....9

7 管理平面安全.....12

附录 A（规范性附录） 硬件系统和操作系统的安全要求.....17

附录 B（资料性附录） 安全日志的严重等级定义.....18

前 言

本标准是“路由器设备安全”系列标准之一，本系列的标准结构和名称预计如下：

1. YD/T 1358-2005 路由器设备安全技术要求——中低端路由器（基于 IPv4）
2. YD/T 1359-2005 路由器设备安全技术要求——高端路由器（基于 IPv4）
3. YD/T 1439-2005 路由器设备安全测试方法——高端路由器（基于 IPv4）
4. YD/T 1440-2005 路由器设备安全测试方法——中低端路由器（基于 IPv4）
5. YD/T 1907-2009 IPv6 网络设备安全技术要求——边缘路由器
6. IPv6 网络设备安全测试方法——边缘路由器
7. YD/T 1906-2009 IPv6 网络设备安全技术要求——核心路由器
8. IPv6 网络设备安全测试方法——核心路由器

本标准与《IPv6 网络设备安全测试方法——核心路由器》配套使用。

与本系列标准相关的标准还有“支持 IPv6 的路由器设备”系列标准，该系列的标准结构和名称如下：

1. YD/T 1452-2006 IPv6 网络设备技术要求——支持 IPv6 的边缘路由器
2. YD/T 1453-2006 IPv6 网络设备测试方法——支持 IPv6 的边缘路由器
3. YD/T 1454-2006 IPv6 网络设备技术要求——支持 IPv6 的核心路由器
4. YD/T 1455-2006 IPv6 网络设备测试方法——支持 IPv6 的核心路由器

本标准的附录 A 为规范性附录，附录 B 为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院

本标准主要起草人：赵 锋、马军锋、魏 亮

IPv6 网络设备安全技术要求

——核心路由器

1 范围

本标准规定了支持 IPv6 协议的核心路由器的安全技术要求,包括数据转发平面安全、控制平面安全、管理平面安全等。

本标准下文中所有对路由器的安全规定均指对支持 IPv6 的核心路由器的规定。

本标准适用于支持 IPv6 的核心路由器设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准。然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 18336.2	信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求
YD/T 1454-2006	IPv6 网络设备技术要求——支持 IPv6 的核心路由器
IETF RFC2827(2000)	网络入口过滤:防范基于 IP 源地址伪造的拒绝服务攻击
IETF RFC3704(2004)	用于 Multihome 网络的入口过滤

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

路由器 Routers

路由器是通过转发数据包来实现网络互连的设备。路由器可以支持多种协议,可以在多个层次上转发数据包(例如数据链路层,网络层,应用层)。如果没有特殊指明,本标准的正文中路由器特指基于 TCP/IP 协议簇,工作在 IP 层上的网络设备。

路由器需要连接两个或多个由 IPv6 链路本地地址或点到点协议标识的逻辑端口,至少拥有一个物理端口。路由器根据收到的数据包中网络层地址以及路由器内部维护的路由表决定输出端口以及下一条路由器地址或主机地址并且重写链路层数据包头。

路由表必须动态维护来反映当前的网络拓扑。路由器通常通过与其他路由器交换路由信息来完成动态维护路由表。

路由器只提供数据包传输服务。为实现路由选择的通用性和鲁棒性(Robust),路由器的实现应使用最少状态信息来维持上述服务。

3.1.2

核心路由器 Core Routers

通常位于网络骨干层，用作扩大互联网的路由处理能力和传输带宽的路由器。在本标准中，要求核心路由器的系统交换容量至少达到 60Gbit/s。

3.1.3

访问控制 Access Control

防止未经授权使用资源。

3.1.4

授权 Authorization

授予权限，包括根据访问权进行访问的权限。

3.1.5

密钥管理 Key Management

根据安全策略产生、分发、存储、使用、更换、销毁和恢复密钥。

3.1.6

安全审计 Security Audit

对系统的记录及活动独立的复查与检查，以便检测系统控制是否充分，确保系统与现行策略和操作系统保持一致、探测违背安全性的行为，并介绍控制、策略和程序中所显示的任何变化。

3.1.7

数字签名 Digital Signature

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者证明数据的来源和完整性，保护数据不被伪造，并保证数据的不可否认性。

3.1.8

否认 Repudiation

参与通信的实体否认参加了全部或部分的通信过程。

3.1.9

可用性 Availability

根据需要，信息允许有权实体访问和使用的特性。

3.1.10

保密性 Confidentiality

信息对非授权个人、实体或进程是不可知、不可用的特性。

3.1.11

数据完整性 Data Integrity

数据免遭非法更改或破坏的特性。

3.1.12

安全服务 Security Service

由通信的系统提供的，对系统或数据传递提供充分的安全保障的一种服务。

3.1.13

安全策略 Security Policy

提供安全服务的一套规则。

3.1.14

安全机制 Security Mechanism

实现安全服务的过程。

3.1.15

拒绝服务 Denial of Service

阻止授权访问资源或延迟时间敏感操作。

3.1.16

防重放 Anti-Replay

防止对数据的重放攻击。

3.1.17

信息泄露 Information Disclosure

指信息被泄露或透漏给非授权的个人或实体。

3.1.18

完整性破坏 Integrity Compromise(Damage)

