Inspur NOS 安全技术白皮书

文档版本 V1.0

发布日期 2022-12-16

商标说明

Inspur 浪潮、Inspur、浪潮、Inspur NOS 是浪潮集团有限公司的注册商标。

本手册中提及的其他所有商标或注册商标，由各自的所有人拥有。

技术支持

技术服务电话：400-860-0011

地　　址：中国济南市浪潮路 1036 号

浪潮电子信息产业股份有限公司

邮　　箱：lckf@inspur.com

邮　　编：250101

前言

文档用途

本文档阐述了浪潮交换机产品 Inspur NOS 的安全能力及技术原理。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

读者对象

本文档提供给以下相关人员使用：

- 产品经理
- 运维工程师
- 售前工程师
- LMT 及售后工程师

变更记录

版本	时间	变更内容
V1.0	2022-12-16	首版发布

目 录

1 概述

随着开放网络的快速发展，白盒交换机做为一种软硬件解耦的开放网络设备，应用越来越广泛。白盒交换机采用开放的设备架构和软硬解耦思想，可以按需定制上层软件。网络操作系统方面，基于开源软件进行二次开发，支持硬件数据面可编程和软件容器化部署，充分利用现代云计算技术，对网络功能进行快速升级迭代，提升网络的灵活性、敏捷性、确定性，优化网络性能，满足复杂的业务需求。同时白盒交换机的开放标准、基于开源形式的本身存在不可忽视的安全问题，安全风险更易暴露，基于保密性、完整性、可用性的安全原则进行安全防护显得至关重要。

浪潮基于 SONIC 开源架构打造新一代网络操作系统 Inspur NOS。Inspur NOS 非常重视开放网络下的网络安全，在保证高性能、高可用性的同时，也为用户提供全方位的安全保障。本文首先分析了白盒网络交换机所面临的安全威胁与挑战，然后介绍了浪潮网络交换机 Inspur NOS 提供的安全技术。

2 缩写和术语

缩写和术语	解释
TACACS+	Terminal Access Controller Access-Control System Plus，终端访问控制器访问控制系统
NOS	Network Operating System，网络操作系统
RBAC	Role-Based Access Control，基于角色的访问控制
CACL	Control Plane Access Control List ，控制面访问控制
COPP	Control Plane Policing，控制面策略
DOS	Denial of Service，拒绝服务
DDOS	Distributed Denial of Service ，分布式拒绝服务

3 威胁与挑战

随着网络以及数据中心的发展，做为数据中心的关键系统，网络交换机面临着内部或外部的各种安全风险。Inspur NOS 做为网络交换机系统面临的安全威胁主要归结为两类。

1. 系统存在的脆弱性带来的安全威胁

   - ✧ 拒绝服务，交换机的交换芯片转发处理能力强大，但是控制面和管理面处理能力有限。攻击者通过向交换机发起海量的消息请求，导致交换机 CPU 无法实时处理消息，引发正常的业务交互流程、内部处理流程阻塞，达到拒绝服务的目的。
   - ✧ 信息泄露，交换机面临的信息泄露威胁，最重要的风险就是非授权的访问，还包括流量监控、存储介质泄露导致的信息泄露。
   - ✧ 恶意破坏，交换机的恶意破坏包括恶意报文攻击，传输过程中恶意篡改和非授权人员的恶意配置等。
   - ✧ 非授权访问，通过非授权访问，获得交换机控制权限，或者获取更高权限的信息。
   - ✧ Oday 漏洞，基于 SONIC 开源，安全风险更易暴露，更易发生 Oday 漏洞。

