b

YD

中华人民共和国信息产业部 发布

××××-××-××实施

××××-××-××发布

电信网和互联网安全防护基线配置要求及检测要求 网络设备

Baseline Requirements of Security Configuration for Telecom Network and Internet Network Equipment

（报批稿）

YD/T ××××—××××

中华人民共和国通信行业标准

# 目 次

目 次 I

前 言 II

电信网和互联网安全防护基线配置要求及检测要求 网络设备 1

1 范围 1

2 规范性引用文件 1

3 缩略语 1

4 网络设备安全防护基线配置要求及检测要求 1

4.1 网络设备安全防护基线配置及检测总体要求 1

4.2 Cisco路由器/交换机 3

4.3 HUAWEI路由器/交换机 25

4.4 Juniper路由器/交换机 34

# 前 言

本标准是“电信网和互联网安全防护体系”系列标准之一，该系列标准的结构及名称预计如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定通信网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》
25. 《传送网安全防护检测要求》
26. 《IP承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》
31. 《电信网和互联网物理环境安全等级保护检测要求》
32. 《电信网和互联网管理安全等级保护检测要求》
33. 《域名系统安全防护要求》
34. 《域名系统安全防护检测要求》
35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP网关系统安全防护要求》
38. 《WAP网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网 即时消息业务系统安全防护要求》
42. 《增值业务网 即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》（本标准）
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《移动互联网联网应用安全防护要求》
52. 《移动互联网联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》
54. 《公众无线局域网安全防护检测要求》
55. 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》（本标准）
56. 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》
61. 《电信和互联网用户个人电子信息保护通用技术要求和管理要求》
62. 《电信和互联网用户个人电子信息保护检测要求》

本标准与YD/T xxxx-xxxx《电信网和互联网安全防护基线配置要求及检测要求 安全设备》、YD/T xxxx-xxxx《电信网和互联网安全防护基线配置要求及检测要求 操作系统》、YD/T xxxx-xxxx《电信网和互联网安全防护基线配置要求及检测要求 中间件》、YD/T xxxx-xxxx《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》、YD/T xxxx-xxxx《电信网和互联网安全防护基线配置要求及检测要求 数据库》配套使用。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

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：中国联合网络通信集团有限公司、工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、华为技术有限公司

本标准主要起草人：张尼、李正、刘镝、魏薇、陈军、曹一生、樊洞阳

# 电信网和互联网安全防护基线配置要求及检测要求 网络设备

## 范围

本标准规定了路由器/交换机在安全配置方面的基本要求及参考操作。

本标准适用于安全防护体系中使用路由器/交换机的所有安全防护等级的网络和系统。

## 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。

YD/T xxxx-xxxx 《电信网和互联网安全防护管理指南》

YD/T xxxx-xxxx 《电信网和互联网安全等级保护实施指南》

YD/T xxxx-xxxx 《电信网和互联网安全风险评估实施指南》

YD/T xxxx-xxxx 《电信网和互联网灾难备份及恢复实施指南》

YD/T 1478-2006 《电信管理网安全技术要求》

YD/T xxxx-xxxx 《电信网和互联网管理安全等级保护要求》

## 缩略语

ARP Address Resolution Protocol 地址解析协议

BGP Border Gateway Protocol 边界网关协议

EGP Exterior Gateway Protocol 外部网关协议

FTP File Transfer Protocol 文件传输协议

HTTP Hypertext transfer protocol 超文本传输协议

IGP Interior Gateway Protocol 内部网关协议

IP Internet Protocol 网络互联协议

LDP Label Distribution Protocol 标签分发协议

MD5 Message Digest Algorithm 5 消息摘要算法

NTP Network Time Protocol 网络时间协议

OSPF Open Shortest Path First 开放式最短路径优先

RIPV2 Routing Information Protocol 路由信息协议

RSVP Resource Reservation Protocol 资源预留协议

SNMP Simple Network Management Protocol 简单网络管理协议

SQL Structured Query Language 结构化查询语言

SSH Secure Shell 安全壳协议

TCP Transmission Control Protocol 传输控制协议

UDP User Datagram Protocol 用户数据包协议

RW Read and Write 读写操作

## 网络设备安全防护基线配置要求及检测要求

### 网络设备安全防护基线配置及检测总体要求

电信网和互联网的网络设备的安全防护基线配置及检测应满足帐号口令、认证授权、日志安全、协议安全和其他安全等五个方面的要求，具体配置操作及检测方法应结合具体设备。总体要求主要包括：

1. 帐号口令
2. 应按照用户分配帐号，避免不同用户间共享帐号，避免用户帐号和设备间通信使用的帐号共享。为了控制不同用户的访问级别，应建立多用户级别。根据用户的业务需求，将用户帐号分配到相应的用户级别。
3. 应删除与设备运行、维护等工作无关的帐号。
4. 应配置定时帐户自动登出，如TELNET、SSH、HTTP等管理连接和CONSOLE口登录连接等，登出后用户需再次登录才能进入系统。
5. 对于采用静态口令认证技术的设备，口令长度应至少8位，并包括数字、小写字母、大写字母、标点和特殊符号4类中至少3类，且与帐号无相关性，同时应定期更换口令，更换周期不大于90天。
6. 静态口令应使用不可逆加密算法加密后以密文形式存放于配置文件中。
7. 应配置consol口密码保护功能。
8. 应修改root密码。
9. 认证授权
10. 在设备权限配置能力内，应根据用户的业务需要，配置其所需的最小权限。
11. 系统远程管理服务TELNET、SSH应只允许特定地址访问。
12. 应通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。
13. 日志安全
14. 应配置日志功能，对用户登录进行记录，并记录用户对设备的操作。
15. 应配置日志功能，记录对与设备相关的安全事件。
16. 应配置远程日志功能，所有设备日志均能通过远程日志功能传输到日志服务器，并支持至少一种通用的远程标准日志接口，如SYSLOG、FTP等。
17. 应开启NTP服务，保证日志功能记录的时间的准确性。路由器/交换机与NTP SERVER之间应开启认证功能。
18. 设置系统的配置更改信息应保存到单独的change.log文件内。
19. 协议安全
20. 应配置路由策略，禁止发布或接收不安全的路由信息，只接受合法的路由更新，只发布所需的路由更新。
21. 应配置路由器，以防止地址欺骗攻击，不使用ARP代理的路由器应关闭该功能。
22. 对于具备TCP/UDP协议功能的设备，应根据业务需要，配置基于源IP地址、通信协议TCP或UDP、目的IP地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。
23. 网络边界应配置安全访问控制，过滤已知安全攻击数据包，例如UDP1434端口（防止SQL slammer蠕虫）、TCP445、5800、5900（防止Della蠕虫）。
24. 对于使用IP协议进行远程维护的设备，应配置使用SSH等加密协议。
25. 启用动态IGP（RIPV2、OSPF、ISIS等）、EGP（BGP、MP-BGP等）协议或者LDP、RSVP标签分发协议时，应配置路由协议认证功能（如MD5加密认证），确保与可信方进行路由协议交互。
26. 应配置SNMP访问安全限制，设置可接收SNMP消息的主机地址，只允许特定主机通过SNMP访问网络设备。
27. 应修改SNMP的Community默认通行字，通行字应符合口令强度要求。
28. 应关闭未使用的SNMP协议及未使用RW权限。
29. 应配置为SNMP V2或以上版本。如接受统一网管系统管理，应配置为SNMP V3。
30. 其他安全
31. 应关闭未使用端口和不必要的网络服务或功能，使用的端口应添加符合实际应用的描述。
32. 应修改路由缺省BANNER语，BANNER应没有系统平台或地址等有碍安全的信息。
33. 应开启配置文件定期备份功能，定期备份配置文件。

### Cisco路由器/交换机

#### 帐号口令

|  |
| --- |
| 编号：NE-Cisco-帐号口令-01 |
| 要求内容：应按照用户分配帐号，避免不同用户间共享帐号，避免用户帐号和设备间通信使用的帐号共享。 |
| 操作指南：Router # config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# service password-encryptionRouter(config)# username ruser1 password 3d-zirc0niaRouter(config)# username ruser1 privilege 1Router(config)# username ruser2 password 2B-or-3BRouter(config)# username ruser2 privilege 1Router(config)# end Router# |
| 检测方法：使用show running-configrouter# show running-configBuilding configuration...Current configuration:!service password-encryption username ruser1 password 3d-zirc0niausername ruser1 privilege 1username ruser2 password 2B-or-3Busername ruser2 privilege 1 |
| 判定条件：1. 配置文件中，存在不同的帐号分配。
2. 网络管理员确认用户与帐号分配关系明确。
 |
| 补充说明：使用共享帐号容易造成职责不清。 |

|  |
| --- |
| 编号：NE-Cisco-帐号口令-02 |
| 要求内容：应删除与设备运行、维护等工作无关的帐号。 |
| 操作指南：Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# no username ruser3 |
| 检测方法：使用show running-configrouter# show running-configBuilding configuration…Current configuration：!username user1 privilege 1 password password1username nobodyuse privilege 1 password password1 |
| 判定条件：1. 配置文件存在多帐号。
2. 网络管理员确认所有帐号与设备运行、维护等工作有关。
 |
| 补充说明：删除不用的帐号，避免被利用。 |

|  |
| --- |
| 编号：NE-Cisco-帐号口令-03 |
| 要求内容：应配置定时账户自动登出，如TELNET、SSH、HTTP管理连接和CONSOLE口登录连接等。 |
| 操作指南：1. 参考配置操作：

I． Console登录连接超时。Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# line con 0Router(config-line)# exec-timeout 5 0II． 远程登录连接超时。Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# line vty 0 4Router(config-line)# exec-timeout 5 01. 补充操作说明：

