

ICS 33.040.40  
M 32



# 中华人民共和国通信行业标准

YD/T 1907-2009

---

## IPv6 网络设备安全技术要求 ——边缘路由器

Security Requirements of Edge 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.....4

5 数据转发平面安全.....5

6 控制平面安全.....8

7 管理平面安全.....11

附录 A（规范性附录） 硬件系统和操作系统的安全要求.....14

## 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——边缘路由器》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。

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

## ——边缘路由器

### 1 范围

本标准规定了支持 IPv6 协议的边缘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 的边缘路由器的规定。

本标准适用于支持 IPv6 的边缘路由器设备。

### 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

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跳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

##### 边缘路由器 Edge Routers

位于网络边缘，用作接入边缘网的路由器。除非特别指出，边缘路由器应符合 3.1.1 中路由器的要求。

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
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

边缘路由器通常位于网络边缘，往往是专用网络和骨干网络的接入点，所以它是网络攻击从专用网攻击外部网络（包括骨干网络和其他专用网络）或者利用外部网络攻击专用网络的必经之路，在接入网络解决一些安全问题是整个网络安全体系的重要组成部分。

路由器功能在逻辑上可以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，边缘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边缘路由器中，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，边缘路由器之间以及边缘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。

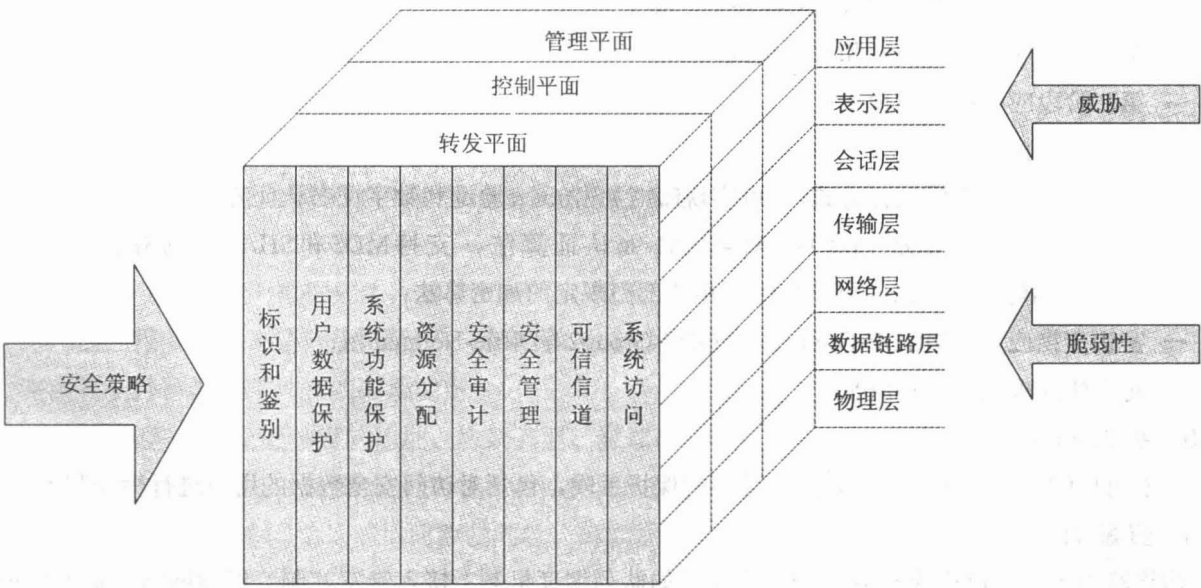


图1 路由器安全框架

硬件系统和操作系统是边缘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。

5 数据转发平面安全

5.1 安全威胁

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；
- 未经授权观察、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

边缘路由器位于网络边缘，需要对接入网络的数据源进行检查和确认，保证报文来自可信/合法的用户或设备。

### 5.2.2 用户数据保护

#### 5.2.2.1 IPsec 功能

IPSec在IP层上提供数据保密性、数据源认证、数据完整性和抗重放等安全服务，由AH、ESP和IKE等协议组成。

边缘路由器可支持IPSec协议，对IPSec的特性要求如下：

- 应支持手工密钥管理，可选支持IKE自动密钥管理；
- 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-MD5-96和HMAC-SHA1-96认证算法，ESP协议应支持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，应支持空加密算法和空认证算法，但二者不应同时使用。

边缘路由器可支持IKE，对IKE的特性要求如下：

- 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；
- 应支持情报模式；
- 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；
- 对于快速模式，支持PFS。

### 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

边缘路由器应能够提供有效的控制机制（如队列调度机制、接入带宽控制）保障网络带宽的合理利用，特别是要能够抵御来自网络的各种侵占网络资源类的攻击，如Ping Flooding、TCP SYN Flooding等，要确保网络在遭受攻击的情况下仍旧能够为合法用户提供必需的数据转发服务。