2. 管理存在的缺陷带来的安全风险

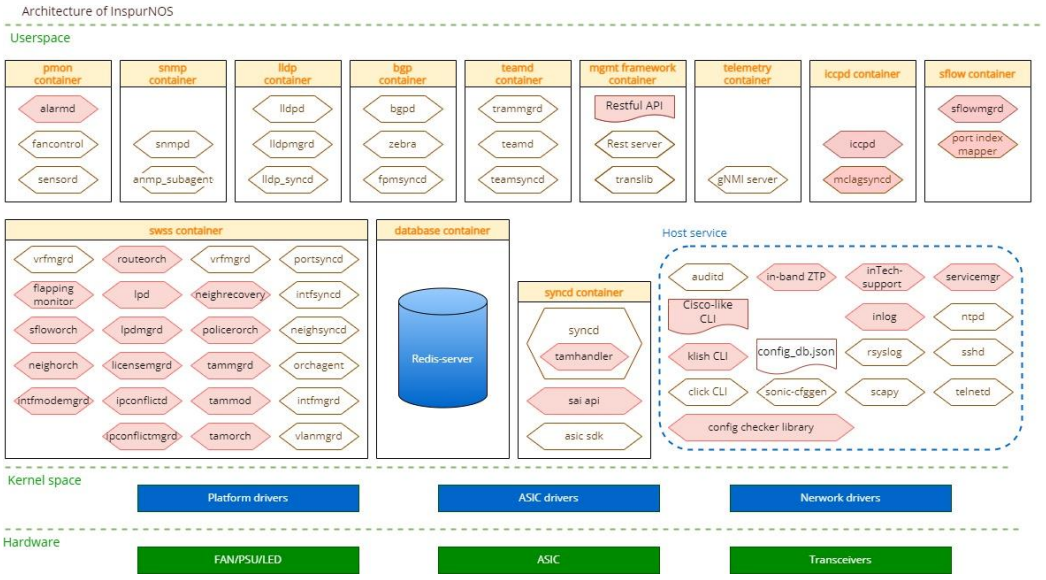
   - ✧ 网络系统复杂，由于 IP 网络规模庞大，系统构造复杂，访问通道灵活复杂、通信协议层出不穷，安全防护技术和管理能力的参差不齐，安全策略没有随着业务的不同阶段进行变更，暴露出部分安全漏洞。
   - ✧ 配置模型复杂，交换机配置模型复杂，管理员往往追求业务可用性，而忽略了安全防御能力，导致必要的安全措施没有得到妥善的配置，交换机本身的安全能力无法发挥。
   - ✧ 人员不慎，人员的不慎或者技能不足，导致配置出错，引发事故。

网络空间中安全问题的本质就是攻与防、矛与盾之间的较量。一方面，攻击者利用网络交换机（Inspur NOS）的安全脆弱性破坏其保密性、完整性和可用性；另一方面，网络交换机的所有者需要识别、减少乃至消除网络交换机的脆弱性，以降低或者消除攻击者利用安全脆弱性对其进行攻击的风险。网络交换机做为网络空间中信息系统的连接纽带，遭受网络攻击、自身出现问题会给整个网络空间带来很大的负面影响，因此网络交换机的安全防御能力是整个网络空间安全的重要组成部分。