数据的一致性通过对数据进行非授权的增加、修改、重排序或伪造而受到损害。

3.1.19

非法使用 Illegal Use

资源被非授权的实体或者授权的实体以非授权的方式或错误的方式使用。

3.2 缩略语

下列缩略语适用于本标准。

3DES	Triple Data Encryption Standard	三重数据加密标准
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	先进加密标准
ARP	Address Resolution Protocol	地址解析协议
BGP	BGP-4 Border Gateway Protocol	边界网关协议
CAR	Committed Access Rate	承诺接入速率
CBC	Cipher Block Chaining	密码块链
CHAP	Challenge-Handshake Authentication Protocol	质询握手认证协议
CoS	Class of Service	业务类别
CPU	Central Processing Unit	中央处理器
DNS	Domain Name Service	域名服务
DoS	Denial of Service	拒绝服务
DSS	Digital Signature Standard	数字签名标准
HMAC	Hashed Message Authentication Code	散列消息认证码
ICMPv6	Internet Control Messages Protocol Version 6	互联网报文控制协议 版本6
IDEA	International Data Encryption Algorithm	国际数据加密算法

YD/T 1906-2009

IKE	Internet Key Exchange	互联网密钥交换
IPv6	Internet Protocol Version 6	互联网协议版本6
IPSec	Internet Protocol Security	互联网协议安全
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统协议
MAC	Media Access Control	媒介访问控制
MD5	Message Digest Version 5	消息摘要版本5
MODP	Modular Exponentiation Group	模求幂组
MPLS	Multi-protocol Label Switching	多协议标记交换
NTP	Network Time Protocol	网络时间协议
OAM&P	Operation, Administration, Maintenance and Provisioning	操作、管理、维护和配置
OSPF	Open Shortest Path First	开放最短路径优先协议
PAP	Password Authentication Protocol	口令认证协议
PFS	Perfect Forward Secrecy	完美前向保密
RIP	Routing Information Protocol	路由信息协议
PPP	Point-to-Point Protocol	点到点协议
RSA	Rivest, Shamir and Adleman Algorithm	RSA算法
SHA	Secure Hash Algorithm	安全散列算法
SHA-1	Secure Hash Algorithm 1	安全散列算法版本1
SNMP	Simple Network Management Protocol	简单网络管理协议
SNMPv1	SNMP version 1	SNMP版本1
SNMPv2c	SNMP version 2c	SNMP版本2c
SNMPv3	SNMP Version 3	SNMP 版本3
SSH	Secure Shell	安全外壳
SSHv1	SSH Version 1	SSH版本1
SSHv2	SSH Version 2	SSH版本2
SSL	Secure Socket Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLS	Transport Layer Security	传输层安全
UDP	User Datagram Protocol	用户数据报协议
URPF	Unicast Reverse Path Forwarding	单播反向路径转发
USM	User-based Security Model	基于用户的安全模型
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
VRF	VPN Routing and Forwarding	VPN路由和转发

4 概述

路由器通过转发数据报文来实现网络的互联，一般支持TCP/IP协议。核心路由器一般位于网络的核心，承担网络骨干段上数据的转发，具有较高的转发性能和较强的路由能力。

核心路由器在网络中处于重要位置，容易受到来自网络和其他方面的威胁。这些安全威胁可以利用设备的脆弱性对设备造成一定的损害。设备被攻击后，网络的性能和正常运行受到很大的影响。因此，核心路由器本身应具备较强的抗攻击能力。

此外，网络上传输的大量报文要通过路由器转发，因此核心路由器要为用户提供一定的安全服务，包括为企业的内部网络和公共网络提供安全服务。

核心路由器的主要功能是承担数据转发。为了完成这个功能，必须通过信令协议获得网络拓扑等信息。另外，核心路由器也要为管理员和网络管理系统提供管理接口，方便系统的管理和维护。因此，本标准将路由器功能在逻辑上划分为三个功能平面。

(1) 数据转发平面：主要指为用户访问和利用网络而提供的功能，如数据转发等。

(2) 控制平面：也可以称为信令平面，主要包括路由协议等与建立会话连接、控制转发路径等有关的功能。

(3) 管理平面：主要指与OAM&P有关的功能，如SNMP、管理用户Telnet登录、日志等，支持FCAPS（Fault, Capacity, Administration, Provisioning, and Security）功能。管理平面消息的传送方式有两种：带内和带外。

为了抵御网络攻击，核心路由器应提供一定的安全功能。本标准引用GB/T 18336.2中定义的安全功能并应用到核心路由器中，这些安全功能包括：

- 标识和鉴别，确认用户的身份及其真实性；
- 用户数据保护，和保护用户数据相关的安全功能和安全策略；
- 系统功能保护，安全数据（完成安全功能所需要的数据，如用户身份和口令）的保护能力；
- 资源分配，对用户资源的使用进行控制，不允许用户过量占用资源造成的拒绝服务；
- 安全审计，能够提供日志等审计记录，这些记录可以用来分析安全威胁活动和对策；
- 安全管理，安全功能、数据和安全属性的管理能力；
- 可信信道/路径，核心路由器之间以及核心路由器同其他设备之间通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来；
- 系统访问，本安全功能要求控制用户会话的建立。

路由器安全框架如图1所示。

为了保证核心路由器及其转发数据的安全，需要为核心路由器制定安全策略，作为指导安全功能实施的纲领，并在实施过程中，将安全策略映射到数据转发平面、控制平面和管理平面中的安全功能和实现技术。

