H3C SECPATH F 系列-CMW340-R1608

版本说明书

杭州华三通信技术有限公司

H3C SECPATH F 系列-CMW340-R1608 版本说明书

关键词： H3C, SecPath，防火墙，版本说明书

摘　要：本文档用以描述 SecPath F 系列版本说明，包括版本信息、变更说明书、存在问题以及规避措施、解决问题单、配套资料以及升级指导等内容。

缩略语：

缩略语	英文全名	中文解释
CMW	Comware	
VPN	Virtual Private Network	虚拟专用网
GRE	General Route Encapsulation	通用路由封装
IPSec	IP Security	IP 安全
IKE	Internet Key Exchange	因特网密钥交换
ASPF	Application State Packet Filter	应用层状态包过滤
NAT	Network Address Translation	网络地址转换
L2TP	Layer 2 Tunnel Protocol	二层隧道协议
SSL	Secure Socket Layer	安全套接层
VRRP	Virtual Route Redundant Protocol	虚拟路由冗余协议
ARP	Address Resolution Protocol	地址解析协议

目 录

表目录

1 版本信息

1.1 版本号

SecPath F100-M Comware software, Version 3.40, Release 1608

SecPath F1000-A Comware software, Version 3.40, Release 1608

SecPath F1000-S Comware software, Version 3.40, Release 1608

SecPath F100-A Comware software, Version 3.40, Release 1608

SecPath F100-E Comware software, Version 3.40, Release 1608

SecPath F100-S Comware software, Version 3.40, Release 1608

SecPath F100-C Comware software, Version 3.40, Release 1608

注：该版本号可在命令行任何视图下用 display version 命令查看，见注①

1.2 历史版本信息

表1 历史版本信息表

版本号	基础版本号	发布日期	备注
CMW340-R1608	CMW340-R1607P02	2007-04-21	
CMW340-R1607P02	CMW340-R1607P01	2007-03-08	其中 F100-M 首次发布
SECPATH1000FA-CMW340-R1607P01	CMW340-R1607	2007-02-07	只发布 F1000-A
CMW340-R1607	CMW340-R1606P01	2007-01-31	正式发布，解决 ASPF，Nat Server 等问题
CMW340-R1606P01	CMW340-R1606	2006-12-11	正式发布
CMW340-R1606	CMW340-R1605P03	2006-11-27	正式发布
CMW340-R1605P03	CMW340-E1605	2006-11-21	正式发布
CMW340-E1605	CMW340-E1604P03	2006-10-25	F 系列解决 IPSec 大包问题
CMW340-E1604P03	CMW340-E1604P01	2006-10-15	F 系列解决 IP-Spoof 配合 VPN 存在问题
CMW340-E1604P01	CMW340-E1604	2006-09-25	F 系列增加百兆口支持 Vlan 透传功能

1.3 版本配套表

表2 版本配套表

产品系列	H3C SecPath Series						
型号	SecPath F1000-A	SecPath F1000-S	SecPath F100-E	SecPath F100-A	SecPath F100-S	SecPath F100-C	SecPath F100-M
内存需求	最小 512M	最小 512M	256M	256M	128M	64M	256M
FLASH 需求	最小 16M	最小 16M	最小 16M	最小 16M	最小 8M	最小 8M	最小 16M
BOOTROM 版本号 (该版本号可在命令行任何视图下用 display version 命令查看，如 F100-C 见注②)	126 及以上	126 及以上	126 及以上	116 及以上	114 及以上	205 及以上	116 及及以上
目标文件名称	SECPATH1000FA-CMW340-R1608.bin	SECPATH100FS-CMW340-R1608.bin	SECPATH100FE-CMW340-R1608.bin	SECPATH100FA-CMW340-R1608.bin	SECPATH100FS-CMW340-R1608.bin	SECPATH100FC-CMW340-R1608.bin	SECPATH100FM-CMW340-R1608.bin
QUIDVIEW 版本号	SecPath F100-M 采用： Quidview DM 3.10-R3112P06 Quidview NMF 3.10-R3112P09 其余对应： Quidview DM 3.10-R3112 Quidview BIMS 3.10-R3112 Quidview VDM 3.10-R3112 Quidview VSM 3.10-R3112 Quidview NCC 3.10-R3112 Quidview NMF 3.10-R3112						
Xlog 版本号	XLog 2.10-R0120						
CAMS 版本号	不支持						

示例：查看 SecPath F100-C 的软件版本和 Bootrom 版本号方式如下：

```
[H3C]display version
H3C Comware Platform Software
 Comware software, Version 3.40, Release 1608------- 注①
 Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
 Without the owner's prior written consent, no decompiling
 nor reverse-engineering shall be allowed.
 H3C SecPath F100-C uptime is 0 week, 0 day, 0 hour, 19 minutes

  CPU type: PowerPC 859DSL 80MHz
  64M bytes SDRAM Memory
  8M bytes Flash Memory
  0K bytes NvRAM Memory
  Pcb      Version:3.0
  Logic    Version:1.0
  BootROM  Version:2.05          ------- 注②
  [SLOT 1] 1FE      (Hardware)3.0, (Driver)1.0, (Cpld)1.0
  [SLOT 2] 1ETH     (Hardware)3.0, (Driver)1.0, (Cpld)1.0
 [H3C]
```

2 版本使用限制及注意事项

1. LFD17847

内容过滤，包括 http 过滤、smtp 过滤不支持分片、重传报文，不支持中文编码的过滤。

2. LFD17846

文件系统中，最大的文件名长度不能超过 64 字节，路径名加文件名长度不能超过 127。

3. LFD17844

IPSEC 模板方式不支持多个策略。

4. LFD17843

动态获取的 IP 不能被其他接口所借用。

5. LFD17842

在 NAT 与 ASPF 同时使用时，清除 ASPF 表项，需要同时清除快转表项，否则会引起某些报文还是能够正常通过防火墙。

6. LFD17760

由于硬件是一个 MAC,SecPaht F100-A 的所有 LAN 口只能配置一个 VRRP 组。

7. LFD18248

NAT 与 VRRP 配合使用时， VRRP 虚拟地址和 NAT 不要配置在同一个网段中。

8. LFD18396

SECPATHF100A-CMW340-E1604 及以后版本，不支持 128M 内存的设备。

9. LFD14087

COMWARE 支持标准的正则表达式，但是对于复杂的命令行表达式，可能存在问题

10. LFD21716

SECPATH 不支持设备侧配置 BIMS 端口为 443， 21，25 等知名端口

11. LFD15632

SECPATH 设备不支持网管 NCC 组件升级功能

12. LFD19751

SECPATH 设备防火墙黑名单日志发送给 XLOG 的日志的老化时间字段是以分为单位的值

13. LFD15632

SECPATH 设备不支持网管 NCC 组件升级功能

14. LFD19751

SECPATH 设备防火墙黑名单日志发送给 XLOG 的日志的老化时间字段是以分为单位的值

3 版本特性说明

3.1 版本硬件特性

表3 产品硬件特性

项目		属性						
机型		SePath 1F1000A	SePath F1000S	SePath F100E	SePath F100A	SePath F100M	SePath F100S	SePath F100C
接口		1 个配置口（CON），1 个备份口（AUX）						
		2 个 10/100/1000M 以太网口	4 个 10/100/1000M 以太网口	4 个 10/100 以太网口	7 个 10/100 以太网口	3 个 10/100 以太网口	4 个 10/100 以太网口	5 个 10/100 以太网口
插槽		1 个 MIM 插槽，支持的模块包括 1FE/2FE/4FE/1GBE/2GBE/1GEF/2GEF/SSL	2 个 MIM 插槽，支持的模块包括 1FE/2FE/4FE/1GBE/2GBE/1GEF/2GEF	1 个 MIM 插槽，支持的模块包括 1FE/2FE/4FE/1GBE/2GBE/1GEF/2GEF	1 个 MIM 插槽，支持的模块包括 1FE/2FE/4FE/NDEC	1 个 MIM 插槽，支持的模块包括 1FE/2FE/4FE/NDEC	无	无
FLASH		16MB	16MB	16MB	16MB	16MB	8M	8M
SDRAM		缺省：512MB 最大：1GB	缺省：512MB 最大：1GB	缺省：256MB 最大：512MB	256MB	256MB	128MB	64MB
外型尺寸（W×D×H）		436mm×420mm×44mm	436mm×44mm×420mm	436mm×44mm×430mm	332mm×44mm×432mm	332mm×44mm×432mm	300mm×42mm×220mm	300mm×180mm×45mm
重量		5.5kg	6kg	5kg	4.5kg	4.5kg	2kg	1kg
电源	AC	额定电压范围：100-240V a.c.；50/60Hz 额定电流：1.0A						
	DC	额定电压范围：-48- -60V d.c. 额定电流：1.5A				NA	12V	