4 安全架构

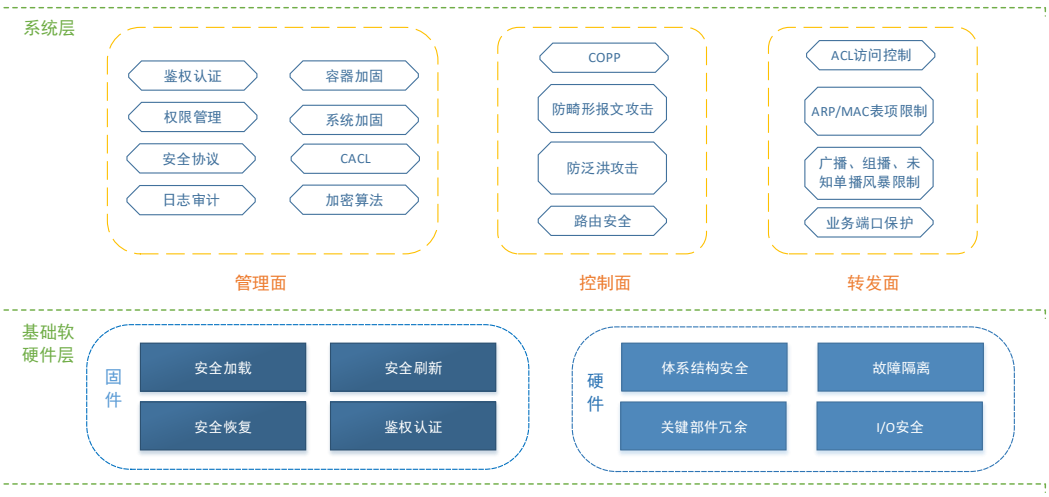
Inspur NOS 是基于 SONIC 开发出的白盒交换机 Network OS，在完善 SONiC 既有功能基础上，基于客户的需求和未来趋势，提供浪潮自研的进阶网络功能与管理功能。Inspur NOS 的架构如图 4-1，图中粉红色的部份，即是 Inspur 自研开发出的功能服务。

图 4-1. Inspur NOS 的架构



Inspur NOS 在架构上充分考虑了用户使用的安全性，在设计中也融入了安全性方案，并遵循三层三面的安全隔离机制，管里面、控制面和转发面隔离，保证任何平面遭受攻击，其它平面不受影响。Inspur NOS 实现软硬件解耦，可以适配不同的硬件平台，同时适配硬件平台相关安全设计。Inspur NOS 安全架构如图 4-2。

图 4-2. Inspur NOS 的安全架构



5 安全设计

5.1 账号安全

Inspur NOS 支持 CLI、Restful API、Netconf 管理接口，并提供了统一的用户管理功能。账号安全措施包括：密码复杂度检查、账户/密码有效期、防暴力破解和超时退出。

- ✧ 密码复杂度检查：对用户配置的密码的复杂度进行校验，避免用户设置过于简单的密码。密码复杂度要求：

  –长度至少为 8 个字符。

  –至少包含“小写字母（a-z）、大写字母（A-Z）、数字（0-9）、特殊字符”中的任意 3 种。

  –不能是用户名或用户名的倒序。

  –不能修改为当前密码。

- ✧ 账户/密码有效期：

  –支持密码有效期配置和检查，密码达到有效期后必须修改新密码才能登陆。

  –支持账户有效期配置和检查，账户超时无法登录，需联系管理员修改账户超时日期后，再重新登录。

- ✧ 防暴力破解：账号支持基于用户连续多次登录失败锁定。当用户连续输入错误密码的次数超过设置的错误次数（默认 5 次）时，该用户被锁定。用户被锁定后，在锁定时长（默认 300 秒）内不能继续登录，需要等待系统自动解锁。

- ✧ 超时退出，支持 SSH 访问超时退出，支持 Restful API、Netconf 会话超时退出。

5.2 权限控制

Inspur NOS 支持划分 0-15 级权限用户，默认只存在权限 15 级权限的 admin 账户，权限 15 级账户拥有进入 bash 维护模式权限；权限 14 账户具有进入全局配置模式权限；账户级

别越低，可执行命令行越少。提供给用户可以基于角色的访问控制模型（RBAC）来管理，可以灵活控制不同级别账户的配置查看和修改权限，防止越权访问导致的恶意破坏或者信息泄露。

Inspur NOS 支持 TACACS+服务器上进行认证、授权。

5.3 访问控制

Inspur NOS 支持 CACL,CACL 设定访问规则允许/拒绝特定 IP 区域的用户访问设备。

- ✧ 对 SSH 访问设备进行控制。
- ✧ 对网管访问设备包括 SNMP、NTP 服务进行控制。

5.4 安全协议

外部接入访问默认使用 SSH、HTTPS 等方式，传输通道通过使用安全协议进行加密。不安全协议 FTP、TFTP、HTTP、Telnet、SNMPv1/v2c 等默认关闭。