硬件系统和操作系统是核心路由器本身的安全的重要因素，对硬件系统和操作系统的要求参见附录A。

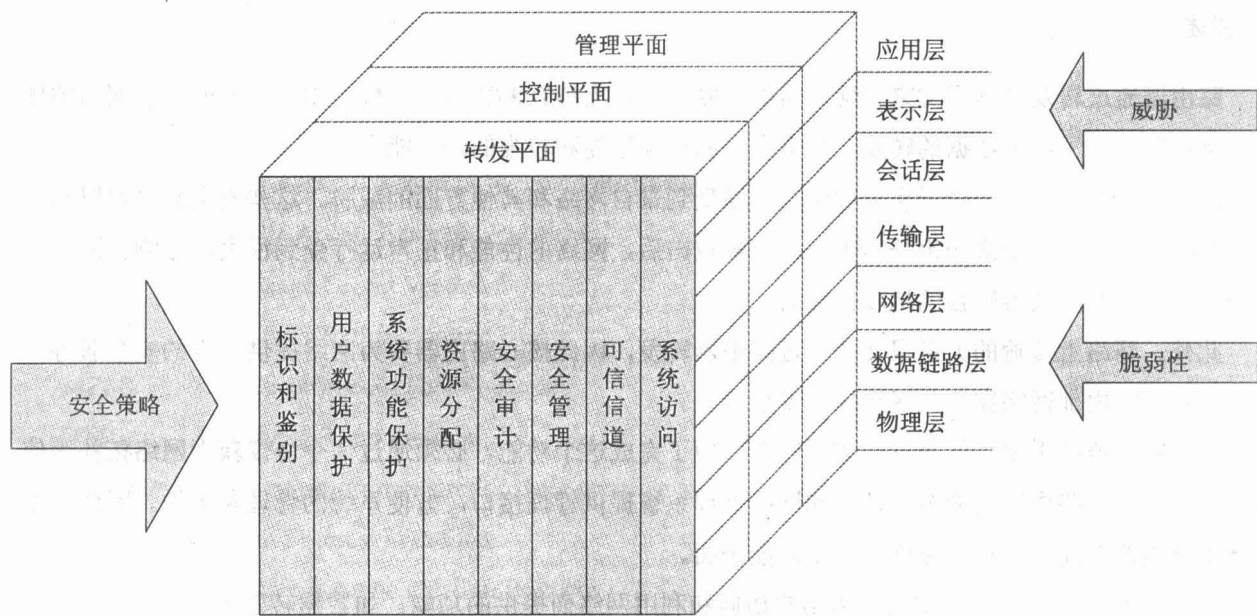


图1 路由器安全框架

5 数据转发平面安全

5.1 安全威胁

数据转发平面负责处理进入设备的流量，因此基于流量的攻击会给路由器的转发带来影响，例如，大流量攻击会造成设备不能正常处理合法流量，而畸形的报文可能会占用设备大量的处理时间，非授权用户可能使用网络资源，造成网络的可用性降低，甚至崩溃。

未授权观察、修改、插入、删除报文，对数据流的流量分析，都会使报文和数据流的保密性和完整性受到影响。

对数据转发平面的安全威胁主要有以下方面，但并不局限于这些方面：

- 对数据流的流量分析，从而获得敏感信息；
- 未授权观察、修改、插入、删除数据流；
- 拒绝服务攻击，降低设备的转发性能。

5.2 安全功能

5.2.1 标识和鉴别

核心路由器提供用户访问控制能力，通过标识和鉴别功能决定用户的身份，并通过授权系统向每个用户分配相应的权限，相关能力要求参见 YD/T 1454-2006《IPv6 网络设备技术要求——支持 IPv6 的核心路由器》。

5.2.2 用户数据保护

用户数据保护功能实现对用户数据的完整性、可用性和保密性保护。

完整性、可用性和保密性一般可以通过验证技术和加密技术获得，如IPSec，也可以通过隔离用户流量，不允许一个用户访问其他的用户数据来实现。

通过VPN能够实现将属于不同管理域的用户进行隔离，能够防止一个管理域的用户访问另外一个管理域的数据，也是用户数据保护的一个重要机制。

5.2.2.1 用户数据保护

IPSec在IP层上为IP报文提供安全保证, IPSec提供了数据保密性、数据源认证、数据完整性和抗重放等安全服务。IPSec是一个IP安全体系, 由IPSec框架、AH和ESP安全协议以及IKE 密钥管理协议组成。

核心路由器可支持IPSec协议。当支持IPsec协议时, 对IPSec的特性要求如下:

- 应支持AH和ESP协议,对于这两种协议, 应支持隧道和传送两种封装模式, 可支持AH和ESP协议的嵌套封装;

- AH和ESP协议应支持HMAC-SHA1-96算法, 可支持HMAC-SHA1-96认证算法, ESP协议应支持3DES-CBC、AES等加密算法, 可支持国家相关部门规定的加密算法, 应支持空加密算法和空认证算法, 但二者不应同时使用。

对IKE的特性要求如下:

- 支持安全联盟的手工管理, 可支持IKE自动管理。手工管理安全联盟时, 可支持以十六进制配置算法所需密钥, 应支持任意长度字符串形式配置密钥;

- 第一阶段应支持主模式和野蛮模式, 第二阶段应支持快速模式, 还应支持信息交换;

- 第二阶段交换中应支持完美前向保护特性;

- 第一阶段中应能指定发起模式;

- 应支持预共享密钥认证方式, 可实现RSA加密nonce验证和数字证书认证方式;