项目	属性						
额定功率	100W	100W	57W	54W	54W	11W	10W
工作环境温度	0～40℃						
环境相对湿度	10～90%（不结露）						

3.2 版本软件特性

表4 产品软件特性

属性	说明	
网络安全性	验证、授权和计帐（AAA）服务	RADIUS HWTACACS CHAP 验证 PAP 验证 域认证
	防火墙	包过滤 基于接口的访问控制列表 基于时间段的访问控制列表 ASPF 状态防火墙 防攻击特性： Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、ARP Flood、ARP 欺骗攻击防范 ARP 主动反向查询 TCP 报文标志位不合法攻击防范 超大 ICMP 报文攻击防范 地址/端口扫描的防范 DoS/DDoS 攻击防范

属性	说明	
		反向路由检查功能
	邮件/网页过滤	邮件过滤： SMTP 邮件地址过滤 SMTP 邮件标题过滤 SMTP 邮件内容过滤 SMTP 邮件附件过滤 支持 SQL/Java Applet/ActiveX 过滤 网页过滤： HTTPURL 过滤 HTTP 内容过滤
	安全管理	攻击实时日志 黑名单日志 地址绑定日志 流量告警日志 流量统计和分析功能 全局/基于安全域连接速率监控 全局/基于安全域协议报文比例监控 安全事件统计功能 E-Mail 邮件实时告警功能 E-Mail 邮件定期信息发布功能

属性	说明	
	数据安全	IPSec IKE
	NAT	支持地址池方式的地址变换 支持使用 ACL 控制地址转换 支持 Easy IP 支持 NAT Server 可配置支持地址转换的有效时间 支持多种 ALG，包括 FTP，H323，DNS 等
VPN	L2TP VPN	可以根据 VPN 用户完整用户名和用户域名向指定 LNS 发起连接 可以为 VPN 用户分配地址 可以进行 LCP 重协商和二次 CHAP 验证
	IPSec/IKE	支持 AH、ESP 协议 支持手工或通过 IKE 协商自动建立安全联盟 ESP 支持 DES、3DES 和 AES 三种加密算法 支持 MD5 及 SHA-1 验证算法 支持 IKE 主模式及野蛮模式 支持 NAT 穿越
	GRE VPN	
	DVPN	支持自动建立隧道技术 支持 UDP 封装，以实现 NAT 穿越 支持提供对报文的校验 支持静态 MAP 支持 client 端接入认证及节点间的加密认证 支持使用动态 IP 地址构建 VPN 同一个节点可以属于不同的 VPN 域 支持多个 VPN 域 支持数据加密 通过动态建立隧道节省 Server 带宽
网络互连	局域网协议	Ethernet_II Ethernet_SNAP VLAN
	链路层协议	PPP

属性	说明	
		PPPoE
网络协议	IP 服务	ARP ARP Proxy 静态域名解析 IP 地址借用 DHCP 中继 DHCP 服务器 DHCP 客户端 L3 Monitor HWPing
	IP 路由	静态路由管理 RIP-1/RIP-2 OSPF BGP 路由策略 策略路由
网络可靠性	VRRP	
服务质量保证（QoS）	流量监管	Traffic Policing
	拥塞管理	FIFO、PQ、CQ、WFQ、CBWFQ、RTPQ
	拥塞避免	WRED
	流量整形	GTS
	接口速率限制	LR、CAR
配置管理	命令行接口	通过 Console 口进行本地配置 通过 AUX 口进行远程配置 通过 Telnet 或 SSH 进行本地或远程配置 配置命令分级保护，确保未授权用户无法配置设备 提供全中文的提示和帮助信息 详尽的调试信息，帮助诊断网络故障 提供网络测试工具，如 Tracert、Ping 命令等，迅速诊断网络是否正常 用 Telnet 命令直接登录并管理其它网络设备 FTP Server/Client，可以使用 FTP 下载、上载配

属性	说明	
		支持 TFTP 上传下载文件 支持通过 BIMS 更新配置文件和应用程序 支持通过 VPN Manager 来完成 VPN 的部署和配置 支持日志功能 文件系统管理
	WEB 网管接口	系统管理： 系统资源管理 设备重启，软件升级支持 配置浏览，保存，下载，上传支持 用户配置 接口管理 静态路由，域名服务支持 IPSec 配置 支持防火墙： 攻击防范 ACL 黑名单 安全区域 IP/MAC 地址绑定 支持网页过滤： HTTP URL 过滤 HTTP 内容过滤

属性	说明	
		NAT 管理 DHCP 管理 SNMP 管理 常用工具支持（包括 Ping，Tracert 等） 帮助信息 注销身份
	支持标准网管 SNMPV3，并且兼容 SNMP V2C、SNMP V1 支持 NTP 时间同步	

4 版本变更说明

4.1 特性变更说明

表5 特性变更说明

版本号	项目	描述
H3C SecPath F 系列-CMW340-R1607P02	软件特性更新	无
	硬件特性变更	无
H3C SecPath F 系列-CMW340-R1607P02	软件特性更新	无
	硬件特性变更	增加新的款型 F100-M
H3C SecPath F 系列-CMW340-R1607P01	软件特性更新	无
	硬件特性变更	无

版本号	项目	描述
H3C SecPath F 系列-CMW340-R1607	软件特性更新	无
	硬件特性变更	无
H3C SecPath F 系列-CMW340-R1607	软件特性更新	新增特性： 流日志软件特性： 通过实现此特性，防火墙设备将流经防火墙的所有的业务流都进行日志记录的能力，从而使用远端的日志主机能够对防火墙的日志进行分析，达到更细粒度的流分析能力。

版本号	项目	描述
	硬件特性变更	无
H3C SecPath F 系列-CMW340-R160601	软件特性更新	无

版本号	项目	描述
	硬件特性变更	无
H3C SecPath F 系列-CMW340-R1605P03	软件特性更新	无

版本号	项目	描述
	硬件特性变更	无
H3C SecPath F 系列-CMW340-E1605	软件特性更新	无

版本号	项目	描述
	硬件特性变更	无
H3C SecPath F 系列-CMW340-E1604P03	软件特性更新	无

版本号	项目	描述
	硬件特性变更	无
H3C SecPath F 系列-CMW340-E1604P01	软件特性更新	新增特性： 桥支持透传 VLAN ID 特性的软件特性 通过实现此特性，可以让加入桥组的非以太出接口也能转发带有 VLAN ID 的报文，而不会因此丢失 VLAN ID，并使桥出接口有 VLAN ID 的情况也不会，改变原包文的 VLAN ID。从而实现桥接的本地或异地网络隔离