各种安全传输协议的特性如下：

- ✧ SSH
  1. 支持用户密码认证、public key 认证两种方式
  2. 使用 Protocol 2
  3. 支持安全的加密算法 AES128-CTR，AES192-CTR，AES256-CTR
- ✧ HTTPS
  1. 支持 TLS1.2 及以上版本，不支持 TLS1.0、TLS1.1、SSL v3 及以下版本
  2. 支持安全的加密算法 AES_128_CBC_SHA256、AES_256_CBC_SHA256
- ✧ SNMPv3
  1. 认证算法支持 SHA
  2. 加密算法支持 AES
- ✧ Netconf over SSH
- ✧ Syslog over TLS

5.5 数据保护

存储加密保护，Inspur NOS 系统中敏感数据包括：密码、密钥等所有敏感数据都进行了加密保护、并使用 SHA-256/AES 等安全加密算法。

内存数据保护，Inspur NOS 除了对保存在存储介质中的敏感数据进行加密保护还对在系统运行过程中产生的，堆、栈、数据段中的未加密的敏感数据，使用类似 memset 函数覆盖或清空。

剩余信息保护，Inspur NOS 敏感数据的存储空间被释放或重新分配前进行完全清除，通过安全擦除命令进行写随机数和多次擦写的方式，保证用户数据不能通过技术手段进行恢复。

5.6 安全加固

CLI 封装，Inspur NOS CLI 是浪潮开发的命令行框架体系，对 CLI 命令行进行了封装加固，除 15 级用户的 bash 模式，屏蔽了原命令行对 Linux 系统命令支持，只能执行白名单定义的命令，减少攻击风险。

OS 加固，15 级用户的 bash 模式的原生 SONIC 系统基于 S3A3G3 安全级别默认进行了系统安全加固。

Docker 容器加固，Docker 容器配置使用 Docker CIS 基准进行安全加固，基于 SONIC 业务场景，实现 L1 级别的配置安全要求或等效控制方案及部分 L2 级别的安全配置加固。

5.7 日志审计

Inspur NOS 的日志记录系统可以对系统的任何配置操作、系统运行过程中的各种异常状态，都能够记录，以便用于审计：

日志格式，操作日志信息中包含用户名、用户 IP 地址、操作时间、操作内容等信息。

日志存储，日志实时保存在独立分区文件系统中，当达到设定大小后自动备份，超过设定备份数后自动将最早的备份文件删除，并支持日志转储功能，不同的型号有差异。

日志安全，保持日志的文件按照最小权限原则，禁止非授权用户的删除和篡改。

5.8 转发面安全防护

风暴抑制，风暴抑制是用来防止广播、组播以及未知单播报文产生广播风暴。Inspur NOS 可以在该接口上配置对应报文类型的风暴控制功能，限制进入接口的广播、组播或单播类型

报文的速率，避免设备受到大的流量冲击。通过配置风暴控制，防范广播风暴，保障设备转发性能。

Port Rate-limit 流量限速，实现对通过接口的全部报文流量速率的限制，以保证带宽不超过规定大小。

ACL 访问控制，通过应用访问控制列表 ACL，来保障网络传输的安全可靠和性能稳定，Inspur NOS 实现基于 IP、MAC 通过 ACL 实现特定用户访问特定网络资源，并支持通过 TCP 或 UDP 端口号来控制流量转发或丢弃，来限制流量传输，确保网络性能。

ACL counter and meter，监控进入网络的某一流量的规格，把它限制在一个合理的范围之内，丢弃超出部分的流量。Inspur NOS 实现 QOS policy 流量速率限制，用户自定义优先级和流速，支持基于 IP 地址、MAC、协议类型、dscp 值等速率限制。