- 应支持HMAC-MD5-96和HMAC-SHA1-96认证算法, 支持MD5和SHA1散列算法, 应支持3DES-CBC和AES等加密算法, 可支持国家相关部门规定的加密算法;

- 密钥交换应支持MODP-Group1、MODP-Group2等Diffie-Hellman组。

5.2.3 系统功能保护

对于用户的安全数据, 系统要提供妥善的保护手段, 包括对访问安全数据的用户进行标识和鉴别。

5.2.4 资源分配

用户能够占用的网络资源数量和方式对网络的可用性有很大影响, 所以核心路由器必须要提供资源分配能力, 包括抗大流量攻击能力、抗畸形包处理能力和流量控制能力。访问控制列表和流量控制能够有效限制非法的用户资源访问。

5.2.4.1 常见网络攻击抵抗能力

针对已知的各种攻击, 核心路由器设备应能够进行处理, 并且不影响路由器正常的数据转发。当核心路由器检测到攻击发生, 应该生成告警。下面几种常见的攻击, 核心路由器应也能够处理。

5.2.4.1.1 抗大流量攻击能力

大流量可以分成两种类型, 一种是流经流量, 即需要宽带接入服务器转发的流量, 对于这类攻击, 核心路由器宜具有端口线速转发的能力, 对于超过端口处理能力的流量可以采用按比例丢弃的策略; 另一种流量的目的地就是核心路由器本身, 这类攻击可能会占用被攻击设备的大量CPU处理时间和内存, 严重的甚至会造成设备崩溃, 导致中断无法为用户提供正常服务。对这类攻击流量, 核心路由器可采取过滤和丢弃策略, 同时应将必要的信息(如报文类型、源地址以及攻击时间等)记录到安全日志中, 同时路由器还应完成路由协议和管理报文的正常发送和接收处理。

5.2.4.1.2 抗畸形包能力

由于网络环境的复杂性以及恶意攻击、用户好奇和病毒等, 也可能由于传输链路本身被干扰和程序处理错误等原因, 会导致网络上出现各种各样的错误报文和畸形报文。这些报文如果不能妥善处理, 往

往会造成路由器设备瘫痪、崩溃，失去服务能力。路由器设备不断发生崩溃恢复的过程可能导致整个网络处于不稳定状态，所以核心路由器设备应具有良好的畸形报文处理能力：

- 核心路由器应能够检测超短/长报文并采取丢弃策略，同时对这种报文进行统计；
- 核心路由器应能够检测到链路层错误报文并采取丢弃策略，同时要求进行日志记录和统计；
- 核心路由器应能够检测网络层报文错误并采取丢弃策略，同时必须进行错误报文统计；
- 核心路由器对各种路由器必须处理的上层协议报文错误应能够检测出来并采取丢弃策略，同时进行统计；
- 核心路由器不能由于错误报文/畸形报文而崩溃；
- 核心路由器本身不应发出错误报文/畸形报文。

5.2.4.1.3 IP 地址哄骗防范

针对网络中源地址哄骗报文，核心路由器应实现单播逆向路径转发（uRPF）技术来过滤这类报文，禁止其在网络中传播。

5.2.4.2 流量控制

核心路由器需要转发大量的网络流量，其中一些流量的目标可能是攻击网络中其他设备，核心路由器应提供流量控制能力，为网络提供安全保护服务。

对流量控制需要通过访问控制列表的方式实现，关于访问控制列表的具体要求参见5.2.8.2节，本标准要求在启动大量访问控制列表的情况下不能影响核心路由器的线速转发能力。

5.2.4.2.1 流量监管

流量监管也就是通常所说的CAR，是流分类之后的动作之一。通过CAR可以限制从网络边缘进入的各类业务的最大流量，控制网络整体资源的使用，从而保证网络整体的可靠运行。针对可能被攻击的流都应制定服务水平协议（SLA）。SLA中包含每种业务流的流量参数：承诺速率、峰值速率、承诺突发流量和峰值突发流量，对超出SLA约定的流量报文可指定给予通过、丢弃或降级等处理。此处降级是指提高丢弃的可能性，降级报文在网络拥塞时将被优先丢弃，从而保证在SLA约定范围内的报文享受到SLA约定的服务。

5.2.5 安全审计

对于用户流量，核心路由器要求能够提供流量日志能力，相关的要求见7.2.5节。

5.2.6 安全管理

要能够提供对本章提供的安全功能和数据的管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

5.2.7 可信信道/路径

核心路由器间以及核心路由器同其他设备间通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

VPN能够将VPN内的用户数据同VPN外部或其他VPN的数据隔离开来，能够提供可信的通信信道/路径，对VPN功能的要求见5.2.8.3节。

5.2.8 系统访问

5.2.8.1 过滤功能

应支持IETF RFC 2827和IETF RFC 3704规定的包过滤器。

5.2.8.2 访问控制列表

访问控制列表（ACL）是基于报文的内容，如MAC地址、IP地址、协议和端口等，指定的安全规则表，对每个进出路由器的报文通过与这些规则匹配，确定对其处理动作。

ACL在定义上应分为两级，第一级称为规则组，第二级称为规则。使用时以规则组为单位，每个规则组由一系列规则组成，规则和规则组共同完成对某类报文的访问控制功能。ACL规则组应支持使用数字或者字符串作为标识，以便于使用。ACL规则组可支持设定内部规则在查找时的匹配顺序，至少实现按照配置顺序查找。