本例配置连接超时时间为5分钟。 |
| 检测方法：使用show running-configrouter# show running-configBuilding configuration...Current configuration：!…line con 0login localexec-timeout 10 0exit…line vty 0 4login localaccess-class 2 inexec-timeout 10 0exit…ip ssh timeout 90… |
| 判定条件：每种登录方式均设置了timeout值。 |
| 补充说明：账户永久在线，会造成不合法的登录。 |

|  |
| --- |
| 编号：NE-Cisco-帐号口令-04 |
| 要求内容：静态口令应使用不可逆加密算法加密，以密文形式存放。如使用enable secret配置Enable密码，不使用enable password配置Enable密码。 |
| 操作指南： Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# enable secret 2-mAny-rOUtEsRouter(config)# no enable passwordRouter(config)# end |
| 检测方法：使用show running-configrouter# show running-configBuilding configuration...Current configuration:!service password-encryptionenable secret 5 $1oxphetTb$rTsF$EdvjtWbi0qA2gusername ciscoadmin password 7 Wbi0qA1$rTsF$Edvjt2gpvyhetTb |
| 判定条件：配置文件无明文密码字段。 |
| 补充说明：如果不加密，使用show running-config可以看到未加密的密码。 |

|  |
| --- |
| 编号：NE-Cisco-帐号口令-05 |
| 要求内容：应配置consol口密码保护功能。 |
| 操作指南：启用密码保护命令。Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# username brian privilege 1 password g00d+pa55w0rdRouter(config)# line con 0Router(config-line)# login localRouter(config-line)# endRouter # |
| 检测方法：使用show running-configrouter# show running-configBuilding configuration...Current configuration：!service password-encryptionusername myuser1 password mypasswordline con 0login localexec-timeout 10 0exit |
| 判定条件：通过consol登录，需要密码。 |
| 补充说明：不设置密码保护，则无须输入密码就可以登录到设备，并获得低级权限。 |

#### 日志安全

|  |
| --- |
| 编号：NE-Cisco-日志安全-01 |
| 要求内容：应配置远程日志功能，所有设备日志均能通过远程日志功能传输到日志服务器，并支持至少一种通用的远程标准日志接口，如SYSLOG、FTP等。 |
| 操作指南：1. 参考配置操作：

路由器/交换机侧配置。Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# logging onRouter(config)# logging trap informationRouter(config)# logging 192.168.0.100Router(config)# logging facility local6Router(config)# logging source-interface loopback0Router(config)# exitRouter# show loggingSyslog logging: enabled (0 messages dropped, 11 flushes, 0overruns)Console logging: level notifications, 35 messages loggedMonitor logging: level debugging, 35 messages loggedBuffer logging: level informational, 31 messages loggedLogging to 192.168.0.100, 28 message lines logged…Router#1. 补充操作说明：

假设把router日志存储在192.168.0.100的syslog服务器上。1. 路由器/交换机侧配置描述如下。

启用日志。记录日志级别设定“information”。记录日志类型设定“local6”。日志发送到192.168.0.100。日志发送源loopback0。配置完成可以使用“show logging”验证。1. 服务器侧配置描述如下。

Syslog服务器配置参考。在Syslog.conf上增加一行。# Save router messages to routers.loglocal6.debug /var/log/routers.log创建日志文件。# touch /var/log/routers.log1. 如果使用snmp存储日志配置描述如下。

Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# logging trap informationRouter(config)# snmp-server host 192.168.0.100 traps publicRouter(config)# snmp-server trap-source loopback0Router(config)# snmp-server enable traps syslogRouter(config)# exit Router# |
| 检测方法：使用show loggingRouter# show loggingSyslog logging: enabledConsole logging: disabledMonitor logging: level debugging, 266 messages logged.Trap logging: level informational, 266 messages logged.Logging to 192.180.2.238SNMP logging: disabled, retransmission after 30 seconds0 messages loggedRouter# |
| 判定条件：1. Syslog logging和SNMP logging至少有一个为“enabled”。
2. Logging to后面的主机名或IP指向日志服务器。
3. 通常记录日志数不为0。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-日志安全-02 |
| 要求内容：与记账服务器(如TACACS服务器)配合，应配置日志功能，记录用户对设备的操作，如帐号创建、删除和权限修改，口令修改，读取和修改设备配置，读取和修改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户帐号，操作时间，操作内容以及操作结果。 |
| 操作指南： 1. 参考配置操作：

Router# configure terminalEnter configuration commands，one per line. End with CNTL/Z.Router(config)# aaa new-modelRouter(config)# aaa accounting commands 1 default start-stop group tacacs+Router(config)# aaa accounting commands 15 default start-stop group tacacs+Router(config)# endRouter1#1. 补充操作说明：

使用TACACS+server |
| 检测方法：使用show running-configrouter1# show runn|include aaaBuilding configuration...Current configuration:!aaa new-modelaaa accounting commands 1 default start-stop group tacacs+aaa accounting commands 15 default start-stop group tacacs+ |
| 判定条件：配置了AAA模板的上述具体条目。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-日志安全-03 |
| 要求内容：应开启NTP服务，保证日志功能记录的时间的准确性。 |
| 操作指南： 1. 参考配置操作：

Router# config tEnter configuration commands，one per line. End with CNTL/Z.Router(config)# interface eth0/0Router(config-if)# no ntp disableRouter(config-if)# exitRouter(config)# ntp server 14.2.9.2 source loopback0Router(config)# exit1. 补充操作说明：

需要到每个端口开启NTP。 |
| 检测方法：1. 使用show running-config

router# show running-configBuilding configuration...Current configuration:!…no ntp disablentp update-calendarntp server 128.237.32.2ntp server 142.182.31.61. 使用show logging|include NTP

000019: Jan 29 10:57:52.633 EST: %NTP-5-PEERSYNC: NTP synced to peer 172.25.1.5000020: Jan 29 10:57:52.637 EST: %NTP-6-PEERREACH: Peer 172.25.1.5 is reachable |
| 判定条件：1. 存在ntp server配置条目。
2. 日志记录时间准确。
 |
| 补充说明：日志时间不准确导致安全事件定位的不准确。 |

#### 协议安全

|  |
| --- |
| 编号：NE-Cisco-协议安全-01 |
| 要求内容：应配置路由器/交换机，以防止地址欺骗。 |
| 操作指南： 1. 参考配置操作：
2. 对向内流量配置。

Router(config)# no access-list 100Router(config)# access-list 100 deny ip 192.168.10.0 0.0.0.255 any logRouter(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any logRouter(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any logRouter(config)# access-list 100 deny ip 0.0.0.0 0.255.255.255 any logRouter(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any logRouter(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any logRouter(config)# access-list 100 deny ip 192.0.2.0 0.0.0.255 any logRouter(config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any logRouter(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any logRouter(config)# access-list 100 deny ip host 255.255.255.255 any logRouter(config)# access-list 100 permit ip any 192.168.10.0 0.0.0.255Router(config)# access-list 100 deny ip any any logRouter(config)# interface eth0Router(config-if)# description External interface to 192.168.0./16 netRouter(config-if)# ip address 192.168.10.20 255.255.0.0Router(config-if)# ip access-group 100 inRouter(config-if)# exitRouter(config)# interface eth1Router(config-if)# description Internal interface to 192.168.10.0/24 netRouter(config-if)# ip address 192.168.10.250 255.255.255.0Router(config-if)# end1. 对向外流量配置。

Router(config)# no access-list 102Router(config)# access-list 102 permit ip 192.168.10.0 0.0.0.255 anyRouter(config)# access-list 102 deny ip any any logRouter(config)# interface eth 0/1Router(config-if)# description "internal interface"Router(config-if)# ip address 192.168.10.250 255.255.255.0Router(config-if)# ip access-group 102 in1. 补充操作说明：

假设内部网络是192.168.10.0。 |
| 检测方法：使用show running-configrouter# show running-config…access-list 10 deny ip 192.168.0.0 0.0.0.255 any logaccess-list 10 deny ip 127.0.0.0 0.255.255.255 any log…int f1/1description the outside interface of permeter routerip access-group 10 in…access-list 11 permit ip 192.168.0.0 0.0.0.255 anyaccess-list 11 deny ip any any loginterface s1/1description inside interface of perimeter routerip address 192.168.0.254 255.255.255.0ip access-group 11 in |
| 判定条件：各接口只转发属于自己ip范围内的源地址数据包流出 |
| 补充说明：地址欺骗可以造成内部网络的混乱，让某些被欺骗的计算机无法正常访问内外网，让网关无法和客户端正常通信。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-02 |
| 要求内容：路由器/交换机以UDP/TCP协议对外提供服务，供外部主机进行访问，如作为NTP服务器、TELNET服务器、TFTP服务器、FTP服务器、SSH服务器等，应配置路由器/交换机，只允许特定主机访问。 |
| 操作指南： 1. 要配置允许目的为14.1.1.2的所有DNS访问流量。

Router(config)# no access-list 140Router(config)# access-list 140 permit udp any host 14.1.1.2 eq 53Router(config)# access-list 140 deny udp any any log1. 要配置仅允许192.168.0.200访问路由器/交换机。

Router(config)# no access-list 12Router(config)# access-list 12 permit host 192.168.0.200 |
| 检测方法：使用show running-configrouter# show running-config…！telnet 、ssh服务器line vty 0 4login localaccess-class 2 inexec-timeout 10 0exit…！NTP服务器access-list 1 permit 10.1.1.1 0.0.0.255ntp access-group query-only 1…！ftp、tftp服务器ip ftp source-interface fastEthernet 0/0ip tftp source-interface fastEthernet 0/0 |
| 判定条件：相关服务存在access绑定。 |
| 补充说明： 对不信任的主机开启NTP、FTP等服务，会加大设备的危险。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-03 |
| 要求内容：对于具备TCP/UDP协议功能的设备，应根据业务需要，配置基于源IP地址、通信协议TCP或UDP、目的IP地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。 |
| 操作指南：1. 参考配置操作：
2. 要配置允许目的为14.1.1.2的所有DNS访问流量。

Router(config)# access-list 140 permit udp any host 14.1.1.2 eq 53Router(config)# access-list 140 deny udp any any log1. 要配置允许目的为14.1.0.0/16的所有DNS访问流量。

Router(config)# access-list 140 permit tcp any 14.1.0.0 0.0.255.255Router(config)# access-list 140 deny ip any any log1. 补充操作说明：