黑洞路由，将所有无关的路由吸入其中，使流量在此终结，缓解网络中 DDoS 攻击，Inspur NOS 设置黑洞路由的出接口为 NULL0。

异常报文保护，通过对接收的报文进行检查，发现非法报文，则自动丢弃，阻止非法报文在网络中的传递，非法报文类型包括源 MAC 等于目的 MAC、源 IP 等于目的 IP、SYN 和 FIN 同时设置的 TCP 报文等。

5.9 控制面安全防护

COPP 即控制面策略，Inspur NOS 通过限制上送 CPU 的报文速率，报文类型包括 ARP、BGP、DHCP-RELAY、IP、LACP、LLDP、SFLOW 等，从而保护交换机 CPU 处理能力免受 DOS 的攻击。

Inspur NOS 防畸形报文攻击，默认支持 IGMP 空报文防范、Ping of Death 攻击防范、Teardrop 攻击防范、TCP 标志位非法攻击防范。

Inspur NOS 防泛洪攻击，默认支持 TCP SYN 泛洪攻击防范、UDP 泛洪攻击防范、ICMP 泛洪攻击防范。

6 安全准测和策略

Inspur NOS 安全加固配置之前，请遵循如下原则，以免对本章的安全准则和策略机械的照搬，从而影响你的业务。

✧ 安全服务于业务：安全永远是为业务服务的，需要深入了解业务系统对安全防护的要求，才能合理的制定安全策略。

✧ 安全基于风险评估：综合分析业务系统面临的安全威胁和脆弱点，权衡业务系统的价值与安全加固的代价，全面实施安全风险评估，把不可接受的安全风险进行防护，把能够接受的风险作为残留风险接纳，并在业务系统生命周期中定期审视这些残留风险，评估其是否需要进行升级处理。

✧ 安全源于设计：安全是设计出来的，在全面的风险评估基础上，考虑投入产出比，设计满足业务需求和安全需求的合理方案。

✧ 安全策略实施影响：安全加固策略实施之前，请务必评估因为安全策略对业务带来的影响，避免由于不合理的安全策略造成业务损伤。

✧ 安全持续改进：没有一蹴而就的安全，也没有一劳永逸的安全，安全是一个持续改进的过程。安全策略实施后，需要不断的监控和维护业务系统，以确保安全策略已经切实发挥作用并达到安全预期，并及时发现问题，并调整安全策略。

6.1 版本安全维护

浪潮会定期发布新版本和补丁解决之前版本存在的安全风险问题，请定期检查交换机发布的新版本和补丁，查看解决的问题列表，判断是否需要升级版本或加载新补丁。

Inspur NOS 的查看版本方法如下：

DUT# show version	查看当前软件版本

Inspur NOS 补丁包包含了若干功能组件的补丁，升级该包可以依次为各功能组件包打上

补丁。如果是热补丁无需重启设备，如果是冷补丁，需要重启设备才具有新的功能特性。

Inspur NOS 补丁包配置方法如下：

DUT (config)# patch install ***.PAT	安装补丁
DUT(config)# show patch verbose	查看补丁安装信息
DUT(config)# show version	查看补丁信息