ACL规则是对报文进行分类的实际依据，核心路由器支持的ACL规则要求如下：

- 支持基于源地址、目的地址、协议类型、源端口号、目的端口号等元素的访问控制；
- 可支持基于源MAC地址的访问控制；
- ACL规则中定义，同时指定匹配时应执行的动作：允许或禁止；
- ACL规则应提供选项，支持对ICMPv6报文过滤；
- 可支持基于IPv6 头部的流量类别域和流标签域过滤；
- 应支持对报文优先级过滤；
- 可支持仅在指定的时间段对报文过滤；
- 可支持对报文匹配情况统计计数和记入日志等。

在核心路由器中，每端口可支持1k项或每接口板可支持4k以上的ACL规则，而不使性能明显下降。

5.2.8.3 VPN 功能

VPN利用公共网络的资源，建立虚拟的专用网络，利用VPN可以实现不同专用网络用户流量的隔离。

核心路由器应根据设备处于网络不同位置，支持相应的VPN技术和特性，对于基于MPLS实现的VPN：

- 不管是L2 VPN还是L3 VPN，数据应严格基于标签沿着LSP转发，除非需要，一个VPN的数据不应被发送到该VPN之外，一个VPN的数据不应进入到另一个VPN；
- 当同时支持VPN服务和互联网服务时，特别是在同一个物理接口上通过不同的逻辑接口支持VPN服务和互联网服务时，可基于逻辑接口对接入速率进行限制。

6 控制平面安全

6.1 安全威胁

对控制平面的安全威胁主要有以下几个方面，但并不局限于这些方面：

- 对协议流进行探测、或者进行流量分析，从而获得转发路径信息；
- 获得设备服务的控制权，暴露转发路径信息，包括将转发路径信息暴露给非授权设备，一个VPN转发路径信息暴露给另一个VPN等；
- 利用协议流实施的拒绝服务攻击；
- 非法设备进行身份哄骗，建立路由协议的信任关系，非法获得转发路径信息；
- 针对路由协议、MPLS标签分配协议等的转发路径信息的欺骗。

6.2 安全功能

6.2.1 标识和鉴别

控制平面的信息应验证数据源的身份，只有其来源于验证通过的数据才被接受，路由协议应提供这个功能。

6.2.1.1 ND 用户认证

当用户通过邻居发现（ND）协议自动配置IPv6地址时，路由器应能对该类用户进行认证，认证方式可采用本地认证、RADIUS认证等。

6.2.1.2 PPP 用户认证

PPP作为一种数据链路层协议，本身并不具备完善的安全能力。其认证阶段应选用CHAP协议，而不能选用明文口令的PAP协议，以避免用户口令被侦听。

6.2.1.3 路由认证

路由的安全是路由器执行正常功能的重要基础。动态路由协议可以分为IGP和EGP两类，对于核心路由器，目前广泛采用的IGP有OSPFv3和IS-ISv6协议，EGP主要是BGP4+协议。其中：

- OSPFv3应支持协议报文的MD5 认证，在实现上应依赖IP认证头和IP安全载荷封装头来提供交互实体的鉴别和路由交互信息的完整性和保密性；

- IS-ISv6应支持明文认证和MD5认证，应实现基于链路、Level1和level2域的认证；

- BGP-4+应支持协议报文的MD5认证，应通过使用TCP MD5签名选项来保护BGP会话。

对于MPLS，用于建立LSP的标记分配协议主要有RSVP-TE和LDP/CR-LDP两种。

- LDP/CR-LDP

发现交换过程使用的消息由UDP协议承载，对于基本Hello消息，核心路由器应只接受与可信LSR直接相连的接口上的基本Hello消息，忽略地址不是到该子网组播组的所有路由器的基本Hello消息；对于扩展Hello消息，可利用访问列表控制只接受允许的源发送来的扩展Hello消息。LDP会话过程使用的消息由TCP协议承载，应通过TCP MD5签名选项对会话消息进行真实性和完整性认证。

- RSVP-TE

应通过加密的散列算法支持实体的认证，从而实现逐跳的认证机制，应支持HMAC-MD5算法和HMAC-SHA1算法。

6.2.2 用户数据保护

对于控制平面的信息，应能够防止恶意用户篡改，因此对控制数据要提供完整性保护，路由协议应支持对路由信息的完整性验证，如路由协议本身的验证机制。此外，也可以采用通用安全协议来保护控制信息，如用IPSec为BGP协议提供保密性和完整性保护。

6.2.3 系统功能保护

安全数据应要得到妥善的保护。

6.2.4 资源分配

核心路由器中控制信息数量相对于用户数据要少，但是核心路由器要具有能够拒绝明显的利用控制信息过量耗用资源的能力，如策略路由和路由过滤能力。此外，一些攻击利用控制协议及其实现技术上的安全缺陷，对核心路由器发起攻击，造成通信和设备故障。核心路由器要具备抵御此类攻击的能力，包括能够关闭一些不常用但是容易被攻击者利用的IP服务。

6.2.4.1 关闭一些 IP 服务

6.2.4.1.1 ICMPv6 协议

ICMPv6用于网络操作和排障，核心路由器需要实现ICMPv6协议的一些功能，但设备应具有关闭这些功能的能力。这些ICMP消息类型包括：

- Type = 1 目的地不可达；
- Type = 2 分组过大；
- Type = 3 超时；
- Type = 4 参数错误；
- Type = 128 回显请求；
- Type = 129 回显应答。