访问控制列表命令格式。1. 标准访问控制列表。

access-list list-number {deny | permit} source [source-wildcard] [log]1. 扩展访问控制列表。

access-list list-number {deny | permit} protocolsource source-wildcard source-qualifiersdestination destination-wildcard destination-qualifiers [ log | log-input] |
| 检测方法：使用show ip access-list[access-list-number | name]Router# show ip access-listExtended IP access list 101deny udp any any eq ntppermit tcp any anypermit udp any any eq tftppermit icmp any anypermit udp any any eq domain |
| 判定条件：1. 针对每个业务所需通讯，存在一条acl。
2. 对于非公共性服务，源IP和目标IP不能含有any。
3. 目标端口明确。
 |
| 补充说明：防止非正常业务占用过多带宽流量。 |

|  |
| --- |
| 编号： NE-Cisco-协议安全-04 |
| 要求内容：对于使用IP协议进行远程维护的设备，应配置使用SSH等加密协议。 |
| 操作指南： 1. 参考配置操作：
2. 配置主机名和域名。

router# config tEnter configuration commands, one per line. End with CNTL/Z.router(config)# hostname RouterRouter(config)# ip domain-name Router.domain-name1. 配置访问控制列表。

Router(config)# no access-list 12Router(config)# access-list 12 permit host 192.168.0.200Router(config)# line vty 0 4Router(config-line)# access-class 12 inRouter(config-line)# exit1. 配置帐号和连接超时。

Router(config)# service password-encryptionRouter(config)# username normaluser password 3d-zirc0niaRouter(config)# username normaluser privilege 1Router(config)# line vty 0 4Router(config-line)# login localRouter(config-line)# exec-timeout 5 01. 生成rsa密钥对。

Router(config)# crypto key generate rsaThe name for the keys will be: Router.domain-nameChoose the size of the key modulus in the range of 360 to2048 for your General Purpose Keys. Choosing a key modulusgreater than 512 may take a few minutes.How many bits in the modulus [512]: 2048Generating RSA Keys ...[OK]1. 配置仅允许ssh远程登录。

Router(config)# line vty 0 4Router(config-line)# transport input sshRouter(config-line)# exitRouter(config)#1. 补充操作说明：
2. 配置ssh要求路由器/交换机已经存在主机名和域名。
3. 配置访问控制列表，仅授权192.168.0.200访问192.168.0.100 ssh。
4. 配置远程访问里连接超时。
5. 生成rsa密钥对，如果已经存在可以使用以前的。默认存在rsa密钥对sshd就启用，不存在rsa密钥对sshd就停用。
6. 配置远程访问协议为ssh。
 |
| 检测方法：1. 使用show crypto key mypubkey rsa

Router(config)# show crypto key mypubkey rsa% Key pair was generated at: 06:07:49 UTC Jan 13 1996Key name: myrouter.example.comUsage: Signature KeyKey Data:005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001% Key pair was generated at: 06:07:50 UTC Jan 13 1996Key name: myrouter.example.comUsage: Encryption KeyKey Data:00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5 18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB 07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE211. 使用show running-config

router# show running-configBuilding configuration...Current configuration:!line vty 0 4transport input ssh |
| 判定条件1. 存在rsa密钥对。
2. 远程登录指定ssh协议。
 |
| 补充说明：使用非加密协议在传输过程中容易被截获口令。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-05 |
| 要求内容：网络边界应配置安全访问控制，过滤已知安全攻击数据包，例如udp 1434端口（防止SQL slammer蠕虫）、tcp445，5800，5900（防止Della蠕虫）。 |
| 操作指南： Router(config)# no access-list 102Router(config)# access-list 102 deny tcp any any eq 445 logRouter(config)# access-list 102 deny tcp any any eq 5800 logRouter(config)# access-list 102 deny tcp any any eq 5900 logRouter(config)# access-list 102 deny udp any any eq 1434 logRouter(config)# access-list 102 deny udp destination-port eq tftp logRouter(config)# access-list 102 deny tcp destination-port eq 135 logRouter(config)# access-list 102 deny udp destination-port eq 137 logRouter(config)# access-list 102 deny udp destination-port eq 138 logRouter(config)# access-list 102 deny tcp destination-port eq 139 logRouter(config)# access-list 102 deny udp destination-port eq netbios-ssn logRouter(config)# access-list 102 deny tcp destination-port eq 539 logRouter(config)# access-list 102 deny udp destination-port eq 539 logRouter(config)# access-list 102 deny tcp destination-port eq 593 log |
| 检测方法：使用show running-configrouter# show running-config…access-list 102access-list 102 deny tcp any any eq 445 logaccess-list 102 deny tcp any any eq 5800 logaccess-list 102 deny tcp any any eq 5900 logaccess-list 102 deny udp any any eq 1434 log… |
| 判定条件：存在类似acl，拒绝上述端口。 |
| 补充说明： 如果不进行上述设置将导致远程攻击者对部分常见应用发功攻击或病毒感染。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-06 |
| 要求内容：应禁用IP源路由功能，除非特别需要。应禁用PROXY ARP功能，除非路由器/交换机端口工作在桥接模式。应禁用直播（IP DIRECTED BROADCAST）功能。应在非可信网段内禁用IP重定向功能。应在非可信网段内禁用IP掩码响应功能。 |
| 操作指南：1. 禁用IP源路由。

Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# no ip source-route1. 禁用PROXY ARP。

Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# interface eth 0/0Router(config-if)# no ip proxy-arpRouter(config-if)# exitRouter(config)# interface eth 0/1Router(config-if)# no ip proxy-arpRouter(config-if)# exitRouter(config)# interface eth 0/2Router(config-if)# no ip proxy-arpRouter(config-if)# exitRouter(config)# interface eth 0/3Router(config-if)# no ip proxy-arpRouter(config-if)# end1. 禁用直播功能。

Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# interface eth 0/0Router(config-if)# no ip directed-broadcastRouter(config-if)# end1. 禁用IP重定向。

Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# interface eth 0/0Router(config-if)# no ip redirectsRouter(config-if)# end1. 禁用IP掩码响应。

Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# interface eth 0/0Router(config-if)# no ip mask-replyRouter(config-if)# end |
| 检测方法：1. 禁用IP源路由。

no ip source-route…1. 禁用PROXY ARP。

int s0/0no ip proxy-arp…1. 禁用直播功能，12.0之后默认。

int s0no ip directed-broadcast…1. 禁用IP重定向。

int s0no ip unreachableno ip redirects1. 禁用IP掩码响应。

no ip mask-repy |
| 判定条件：上述条目，在相应版本IOS中是“no”掉的。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-协议安全-07 |
| 要求内容：与RADIUS服务器、TACACS服务器、NTP服务器、SNMP V3主机等支持认证加密功能的主机进行通信时，应配置协议的认证加密功能，保证通信安全。 |
| 操作指南： 1. 参考配置操作：
2. TACACS服务器。

Router# configure terminalEnter configuration commands, one per line. End with CNTL/Z.Router(config)# tacacs-server host 192.168.6.18Router(config)# tacacs-server key Ir3@1yh8n#w9@swDRouter(config)# endRouter#1. RADIUS服务器。

Router# configure terminalEnter configuration commands, one per line. End with CNTL/Z.Router(config)# radius-server host 192.168.6.18Router(config)# radius-server key i\*Ma5in@u9p#s5wD1. 补充操作说明：

启用TACACS服务器、RADIUS服务器认证。 |
| 检测方法：使用show running-configrouter# show running-config…！TACACS服务器tacacs-server host 192.168.6.18acacs-server key Ir3@1yh8n#w9@swD…！RADIUS服务器 radius-server host 192.168.6.18  radius-server key i\*Ma5in@u9p#s5wD |
| 判定条件：1. 指定了服务器。
2. 设定了认证key。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-协议安全-08 |
| 要求内容：启用动态IGP（RIPV2、OSPF、ISIS等）或EGP（BGP）协议时，应配置路由协议认证功能，如MD5加密，确保与可信方进行路由协议交互。 |
| 操作指南：1. 配置Router1和Router2间Ospf启用MD5验证。
2. Router1配置。

Router1# config tEnter configuration commands, one per line. End with CNTL/Z.Router1(config)# router ospf 1Router1(config-router)# network 14.1.0.0 0.0.255.255 area 0Router1(config-router)# area 0 authentication message-digestRouter1(config-router)# exitRouter1(config)# int eth0/1Router1(config-if)# ip ospf message-digest-key 1 md5 r0utes-4-allRouter1(config-if)# endRouter1#1. Router2配置。

Router2# config tEnter configuration commands, one per line. End with CNTL/Z.Router2(config)# router ospf 1Router2(config-router)# area 0 authentication message-digestRouter2(config-router)# network 14.1.0.0 0.0.255.255 area 0Router2(config-router)# network 14.2.6.0 0.0.0.255 area 0Router2(config-router)# exitRouter2(config)# int eth0Router2(config-if)# ip ospf message-digest-key 1 md5 r0utes-4-allRouter2(config-if)# endRouter2#1. 配置Router1和Router2间EIGRP启用MD5验证。
2. Router1配置。

Router1# config tEnter configuration commands, one per line.End with CNTL/Z.Router1(config)# router eigrp 100Router1(config-router)# network 14.1.0.0 255.255.0.0Router1(config-router)# exitRouter1(config)# interface eth 0/1Router1(config-if)# ip authentication mode eigrp 100 md5Router1(config-if)# ip authentication key-chain eigrp 100 Router1-KCRouter1(config-if)# exitRouter1(config)# key chain Router1-KCRouter1(config-keychain)# key 1Router1(config-keychain-key)# key-string my-secret-keyRouter1(config-keychain-key)# send-lifetime 00:00:00 Oct 1 200300:00:00 Jan 1 2004 Router1(config-keychain-key)# accept-lifetime 00:00:00 Oct 1 200300:00:00 Jan 7 2004Router1(config-keychain-key)# endRouter1#1. Router2配置。