版本号	项目	描述
	硬件特性变更	无
H3C SecPath F 系列-CMW340-E1604	软件特性更新	热插拔特性： 当接口卡出现故障或者其他原因需要更换接口卡，同时保障系统其他服务不中断的情况下，完成接口卡的替换 静态 NAT 支持 EASY IP 项目软件特性 **NAT SERVER** 支持 **EASY IP** 特性是在 **NAT SERVER** 特性的基础上新增的。主要是为了支持在配置 **NAT SERVER** 公网地址时，可以直接指定为本接口（**NAT SERVER** 配置所属的当前接口）或指定为已存在的 **Loopback** 接口 **IPSec** 流模板支持 **per host** 方式 **Per Host** 方式，为每条源 目的地址相同的流创建一个隧道，对于采用的 **L2TP+IPSEC** 组网方式，**per session** 方式能有效解决中心无法区分数据应该发送到哪个客户端的问题 **HWtacacs** 支持 **Super** 认证模块的软件特 用户通过登录到 **router** 来管理设备。如果登录过程中获取了较小的权限，用户可以通过 **super** 命令来获取更高的权限，本特性在原来 **super password** 认证的基础上，增加了通过 **tacacs+ server** 的 **enable** 密码认证。 **NAT** 限制每个源地址最大 **TCP** 连接数的软件特性 在支持 NAT 的路由器中通常会保存地址转换对应的表项，由于路由器的内存资源有限，因此地址转换对应表项的个数有一定的规格限制。当达到规格限制时，后续要求进行地址转换的

版本号	项目	描述
		报文就不会被处理。 正常情况下，在规格限制的范围内，所有请求地址转换的报文都会被处理。通常情况并非如此，很多时候，某些恶意攻击或感染病毒的主机，会发送大量的要求地址转换的连接，创建大量的地址转换对应关系表项。使得地址转换表项个数迅速达到规格限制。此时，其他正常要求地址转换的连接将不会被处理。这不仅会影响正常用户的使用，而且会占用大量的路由器资源，导致路由器性能迅速下降。为了防止这种情况的发生，本解决方案就是在路由器上增加连接统计和限制功能。连接统计和限制功能可以根据不同的策略，对不同特征的连接进行统计和限制。 通过 MIB 升级 bootrom 软件特性 用户可通过 MIB 节点 h3cSysCurBtmFileName 获取当前使用的 bootrom 文件名信息，通过 h3cSysCurUpdateBtmFileName 节点获取 bootrom 更新成功后 bootrom 文件名信息，如果没有更新 bootrom 操作，该节点取值和 h3cSysCurBtmFileName 相同。 当需要更新 bootrom 的时候，可通过网管软件对 h3cSysBtmLoadTable 表创建更新我司设备 bootrom。用于更新的 bootrom 文件必须合法，其合法性由设备在更新过程中检测，如果文件不适用于设备，会导致 bootrom 更新失败。更新完成后，记录操作结果，记录包括：更新的时间，更新是否成功，更新时所使用的 bootrom 文件名。
	硬件特性变更	无

4.2 命令行变更说明

表6 命令行变更说明

版本号	项目	描述
H3C SecPath F 系列-CMW340-R1608	新增命令	无
	删除命令	无
	修改命令	无
H3C SecPath F 系列-CMW340-R1607P02	新增命令	无
	删除命令	无
	修改命令	无
H3C SecPath F 系列-CMW340-R1607P01	新增命令	无
	删除命令	无
	修改命令	无
H3C SecPath F 系列-CMW340-R1607	新增命令	流日志相关命令：详细见《FLOWLOG 流日志特性说明书》 [undo]session log enable [acl-number access-list] [undo] firewall session log-type{ syslog | binary} [undo] firewall nat log-type{ syslog | binary} [undo] firewall binary-log host ip-address [port-number] [undo] firewall session log-threshold time value [undo] firewall session log-threshold Mega-byte value [undo] firewall session log-threshold Mega-packet value display firewall log-buffer session reset firewall log-buffer session
	删除命令	无
H3C SecPath F 系列-CMW340-R160601	修改命令	无
	新增命令	无
	删除命令	无
H3C SecPath F 系列-CMW340	修改命令	无
	新增命令	无
	删除命令	无

版本号	项目	描述
-R1605P03		
H3C SecPath F 系列-CMW340-E1605	修改命令	无
	新增命令	无
	删除命令	无
H3C SecPath F 系列-CMW340-E1604P03	修改命令	无
	新增命令	无
	删除命令	无
H3C SecPath F 系列-CMW340-E1604P01	修改命令	无
	新增命令	**命令一 bridge vlanid-transparent-transmit enable** 【命令】 **bridge vlanid-transparent-transmit enable** **undo bridge vlanid-transparent-transmit enable** 【视图】 在接口视图下 【参数】 无 【描述】 这个命令用于配置加入桥组的出接口，是否使能 VLANID 透传。 在接口视图下，通过 bridge vlanid-transparent-transmit enable 命令可以配置支持 VLANID 透传， 接口不对报文的 VLANID 做任何修改。通过 undo bridge vlanid-transparent-transmit enable 命

版本号	项目	描述
		令可以取消配置，接口将不进行 VLANID 透传。 在默认情况下接口不支持 VLANID 透传。 【举例】 在 SecPath 的系统视图下 **[H3C]bridge enable** **[H3C]bridge 1 enable** 在路由器的 ATM 接口视图下 **[H3C-Atm2/0/0]bridge-set 1** **[H3C-Atm2/0/0]bridge vlanid-transparent-transmit enable** **[H3C-Atm2/0/0]pvc 1/100** **[H3C-Atm2/0/0]map bridge-group broadcast**
H3C SecPath F 系列-CMW340-E1604	新增命令	**以下命令具体操作请参见** 《H3C SecPath 系列安全产品 新特性手册-CMW340-B1603(V1.00)》 《-H3C SecPath 系列安全产品 命令手册(V2.02,for COMWAREV300R002)》06-安全命令 **命令一 remove slot 1** 【命令】 remove slot 1 undo remove slot 1 【视图】 用户视图 【参数】 无 【描述】 **remove slot 1** 命令用来对插槽上的板卡做拔出预处理。执行该命令后，将会暂停板卡上承载的业务，以确保在拔出板卡的过程中系统不会出现异常。**Undo remove slot 1** 命令用来取消板卡拔出预处理，恢复此前暂停的业务。 【举例】 <H3C> remove slot 1 You can config and use the board now. <H3C> undo remove slot 1 The state of the board is already normal.

版本号	项目	描述
		You can config and use the board now. 【更新记录】无 **命令二　Display device** 【命令】 display device [interface-slot] 【视图】 用户视图、系统视图 【参数】 **interface-slot**：接口槽位，缺省情况下显示所有设备信息 【描述】 display device 命令用来显示设备在位和状态信息，disp device interface-slot 命令用来显示对应接口槽位上的设备在在位和状态信息 【举例】 <H3C> display device Slot # Type Online Status - 0 2GBE Present Normal 1 1FE Present Normal <H3C> display device 1 Slot # Type Online Status - 1 1FE Present Normal 【更新记录】 无 **命令三 security acl** 【命令】 security acl *acl-number* [aggregation | per-session] undo security acl 【视图】 安全策略视图、安全策略模板视图 【参数】 *acl-number*：指定安全策略所引用的访问控制列表号，取值范围是 3000～3999。 *aggregation*：指定安全策略的数据流保护方式为聚合方式，一条