路由器可按照ICMPv6消息的类型、源、目的地址类型和范围（单播、组播，本地链路、全局）或者是错误消息的错误码对ICMPv6消息进行过滤。

6.2.4.1.2 重定向功能

路由器应能够关闭路由重定向功能，避免攻击者通过路由重定向截取用户数据。

6.2.4.1.3 其他服务

对于下列TCP和UDP小端口服务，应缺省关闭这些服务，或者不提供这些服务：

- Echo；
- Chargen；
- Finger；
- NTP等。

6.2.5 安全审计

对控制平面的信息要提供日志记录功能，特别是对设备的路由表等重要数据有影响的控制数据，关于日志的要求见7.2.5节。

核心路由器可以支持端口镜像功能，通过配置，将系统中某个端口的部分或全部流量镜像到其他端口，出方向的报文和入方向的报文可以分别镜像到不同的端口。

端口镜像时，对报文不作修改，有如下两种镜像方式：

- 一对一端口镜像，把一个端口的流量全部原封不动地拷贝到指定的镜像端口；
- 多对一端口镜像，从多个端口上分别拷贝部分流量到指定的镜像端口。

6.2.6 安全管理

要能够提供控制平面的安全功能和安全数据管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

6.2.7 可信信道/路径

核心路由器之间以及核心路由器同其他设备之间的控制信息通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

6.2.8 系统访问

控制平面的系统访问应建立在对控制信息及其数据源的标识和验证的基础上，对于不能通过验证的数据源，来自该数据源的报文被丢弃，并记录在本地或远程的日志系统中。

对于MPLS VPN，VPN内部的控制信息在VPN之间和VPN与MPLS骨干之间应该相互隔离，互不干扰。

6.2.8.1 路由过滤

路由过滤可以控制路由协议对路由信息的发布和接收，可以只发布某些指定的路由，也可以只接收符合某些条件的路由，这样可以在满足需要的前提下减少路由器的资源消耗，达到更好的性能，避免路由攻击。在接收和发布路由信息时，应支持按IP地址、自治系统路径、团体属性进行过滤。

6.2.8.2 MPLS VPN

6.2.8.2.1 L2 VPN

— VPN之间MAC 地址和VLAN 信息应相互隔离，VPN之间或VPN和MPLS骨干之间应可以复用MAC地址空间和VLAN空间。

— 除非需要，VPN之间或VPN和MPLS骨干之间的交换信息应相互隔离。

— 可实现VPN使用的路由器资源（如CPU、内存等）的相互隔离，防止因一个VPN独占资源而造成的对于其他VPN的DoS攻击。

6.2.8.2.2 L3 VPN

常用的L3 VPN技术是BGP/MPLS VPN，BGP/MPLS VPN实质上是通过BGP协议约束路由信息分配的MPLS，对L3 VPN要求如下：

— 应支持静态路由算法和动态路由算法。对于动态路由算法，建议具有在接口上过滤路由更新的能力，IGP和EGP路由协议都应支持MD5认证，并可基于VRF实例限制路由更新的速度。

— VPN之间的拓扑和编址信息应相互隔离，一个VPN应能使用所有互联网地址范围，VPN之间或VPN和MPLS骨干之间应可以复用IP地址空间。

— 应为每个VPN维持一个独立的VRF实例，除非需要，VPN之间或VPN和MPLS骨干之间的路由信息及其分发和处理应相互独立，互不干扰。

7 管理平面安全

7.1 安全威胁

对管理平面的安全威胁主要有以下方面，但并不局限于这些方面：

- 对数据流进行流量分析，从而获得设备有关的系统配置信息；
- 未授权观察、修改、插入、删除数据流。
- 未授权地访问管理接口，控制整个设备。
- 利用管理信息流实施拒绝服务攻击。

7.2 安全功能

7.2.1 标识和鉴别

对设备的管理用户都需要标识和鉴别，标识和鉴别是系统访问的基础。

7.2.1.1 Telnet 访问

核心路由器应支持Telnet访问功能。Telnet访问时应提供用户身份验证和对用户账号的分级管理机制。能够限制Telnet连接的数量，Telnet访问应提供终端超时锁定功能，还要支持对Telnet用户权限的控制功能。能够对针对Telnet的密码试探攻击进行防护，可对同一个IP地址使用延时响应机制，也可利用限定来自同一个IP地址的登录尝试次数。

7.2.1.2 串口访问

核心路由器可支持串口访问功能。串口访问时应提供用户身份验证和对用户账号的分级管理机制。串口访问应提供终端超时锁定功能。

7.2.1.3 SSH 访问

SSH是在不安全的网络上为远程登录会话和其他网络服务提供安全性的一种协议，对SSH服务的要求如下：

- 应支持SSHv1和SSHv2两种版本；
- 用户应通过身份验证才能进行后续的操作，用户地址和操作记入日志，核心路由器应支持口令验证，可支持公钥验证，可实现基于主机的验证；
- SSH服务器可采用验证超时机制，在超时范围内没有通过验证应断开连接，可限制客户端在一个会话上验证尝试的次数；
- SSHv2应支持用于会话的加密密钥和验证密钥的动态管理，支持Diffie-Hellman组14的密钥交换，在密钥交换过程中协商密钥交换算法、对称加密算法和验证算法等，并对服务器端进行主机验证；
- 应支持HMAC-SHA1验证算法，可支持HMAC-SHA1-96验证算法，可实现HMAC-MD5、HMAC-MD5-96等验证算法；
- 应支持3DES-CBC对称加密算法，可实现Blowfish-CBC、IDEA-CBC、CAST128-CBC、AES256-CBC、AES128-CBC等对称加密算法；
- 对于不对称加密算法，应支持SSH-DSS，可实现SSH-RSA；
- 可限定用户通过哪些IP地址使用SSH服务对设备进行访问；
- 应支持必要时关闭SSH服务。