Router2# config tEnter configuration commands, one per line. End with CNTL/Z.Router2(config)# router eigrp 100Router2(config-router)# network 14.1.0.0 255.255.0.0Router2(config-router)# network 14.2.6.0 255.255.255.0Router2(config-router)# passive-interface eth1Router2(config-router)# exitRouter2(config)# interface eth 0Router2(config-if)# ip authentication mode eigrp 100 md5Router2(config-if)# ip authentication key-chain eigrp 100 Router2-KCRouter2(config-if)# exitRouter2(config)# key chain Router2-KCRouter2(config-keychain)# key 1Router2(config-keychain-key)# key-string my-secret-keyRouter2(config-keychain-key)# send-lifetime 00:00:00 Oct 1 200300:00:00 Jan 1 2004Router2(config-keychain-key)# accept-lifetime 00:00:00 Oct 1 200300:00:00 Jan 7 2004Router2(config-keychain-key)# endRouter2# |
| 检测方法：使用show running-configrouter# show running-config…！RIPV2router ripversion 2network 1.0.0.0int ethernet0/1ip rip authentication key-chain xxxxip rip authentication mode md5…！OSPFip ospf message-digest-key 1 md5 xxxxx…！EIGRPip authentication mode eigrp 1 md5 |
| 判定条件：有ip rip(ospf、eigrp等) md5的字段。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-协议安全-09 |
| 要求内容：采用BGP协议作为EGP协议时，应使用Route flap damping功能防止路由风暴。 |
| 操作指南： Router(config)# router bgp 27701Router(config-router)# neighbor 14.2.0.20 remote-as 26625Router(config-router)# bgp dampeningRouter(config-router)# end |
| 检测方法：使用show running-configrouter# show running-config…router bgp 27701neighbor 14.2.0.20 remote-as 26625bgp dampening |
| 判定条件：做了bgp dampening配置。 |
| 补充说明：bgp dampening用来抑制频繁浮动路由，当超过抑制阀值时就被抑制，从而防止bgp表的抖动。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-10 |
| 要求内容：在网络边界运行IGP或EGP动态路由协议时，应配置路由更新策略，只接受合法的路由更新，防止非法路由注入；应只发布所需的路由更新，防止路由信息泄漏。 |
| 操作指南： 使用ACL限制EIGRP不能向192.168.10.0/24传递。Router(config)# access-list 10 deny 192.168.10.0 0.0.0.255Router(config)# access-list 10 permit anyRouter(config)# router eigrp 100Router(config-router)# distribute-list 10 outRouter(config-router)# end |
| 检测方法：使用show running-configrouter# show running-config…access-list 10 deny 192.168.10.0 0.0.0.255access-list 10 permit anyrouter eigrp 100distribute-list 10 out |
| 判定条件：做了distribute-list的acl控制。 |
| 补充说明： 不进行访问控制容易引起非法路由注入和路由信息泄漏。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-11 |
| 要求内容：应修改SNMP的Community默认通行字，通行字符串应符合口令强度要求。 |
| 操作指南： 修改SNMP的Community默认通行字命令。Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# snmp-server community my\_readonly RORouter(config)# snmp-server community my\_readwrite RW |
| 检测方法：Router# show ru|include snmp-server communitysnmp-server community FullHardPassword |
| 判定条件：Fullhardpassword非默认，密码有一定强度。 |
| 补充说明： Fullhardpassword非默认，密码有一定强度。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-12 |
| 要求内容：应只与特定主机进行SNMP协议交互。 |
| 操作指南： 1. 参考配置操作：

使用ACL限制只与特定主机进行SNMP协议交互。Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# access-list 75 permit host 14.2.6.60Router(config)# access-list 75 deny any log 2.1. 补充操作说明：

仅允许14.2.6.60收集路由器/交换机SNMP信息。 |
| 检测方法：Router# show running….access-list 3 permit host 10.1.1.1access-list 3 deny any logsnmp-server community testc 3 |
| 判定条件：snmp绑定了acl。 |
| 补充说明： 有效设置对snmp服务的访问控制可以减少信息泄露。 |

|  |
| --- |
| 编号：NE-Cisco-协议安全-13 |
| 要求内容：未使用SNMP的WRITE功能时，应禁用SNMP的写（WRITE）功能。 |
| 操作指南：Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router (config)# no snmp-server community admin RW |
| 检测方法：Router# show running|include snmp-server….snmp-server community test ro |
| 判定条件：snmp权限为RO。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-协议安全-14 |
| 要求内容：启用LDP标签分发协议时，应配置LDP协议认证功能，如MD5加密，确保与可信方进行LDP协议交互。 |
| 操作指南： 1. 参考配置操作：

Router# mpls ldp vrf vpn1 password requiredRouter# configure terminalEnter configuration commands, one per line. End with CNTL/Z.Router(config)# mpls ldp neighbor vrf vpn1 10.1.1.1 password 7 nbrce1pwd1. 补充操作说明：

Router(config)# mpls ldp neighbor[vrf vrf-name]ip-address password[0|7]password- |
| 检测方法：使用show running-configrouter# show running-config|include mplsBuilding configuration...mpls ldp vrf vpn1 password requiredmpls ldp neighbor vrf vpn1 10.1.1.1 password 7 nbrce1pwd |
| 判定条件：配置认证功能及密码。 |
| 补充说明： |

#### 其他安全

|  |
| --- |
| 编号：NE-Cisco-其他安全-01 |
| 要求内容：应关闭未使用的端口，如路由器/交换机的AUX口。 |
| 操作指南： 关闭AUX。Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# line aux 0Router(config-line)# transport input noneRouter(config-line)# login localRouter(config-line)# exec-timeout 0 1Router(config-line)# no execRouter(config-line)# exit |
| 检测方法：使用show running-configrouter# show running-configBuilding configuration...Current configuration:!…line aux 0no exectransport input noneexit |
| 判定条件：Line aux应该设置为transport input none。 |
| 补充说明： 开启太多不必要的接口，很容易被外界扫描后被利用。 |

|  |
| --- |
| 编号：NE-Cisco-其他安全-02 |
| 要求内容：应修改路由缺省BANNER语，BANNER应没有系统平台或地址等有碍安全的信息。 |
| 操作指南：修改banner命令。Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# banner motd ^TLegal Notice: Access to this device is restricted.^T |
| 检测方法：通过vty，consol登录到路由器/交换机。 |
| 判定条件：欢迎界面、提示符等不包含敏感信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Cisco-其他安全-03 |
| 要求内容：应关闭不必要的网络服务或功能。应禁用TCP SMALL SERVERS。应禁用UDP SMALL SERVERS。应禁用Finger。应禁用HTTP SERVER。应禁用BOOTP SERVER。应关闭DNS查询功能；如要使用该功能，则显式配置DNS SERVER。 |
| 操作指南： 1. 参考配置操作：
2. 禁用tcp/udp small服务。

Router# config tEnter configuration commands, one per line. End with CNTL/Z.Router(config)# no service tcp-small-serversRouter(config)# no service udp-small-serversRouter(config)# exit1. 禁用Finger。

Router(config)# no ip fingerRouter(config)# no service finger1. 禁用HTTP SERVER。

Router(config)# no ip http server1. 禁用BOOTP SERVER。

Router(config)# no ip bootp server1. 关闭DNS查询功能。

Router(config)# no ip domain-lookup1. 显式配置DNS SERVER。

Router(config)# ip name-server 192.168.0.1Router(config)# ip domain-lookup1. 补充操作说明：

显式配置DNS SERVER指向192.168.0.1 |
| 检测方法：Router2# show auto secure config或show running…！禁用tcp/udp small服务。no service udp-small-serversno service tcp-small-servers…！禁用Finger。no service finger…！禁用HTTP SERVER。no ip http server…！禁用BOOTP SERVER。no ip bootp server！关闭DNS查询功能。no ip domain-lookup！显式配置DNS SERVER。ip name-server 192.168.0.1ip domain-lookup |
| 判定条件：上述条目的状态全部都是“no”。 |
| 补充说明：不必要的服务会加大设备的危险。 |

### HUAWEI路由器/交换机

#### 帐号口令

|  |
| --- |
| 编号：NE-HUAWEI-帐号口令-01 |
| 要求内容：应按照用户分配帐号，避免不同用户间共享帐号，避免用户帐号和设备间通信使用的帐号共享。 |
| 操作指南：aaalocal-user user1 password cipher PWD1local-user user1 service-type telnetlocal-user user2 password cipher PWD2local-user user2 service-type ftp#user-interface vty 0 4authentication-mode aaa |
| 检测方法：display current-configuration configuration aaa |
| 判定条件：用配置中没有的帐号去登录，结果是不能登录。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-帐号口令-02 |
| 要求内容：应删除与设备运行、维护等工作无关的帐号。 |
| 操作指南：aaaundo local-user test |
| 检测方法：display current-configuration configuration aaa |
| 判定条件：配置中用户信息被删除。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-帐号口令-03 |
| 要求内容：应配置定时账户自动登出，登出后用户需再次登录才能进入系统。 |
| 操作指南： user-interface vty 0 4idle-timeout 20 0user-interface con 0idle-timeout 20 0 |
| 检测方法：display current-configuration configuration user-interface |
| 判定条件：在超出设定时间后，用户自动登出设备。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-帐号口令-04 |
| 要求内容：对于采用静态口令认证技术的设备，口令长度应至少8位，并包括数字、小写字母、大写字母、标点和特殊符号4类中至少3类，且与帐号无相关性，同时应定期更换口令，更换周期不大于90天。 |
| 操作指南： aaalocal-user user1 password cipher NumABC%$ |
| 检测方法：display current-configuration configuration aaa |
| 判定条件：查看用户的口令长度是否至少8位，并包括数字、小写字母、大写字母、标点和特殊符号5类中至少2类，且与帐号无相关性；同时是否定期更换口令，更换周期不大于90天。对于加密的口令，通过登陆检测。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-帐号口令-05 |
| 要求内容：静态口令应使用不可逆加密算法加密后保存于配置文件中。 |
| 操作指南： local-user 8011 password cipher N`C55QK<`=/Q=^Q`MAF4<1!! |
| 检测方法：display current-configuration configuration aaa |
| 判定条件：用户的加密口令在buildrun中显示的密文。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-帐号口令-06 |
| 要求内容：应配置consol口密码保护功能。 |
| 操作指南： user-interface con 0set authentication password cipher consolPWD |
| 检测方法：display current-configuration configuration user-interface |
| 判定条件：用consol口登录，密码输入错误，不能登录。 |
| 补充说明： |