版本号	项目	描述
		隧道保护 ACL 中定义的所有数据流。 *per-session*：指定安全策略的数据流保护方式为 *per-session* 式。*per-session* 方式的处理方法如下：触发报文的源 IP、目的 IP、协议、源端口、目的端口形成了一个五元组，若这个五元组匹配 ACL 的某个数据流，则建立一个隧道保护这个五元组所定义的所有报文。 如果不指定 *aggregation* 和 *per-session* 参数，则安全策略的默认的数据流保护方式为一条隧道保护 ACL 中定义的一条数据流，即标准方式。 【描述】 命令 security acl 用来设置安全策略引用的访问控制列表，命令 undo security acl 用来取消安全策略引用的访问控制列表。 缺省情况下，安全策略没有指定访问控制列表。 安全策略所保护的数据流由此命令指定的 ACL 来定义。在实施 IPSec 安全策略时，系统首先检查通过接口的报文是否与 ACL 中的规则匹配，如果匹配且是被访问控制列表允许（permit）的报文，则系统对报文进行 IPSec 保护后再发送。如果不匹配，或者访问控制列表拒绝（deny）的报文，则直接发送报文。 默认数据流保护方式为标准方式。使用标准方式保护 ACL 下的数据流，ACL 中的每一个规则对应的一个数据流都会创建一条单独的隧道来保护；使用聚合方式保护 ACL 下的数据流，只会创建一条隧道来保护 ACL 中定义的所有规则对应的数据流；使用 per-session 方式保护 ACL 下的数据流，触发报文的源 IP、目的 IP、协议、源端口、目的端口形成了一个五元组，若这个五元组匹配 ACL 的某个数据流，则建立一个隧道保护这个五元组所定义的所有报文。 建议：当协商的对端只能使用一条隧道保护 ACL 中定义的所有数据流时才使用聚合方式。该方式比标准方式安全性稍微差一些。 aggregation 方式对于 isakmp 模式和 manual 模式有效。 per-session 方式对于 isakmp 模式有效。 相关配置可参考命令 ipsec policy（系统视图），ipsec policy（接口视图），tunnel local，tunnel remote，sa duration，proposal。 【举例】 # 设置安全策略引用 3001 号访问控制列表，数据流保护方式为标准方式。 [H3C] acl number 3001 [H3C-acl-adv-3001]rule permit tcp source 10.1.1.1 0.0.0.255 destination 10.1.1.2 0.0.0.255 [H3C] ipsec policy beijing 100 manual [H3C-ipsec-policy-manual-beijing-100] security acl 3001

版本号	项目	描述
		# 设置安全策略引用 3002 号访问控制列表，并设置数据流保护方式为聚合方式。 [H3C] acl number 3002 [H3C-acl-adv-3002] rule 0 permit ip source 10.1.2.1 0.0.0.255 destination 10.1.2.2 0.0.0.255 [H3C-acl-adv-3002] rule 1 permit ip source 10.1.3.1 0.0.0.255 destination 10.1.3.2 0.0.0.255 [H3C] ipsec policy huawei 1 isakmp [H3C-ipsec-policy-isakmp-huawei-1] security acl 3002 aggregation # 设置安全策略引用 3003 号访问控制列表，并设置数据流保护方式为 per-session 方式。 [H3C] acl number 3003 [H3C-acl-adv-3002] rule 0 permit ip source 10.1.2.1 0.0.0.255 destination 10.1.2.2 0.0.0.255 [H3C] ipsec policy huawei 2 isakmp [H3C-ipsec-policy-isakmp-huawei-1] security acl 3003 per-session **命令四 nat connection-limit-policy** 【命令】 nat connection-limit-policy *policy-number* undo nat connection-limit-policy *policy-number* 【视图】 系统视图。 【参数】 *policy-number*：指定与 NAT 模块绑定的连接统计策略编号。范围为[0，19]。 【描述】 此命令用于 NAT 模块引用一条连接统计策略。一个模块只能引用一条策略。只有当一个模块引用了连接统计策略时，才能使用连接统计与限制功能。只有当引用的策略存在时，才能引用成功。 【举例】 #NAT 模块引用连接统计策略 1 [H3C]nat connection-limit-policy 1 #取消引用连接统计策略 1 [H3C]undo nat connection-limit-policy 1

版本号	项目	描述
		命令五 display nat connection-limit 【命令】display nat connection-limit [source *source-addr* { *source-wildcard* | *source-mask-len* }] [destination *destination-addr* { *destination-wildcard* | *destination-mask-len* }] [destination-port { { eq | neq | gt | lt } *destination-port* | range *destination-port1 destination-port2* }] [vpn-instance *vpn-name*] 【视图】 所有视图。 【参数】 nat：显示 NAT 模块创建的连接数信息。 source：指定源 IP 地址。 *source-addr*：源 IP 地址。 *source-wildcard*：源 IP 地址的掩码。 *source-mask-len* ：源 IP 地址掩码长度。 destination：指定目的 IP 地址。 *destination-addr*：目的 IP 地址。 *destination-wildcard*：目的 IP 地址掩码。 *destination-mask-len*：目的 IP 地址掩码长度。 destination-port：指定目的端口号。 eq：指定要显示那种服务的连接数。 neq：指定要显示非那种服务的所有连接数。 gt：指定要显示大于某端口的服务的所有连接数。 lt：指定要显示小于某端口的服务的所有连接数。 range：指定要显示某范围的服务的所有连接数。 *destination-port*：目的端口号。 *destination-port1*、*destination-port2*：按端口范围显示时使用，分别表示要显示的服务端口的上下限。 vpn-instance ：指定 VPN 名字。 *vpn-name*：VPN 名字。 【描述】 用户可以通过此命令，显示与 NAT 模块相关的符合输入条件的连接统计信息表项，表项中包含当前统计到的连接数。使用源地址，目的地址，目的端口，VPN 实例名称的任意组合作为输入条件。此命令可以在所有视图下使用。 当指定源地址为 1.0.0.100 255.255.255.255，表示单一的源地址。当指定源地址为 1.0.0.100 255.255.255.0，表示从地址 1.0.0.100 到 1.0.0.254 的地址段。目的地址的指定方式与源地址

版本号	项目	描述
		的指定方式相同。 当执行命令 display nat connection-limit 时，将所有与 NAT 模块相关的连接统计信息表项都显示出来。 【举例】 #显示与 NAT 模块相关的所有连接统计信息表项 <H3C>display nat connection-limit
	删除命令	
	修改命令	以下命令，具体操作请参见 《-H3C SecPath 系列安全产品 命令手册(V2.02,for COMWAREV300R002)》06-安全命令 命令一：debugging nat 命令二：display nat 命令三：nat address-group 命令四：nat static 命令五：nat outbound 命令六：nat server

4.3 MIB 变更说明

表7 MIB 文件变更说明

版本号	项目	MIB 文件名称	模块名	说明
H3C SecPath F 系列-CMW340-R1608	新增	无	无	
	修改	无	无	
H3C SecPath F 系列-CMW340-R1607P02	新增	无	无	
	修改	无	无	
H3C SecPath F 系列-CMW340-R1607P01	新增	无	无	
	修改	无	无	

H3C SecPath F 系列-CMW340-R1607	新增	无	无	
H3C SecPath F 系列-CMW340-R1606P01	修改	无	无	
	新增	无	无	
H3C SecPath F 系列-CMW340-R1605P03	修改	无	无	
	新增	无	无	
H3C SecPath F 系列-CMW340-E1605	修改	无	无	
	新增	无	无	
H3C SecPath F 系列-CMW340-E1604P03	修改	无	无	
	新增	无	无	
H3C SecPath F 系列-CMW340-E1604P01	修改	无	无	
	新增	无	无	
H3C SecPath F 系列-CMW340-E1604	新增	无	无	
	修改	无	无	

4.4 操作方式变更说明

4.4.1 SecPath F 系列-CMW340-R1608 版本操作方式变更

1. 无

4.4.2 SecPath F 系列-CMW340-R160702 版本操作方式变更

1. 无

4.4.3 SecPath F 系列-CMW340-R160701 版本操作方式变更

1. 无

4.4.4 SecPath F 系列-CMW340-R1607 版本操作方式变更

1. 无

4.4.5 SecPath F 系列-CMW340-R1606P01 版本操作方式变更

1. 无

4.4.6 SecPath F 系列-CMW340-R1605P03 版本操作方式变更

1. 无

4.4.7 SecPath F 系列-CMW340-E1605 版本操作方式变更

1. 无

4.4.8 SecPath F 系列-CMW340-E1604P03 版本操作方式变更

1. 无

4.4.9 SecPath F 系列-CMW340-E1604P01 版本操作方式变更

1. 无

4.4.10 SecPath F 系列-CMW340-E1604 版本操作方式变更

1. 无

5 存在问题与规避措施

1. RTD17180

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：IPsec 加密卡快转+ASPF：加密卡快转导致 ASPF Session 表异常