7.2.1.4 SNMP 安全性

SNMP是最常用的网络管理协议，它提供了网管站和位于被管设备中的代理之间的通信接口。因为网络管理能够改变设备的配置、了解设备的运行状况和运行参数，所以网络管理接口的安全性就非常重要。

SNMPv1本身只能提供非常弱的安全保护能力，在SNMPv1中代理和管理站之间的通信除依靠团体串验证外不作任何安全设置，一旦团体串被泄漏，则会给网络设备带来很大的安全风险。此外，经验丰富的黑客可以对SNMP报文进行截获。如在适当的时候发送报文则会造成网络设备异常，如其恶意更改报文内容并进行发送，则给网络带来的安全威胁更大。

SNMPv2提供了一定的安全机制，但是没有得到广泛的实施，不支持SNMPv2安全机制的实现成为SNMPv2c。

SNMPv3是一个安全的网络管理协议，能够提供支持基于视图的访问控制（VACM）和基于用户的安全模型（USM）等安全机制，能够提供完善的安全保护。

核心路由器可支持SNMPv1、SNMPv2c，但是应提供禁用功能，并且缺省应该是禁用的。核心路由器应支持SNMPv3的网络管理接口。提供SNMPv1和SNMPv2c应可以和访问控制列表相结合，控制非法网管接入设备，同时不使用Public/Private作为缺省团体名，缺省只读团体名和读写团体名称不能够相同，并且在适当的时机提示管理员修改团体名。

7.2.2 用户数据保护

对于管理数据要能够提供保护能力，如SSH和SNMPv3通过本身的数据保护机制实现管理数据的完整性或/和保密性。

7.2.3 系统功能保护

与管理相关的安全数据应得到妥善的保护。

7.2.4 资源分配

管理数据是系统运行的重要数据，系统要保证管理系统获得足够的运行资源，但是不能因此显著影响控制平面和数据转发平面的正常工作。此外，通过管理平面提供的设备补丁下载功能应该得到严格的管理，不应该被用来对设备资源实施恶意占用。

管理平面的资源分配安全参见5.2.4节。

7.2.5 安全审计

管理平面不仅要应提供安全日志功能，如用户操作日志，同时可提供日志分析功能或具备为日志分析提供接口的能力。

7.2.5.1 安全日志

安全日志作为核心路由器重要的输出信息，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。安全日志应按信息的严重等级或紧急程度划分等级，越紧急的日志，严重等级越高。核心路由器应该提供按信息严重等级来进行日志过滤的功能，当向管理员或其他系统提供日志信息的时候，能将严重等级小于所设置阈值的日志过滤。安全日志的严重等级定义可以参考附录B。

核心路由器的安全日志应包括安全事件来源、发生时间和事件描述等内容。

核心路由器设备可提供不借助外部服务器的情况仍然能够记录核心路由器的所有操作记录，同时操作记录应受到保护，只有具有最高权限级别的用户才可能对该记录进行删除操作。同时核心路由器应能够将日志记录保存在本地系统的缓冲区内，也可以发送到专用的日志主机上作进一步处理。

7.2.5.2 操作用户日志

网络设备在运行过程，对网络设备的所有的针对网络设备本身的用户活动都应给予记录，因为在网络设备运行过程中，可能遇到来自外部的密码探测，试图突破网络设备的密码防护并接入到网络设备，从而控制网络设备从事非法活动，也可能有内部员工，通过更改路由器配置来破坏网络安全。因此应提供用户活动记录功能，核心路由器由于网络地位重要，应能够支持该功能。

核心路由器应实现用户登录和操作命令记录功能，记录的内容应包括登录用户名、IP地址、登录时间和退出时间等，同时该用户的所有操作命令应被记录下来，保存在不易失介质中，并提供显式备份功能。用户操作命令的记录信息应该包括命令、命令时间、执行该命令的用户和对应该用户登录的IP地址。

核心路由器设备应提供不借助外部服务器的情况仍然能够记录自核心路由器的所有操作记录，同时操作记录应受到保护，只有具有最高权限级别的用户才允许对该记录进行删除操作。

同时核心路由器应能将日志记录保存在本地系统的缓冲区内，也可发送到专用的日志主机上作进一步处理。

7.2.5.3 基于流的采样

为了提高网络安全性，核心路由器设备可提供基于流的采样功能，利用采样可以对路由器转发的数据报文进行监视，作为一种安全检测手段了解业务运行状况，如配置采样监测具有特定目的地址的报文，可分析对关键服务器的访问流量，发现可能的安全隐患。

采样（Sampling）具有对特定流上的数据包进行采集、分析的功能，将采样的数据报文的报文头部分保存或者发送到网管系统，由网管系统对报文进行分析、统计工作，配置一个采样流可按照如下方式实现：

- 定义一个采样规则，以及相应的ACL；
- 定义采样比率，如每100个报文采集多少个报文；
- 定义一个时间段（可选）；
- 定义保存在本地还是发送到网管工作站；
- 应用到全局或端口。