边缘路由器应能够抵御以下的常见攻击类型，但并不局限于这些方面。

- 大流量攻击：大流量可以分成两种类型，一种是流经流量，即需要路由器转发的流量，对于这类攻击，边缘路由器应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边缘路由器本身，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，边缘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。

— IP地址哄骗：针对网络中源地址哄骗报文，边缘路由器可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。

边缘路由器应能够提供相应机制来控制同一用户建立TCP会话的数量，以防止用户过度消耗网络资源；而且应能够根据用户类型对能够建立的TCP会话数量进行配置。

边缘路由器应实现基于ACL的用户流量控制，通过CAR操作，对用户数据流进行整形，然后依据与用户签订的SLA协定，为用户分配带宽资源。SLA协议包含承诺速率、峰值速率，承诺突发流量、峰值突发流量等，对于超出SLA协定的流量可以采取降级、丢弃等操作。

### 5.2.5 安全审计

对于用户流量，边缘路由器要求能够提供流量日志能力，相关的要求参考7.2.5节有关规定。

### 5.2.6 安全管理

边缘路由器应能够提供对本章提供的安全功能和管理数据的管理能力，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

边缘路由器间以及边缘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功能的要求参考6.2.8.2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

访问控制列表是基于数据包头，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。

路由器支持访问控制列表的要求如下：

- 应支持基于源地址、目的地址、协议类型、源端口号、目的端口号的访问控制列表；
- 可支持基于IPv6头部的流量类别域和流标签域的访问控制列表；
- 可支持基于源MAC地址的访问控制列表，降低系统的无谓开销；
- 可支持在指定时间有效的访问控制列表；
- 应支持对报文匹配情况进行统计和产生日志等。

边缘路由器应支持同时配置2,000项以上的访问控制列表规则，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。边缘路由器支持利用以下技术实现VPN。

- L2TP隧道

应支持通过L2TP隧道技术实现VPN，应支持LAC和LNS功能，支持CHAP鉴别协议。

— IPsec 隧道

可支持通过IPsec隧道技术实现VPN，对IPsec的要求见5.2.2.1节。

— MPLS LSP

可基于MPLS LSP实现MPLS VPN，对MPLS VPN的要求如下：

— 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。

#### 5.2.8.4 防火墙功能

边缘路由器可支持防火墙功能，除包过滤、访问控制列表外，可支持应用代理功能，只允许被保护的网访问允许的网络应用，状态检测应检查网络层和传输层信息，还可检查应用层协议的信息，实时维护这些TCP或UDP的状态信息，使用这些状态信息，确定访问控制，边缘路由器可支持基于状态检测的包过滤功能。

## 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；
- 针对路由协议转发路径信息的欺骗。

### 6.2 安全功能

#### 6.2.1 鉴别与认证

##### 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，对于边缘路由器，目前广泛采用的IGP有OSPFv3和IS-ISv6协议，EGP主要是BGP4+协议。其中：

- RIPng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；

— 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,边缘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

### 6.2.2.1 路由认证

路由认证往往使用加密散列算法,在提供数据源认证的同时,也提供了数据完整性认证,路由认证功能参见6.2.1.3节。

### 6.2.3 系统功能保护

安全数据应得到妥善的保护。

## 6.2.4 资源分配

### 6.2.4.1 抗常见网络攻击

#### 6.2.4.1.1 URPF

URPF是通过在转发表中查找收到分组的源IP地址和接口,只转发源IP地址在IP路由表中存在的分组的一种技术,这种技术可以缓解基于IP地址哄骗的网络攻击,边缘路由器应支持URPF功能。

### 6.2.4.2 关闭一些 IP 服务

#### 6.2.4.2.1 ICMPv6 协议

ICMPv6用于网络操作和排障,边缘路由器需要实现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。

#### 6.2.4.2.2 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。

#### 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，关于日志可以参考7.2.5节。

边缘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；
- 多对一端口镜像。

#### 6.2.6 安全管理

##### 6.2.6.1 口令管理

边缘路由器涉及的口令长度应不少于8个字符，并且应由数字、字符或特殊符号组成，边缘路由器可提供检查机制，保证每个口令至少是由前述的3类符号中的两类组成。

##### 6.2.7 可信信道/路径

边缘路由器之间以及边缘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

##### 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、团体属性等进行过滤。

##### 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。

###### 6.2.8.2.2 L3 VPN

常用的L3 VPN技术是BGP/MPLS VPN，BGP/MPLS VPN实质上是通过对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应可以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。