规避措施：建议 IPSEC 与 ASPF 共存时，去掉 IPSEC 加密卡快转

2. RTD17476

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：l2tp 组合 ipsec per session 测试时，设备重启

规避措施：建议在大流量环境，不建议使用 ipsec persession 特性。

3. RTD17954

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：：将 SecPath 设备与 Cisco 设备互联，当 IPSEC SA 配置流量重协商的值小于默认值时，重协商成功率比较低

规避措施：配置 SecPath IPSEC SA 时间重协商和流量重协商的值大于默认值。

4. RTD18247

首次发现版本：H3C SecPath F 系列-CMW340-E1604P01

问题描述：在配置 子接口和 arp 反向查询的环境中，发动 arp 攻击，会引起系统堆栈

规避措施：在配置子接口的环境中不要配置防火墙反向查询。

5. RTD17587

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：IP-Spoofing 不支持不对称组网和策略路由。

规避措施：IP-Spoofing 不支持不对称组网和策略路由,例如存在报文从一个接口出从另外一个接口回的组网情况，建议关闭 IP 欺骗防范功能

6. RTD18361

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：在进行 WEB 管理时，切换界面到其他的 WEB 网站，会导致 **web** 用户在一定时间内无法登陆，需要等待用户超时以后，才可以登陆。

规避措施：在进行 WEB 管理时，建议不要急性其他 WEB 处理，如果要切换，建议先正常退出。

7. RTD20716

首次发现版本：H3C SecPath F 系列-CMW340-R1606

问题描述：在设备备侧配置 BIMS 端口为 443；BIMS 侧设置监听 https 协议，系统异常重启。

规避措施：目前 BIMS 不支持 https, 不要在设备侧配置 443 端口。

6 解决问题列表

6.1 H3C SecPath F 系列-CMW340-R1608

1. RTOD00680

首次发现版本：H3C SecPath F 系列-CMW340-R1607P01

问题产生的条件： 通过 dis version 察看版本信息

问题现象：显示的版本信息 **Hangzhou Huawei-3Com Tech.**

6.2 H3C SecPath F 系列-CMW340-R1607P02

1. RTOD00022

首次发现版本：H3C SecPath F 系列-CMW340-R1607P01

问题产生的条件： 通过 Quidview 察看 F1000-A 接口 MIB 的统计信息

问题现象：5 分钟以后，接口统计信息溢出，导致数值不准确

6.3 H3C SecPath F 系列-CMW340-R1607P01

1. RT0D000006

首次发现版本：H3C SecPath F 系列-CMW340-E1606

问题产生的条件： 在 SecPath 设备接口上应用的 ACL 上，配置 log 参数，然后发送与 ACL 匹配的数据流

问题现象：设备发送的 syslog 日志信息，没有 rule 信息

6.4 H3C SecPath F 系列-CMW340-R1607

1. RTD17938

首次发现版本：H3C SecPath F 系列-CMW340-E1606

问题产生的条件： 在 SecPath 设备上配置 ipsec 密钥

问题现象：ipsec 密钥显示明文

6.5 H3C SecPath F 系列-CMW340-R1606P01

1. RTD17947

首次发现版本：H3C SecPath F 系列-CMW340-E1605

问题产生的条件：配置 QOSWRED 配置概率丢弃低门限等于上次配置的高门限时

问题现象： 系统异常

2. RTD19587

首次发现版本：H3C SecPath F 系列-CMW340-E1605

问题产生的条件：配置 NAT,QOS 和快转，打大流量数据，导致 QOS 拥塞 ，同时 reset nat session

问题现象：系统异常重起。

6.6 H3C SecPath F 系列-CMW340-R1605P03

1. RTD19159

首次发现版本：H3C SecPath F 系列-CMW340-E1605

问题产生的条件：10f 在处理业务繁忙时，输入复杂的正则表达式

问题现象： 系统重新启动

2. RTD18936

首次发现版本：H3C SecPath F 系列-CMW340-E1605

问题产生的条件：透明模式下，取 RFC1213-MIB,ifOperStatus 节点

问题现象：该节点取值错误

6.7 H3C SecPath F 系列-CMW340-E1605

1. RTD17947

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题产生的条件：SecPath1000 与 AR18 建立 IPSec 后传输大包

问题现象： IPSEC 隧道传输大包，丢包严重

2. RTD18181

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题产生的条件：将 VRRP 的虚拟 IP 地址和 NAT 地址配置在同一网段

问题现象：VRRP 主备切换以后，NAT 无法正常工作。

6.8 H3C SecPath F 系列-CMW340-E1604P03

1. RTD17587

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题产生的条件：在 SecPath F 系列百兆口上配置 L2TP 或则 DVPN，并启动 Ip spoofing 检测

问题现象： Ip spoofing 会产生攻击误报，导致 L2TP 或则 DVPN 连接中断

2. RTD17588

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题产生的条件：F100S IPSEC 加密卡安全提议选择 ah－esp 安全协议，从对端发起符合 ipsec 安全策略保护流时，设备堆栈重启

问题现象：设备堆栈重启

6.9 H3C SecPath F 系列-CMW340-E1604P01

1. RTD16258

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题产生的条件：在 SecPath **F** 系列百兆口上配置 **Vlan** 透传特性

问题现象：SecPathF 系列百兆口不支持 Vlan 透传特性

2. RTD14060

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题产生的条件：VRRP 和 NAT 混合应用

问题现象：VRRP 和 NAT 混合应用后,备份设备用自己的接口实 mac 响应 ARP request 报文,导致对端设备的 arp 表项错误

7 配套资料

7.1 配套资料清单

表8 配套手册清单

手册名称	资料版本
《H3C SecPath 系列安全产品 操作手册》	(V1.03)
《H3C SecPath 系列安全产品 命令手册》	(V1.03)
《H3C SecPath F1000-A 防火墙 安装手册》	(V1.03)
《H3C SecPath F100-A 防火墙 安装手册》	(V1.03)
《H3C SecPath F100-C 防火墙 安装手册》	(V1.03)

《H3C SecPath F1000-S 防火墙 安装手册》	(V1.03)
《H3C SecPath F100-S_F100-E 防火墙 安装手册》	(V1.03)
《H3C SecPath F100-M 防火墙 安装手册》	(V1.01)
《H3C SecPath 系列安全产品 Web 配置手册》	(V1.03)
《H3C SecPath 系列安全产品 Web 配置手册》	(V2.01)

7.2 配套产品资料的获取方法

通过 H3C 网站查询和下载与该版本配套的产品资料，方法如下。

表9 从网站查询和下载资料的说明

如何申请帐号	首先，登录到 http:// www.h3c.com.cn 网站的主页；单击［注册/登录］，然后输入用户名、密码，并单击<注册>即可。
如何获取产品资料	登录到 http:// www.h3c.com.cn 网站的主页，单击主页的［文档中心］，然后即可按产品类别来查询资料； 选择产品后即可弹出相应的产品明细列表； 指定了设备类型后，即可选择与该产品相关的手册。

8 版本升级操作指导

8.1 Boot 菜单

在防火墙的软件维护过程中需要使用 Boot 菜单，因此本节对 Boot 菜单进行介绍。

将配置口电缆的 RJ45 一端与防火墙的配置口相连，DB9 一端与微机的串口相连，然后启动防火墙，当配置终端上出现“Press Ctrl-B to enter Boot Menu”提示信息时，按下<Ctrl+B>键，系统将提示：

```
Please  input Boot ROM password :
```

⚠ 注意：

- 必须在出现“Press Ctrl-B to Enter Boot Menu...”的 3 秒钟之内，按下<Ctrl+B>键，才能进入 Boot 菜单，否则将进入程序解压过程。
- 若您在进入程序解压过程后希望进入 Boot 菜单，需要重新启动防火墙。