采样功能记录的信息包括：

- Dest addr，报文头中的目的IPv6 地址；
- Src addr，报文头中的源IPv6地址；
- Dest port，报文头中的TCP或UDP的目的端口号；
- Src port，报文头中的TCP或UDP的源端口号；
- Protocol，报文头中的协议类型；
- Traffic class，报文头中的Traffic class域；
- Pkt len，以byte为单位的报文长度；
- Interface num，进行采样的端口号；
- Time，报文到达的时间。

7.2.5.4 用户流统计

核心路由器应该能够提供基于接口的流量信息，提供各种异常错误报文统计信息。

核心路由器可以通过网络管理接口或其他管理接口将统计数据传输给网络管理系统或其他的管理系统。

7.2.6 安全管理

要能够提供安全功能和安全数据管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

7.2.6.1 口令管理

核心路由器涉及的口令长度应不短于8个字符，并且由数字、字符或特殊符号组成，核心路由器可提供检查机制来保证每个口令至少是由前述3类字符中的两类组成。

7.2.7 可信信道/路径

管理系统同设备之间的通信信道/路径应保证安全，采用的机制包括但不限于专用物理信道、专用逻辑信道或加密信道。

因为带内管理本身的潜在的安全问题，核心路由器可提供带外管理能力，保证网络管理的通信流量同一般的数据流量隔离，隔离方式包括但不限于独立的网络管理物理端口、MPLS 隧道和IPsec隧道。

可以限制只通过指定接口来管理设备，禁止通过其他非指定接口管理设备，而且应进行身份验证，并根据访问控制列表进行过滤。

对于专门的网络管理接口，对目的地址为设备本身的非管理报文应严格控制，比如禁止或限制到路由器的ICMP 报文种类，限制路由器发出的ICMP 报文种类。限制到数据转发接口的报文。

7.2.8 系统访问

标识和验证功能是系统访问控制的基础，一些通信协议的系统访问可以参见6.2.1 节。

7.2.8.1 设备的访问控制

路由器需提供管理功能来配置设备，管理员能够登录到路由器上维护和管理设备。路由器应能够对管理员用户的访问实现控制：

- 登录到路由器应验证身份；
- 不允许使用不安全的口令登录路由器，如单词作为口令；
- 用户所有的写操作都应有日志；
- 对于不同等级的用户，允许的操作类型和操作对象集合应是不完全相同的。

7.2.8.2 版本管理的控制

核心路由器可提供完善的补丁或版本权限管理功能，缺省情况下应设定为关闭该功能，启用该功能的用户权限应该具有核心路由器的最高管理权限级别才能执行在线升级功能。

附录 A

(规范性附录)

硬件系统和操作系统的安全要求

A.1 硬件系统

硬件系统主要包括硬件系统设计、密钥及系统程序保护设计等方面。

A.1.1 硬件系统设计

- 在安全性要求比较高的场合,对与安全有关的元器件建议尽量采用具有自主知识产权的国产元器件,国内无法生产的元器件可进行安全性测试后使用。
- 可采用模块式的硬件结构,将涉及到安全的功能模块与通用模块分割处置,部分关键模块可使用物理遮盖的方法进行保护,或者采用国家有关管理部门批准使用的安全硬件系统。
- 对硬件系统的设置可采用强身份认证机制保护。
- 对于管理平面,可提供一个专用的管理接口,以用于建立专用的管理网络,实现管理和业务网络的物理隔离。
- 各类安全告警信号可使用多种标示方式,如由打印机打印,在显示终端上显示,且能用不同彩色或其他方式显示出各类安全告警信号的严重程度。

A.1.2 密钥及系统程序保护设计

- 对安全性要求较高的场合,核心路由器的密钥存储、运算和系统关键程序可在硬件系统中单独设计,与系统其他部分物理分割,推荐使用遮盖或胶封等方法进行物理保护。
- 对于以明文存储的密钥可进行分割存储,其他密钥或证书可加密存储,并提供单独的存储空间。
- 可提供密钥销毁功能。可通过菜单操作或某种直观的操作直接销毁硬件中存储的密钥和算法或系统的关键程序。在更进一步的安全要求下,可提供设备开箱自毁功能,即在外力强迫打开机箱时,系统提供对密钥、算法和关键程序的销毁功能。

A.2 操作系统

- 推荐使用专用的操作系统,并对操作系统进行固化,禁止一些不常用的服务和应用,采用的操作系统不应有后门。建议不使用通用操作系统。
- 对加密ASIC 所使用的驱动程序应经过国家有关管理部门的测试,并可在核心路由器内定义到具体的内存、进程上下文。
- 对命令集的结构进行缜密的设计以及对输入的参数进行全面的检查处理。
- 对路由器资源的访问要能够进行权限限制和级别限制,如对管理员用户进行分级,为不同的管理员用户定义不同的管理能力,“网络管理员”用户可显示和修改配置和接口参数,而“操作员”用户只能清除连接和计数器。
- 对各个进程及使用资源进行审计,应提供基于用户的审计功能,用户审计功能应记录用户的登录行为、用户对设备的操作行为等。
- 应具有备份版本、配置、日志记录等功能。

附 录 B
(资料性附录)
安全日志的严重等级定义

显示值	严重等级	描 述
1	Emergencies	极其紧急的错误
2	Alerts	需立即纠正的错误
3	Critical	关键错误
4	Errors	需关注但不关键的错误
5	Warnings	警告, 可能存在某种差错
6	Notifications	需注意的信息
7	Informational	一般提示信息
8	Debugging	调试信息