6.2 加强账号和权限管理

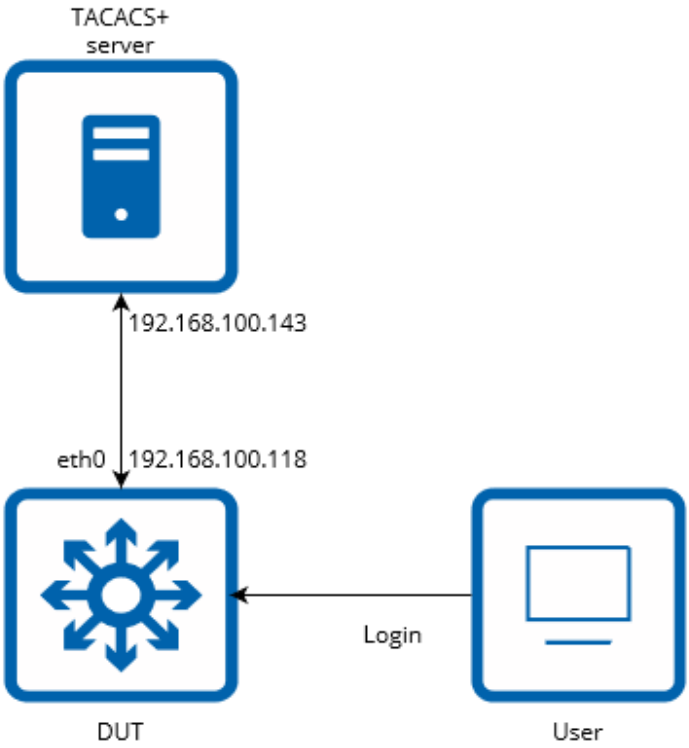
- ✧ 避免多人共享同一个账号口令。
- ✧ 密码需要定期更新。
- ✧ 密码复杂度应该满足安全要求。
- ✧ 访问超时退出。
- ✧ 在分配账号权限时，遵循最小授权原则，避免授予超出职责范围的权限。
- ✧ 严禁配置免认证的接入模式，任何接入交换机的通道都需要进行鉴权认证和授权审计。
- ✧ 严格记录所有账户的活动日志，以便事后审计。
- ✧ 账号鉴权，要求配置全网统一的 AAA 鉴权系统，避免交换机进行本地认证。

6.3 TACACS+服务授权

由于交换机的配置模型和业务极其复杂，导致交换机的命令行规模庞大。交换机本地认证使用基于角色的权限管理，会将角色对应的全部命令行开放给管理员。在实际的网络运维过程中，此管理员并不需要其对应等级权，因此，需要部署 TACACS+系统，来限制该管理员可以使用的命令行集合。

如图 6-1 所示。为了实现 Inspur NOS 精细化管理，保证设备的安全性，需要通过 TACACS+实现对用户按命令行授权。在 DUT 上开启 AAA 服务，并且配置 TACACS+服务器。TACACS+服务器 IP 地址 192.168.100.143，当 Client 通过网络接入 DUT 设备时，就需要 TACACS+服务器上进行认证、授权，并且该用户的登录、退出以及执行命令行时都会有计费信息发送给 TACACS+服务器进行记录。

图 6-1. TACACS+服务授权



Inspur NOS TACACS+配置方法如下：

DUT(config)# aaa authentication all group tacacs+	配置用户登录时通过TACACS+认证、授权
DUT(config)# aaa accounting default group tacacs+	配置用户计费方式为TACACA+
DUT(config)# tacacs-server authtype chap	配置全局TACACA+服务器认证类型为chap
DUT(config)# tacacs-server key testing123	配置全局TACACA+服务器key为testing123
DUT(config)# tacacs-server timeout 3	配置全局TACACA+服务器超时时间为3s
DUT(config)# tacacs-server host add 192.168.100.143 priority 10	添加地址为192.168. 100.143的TACACA+服务器，优先级为10
DUT(config)# tacacs-server host add 192.168.100.143 priority 5 key testing type pap timeout 5	添加地址为192.168. 100.143的TACACA+服务器，优先级为5，key为testing，认证类型为pap，超时时间为5s
DUT(config)# end	退回到特权模式
DUT# write	执行保存配置
DUT# show aaa	显示AAA相关配置信息
DUT# show tacacs-server	显示TACACS+服务器相关信息

6.4 加固系统安全

6.4.1 关闭不使用的服务和端口

依据最小授权原则，默认关闭非必要的访问通道，关闭不使用的服务，关闭不需要开启的 TCP/UDP 端口。以关闭 Telnet 为例。

Inspur NOS 的关闭 Telnet 服务方法如下：

DUT(config)# no feature telnet	配置telnet连接去使能
DUT(config)# end	退回到特权模式
DUT# show telnet	查看telnet的配置
DUT# show feature	查看整个feature配置