输入正确的口令后，键入<Enter>（如没有设置 Boot ROM 口令，直接键入<Enter>即可）系统将进入 Boot 菜单，显示如下：

8.1.1 SecPath F100C 防火墙 Boot 菜单

1. H3C SecPath F100C 防火墙的 Boot 菜单

```
Boot Menu:
     1:  Download application program with XMODEM
     2:  Download application program with NET
     3:  Start up and ignore configuration
     4:  Enter debugging environment
     5:  Boot Rom Operation Menu
     6:  Do not check the version of the software
     7:  Exit and reboot
Enter your choice(1-7):
```

Boot 菜单各选项含义如下：

(1) 通过 XModem 下载应用程序，具体升级步骤请参见8.2 ；

(2) 通过以太网下载应用程序；

(3) 忽略配置文件并以缺省配置启动；

(4) 进入调试环境；

(5) 进入 Boot ROM 操作子菜单；

(6) 不检查 Boot ROM 程序扩展段、Boot ROM 程序和应用程序的软件版本，此项用于版本升级时的后向兼容。当升级软件时，如采用的软件版本完全正确，仍无法升级成功，系统提示软件为“invalid version”，此时可选中此项，以便在软件升级时取消版本检查。此项被选中时只起作用一次，重新启动防火墙后即恢复版本检查。

(7) 退出 Boot 菜单并重新启动防火墙。

2. H3C SecPath F100C 防火墙的 Boot ROM 子菜单

如前所述，进入 Boot ROM 菜单后选择第五项即可进入 Boot ROM 子菜单，其内容如下：

```
Boot ROM Operation Menu:
     1:  Download Boot ROM with XModem
     2:  Download Extended Segment of Boot ROM with XModem
     3:  Restore Extended Segment of Boot ROM from FLASH
     4:  Backup Extended Segment of Boot ROM to FLASH
     5:  Exit to Main Menu
     Enter your choice(1-5):
```

各项含义如下：

(1) 通过 XModem 升级 Boot ROM 程序；

(2) 通过 XModem 升级 Boot ROM 程序扩展段；

(3) 从 FLASH 中恢复 Boot ROM 程序扩展段；

(4) 备份 Boot ROM 程序扩展段到 FLASH 中；

(5) 退回到主菜单。

该菜单中提供了 Boot ROM 程序升级、备份、恢复等方法，具体操作请参见8.2 、8.3 。

注意：

请勿轻易进行防火墙的软件升级，最好在技术支持人员的指导下进行。另外在进行防火墙升级时，请注意 Boot ROM 软件和应用程序的版本匹配。

8.1.2 SecPath F100A/F100S/F100E/F1000S/F1000A/F100M 防火墙 Boot 菜单

1. H3C SecPath F1000A 的 Boot 菜单

```
Boot Menu:
     1:  Download application program with XMODEM
     2:  Download application program with NET
     3:  Display file in flash
     4:  Delete file from flash
     5:  Start up and ignore configuration
     6:  Enter debugging environment
     7:  Boot Rom Operation Menu
     8:  Do not check the version of the software
     9:  Exit and reboot
Enter your choice(1-9):
```

Boot 菜单各选项含义如下：

(1) 通过 XModem 下载应用程序，具体升级步骤请参见8.2 ；

(2) 通过以太网下载应用程序，H3C SecPath F1000A 仅提供通过 TFTP 升级应用程序的方法，具体升级步骤请参见8.4 ；

(3) 显示 flash 中的文件；

(4) 从 flash 中删除文件；

(5) 忽略配置文件并以初始配置启动；

(6) 进入调试环境；

(7) 进入 Boot ROM 操作子菜单；

(8) 不检查 Boot ROM 程序扩展段、Boot ROM 程序和应用程序的软件版本，此项用于版本升级时的后向兼容。当升级软件时，如采用的软件版本完全正确，仍无法升级成功，系统提示软件为“invalid version”，此时可选中此项，以便在软件升级时取消版本检查。此项被选中时只起作用一次，重新启动防火墙后即恢复版本检查。

(9) 退出 Boot 菜单并重新启动防火墙。

2. H3C SecPath F1000A 的 Boot ROM 子菜单

如前所述，进入 Boot ROM 菜单后选择第七项即可进入 Boot ROM 子菜单，其内容如下：

```
Boot ROM Operation Menu:
    1:  Download Boot ROM with XModem
    2:  Download Extended Segment of Boot ROM with XModem
    3:  Restore Extended Segment of Boot ROM from FLASH
    4:  Backup Extended Segment of Boot ROM to FLASH
    5:  Exit to Main Menu
    Enter your choice(1-5):
```

各项含义如下：

(1) 通过 XModem 升级 Boot ROM 程序；

(2) 通过 XModem 升级 Boot ROM 程序扩展段；

(3) 从 FLASH 中恢复 Boot ROM 程序扩展段；

(4) 备份 Boot ROM 程序扩展段到 FLASH 中；

(5) 退回到主菜单。

该菜单中提供了 Boot ROM 程序升级、备份、恢复等方法，具体操作请参见8.2 、8.3 。

⚠ 注意：

请勿轻易进行防火墙的软件升级，最好在技术支持人员的指导下进行。另外在进行防火墙升级时，请注意 Boot ROM 软件和应用程序的版本匹配。

8.2 利用 XModem 协议完成应用程序和 Boot ROM 程序升级

利用 XModem 协议完成软件升级时直接使用配置口，不必另外搭建配置环境。

1. 应用程序的升级

第一步：进入 Boot 菜单（参见8.1 小节），键入<1>，选择通过 XModem 协议下载应用程序。防火墙将提供如下可供选择的下载速率：

```
Downloading application program from serial ...
Please choose your download speed:
1: 9600 bps
2: 19200 bps
3: 38400 bps
4: 57600 bps
5: 115200 bps
6: Exit to Main Menu
Enter your choice(1-6):
```

第二步：选择合适的下载速率，如键入<5>，选择 115200 bps 的下载速率，防火墙将提示如下信息：

```
Download speed is 115200 bps. Change the terminal's speed to 115200 bps,
and select XModem protocol. Press ENTER key when ready.
```

第三步：根据上面提示，改变配置终端设置的波特率，使其与所选的软件下载波特率一致。设置完终端波特率后，应做一次终端的断开（即[拨入/断开]）和拨号（即[拨入/拨号]）操作，然后按<Enter>键即可开始下载，系统提示如下：

```
Downloading ... CCCCC
```

& 说明：

设置完配置终端的波特率后，只有做一次终端仿真程序的断开和连接操作，新的设置才会有效。

第四步：从终端窗口选择[传送/发送文件]，弹出如下图所示的对话框：

图1 [发送文件]对话框

第五步：点击[浏览]按钮，选择需要下载的应用程序文件，并将协议设置为XModem，然后点击[发送]按钮，系统弹出如下界面：

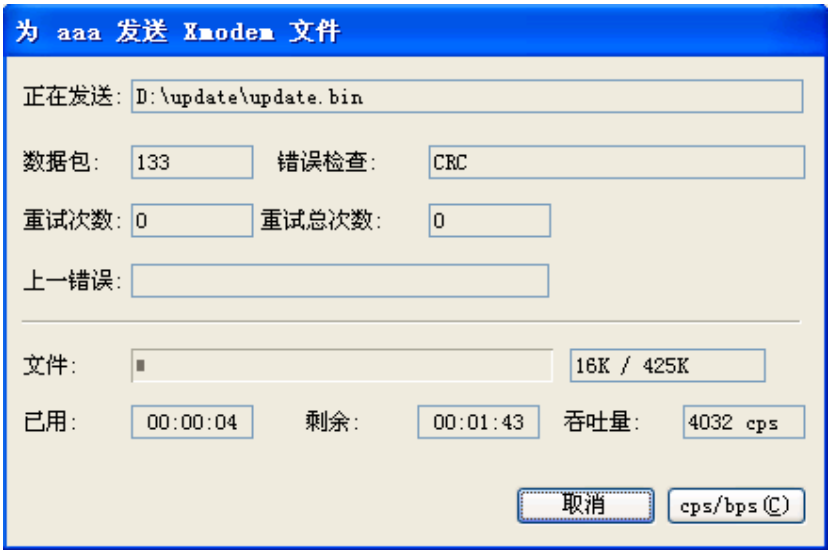

图2 正在发送文件界面

第六步：下载完成后，系统开始写 Flash（闪速存储器）操作，当这一操作完成后，终端界面出现如下信息，表明下载完成：

```
XModem download completed, Packet length 8790321 bytes.
    System file length 7868992 bytes, http.zip file length 921329 bytes.

    Writing file flash:/system to FLASH...
    Please wait, it may take a long time
################################################
    Writing into Flash Succeeds.

    Writing file flash:/http.zip to FLASH...
    Please wait, it may take a long time
#########################################################################
######
#########
    Writing into Flash Succeeds.
Please use 9600 bps.Press <ENTER> key to reboot the system.
```