### 6.2.8.3 防火墙功能

防火墙功能请参见5.2.8.4节。

## 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，对有关SNMP管理、Web管理、远程登录管理中用户认证的要求参见7.2.8节。

#### 7.2.2 用户数据保护

对于边缘路由器，一般使用以下远程管理方式。

- SNMP

应支持SNMPv3，支持USM等安全机制。

- 远程登录

可支持SSHv1和SSHv2，通过认证算法和加密算法实现对管理用户数据的保密性和完整性保护。

- Web管理

可通过支持SSL/TLS安全协议，实现对管理用户数据的完整性保护。

有关这3种远程管理方式的详细要求参见7.2.8.1、7.2.8.2、7.2.8.4等节。

#### 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。

#### 7.2.5 安全审计

日志应记录过滤规则拒绝访问、配置修改等安全相关事件，告警记录发生的安全违章事件，并可以一定的方式提示管理员，审计可对记录的安全事件进行回顾和检查，分析和报告安全信息，管理员基于该信息了解安全策略的执行情况，并据此进行修改。安全日志、安全告警等安全记录往往是安全审计的素材。

对日志的要求：

- 每个安全日志条目应包含事件的主体、发生时间和事件描述等；
- 应可以保存在本地系统的缓存区内，也可以发送到专用的日志主机上作进一步处理；

- 应可以实时打印在专用打印机或连接路由器的显示终端上，以备最坏的情况下使用（如日志主机因安全危害而不能使用）；

- 应定义日志的严重程度级别，并能够根据严重程度级别过滤输出；

- 应支持和日志主机之间的接口。

对告警的要求：

- 应定义告警的严重程度级别，并根据严重程度级别确定是否以一定的方式（如声光显示）提示管理员；

- 应支持告警输出到打印机或显示终端，可根据严重程度级别输出到不同的显示终端；

- 告警应保存在本地或通过网络存储到其他主机。

## 7.2.6 安全管理

### 7.2.6.1 口令管理

有关口令管理的要求参见6.2.6.1 节。

## 7.2.7 可信信道/路径

### 7.2.7.1 带外管理

由于带内管理面临的潜在的安全问题，边缘路由器可通过如独立的管理端口、VPN虚接口等方式支持专用的管理网络，将管理通信流和其他通信流量隔离。边缘路由器可提供关闭带内接口的能力，以实现只通过专用管理网络管理设备。

## 7.2.8 系统访问

### 7.2.8.1 SNMP 的安全性

SNMP是一种应用非常广泛的网络管理协议，主要用于设备的监控和配置的更改等，目前使用的SNMP协议有3个版本，分别是SNMPv1、SNMPv2c和SNMPv3。边缘路由器应支持安全性较好的SNMPv3作为网管协议。

此外，建议边缘路由器实现对网管站的访问控制，限定用户通过哪些IP地址使用SNMP对设备进行访问。

### 7.2.8.2 Telnet 访问

Telnet协议用于通过网络对设备进行远程登录。在边缘路由器中，如果为用户提供Telnet服务，则应满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；

- 应限制同时访问的用户数目；

- 在设定的时间内不进行交互，用户应自动被注销；

- 可限定用户通过哪些IP地址使用Telnet服务对设备进行访问；

- 必要时可关闭Telnet服务；

### 7.2.8.3 串口访问

边缘路由器应支持串口访问功能，应满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作；

- 在设定的时间内不进行交互，用户应自动被注销。

### 7.2.8.4 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；
- 用户应通过身份认证才能进行后续的操作，用户地址和操作记入日志，边缘路由器应支持口令认证，可支持公钥认证，可实现基于主机认证；
- SSH服务器可采用认证超时机制，在超时范围内没有通过认证应断开连接，可限制客户端在一个会话上认证尝试的次数；
- SSHv2应支持用于会话的加密密钥和认证密钥的动态管理，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、对称加密算法和认证算法等，并对服务器端进行主机认证；
- 应支持HMAC-SHA1认证算法，可支持HMAC-SHA1-96认证算法，可实现HMAC-MD5、HMAC-MD5-96等认证算法；
- 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；
- 对于非对称加密算法，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。

#### 7.2.8.5 Web 管理

Web管理基于HTTP协议，边缘路由器可支持Web管理，可满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- 可限定用户通过哪些IP 地址使用HTTP对设备进行访问；
- 必要时可关闭HTTP服务；
- 应支持SSL/TLS。

#### 7.2.8.6 软件升级

路由器一般使用FTP/TFTP协议实现设备的软件升级，软件升级包括软件版本、设备配置等，有本地和远程两种途径。软件升级通过建立FTP/TFTP服务器和客户端的连接来实现，FTP/TFTP协议应支持口令认证功能。

对于远程软件升级，可支持SSHv2，实现文件的安全传送。



## 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可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，边缘路由器的密钥存储、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，并可在边缘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”用户只能够清除连接和计数器。
- 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。