6.4.2 废弃不安全通道

同一访问需求有多种访问协议的情况下，废弃不安全的访问协议，而选择安全的访问通道。下表列出了各种访问通道安全水平，优先选择高安全等级的访问通道。

访问需求	**安全通道**	**不安全通道**
远程登录	SSHv2	Telnet、SSHv1
网络管理	SNMPv3	SNMPv1、SNMPv2
数据传输	HTTPS	UDP、HTTP
文件传输	SFTP、SCP	FTP、TFTP

6.4.3 善用安全配置

交换机业务口默认支持管理协议，同时交换机支持专用的管理网口使用管理协议登录，如果客户网络有专门的管理面规划，建议仅通过专用管理网口对设备进行管理，通过各管理协议支持的 CACL 来限制登录 IP，并支持服务的缺省知名端口变更，减小被扫描攻击的概率。

以 SSH 协议为例，在 SSH 服务器端配置优先级为 1 的访问控制列表，拒绝源 IP 地址 1.1.1.0/24 登录到交换机。

Inspur NOS 的 SSH 配置拒绝 IP 访问方法如下：

DUT(config)# cacl ssh	进入cacl全局配置模式
DUT(config-cacl-ssh)# priority 1 action deny src-ip 1.1.1.0 24	配置拒绝源ip为1.1.1.0/24网段ssh访问设备
DUT(config-cacl-ssh)# exit	退出cacl模式

缺省情况下，SSH 服务器的端口号为 22。端口号 22 属于知名端口号，易被扫描和攻击。可以修改 SSH Server 的知名端口为私有端口 50。

Inspur NOS 的 SSH 变更端口方法如下：

DUT# configure terminal	进入全局配置模式
DUT(config)# ssh port 50	配置连接端口号
DUT(config)# end	退回到特权模式
DUT# show ssh	查看ssh的配置

Inspur NOS 安全配置涉及不同服务、不同协议和不同的业务场景，可以依据业务影响配置加固。

6.5 关注数据安全

用户对于设备的流量监控、故障检测、设备运行等情况有明确的需求。Inspur NOS 支持数据采集技术如下：

- ✧ 端口镜像是指将镜像端口（源端口）的报文复制一份到观察端口（目的端口），对报文进行获取和分析。
- ✧ sFlow 基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。
- ✧ ERSPAN 需要将交换机上某些端口上收发的数据通过三层网络发送给远端的分析仪进行分析。
- ✧ TAM(Telemetry and Monitor)是一项远程的从物理设备上高速采集数据的技术，设备通过主动向采集器上送设备的接口、延时、丢包原因等信息，提供了更实时更高速的数据采集功能。

监控采集数据安全主要考虑如下方面：

1. 数据安全技术要求，不同的数据监控技术应用到不同的业务场景，为了防止数据在传输、存储过程中被窃取和仿冒，对数据进行加密认证保护。

2. 数据安全合规要求，数据的采集和全生命周期防护应当满足所适用国家或地区的法律法规，采取足够的措施以确保用户的通信内容受到严格保护后，方可启用上述功能。

6.6 保障网络隔离

Inspur NOS 支持业务网和管理网进行网络隔离。如：管理口收到的报文不会从业务口转发出去，同样，从业务口收到的报文也不会从管理口转发出去；业务口接收到目的地址是管理口地址的报文不能访问设备。推荐管理口配置 VRF 进行隔离。

Inspur NOS 的管理口配置 VRF 方法如下：

DUT(config)# vrf mgmt	创建管理口VRF，管理口会自动加入vrf mgmt
DUT# show vrf mgmt	查看管理口vrf信息
DUT# show ip interface	查看管理口信息