此时按提示将配置终端速率恢复为 9600bps（并进行一次断开和拨号操作），然后系统正常启动。

2. Boot ROM 程序的升级

第一步：进入 Boot 菜单（参见8.1 小节），选择<7>，进入 Boot ROM 操作子菜单。

第二步：在 Boot ROM 操作子菜单中选择<1>，通过 XModem 升级 Boot ROM 程序，防火墙将提供多种可选择的速率，随后操作与0中的“1. 应用程序的升级”中的描述相同。

注意：

- 如果整个 Boot ROM 程序升级失败，将无法现场恢复，故只有在必要且有技术支持人员协助的情况下方可升级整个 Boot ROM 程序。
- 整个 Boot Rom 程序的文件大小为 512KB，Boot Rom 程序扩展段的大小小于 512KB。

3. Boot ROM 程序扩展段的升级

第一步：进入 Boot 菜单（参见8.1 小节），选择<7>，进入 Boot ROM 操作子菜单；

第二步：在 Boot ROM 操作子菜单中选择<2>，通过 XModem 升级 Boot ROM 程序扩展段，防火墙将提供多种可选择的速率，随后操作与0中的“1. 应用程序的升级”中的描述相同。

注意：

- 采用这种方法升级 Boot ROM 程序只是升级了程序的一部分，一旦出现错误可以重新升级。
- 整个 Boot Rom 程序的文件大小为 512KB，Boot Rom 程序扩展段的大小小于 512KB。

8.3 Boot ROM 程序扩展段的备份及恢复

1. 在 FLASH 中备份 Boot ROM 程序的扩展段

如果防火墙需要备份 Boot ROM 程序的扩展段，可以采用如下方法：

第一步：进入 Boot 菜单（操作方法见8.1 ），选择<7>，进入 Boot ROM 操作子菜单；

第二步：在 Boot ROM 操作子菜单中选择<4>，这样当前的 Boot ROM 程序扩展段将被复制到 FLASH 中。

```
Backup Extended Segment, are you sure?[Y/N]
```

键入<Y>，则开始备份；

如果备份成功，则提示信息如下：

```
Writing to FLASH.Please wait...####
Backuping Boot ROM program to FLASH successed!
```

第三步：当再次出现 Boot 子菜单时，选择<5>，退出并重启防火墙即可。

2. 从 FLASH 中恢复 Boot ROM 程序扩展段

在 Boot ROM 程序扩展段出现问题或被误升级的情况下，可以将以前在 FLASH 中备份的 Boot ROM 程序扩展段重新恢复到 Boot ROM 中，方法如下：

第一步：进入 Boot 菜单，选择<7>，进入 Boot ROM 操作子菜单（菜单内容如上所示）；

第二步：在 Boot ROM 操作子菜单中选择<3>，从 FLASH 中恢复 Boot ROM 程序扩展段，会出现如下提示：

```
Restore Extended Segment, are you sure?[Y/N]
```

键入<Y>，则开始恢复；

如果成功恢复，则出现如下提示：

```
Writing to Boot ROM.Please wait...######
Restoring Boot ROM program successed!
```

第三步：当再次出现 Boot 子菜单时，选择<5>，退出并重启防火墙即可。

8.4 通过 TFTP 完成应用程序的升级

通过网络下载应用程序是指通过以太网口下载应用程序，此时防火墙作为 Client，需要在防火墙的固定以太网口上连接 TFTP Server。具体的升级方法如下：

⚠ 注意：

TFTP Server 程序由用户自己购买、安装，H3C SecPath 系列防火墙不提供此软件。

H3C SecPath F1000A 仅提供 TFTP client 的功能，故仅提供通过 TFTP 升级应用程序的方法，升级步骤如下：

(1) 启动 TFTP Server

在防火墙的以太网口所连接的 PC 上启动 TFTP Server，并设置好欲加载文件的所在路径。

(2) 配置防火墙

第一步：进入 TFTP 配置状态；

启动防火墙，进入 Boot 菜单（操作方法见8.1 ），选择<2>，进入 Net Port Download Menu(网络下载菜单)；

显示如下：

```
Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 1
```

第二步：配置 TFTP 参数；

选择<1>，可配置防火墙的网络接口参数，包括防火墙使用的接口、接口 IP 地址、子网掩码等；以及 TFTP Server 参数，包括 TFTP Server 的以太网口 IP 地址、应用程序的文件名等。

```
    Change Download parameter
     Download device             :ETH0                    下载所使用的设备名
     Download file(Max 60 char)  : system.bin             服务器上的应用程序文件名
     IP address of ETH0          :192.168.1.15            防火墙接口的 IP 地址
     Subnet mask for ETH0        :255.255.255.0      防火墙接口的子网掩码
     IP address of the server    :192.168.1.10            TFTP 服务器的 IP 地址
     IP address of the gateway   :10.110.95.117      网关的 IP 地址
```

⚠ 注意：

- 必须使用防火墙的 ETH 0 接口进行升级。SecPath F1000A 必须使用 ETH0; SECPATH F1000S 必须使用 ETH0/1; SECPATH F100A 必须使用 WAN2; SECPATH F100C 必须使用 LAN0; SECPATH F100E 必须使用 ETH0/3; SECPATH F100C 必须使用 ETH0/2; SECPATH F100M 必须使用 ETH0/2。
- “IP address of the server： [192.168.1.10]”一项必须设为防火墙以太网口所连的 TFTP Server 的 IP 地址。
- 建议将 TFTP Server 的网口 IP 地址与防火墙 ETH0 接口的 IP 地址设置为同一网段。

第三步：确认配置参数；

键入最后一项值后，将会出现如下提示并返回 Net Port Download Menu 菜单：

```
Saving config, please wait...OK!
Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 2
```

(3) 通过 TFTP 下载应用程序

按下<2>键，进入 TFTP 下载状态，提示如下：

```
Starting the TFTP download...
.....................................................................
.....................
    TFTP download completed, Packet length 8790321 bytes.
    System file length 7868992 bytes, http.zip file length 921329 bytes.

    Writing file flash:/system to FLASH...
    Please wait, it may take a long time
#####################################################################
Writing into Flash Succeeds.

    Writing file flash:/http.zip to FLASH...
    Please wait, it may take a long time
#########################################################################
######
#########
    Writing into Flash Succeeds.
```

加载成功，键入<Enter>后，系统正常启动。

8.5 利用 FTP 完成程序/文件的上传下载

H3C SecPath 系列防火墙提供 FTP Server 功能，为用户提供了另外一种更新配置文件、升级应用程序及 Boot ROM 程序的途径。任何 FTP Client（包括本地用户和远端用户）只要与防火墙连通即可。当通过用户验证后，即可进行配置文件或应用程序的上传下载。利用 FTP 上传/下载应用程序、配置文件及上传 Boot ROM 程序操作步骤如下：