#### 认证授权

|  |
| --- |
| 编号：NE-HUAWEI-认证授权-01 |
| 要求内容：在设备权限配置能力内，应根据用户的业务需要，配置其所需的最小权限。 |
| 操作指南：aaalocal-user 8011 password cipher 8011local-user 8011 service-type telnetlocal-user 8011 level 0#user-interface vty 0 4authentication-mode aaa |
| 检测方法：display current-configuration configuration aaa |
| 判定条件：查看所有用户的级别都配置为其所需的最小权限。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-认证授权-02 |
| 要求内容：系统远程管理服务TELNET、SSH应只允许特定地址访问。 |
| 操作指南：Acl 2000Rule permit ip source 10.0.0.1 0User-interface vty 0 4acl 2000 inbound |
| 检测方法：display current-configuration configuration user-interface |
| 判定条件：通过设定acl，成功过滤非法访问。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-认证授权-03 |
| 要求内容：应通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。 |
| 操作指南：# 对远程登录用户先用RADIUS服务器进行认证，如果没有响应，则不认证。# 认证服务器IP地址为129.7.66.66，无备用服务器，端口号为默认值1812。# 配置RADIUS服务器模板。[Router]radius-server template shiva# 配置RADIUS认证服务器IP地址和端口。[Router-radius-shiva]radius-server authentication 129.7.66.66 1812# 配置RADIUS服务器密钥、重传次数。[Router-radius-shiva]radius-server shared-key it-is-my-secret[Router-radius-shiva]radius-server retransmit 2[Router-radius-shiva]quit# 进入AAA视图。[Router]aaa# 配置认证方案r-n，认证方法为先RADIUS，如果没有响应，则采用本地认证。[Router–aaa]authentication-scheme r-n[Router-aaa-authen-r-n]authentication-mode radius local[Router-aaa-authen-r-n]quit# 配置default域，在域下采用r-n认证方案、缺省的计费方案（不计费），shiva的RADIUS模板。[Router-aaa]domain default[Router-aaa-domain-default] authentication-scheme r-n[Router-aaa-domain-default]radius-server shiva |
| 检测方法：display current-configuration |
| 判定条件：对远程登陆用户先用RADIUS服务器进行认证，非法用户不可以登录。 |
| 补充说明： |

#### 日志安全

|  |
| --- |
| 编号：NE-HUAWEI-日志安全-01 |
| 要求内容：应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐号，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址。 |
| 操作指南： info-center console channel 0 |
| 检测方法：display logbuffer |
| 判定条件：在日志缓存上正确记录了日志信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-日志安全-02 |
| 要求内容：应配置日志功能，记录对与设备相关的安全事件。 |
| 操作指南： 1. 参考配置操作：

info-center enable1. 补充操作说明：

在系统模式下进行操作。 |
| 检测方法：display logbuffer |
| 判定条件：在日志缓存上正确记录了日志信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-日志安全-03 |
| 要求内容：应配置远程日志功能，所有设备日志均能通过远程日志功能传输到日志服务器，并支持至少一种通用的远程标准日志接口，如SYSLOG、FTP等。 |
| 操作指南： 1. 参考配置操作：

info-center loghost 202.38.1.10 facility local4 language english1. 补充操作说明：

在系统模式下进行操作。 |
| 检测方法：display current-configuration |
| 判定条件：是否正确配置了相应的日志服务器地址，日志服务器正确记录了日志信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-日志安全-04 |
| 要求内容：应开启NTP服务，保证日志功能记录的时间的准确性。路由器/交换机与NTP SERVER之间应开启认证功能。 |
| 操作指南：1. 参考配置操作：

ntp-service authentication-keyid 1 authentication-mode md5 N`C55QK<`=/Q=^Q`MAF4<1!!ntp-service unicast-server 2.2.2.2 authentication-keyid 11. 补充操作说明：

在系统模式下进行操作。 |
| 检测方法：disp ntp-service status |
| 判定条件：本地时钟与时钟源同步。 |
| 补充说明： |

#### 协议安全

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-01 |
| 要求内容：为防止ARP欺骗攻击，不使用ARP代理的路由器/交换机应关闭该功能。 |
| 操作指南：arp-proxy disable |
| 检测方法：display current-configuration configuration user-interface |
| 判定条件：不使用ARP代理服务的路由器/交换机关闭了该功能。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-02 |
| 要求内容：对于具备TCP/UDP协议功能的设备，应根据业务需要，配置基于源IP地址、通信协议TCP或UDP、目的IP地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。 |
| 操作指南： 1. 参考配置操作：

acl number 20000rule tcp source 1.1.1.1 0.0.0.0 destination 2.2.2.2 0.0.0.0 source-port eq ftp-data destination-port eq 30traffic classifier ddif-match acl 20000traffic behavior ddcar cir 2000 cbs 12288 green pass yellow remark red discardtraffic policy ddclassifier dd behavior dd precedence 0interface GigabitEthernet4/0/0undo shutdownip address 4.4.4.4 255.255.255.0traffic-policy dd inbound1. 补充操作说明：

在系统模式下进行操作。 |
| 检测方法：display traffic policy |
| 判定条件：通过测试打流，相关流被成功过滤。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-03 |
| 要求内容：对于使用IP协议进行远程维护的设备，应配置使用SSH等加密协议。 |
| 操作指南：# rsa peer-public-key quidway002public-key-code begin308186028180739A291ABDA704F5D93DC8FDF84C4274631991C164B0DF178C55FA833591C7D47D5381D09CE82913D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE40861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DCC48E3306367FE187BDD944018B3B69F3CBB0A573202C16BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125public-key-code endpeer-public-key end#aaalocal-user client001 password simple HUAWEIlocal-user client002 password simple quidwayauthentication-scheme default#authorization-scheme default#accounting-scheme default#domain default#ssh user client002 assign rsa-key quidway002ssh user client001 authentication-type passwordssh user client002 authentication-type RSA#user-interface con 0user-interface vty 0 4authentication-mode aaaprotocol inbound ssh# |
| 检测方法：disp current-configuration|begin ssh |
| 判定条件：通过抓包确定ssh登录的信息为加密信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-04 |
| 要求内容：动态路由协议口令应配置MD5加密。 |
| 操作指南：ospf 2area 0.0.0.0authentication-mode md5 1 cipher N`C55QK<`=/Q=^Q`MAF4<1!! |
| 检测方法：display current-configuration configuration ospf |
| 判定条件：Md5验证不通过的ospf邻居建立部不成功。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-05 |
| 要求内容：应制定路由策略，禁止发布或接收不安全的路由信息。 |
| 操作指南：acl number 2000rule 5 permit source 2.2.2.2 0route-policy dd permit node 0if-match acl 2000ospf 2area 0.0.0.0authentication-mode md5 1 cipher N`C55QK<`=/Q=^Q`MAF4<1!!filter route-policy dd import |
| 检测方法：display current-configuration configuration ospfdisplay route-policy |
| 判定条件：被禁止接收和发布的路由成功。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-06 |
| 要求内容：应关闭未使用的SNMP协议及未使用RW权限。 |
| 操作指南：Undo snmp enableundo snmp-agent community RWuser |
| 检测方法：display current-configuration |
| 判定条件：关闭snmp的设备不能被网管检测，关闭写权限的设备不能进行写操作。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-07 |
| 要求内容：应修改SNMP的Community默认通行字，通行字应符合口令强度要求。 |
| 操作指南：snmp-agent community read XXXX01 |
| 检测方法：display current-configuration |
| 判定条件：系统成功修改SNMP的Community为用户定义口令，非常规private或者public，并且符合口令强度要求。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-08 |
| 要求内容：应配置为SNMPV2或以上版本。 |
| 操作指南： snmp-agent sys-info version v3 |
| 检测方法：display current-configuration |
| 判定条件：成功使能snmpv2c、和v3版本。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-09 |
| 要求内容：应配置SNMP访问安全限制，只允许特定主机通过SNMP访问网络设备。 |
| 操作指南： snmp-agent community read XXXX01 acl 2000 |
| 检测方法：display current-configuration |
| 判定条件：通过设定acl来成功过滤特定的源才能进行访问。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-10 |
| 要求内容：启用LDP标签分发协议时，应配置LDP协议认证功能，如MD5加密，确保与可信方进行LDP协议交互。 |
| 操作指南：Mpls ldpmd5-password chiper LDPpwdMd5 |
| 检测方法：display current-configuration configuration mpls |
| 判定条件：认证不匹配的ldp邻居不能成功建立。 |
| 补充说明： |

#### 其他安全

|  |
| --- |
| 编号：NE-HUAWEI-其他安全-01 |
| 要求内容：应关闭未使用的端口。 |
| 操作指南： [HW-Ethernet3/0/0]shutdown |
| 检测方法：Display interface |
| 判定条件：未使用端口状态为admin down。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-其他安全-02 |
| 要求内容：应关闭不必要的服务，如FTP、TFTP服务等。 |
| 操作指南： undo ftp server |
| 检测方法：display current-configuration |
| 判定条件：不能访问设备的ftp等服务。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-其他安全-03 |
| 要求内容：系统使用的端口应添加符合实际应用的描述。 |
| 操作指南：set port name module/number description-string |
| 检测方法：display current-configuration configuration user-interface |
| 判定条件：正在使用中的端口配置了相应描述。 |
| 补充说明： |

### Juniper路由器/交换机

#### 帐号口令

|  |
| --- |
| 编号：NE-Juniper-帐号口令-01 |
| 要求内容：应按照不同的用户分配不同的帐号，避免不同用户间共享帐号，避免用户帐号和设备间通信使用的帐号共享。 |
| 操作指南： 1. 参考配置操作：

set system login user abc1set system login user abc21. 补充操作说明：
2. abc1和abc2是两个不同的帐号名称，可根据不同用户，取不同的名称。
3. 帐号取名建议使用，姓名的简写＋手机号码。
 |
| 检测方法：1. 用show configuration system login查看配置是否正确。
2. 在终端上用telnet方式登录路由器/交换机，输入帐号abc1和密码。
3. 在终端上用telnet方式登录路由器/交换机，输入帐号abc2和密码。
 |
| 判定条件：各帐号都可以登录路由器/交换机。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-帐号口令-02 |
| 要求内容：应删除与设备运行、维护等工作无关的帐号。 |
| 操作指南： 1. 参考配置操作：

delete system login user abc31. 补充操作说明：

abc3是与工作无关的帐号。 |
| 检测方法：1. 用show configuration system login查看配置是否正确。
2. 在终端上用telnet方式登录路由器/交换机，输入帐号abc3和密码。
 |
| 判定条件：被删除的与工作无关的帐号abc3不能登录。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-帐号口令-03 |
| 要求内容：为了控制不同用户的访问级别，应建立多用户级别。根据用户的业务需求，将用户帐号分配到相应的用户级别。 |
| 操作指南： 1. 参考配置操作：
2. 创建用户级别：

set system login class ABC1 permissions[view view-configuration]1. 将用户帐号分配到相应的用户级别：

set system login user abc1 class read-onlyset system login user abc2 class ABC1set system login user abc3 class super-user1. 补充操作说明：
2. ABC1是手工创建的组，该组具有的权限：查看设备运行状态（如接口状态、设备硬件状态、路由状态等），并且可以查看设备的配置。
3. read-only组具有的权限：查看设备运行状态，但不能查看设备的配置。
4. super-user是超级用户组，具有所有权限。
5. read-only和super-user是路由器/交换机已经创建的组，不需要手工创建。
6. abc1、abc2、abc3是不同的用户，它们分别分配到相应的用户级别。
 |
| 检测方法：用show configuration system login class ABC1查看配置。1. 在终端上用telnet方式登录路由器/交换机，输入帐号abc1和密码登录路由器/交换机。

