

H3C SECPATH1000FA&1000FS&100FA-CMW340-R1662P12版本发布

一、使用范围及配套说明：

H3C SECPATH1000FA&1000FS&100FA-CMW340-R1662P12版本正式发布，使用范围为国内市场。

表1：版本配套表

产品系列	H3C SecPath Series		
型号	SecPath F1000-A	SecPath F1000-S	SecPath F100-A
内存需求	512M	512M	256M
FLASH需求	最小16M	最小16M	最小16M
BootRom版本号	129	129	119
目标文件名称	SecPath 1000F A-CMW340-R1662P12.bin	SecPath 1000F S-CMW340-R1662P12.bin	SecPath 100FA-CMW340-R1662P12.bin
iMC版本号	iMC EAD 5.0 (E0101) iMC PLAT 5.0 (E0101) + L02 iMC UAM 5.0 (E0101)		
iNode	iNode PC 5.0 (E0101)		
NSM版本号	NSM V101		
备注	支持NSM的主机为：SecPath F1000-A/F1000-S/F1000-A		

二、增减特性说明：

表2：特性变更说明

版本号	项目	描述
SECPATH1000FA&1000FS&100FA-CMW340-R1662P12	硬件特性更新	新增特性：无。 增加单板：无。 删除特性：无。
	软件特性更新	新增特性：无。 删除特性：无。 修改特性：无。

三、相比前一版本解决的问题说明：

1. 问题ID—RTOD05491

首次发现版本：H3C SecPath 系列-CMW340-R1661

问题产生的条件：无。

问题现象：英文界面下，当修改默认URL动作的时候无法从deny修改为permit。

2. 问题ID—RTOD05493

首次发现版本：H3C SecPath 系列-CMW340-R1661

问题产生的条件：无。

问题现象：SSL VPN存在内存重复释放问题。

四、版本使用限制及注意事项：

1. 问题ID—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. 问题ID—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. 问题ID—LFD17844

IPSEC模板方式不支持多个策略。

4. 问题ID—LFD17843

动态获取的IP不能被其他接口所借用。

5. 问题ID—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通过防火墙。

6. 问题ID—LFD17760

由于SecPath F100-A LAN口硬件共用一个MAC，其LAN口只能配置一个VRRP组。

7. 问题ID—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. 问题ID—LFD18396

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

9. 问题ID—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. 问题ID—LFD15632

SECPATH设备不支持网管NCC组件升级功能。

11. 问题ID—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。

12. 问题ID—LFD00051

SECPATH 双机热备不支持NAT Server, NAT Static, NAT easy IP。

13. 问题ID—LFD20716

SECPATH不支持设备BIMS。

14. 问题ID—LFD00371

SECPATH防火墙双机热备不支持双主模式。

15. 问题ID—LFD18201

SECPATH防火墙双机热备不支持HA口与业务口绑定在同一接口。

16. 问题ID—LFD00394

SECPATH防火墙双机热备不支持子接口作为HA口。

17. 问题ID—LFD00330

双机热备大配置文件批量备份需要调大AD（报文通告）时间。

18. 问题ID—LFD00393

混合模式桥组虚接口上仅支持路由转发，GRE封装，防火墙包过滤和双机热备，其他不支持，只有以太网物理口，子接口及Tunnel口（GRE封装）方能加入桥组。

19. 问题ID—LFD00391

面向对象不支持除nat outbound及包过滤外的其他业务。

20. 问题ID—LFD19830

面向对象在用WEB配置时，不建议配置规格一半以上的地址对象，服务对象（会导致数据量大，导致网页反映慢）。

21. 问题ID—LFD00396

DAR只支持BT限流，其他协议不支持(HTTP、FTP、SMTP等)。

五、版本存在问题与规避措施：

1. RTOD01806

首次发现版本：H3C SECPATH 系列-CMW340-E1641

问题描述：当进行设备的flash读写操作时，有可能会造成Web服务器对客户端的响应有较大的时延。

规避措施：预先做一些访问该网关页面的操作，使页面加载进内存。可加速后继访问Web页面的速度。

2. RTOD01807

首次发现版本：H3C SECPATH 系列-CMW340-E1641

问题描述：TLAC(IP+port)有可能与本地已有的TCP服务发生冲突。

规避措施：远程主机上一般不提供TCP服务，可以停掉这些冲突的本地服务。

3. RTOD01808

首次发现版本：H3C SECPATH 系列-CMW340-E1641

问题描述：主机检查不支持对防火墙和杀毒软件的检查。

规避措施：目前不支持。

4. RTOD01810

首次发现版本：H3C SECPATH 系列-CMW340-E1641

问题描述：改变网关上的配置，新配置不能更新到已启动的客户端。

规避措施：建议管理员在用户不上线的时候进行配置修改。

5. RTD09272

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：DVPN性能较低，在持续流量较大的情况下，会导致Session中断

规避措施：在流量较大的应用环境中，建议采用GRE + IPSEC的方式来规避使用。

6. 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 per session特性。

7. RTD17677

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：在默认deny的包过滤规则下，透明模式接口在原先绑定以太网帧过滤acl的基础上，不能正常转发报文。

规避措施：在默认deny的包过滤规则下，透明模式接口必须在原先绑定ACL 以太网帧过滤规格（ACL 4000 - 4999规则）的基础上再绑定 ACL接口规则（ACL 1000 - 1999），才能正常转发报文,否则会被deny掉。

8. 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。

9. RTD09677

首次发现版本：H3C SecPath F 系列-CMW340-E1604

问题描述：设备作为LNS，当存在域用户和非域用户时，由不带域用户触发隧道选择L2TP组错误。

规避措施：配置时不让相同用户名的域用户与非域用户共存。

10. 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。

11. 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。

12. RTD00338

首次发现版本：H3C SecPath F 系列-CMW340-E1621

问题描述：SecPath作为安全设备LNS，EAD客户端成功拨入并且在线。SecPath下发安全区ACL，导致LNS设备内存错误。

规避措施：SecPath不配置ACL。

六、 升级时注意事项：

请务必参照《H3C SECPATH 系列-CMW340-R1662P12 版本使用指导书.doc》中的版本升级指导进行升级。

如要完整的了解该版本累计解决的问题，请参看配套的《H3C SECPATH 系列-CMW340-R1662P12 版本说明书.doc》。