& 说明：

- 上传：从 FTP 客户端的微机向防火墙传送文件，即 put 操作。
- 下载：从防火墙向 FTP 客户端的微机传送文件，即 get 操作。

1. 搭建上传/下载环境

- 搭建 FTP 本地上传/下载环境

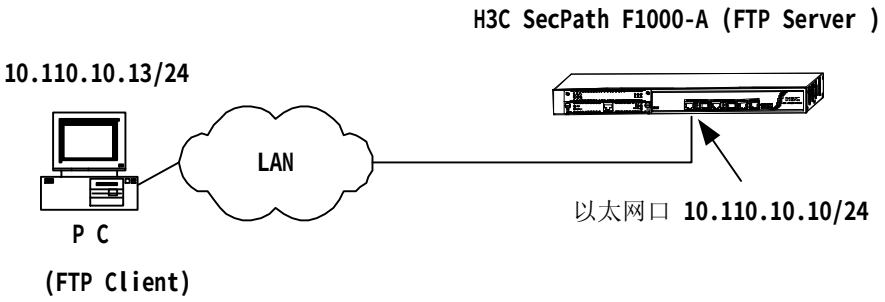

图3 搭建 FTP 本地上传/下载环境

第一步：通过防火墙以太网口连接微机；

第二步：配置防火墙以太网口 IP 地址，假设为 10.110.10.10；

第三步：配置微机以太网口 IP 地址，假设为 10.110.10.13；

第四步：将应用程序/Boot ROM 程序/配置文件等拷贝到某一路径下，假设路径为 C:\ version；

⚠ 注意：

微机网口 IP 地址与防火墙以太网口 IP 地址应位于同一网段。

- 搭建 FTP 远程上传/下载环境

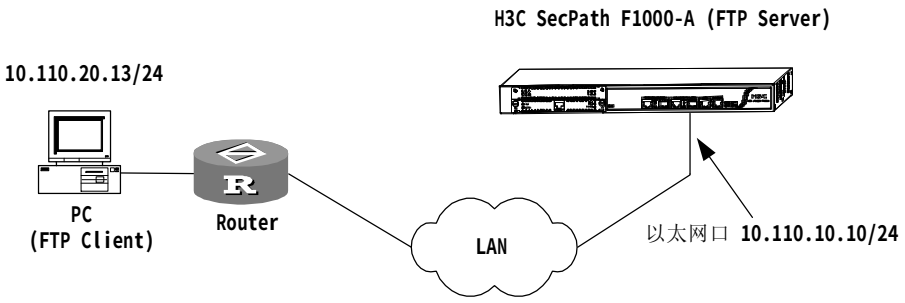

图4 搭建 FTP 远程上传/下载环境

第一步：将微机通过 WAN 连接至防火墙任意接口。这种方法不要求微机与防火墙在同一网段，用于防火墙远程升级；

第二步：将应用程序、Boot ROM 程序或配置文件拷贝到某一路径下，假设路径为 C:\version。

2. 启动 FTP 服务器

请防火墙侧维护人员进行配合，作如下配置：

第一步：设置验证方式；

& 说明：

AAA 验证的具体配置您可以根据自己的实际情况进行选择，命令的详细介绍请参见本产品操作手册和命令手册的 AAA 和 RADIUS 配置。

第二步：添加用户名；

```
[VPNGateway] local-user VPNGateway
```

VPNGateway 表示用户名。

第三步：添加口令；

```
[VPNGateway-luser-vpngateway] password simple 123
```

第四步：添加服务类型，指定 FTP 目录；

```
[VPNGateway-luser-vpngateway] service-type ftp ftp-directory flash:
```

第五步：添加权限等级；

```
[VPNGateway] level 3
```

第六步：启动 FTP 服务器。

```
[VPNGateway] ftp server enable
```

经过以上操作，在防火墙上已经启动了 FTP 服务器，并设置了用户，这样任何一个 FTP 客户端程序均可使用该用户名、口令登录 FTP 服务器。

3. 上传/下载应用程序、配置文件及上传 Boot ROM 程序

第一步：在 DOS 下进入应用程序、Boot ROM 程序或配置文件所在路径，然后执行 FTP 命令，与防火墙建立 FTP 连接，如：

```
C:\version\ftp 10.110.10.10
```

若连接成功，则显示（以 Windows98 为例）：

```
Connected to 10.110.10.10
220 FTP server ready on VPNGateway at
User(10.110.10.10:(none)):
```

第二步：使用已经在防火墙上设置好的用户名、口令登录 FTP 服务器；

```
User(10.110.10.10:(none)): VPNGateway                    键入用户名
331 Password required for ftp
Password:                                                键入口令（屏幕上不显示用户输入的口令）
230 User ftp logged in
ftp>
```

当出现提示符 ftp>时，表示可以进行上传下载操作了。

第三步：上传/下载应用程序、配置文件或上传 Boot ROM 程序；

& 说明：

防火墙端应用程序缺省名称为 system，配置文件缺省名称为 config.cfg，Boot ROM 扩展段文件缺省名称为 bootrom，整个 Boot ROM 文件缺省名称为 bootromfull。

- 上传应用程序/Boot ROM 程序/配置文件

```
ftp>        put                  键入<put>，表示进行上传操作。
local file          键入要上传的应用程序/Boot ROM 程序/配置文件的名称。
remote file                 键入防火墙端上传后所要保存的应用程序/Boot ROM 程序/配置文件名称。
```

上传文件结束后，重新显示“ftp>” 提示符，可键入<dir>显示防火墙上的文件名称和大小，上传成功则配置文件大小与主机上的文件大小一致。

⚠ 注意：

- 当使用 put 命令完成启动程序的上传后，必须要将文件名，改为“system”，放在文件系统的根目录下。
- 当使用 put 命令完成配置文件的上传后，必须要将文件名，改为“config.cfg”，放在文件系统的根目录下。
- 系统默认的启动文件的文件名是“system”，且只能放在文件系统的根目录下。因此在 COMWARE 下升级系统文件时，如果下载的文件名不是“system”，需要手工将文件名改为“system”，否则执行 reboot 命令后 BootRom 会提示找不到系统文件，无法完成引导过程。
- 由于多种原因，升级过程中可能会出现升级失败的情况，所以如果 flash 空间足够的情况下，升级前最好保留原有的 system 文件，将待升级的文件命名为其它的文件下载，下载成功后在删除原有的 system 文件，然后将新文件改名为“system”。
- 升级时一定要注意提示信息，如果提示失败，不要轻易重启机器，而应再次尝试升级操作或连续客服。
- 当使用 put 命令完成 Boot ROM 程序的上传后，还应接着使用 upgrade bootrom [full]命令将 bootrom/bootromfull 程序从 Flash 的根目录中解出，写到 Boot ROM 中，才能完成 Boot ROM 的升级。
- 当使用 FTP 对应用程序进行升级时，请确保防火墙的 Flash 中有足够的空间。若剩余空间不足，需使用 **delete /unreserved** 命令将旧版本或其他文件永久删除，否则无法上传新文件。

- 下载应用程序/配置文件

```
ftp>      get                    键入<get>，表示进行下载操作。
remote file              键入防火墙端应用程序/配置文件名称。
local file        键入要保存的应用程序/配置文件的名称。
```

第四步：上传/下载成功后，退出 FTP 客户端程序。

```
ftp>quit                    键入<quit>，表示退出 ftp 连接。
```

4. 使用 detach 命令将 Web 文件解包分离出来。

FTP 方式下载完成应用程序/配置文件后。当应用程序中包含 Web 文件时，还需使用 **detach** 命令将其解包分离出来才能使用。

```
<VPNGateway> detach system
    System file length 7856557 bytes, http file length 834724 bytes.
<VPNGateway> dir
Directory of flash:/
   0   -rw-   8691281  Jun 16 2009 06:46:36   system
   1   -rw-      1830  Jun 17 2009 07:47:16   config.cfg
   2   -rw-    834724  Jun 18 2009 02:22:39   http.zip
```

如果要解包的文件没有捆绑 Web 文件，则提示文件中没有捆绑 Web 文件；如果没有指定解包出的 Web 文件名，则 Web 文件名缺省为 http.zip。