用show interfaces terse查看端口状态。用show configuration查看路由器/交换机配置。用configure进入路由器/交换机的配置模式。1. 在终端上用telnet方式登录路由器/交换机，输入帐号abc2和密码登录路由器/交换机。

用show interfaces terse查看端口状态。用show configuration查看路由器/交换机配置。用configure进入路由器/交换机的配置模式。1. 在终端上用telnet方式登录路由器/交换机，输入帐号abc3和密码登录路由器/交换机。

用show interfaces terse查看端口状态。用show configuration查看路由器/交换机配置。用configure进入路由器/交换机的配置模式。 |
| 判定条件：1. 用户abc1属于组read-only，这个组只设置了查看设备运行状态权限,因而可使用show interfaces ters及其它查看路由器/交换机状态的命令，而不能使用show configuration和configure
2. 用户abc2属于组ABC1，这个组设置了查看设备运状态和查看路由器/交换机配置权限，因而可使用show interfaces ters和其它查看路由器/交换机状态命令及show configuration，不能使用configure
3. 用户abc3属于组super-user，这是超级用户组，具有所有权限，因而可使用全部命令。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-帐号口令-04 |
| 要求内容：应配置定时账户自动登出。 |
| 操作指南： 1. 参考配置操作：

set system login class abc idle-timeout 101. 补充操作说明：
2. abc是class组的名称。
3. 配置定时账户自动登出功能，仅能在自定义的class组里定义，不能在系统默认的组（如：super-user、read-only）中配置，因此建议自定义class组。
 |
| 检测方法：1. 使用show configuration system login class abc查看配置。
2. 在终端上用telnet方式登录路由器/交换机，输入帐号密码。
3. 让用户处于空闲状态，查看当时间超时是否自动登出。
 |
| 判定条件：当时间超时（这里设了10分钟），用户会自动退出路由器/交换机。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-帐号口令-05 |
| 要求内容：对于采用静态口令认证技术的设备，口令长度应至少8位，并包括数字、小写字母、大写字母、标点和特殊符号4类中至少3类，且与帐号无相关性，同时应定期更换口令，更换周期不大于90天。 |
| 操作指南： 1. 参考配置操作：

set system login user abc1 authentication plain-text-password1. 补充操作说明：
2. 输入指令回车后，将两次提示输入新口令（New password和Retype new password）。
3. 口令要求长度至少8位，并包括数字、小写字母、大写字母、标点和特殊符号5类中至少2类，且与帐号无相关性；同时定期更换口令，更换周期不大于90天。
 |
| 检测方法：1. 用show configuration system login查看配置是否正确。
2. 在终端上用telnet方式登录路由器/交换机，输入帐号abc1和密码。
 |
| 判定条件：可以登录路由器/交换机。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-帐号口令-06 |
| 要求内容：应修改root密码。 |
| 操作指南： 1. 参考配置操作：

set system root-authentication plain-text-password 1. 补充操作说明：
2. 输入指令回车后，将两次提示输入新口令（New password和Retype new password）；
3. 口令要求长度至少6位，并包括数字、小写字母、大写字母和特殊符号4类中至少2类。
 |
| 检测方法：1. 用show configuration system login查看配置是否正确。
2. 通过console口方式登录路由器/交换机，输入root帐号和密码。
3. 通过console口方式登录路由器/交换机，输入root帐号和空密码。
 |
| 判定条件：1. 输入root帐号和正确密码可以正常登录路由器/交换机。
2. 输入root帐号和空密码无法登录路由器/交换机。
 |
| 补充说明： |

#### 认证授权

|  |
| --- |
| 编号：NE-Juniper-认证授权-01 |
| 要求内容：在设备权限配置能力内，应根据用户的业务需要，配置其所需的最小权限。 |
| 操作指南： 1. 参考配置操作：
2. 创建用户级别，即创建用户的配置权限。

set system login class ABC1 permissions configureset system login class ABC1 allow-configuration "routing-可选ions static|interfaces|chassis fpc" set system login class ABC2 permissions[configure routing-control]1. 将用户帐号分配到相应的用户级别。

set system login user abc1 class ABC1set system login user abc2 class ABC2set system login user abc3 class super-user1. 补充操作说明：
2. ABC1组具有的权限：可配置interfaces，可配置routing-可选ions中的static，可配置chassis中的fpc。
3. ABC2组具有的权限：可配置有关于路由的所有配置，包括routing-可选ions、protocols、policy-可选ions、routing-instances等。
4. allow-configuration参数是以等级来限制，可以限制各个等级的配置，可以细化到各个小等级。
5. permissions参数是以功能来限制，限制的范围较大。
6. allow-commands参数是以具体的指令来限制，allow-comands参数需要设定具体指令，不建议使用。
 |
| 检测方法：1. 用show configuration system login class ABC1查看配置。

用show configuration system login class ABC2查看配置。1. 在终端上用telnet方式登录路由器/交换机，输入帐号abc1和密码。

使用configure进入配置模式。set routing-可选ions staticset interfacesset chassis fpc使用其它set命令检测。在终端上用telnet方式登录路由器/交换机,输入帐号abc2和密码。 使用configure进入配置模式。set policy-可选ionsset protocolsset routing-instancesset routing-可选ions使用其它set命令检测。在终端上用telnet方式登录路由器/交换机，输入帐号abc3和密码。 使用configure进入配置模式。使用set命令以及其它命令检测。 |
| 判定条件：1. 帐号abc1属于组ABC1，该组只能配置routing-可选ions static、interfaces、Chassis fpc项里的内容，不能做其它未授权的配置。
2. 帐号abc2属于组ABC2，该组只能配置关于路由的所有配置，包括routing-可选ions、protocols、policy-可选ions、routing-instances等，不能做其它未授权的配置。
3. 帐号abc3属于组super-user，拥有全部配置权限。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-认证授权-02 |
| 要求内容：系统远程管理服务TELNET、SSH应只允许特定地址访问。 |
| 操作指南： 1. 参考配置操作：

set firewall filter abc term a from source-address 10.1.1.1/32set firewall filter abc term a from source-address 10.1.1.2/32set firewall filter abc term a then acceptset firewall filter abc term b from protocol tcp port telnetset firewall filter abc term b then rejectset firewall filter abc term c then accept1. 补充操作说明：
2. abc为filter名称，可自定义。
3. 10.1.1.1/32和10.1.1.2/32上允许telnet的主机IP地址。
4. term a实现的功能：允许特定地址访问。
5. term b实现的功能：除了允许特定地址访问之外，不允许其它地址访问telnet端口。
 |
| 检测方法：1. 使用show configuration firewall filter abc查看配置。
2. 在终端上以源地址10.1.1.1或10.1.1.2 通过telnet方式登录路由器/交换机。
3. 在终端上以非允许的IP地址为源地址使用telnet连接到路由器/交换机。
 |
| 判定条件：1. 以源地址10.1.1.1或10.1.1.2通过telnet方式能够登录路由器/交换机。
2. 以非允许的IP为源地址通过telnet方式无法登陆路由器/交换机。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-认证授权-03 |
| 要求内容：应通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。 |
| 操作指南： 1. 参考配置操作：

set system authentication-order radiusset system authentication-order passwordset system radius-server 10.1.1.1set system radius-server 10.1.1.2set system radius-server 10.1.1.1 port 1645set system radius-server 10.1.1.2 port 1645set system radius-server 10.1.1.1 secret abc123set system radius-server 10.1.1.2 secret abc1231. 补充操作说明：
2. 配置认证方式可通过radius和本地认证。
3. 10.1.1.1和10.1.1.2是radius认证服务器的IP地址，建议建立两个radius认证服务器作互备。
4. port 1645是radius认证开启的端口号，可根据本地radius认证服务器开启的端口号配置。
5. abc123是与radius认证系统建立连接所设定的密码，建议与radius认证服务器建立连接时使用密码认证建立连接。
 |
| 检测方法：1. 使用show configuration system查看配置。
2. 查看Radius服务器配置。
3. 用本地帐号登录到路由器/交换机，ping Radius服务器地址10.1.1.1和10.1.1.2。
4. 使用Raidus服务器建立的帐号通过telnet方式登录路由器/交换机。
5. 检查授权内的命令是否可用及其它未授权的命令。
 |
| 判定条件：1. 可以正常ping通Radius服务器的IP地址。
2. 用户可以登录路由器/交换机。
3. 用户只能使用授权内的命令。
 |
| 补充说明： |

#### 日志安全

|  |
| --- |
| 编号：NE-Juniper-日志安全-01 |
| 要求内容：应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐号，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址。 |
| 操作指南：1. 参考配置操作：

set system syslog file author.log authorization info1. 补充操作说明：
2. author.log是记录登录信息的log文件，该文件名可手工定义。
3. author.log保存在路由器/交换机上。
 |
| 检测方法：1. 使用show configuration system syslog查看配置。
2. 在终端上使用telnet方式登录路由器/交换机，输入帐号密码。
3. 使用show log author.log查看日志。
 |
| 判定条件：在author.log中查看到帐号、登录时间和源IP等内容。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-日志安全-02 |
| 要求内容：应配置日志功能，记录用户对设备的操作，比如帐号创建、删除和权限修改，口令修改，读取和修改设备配置。记录需要包含用户帐号，操作时间，操作内容以及操作结果。 |
| 操作指南： 1. 参考配置操作：

set system syslog file messages any any1. 补充操作说明：
2. messages是记录所有log的文件，该文件名可手工定义。
3. messages保存在路由器/交换机上。
 |
| 检测方法：1. 使用show configuration system syslog查看配置。
2. 在终端上以telnet方式登录路由器/交换机，输入帐号密码。
3. 进行创建删除帐号修改帐号密码修改设备配置操作；
4. 用show log message.log查看日志。
 |
| 判定条件：在message.log中查看到用户的操作内容、操作时间、操作结果等所有路由器/交换机的log信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-日志安全-03 |
| 要求内容：应配置日志功能，记录对与设备相关的安全事件，比如记录路由协议事件和错误。 |
| 操作指南： 1. 参考配置操作：

set system syslog file daemon.log daemon warningset system syslog file firewall.log firewall warning1. 补充操作说明：
2. daemon.log是记录路由协议事件的文件，该文件名可手工定义。
3. firewall.log是记录路由安全事件的文件，该文件名可手工定义。
4. daemon和firewall可定义九个等级，建议将其设定为warning级，即仅记录warning级以上的安全事件。
 |
| 检测方法：1. 使用show configuration查看配置。
2. 重启路由进程，如bgp，ospf。（该操作可能会影响业务、不建议现网操作）
3. 使用show log daemon.log和show log firewall.log查看日志。
 |
| 判定条件：在daemon.log中查看到路由事件及相关路由信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-日志安全-04 |
| 要求内容：应配置远程日志功能，将需要重点关注的日志内容上传到日志服务器。 |
| 操作指南： 1. 参考配置操作：

set system syslog host 10.1.1.1 any noticeset system syslog host 10.1.1.1 log-prefix Router1set system syslog host 10.1.1.2 any noticeset system syslog host 10.1.1.2 log-prefix Router21. 补充操作说明：
2. 10.1.1.1和10.1.1.2是远程日志服务器的IP地址，建议建设两个远程日志服务器作为互备。
3. syslog有九个等级的记录信息，建议将notice级以上的信息上传到远程日志服务器。
4. Router1为路由器/交换机的主机名称。
 |
| 检测方法：1. 使用show configuration system syslog查看配置。
2. 登录远程日志服务器查看日志。
 |
| 判定条件：日志服务器上记录相关路由器/交换机的notice级以上的信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-日志安全-05 |
| 要求内容：设置系统的配置更改信息应保存到单独的change.log文件内。 |
| 操作指南： 1. 参考配置操作：

set system syslog file change.log change-log info1. 补充操作说明：
2. change.log是记录配置更改的文件，该文件名可手工定义。
3. change.log保存在路由器/交换机上。
 |
| 检测方法：1. 使用show configuration system syslog查看配置。
2. 在终端上以telnet方式登录路由器/交换机，输入帐号密码。
3. 进行创建/删除帐号、修改用户密码和修改设备配置操作。
4. 用show log change.log查看日志。
 |
| 判定条件：在change.log中查看到用户的操作内容、操作时间。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-日志安全-06 |
| 要求内容：应开启NTP服务，保证日志功能记录的时间的准确性。路由器/交换机与NTP SERVER之间应开启认证功能。 |
| 操作指南： 1. 参考配置操作：

set system ntp authentication-key 1 type md5 value abc123set system ntp server 10.1.1.1set system ntp server 10.1.1.21. 补充操作说明：
2. abc123是路由器/交换机与NTP SERVER之间md5认证密码。
3. 10.1.1.1和10.1.1.2是NTP SETVER的IP地址，建议建立两个NTP服务器作为互备。
 |
| 检测方法：1. 使用show configuration system ntp查看配置。
2. 使用show system uptime查看路由器/交换机时间，并与北京时间对比。
3. 使用show ntp associations查看路由器/交换机是否与NTP服务器同步。
4. 使用show ntp status查看路由器/交换机时间同步状态。
 |
| 判定条件1. 用show ntp associations查看信息。

remote refid st t when poll==============================\* ROUTER1 10.1.1.1 2 u 641 1024+ ROUTER2 10.1.1.2 2 u 713 1024reach delay offset jitter==============================377 0.964 -24.126 0.067377 4.490 -12.013 0.457ROUTER1前面的(\*)表示ROUTER1是已与路由器/交换机时间同步的NTP服务器，(+)为备用的NTP服务器。1. 用show ntp status查看信息。

status=0644 leap\_none, sync\_ntp, 4 events, event\_peer/strat\_chg,version="ntpd 4.1.0-a Wed Oct 5 18:44:40 GMT 2005 (1)",processor="i386", system="JUNOS7.3R2.7", leap=00, stratum=3,precision=-28, rootdelay=9.814, rootdispersion=102.250, peer=42484,refid=ROUTER1.gd.cnmobile.net,reftime=ca227da4.4b3ffac1 Wed, Jun 20 2007 0:07:00.293, poll=10,clock=ca2280ce.02849cb2 Wed, Jun 20 2007 0:20:30.009, state=4,offset=-17.830, frequency=85.438, jitter=28.377, stability=0.048“sync\_ntp”表示路由器/交换机时间已与NTP服务器同步，“sync\_unspec”即未同步。 |
| 补充说明： |

#### 协议安全

|  |
| --- |
| 编号：NE-Juniper-协议安全-01 |
| 要求内容：对于具备TCP/UDP协议功能的设备，应根据业务需求，配置基于源IP地址、TCP/UDP、目的IP地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。 |
| 操作指南：1. 参考配置操作：

set firewall filter abc term a from source-address 10.1.1.1/32set firewall filter abc term a from destination-address 10.1.2.1/32set firewall filter abc term a from protocol tcpset firewall filter abc term a from protocol udpset firewall filter abc term a from source-port 445set firewall filter abc term a from destination-port 145set firewall filter abc term a then acceptset firewall filter abc term b then reject1. 补充操作说明：
2. abc为filter的名称，可手工定义。
3. a、b为term的名称，可手工定义，一个filter可设定多个term。
4. 第一条指令为配置基于源IP地址的过滤，10.1.1.1/32为源IP地址，源地址可以是主机IP，也可以是网段。
5. 第二条指令为配置基于目的IP地址的过滤，10.1.1.2/32为目的IP地址，目的IP地址可以是主机IP，也可以是网段。
6. 第三条指令为配置TCP。
7. 第四条指令为配置UDP。
8. 第五条指令为配置基于源端口，445是端口号，端口号可根据需求设置。
9. 第六条指令为配置基于目的端口，145是端口号，端口号可根据需求设置。
10. 第七条指令为允许，即符合from里的条件时，允许该数据包通过；若设置为reject，则符合from里的条件时，不允许数据包通过。
11. 第八条指令拒绝为所有不符合term a条件的数据包通过（then之后可根据需求设置为reject或者accept）。
12. 必须使用如下指令将filter绑定到指定接口，该filter才能生效：

set interfaces fe-0/0/0 unit 0 family inet filter input abc。 |
| 检测方法：1. 使用show configuration firewall filter abc查看配置。
2. 将终端的IP地址设为10.1.1.1。
3. 在终端安装Nmap端口扫描工具。（本例基于windows XP2系统）
4. 在DOS下输入：nmap -sS -g 445 10.1.2.1 –p 145

该指令为以源端口445访问主机IP地址10.1.2.1的TCP 145端口。1. 用namp访问其它非业务端口，如访问80端口。

在DOS下输入：nmap –sS 10.1.2.1 –p 80该指令为以任何端口访问10.1.2.1的TCP 80端口。1. 运行真实业务测试业务流量和非业务流量。
 |
| 判定条件：1. 用nmap -sS -g 445 10.1.2.1 –p 145扫描端口，出现如下信息为正常：

Interesting ports on 10.1.2.1:PORT STATE SERVICE145/tcp open uaac1. 用nmap –sS 10.1.2.1 –p 80访问非业务端口，出现如下信息为正常：

Interesting ports on 10.1.2.1:PORT STATE SERVICE80/tcp closed http1. 真实业务流量正常通过，非业务流量禁止通过。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-02 |
| 要求内容：网络边界应配置安全访问控制，过滤安全攻击数据包，例如udp 1434端口（防止SQL slammer蠕虫）、tcp445，5800，5900（防止Della蠕虫）。 |
| 操作指南： 1. 参考配置操作：

set firewall filter abc term a from protocol udp destination-port 1434set firewall filter abc term a then discardset firewall filter abc term b from protocol tcp port 445set firewall filter abc term b then discardset firewall filter abc term c from port[5800 5900]set firewall filter abc term c then discardset firewall filter abc term d then accept1. 补充操作说明：
2. term a过滤udp 1434端口。
3. term b过滤tcp 445端口。
4. term c过滤5800和5900端口。
5. 务必在最后的term放通所有业务。
6. 将该filter应用于网络边界端口，使用

set interfaces fe-0/0/0 unit 0 family inet filter input abc |
| 检测方法：1. 使用show configuration firewall查看配置。
2. 路由器/交换机下连接一台服务器，开放1434、445、5800 、5900端口。
3. 路由器/交换机边界外通过telnet方式访问服务器1434、445、5800 、5900端口。
4. telnet服务器其它未被限制的端口。
 |
| 判定条件：1. 不能telnet 1434、445、5800、5900被限制的端口。
2. 能telnet其它未被限制的端口。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-03 |
| 要求内容：启用动态路由协议（BGP/ MP-BGP /OSPF等）时，应配置带加密方式的身份验证功能，相邻路由器/交换机只有在身份验证通过后，才能互相通告路由信息。 |
| 操作指南： 1. 参考配置操作：

set protocols bgp group abc neighbor 10.1.1.1 authentication-key abc123set protocols ospf area 0.0.0.0 authentication-type md51. 补充操作说明：

10.1.1.1为对端BGP peer的IP地址，可根据需求设定。 |
| 检测方法：1. 使用show configuration protocol查看配置。
2. 使用show bgp neighbor查看BGP邻居状态。
3. 使用show route protocol bgp brief查看BGP路由表。
4. 使用show ospf neighbor查看OSPF邻居状态。
5. 使用show route protocol ospf brief查看OSPF路由表。
6. 使用ping检查路由连通性。
 |
| 判定条件：1. 配置已经启用加密的身份认证。
2. BGP邻居处于establish状态，能学到邻居的路由。
3. OSPF邻居处于full状态，能学到邻居的路由。
4. 路由连通。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-04 |
| 要求内容：配置MP-BGP路由协议，应配置MD5加密认证，通过MD5加密认证建立peer。 |
| 操作指南： 1. 参考配置操作：

set protocols bgp group abc neighbor 10.1.1.1 authentication-key abc1231. 补充操作说明：
2. abc为group的名称，可根据需求设定。
3. 10.1.1.1为对端peer的IP地址，可根据需求设定。
4. abc123为MD5加密认证的认证密码，该密码和对端peer的密码一致。
 |
| 检测方法：1. 使用show configuration protocol bgp查看配置。
2. 使用show bgp neighbor查看BGP邻居状态。
3. 使用show route protocol bgp brief查看BGP路由表。
4. 使用ping检查路由的连通性。
 |
| 判定条件：1. 启用加密的身份认证。
2. BGP邻居处于establish状态，能学到邻居的路由。
3. 路由连通。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-05 |
| 要求内容：配置非点对点OSPF协议，应配置MD5加密认证，通过MD5加密认证建立neighbor。 |
| 操作指南：1. 参考配置操作：

set protocols ospf area 0.0.0.0 authentication-type md5set protocols ospf area 0.0.0.0 interface fe-0/0/0.0 authentication md5 1 key abc1231. 补充操作说明：
2. fe-0/0/0为用于建立OSPF的端口，可根据需求设置。
3. abc123为MD5加密认证的认证密码，该密码和对端peer的密码一致。
 |
| 检测方法：1. 使用show configuration查看配置。
2. 使用show ospf neighbor查看OSPF邻居状态。
3. 使用show route protocol ospf brief查看OSPF路由表。
4. 使用ping检查路由连通性。
 |
| 判定条件：1. OSPF邻居处于full状态，能学到邻居路由。
2. 路由连通。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-HUAWEI-协议安全-06 |
| 要求内容：应制定路由策略，禁止发布或接收不安全的路由信息。 |
| 操作指南： 1. 参考配置操作：

set policy-可选ions policy-statement abc term a from route-filter 10.0.0.0/24 exactset policy-可选ions policy-statement abc term a then acceptset policy-可选ions policy-statement abc term b then reject1. 补充操作说明：
2. abc是路由策略的名称，该名称可根据需求定义。
3. 10.0.0.0/24是将发布（或接收）或者禁止发布的（或接收）路由，可根据需求设置。
4. 制定路由策略后，必须将该策略应用于路由协议才生效。
 |
| 检测方法：1. 使用show policy abc查看配置。
2. 在邻居的路由器/交换机上使用show route查看路由表。
3. 在邻居的路由器/交换机上使用ping测试连通性。
 |
| 判定条件：1. 邻居路由器/交换机只收到被允许发布的路由。
2. 所发布的路由连通。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-07 |
| 要求内容：应配置SNMP访问安全限制，只允许特定主机通过SNMP访问网络设备。 |
| 操作指南： 1. 参考配置操作：

set snmp community abcd123 clients 10.1.1.1/32set snmp community abcd123 clients 10.1.2.1/32set snmp community abcd123 clients ready-only1. 补充操作说明：
2. abcd123是communtity字符串，可根据需求定义，但必须和client主机一致。
3. 10.1.1.1和10.1.2.1是主机IP地址，即允许10.1.1.1.和10.1.2.1主机通过SNMP访问网络设备
4. 未在client列表中的主机，不允许通过SNMP访问网络设备。
5. 设置主机访问网络设备具有读权限，可根据需求设置为具有读写权限（read-write）。
 |
| 检测方法：1. 使用show configuration snmp查看配置。
2. 使用show snmp statistics查看snmp统计信息。
3. 使用非允许的主机通过SNMP访问网络设备。
4. 查看SNMP主机。
 |
| 判定条件：1. 主机10.1.1.1.和10.1.2.1收到网络设备的SNMP信息。
2. 非允许的主机不能收到网络设备的SNMP信息。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-08 |
| 要求内容：应关闭未使用的SNMP协议及未使用的RW权限。 |
| 操作指南： 默认关闭所有SNMP功能的，按需求启动相应的功能即可。 |
| 检测方法：1. 使用show configuration snmp查看配置。
2. 使用show snmp statistics查看snmp统计信息。
 |
| 判定条件：查看配置，权限设置符合需求。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-09 |
| 要求内容：应配置为SNMP V2或以上版本。 |
| 操作指南： 1. 参考配置操作：

set snmp trap-group abc123 version v21. 补充操作说明：

abc123是trap-group组的名称，可根据需求设置。 |
| 检测方法：使用show configuration snmp查看配置。 |
| 判定条件：查看配置是V2。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-10 |
| 要求内容：如接受统一网管系统管理，应配置SNMP V3。 |
| 操作指南： 1. 参考配置操作：

set snmp v3 usm local-engine user abc1 authentication-md5 authentication-keyset snmp v3 vacm access group CMNET default-context-prefix security-model usm security-level authentication read-view readonlyset snmp v3 target-address ta1 address 10.1.1.1set snmp v3 target-address ta1 target-parameters tp1set snmp v3 target-parameters tp1 parameters message-processing-model v3set snmp v3 target-parameters tp1 parameters security-model usmset snmp v3 target-parameters tp1 parameters security-level noneset snmp v3 target-parameters tp1 parameters security-name abcset snmp v3 snmp-community index1 community-name ABCset snmp v3 snmp-community index1 security-name abcset snmp engine-id use-mac-addressset snmp view readonly oid .1.3.6.1.2.1.2 include1. 补充操作说明：
2. 第一条指令设SNMP V3的用户abc1采用MD5方式认证。
3. 第二条指令设SNMP的访问控制模块（VACM）的参数，访问组为CMNET，安全模式采用基于用户的模式（USM），安全级别为验证级别，设定视图为readonly。
4. 第三条指令设SNMP主机组ta1，该组包含的地址为211.139.136.100。
5. 第四条指令设主机组ta1的具体参数引用参数集tp1。
6. 第五至八条指令设参数集tp1的具体内容，信息处理采用SNMP V3模式，安全模式采用基于用户的模式（USM），安全级别采用非验证，安全名设为abc。
7. 第九至十条指令设SNMP团体号为ABC，安全名为abc。
8. 第十一条指令设SNMP引擎ID。
9. 第十二条指令设视图readonly管理对象标识。
 |
| 检测方法：1. 使用show configuration snmp查看配置。
2. 使用show snmp v3查看各项状态。
3. 使用show snmp statistics查看SNMP数据包统计。
4. 查看SNMP主机10.1.1.1。
 |
| 判定条件：1. 使用show snmp v3查看时，各项配置状态为active。
2. 使用show snmp statistics查看时，input和output都有流量，Get requests和Get response都有相应统计数值。
3. SNMP主机收到路由器/交换机的SNMP信息。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-11 |
| 要求内容：应配置可接收SNMP消息的主机地址。 |
| 操作指南： 1. 参考配置操作：

set snmp trap-group abc123 targets 10.1.1.1set snmp trap-group abc123 targets 10.1.2.11. 补充操作说明：
2. abc123为trap-group组名称，可根据需求设置。
3. 10.1.1.1和10.1.2.1是主机IP地址，即允许10.1.1.1.和10.1.2.1主机接收该网络设备的SNMP消息。
 |
| 检测方法：1. 使用show configuration snmp查看配置。
2. 查看IP地址为10.1.1.1和10.1.2.1的主机。
 |
| 判定条件：主机10.1.1.1和10.1.2.1收到路由器/交换机的SNMP信息。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-协议安全-12 |
| 要求内容：启用RSVP标签分发协议时，应配置RSVP协议认证功能，如MD5加密。 |
| 操作指南：1. 参考配置操作：

set protocols rsvp interface fe-0/0/0.0 authentication-key abc1231. 补充操作说明：

abc123为MD5加密密码。 |
| 检测方法：1. 使用show configuration protocols rsvp查看配置。
2. 使用show rsvp neighbor查看rsvp邻居状态。
3. 使用show rsvp session查看rsvp session。
 |
| 判定条件：1. 各邻居状态为UP。
2. 各RSVP session状为UP。
 |
| 补充说明： |

#### 其他安全

|  |
| --- |
| 编号：NE-Juniper-其他安全-01 |
| 要求内容：应开启配置文件定期备份功能，定期备份配置文件。 |
| 操作指南： 1. 参考配置操作：

set system archival configuration transfer-interval 2880set system archival configuration archive-sites ftp://juniper@10.1.1.1 password abc123set system archival configuration archive-sites ftp://juniper@10.1.1.2 password abc1231. 补充操作说明：
2. 2880为时间间隔，单位为分钟，时间间隔可设的范围为15－2880。
3. juniper为ftp帐号，10.1.1.1和10.1.1.2为ftp服务器的IP地址，abc123为登录frp服务器的密码，建议设置两个IP地址作为互备。
4. 定期备份仅能通过ftp服务备份。
5. 通过定期备份配置文件，时间间隔较短，即备份比较频繁，建议采用transfer-on-commit 方式，即只要执行commit指令，配置将自动备份到ftp服务器。

set system archival configuration transfer-on-commit1. transfer-interval和transfer-on-commit方式不能共存。
 |
| 检测方法：1. 使用show configuration system archival查看配置。
2. 设为transfer-on-commit模式。
3. 在路由器/交换机上执行commit命令、
4. 在FTP服务器10.1.1.1和10.1.1.2上查看备份文件。
 |
| 判定条件：在路由器/交换机上执行commit后，路由器/交换机将发送当前配置文件到FTP服务器，在FTP服务器上查看到最新的配置备份文件。 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-其他安全-02 |
| 要求内容：应关闭不必要的服务，如FTP、TFTP等。 |
| 操作指南： 1. 参考配置操作：

delete system services ftp1. 补充操作说明：

默认关闭FTP。 |
| 检测方法：1. 使用show configuration system services查看配置。
2. 通过ftp登录juniper设备，查看是否可以正常登录。
 |
| 判定条件：1. 查看路由器/交换机配置FTP。
2. 通过ftp不能登录juniper设备。
 |
| 补充说明： |

|  |
| --- |
| 编号：NE-Juniper-其他安全-03 |
| 要求内容：配置TELNET等远程维护方式时，应配置连接最大数量限制为10个，且每分钟最多为5个，防止TELNET端口上的SYN flood DoS攻击。 |
| 操作指南：set system services telnet connection-limit 10set system services telnet rate-limit 5 |
| 检测方法：1. 使用show configuration system services telnet查看配置。
2. 从终端向路由器/交换机发起超过10个telnet进程。
 |
| 判定条件：1. 路由器/交换机的telnet连接同时不超过10个。
2. 每分钟不超过5个telnet连接为正常。
 |
| 补充说明： |