6.7 基于安全域访问控制

通过应用访问控制列表 ACL，来保障网络传输的安全可靠和性能稳定，ACL 可以应用场景如下：

- ✧ 防止对网络攻击，通过在接口应用 ACL 来阻断协议报文对网络的攻击。
- ✧ 对网络访问行为进行控制，如数据中心网络中可通过 ACL 实现特定数据流访问特定网络资源。
- ✧ 限制网络流量，提升网络性能，如通过限制特定 TCP 或 UDP 端口号的流量速率，保障整体的网络性能。

每个 ACL 中可以定义多个规则，根据规则的功能分为：IP ACL、MAC ACL、IPV6 ACL、CACL 和 ACL counter and meter。

分类	**IP类型**	**ACL规则定义**
IP ACL	IPv4	匹配类型：IP 控制方向：INGRESS(入向)、EGRESS（出向） 处理类型：FORWARD（允许）、DROP（拒绝） 是否支持报文重定向：是 是否支持报文统计：是

MAC ACL	IPv4/ IPv6	匹配类型：MAC 控制方向：INGRESS(入向)、EGRESS（出向） 处理类型：FORWARD（允许）、DROP（拒绝） 是否支持报文重定向：是 是否支持报文统计：是
IPV6 ACL	IPv6	匹配类型：IP 控制方向：INGRESS(入向)、EGRESS（出向） 处理类型：FORWARD（允许）、DROP（拒绝） 是否支持报文重定向：是 是否支持报文统计：是
CACL	IPv4	匹配类型：SSH、NTP、SNMP 控制方向：入向) 处理类型：permit（允许）、deny（拒绝）
ACL counter and meter	IPv4	匹配类型：IP、MAC、DSCP 支持、TCP-FLAG 位、ICMP 报文代码、ICMP 报文类型、TCP 端口、IP 协议号、ARP。 控制方向：in（入向）、out（出向） 处理类型：限速

6.8 攻击防护

基于 COPP 报文速率限制的 CPU 防护

基于 COPP 报文速率限制防攻击，对上送 CPU 的流量进行监督，实现 CAR（Committed Access Rate）访问速率控制。通过对上送报文根据协议类型进行分类，用 COPP 控制转发平面送往 CPU 的报文的带宽、优先级，同时控制总的上送带宽，以达到控制上送报文的数量，优先保证高优先级业务，防止 CPU 过载以及攻击产生时发出告警以达到防御的目的。

目前 CPU 被攻击时对业务的影响主要来自于三方面原因：

1. 没有区分合法协议报文和非法协议报文，CPU 忙于处理大量非法协议报文利用率大幅升高，影响了对正常协议报文的处理。

2. 部分协议报文使用同一通道上送 CPU 处理，当其中一个协议由于网络发生环路，导致海量报文被“链式反应”复制堵塞了上送 CPU 的通道，影响了其他协议。

3. 不同协议报文的上送通道带宽设置不合理，发生流量冲击时影响其他上送通道的协议处理。

Inspur NOS 的 COPP 以 ARP 为例的配置方法如下：

DUT(config)# copp arp	进入COPP ARP组模式，如果不存在COPP组，则不能进入COPP模式。
DUT(config)# no copp arp	删除COPP ARP组设置并恢复默认设置
DUT(config-copp-arp)# rule queue 4 cir 300 cbs 600	配置COPP ARP组限速规则,配置CPU的4号队列为接受队列，cir速率为300pps，cbs的突发速率为600pps
DUT(config-copp-arp)# clear	删除COPP ARP组设置并恢复默认设置
DUT(config-copp-arp)# exit	退出COPP ARP组模式
DUT(config)# show copp summary	查看COPP配置信息

风暴控制

风暴控制特性，可以控制广播、组播以及未知单播这三类报文流量，防范广播风暴。风暴控制主要通过配置阈值来限制流量，策略阈值可以通过丢弃全部报文来阻断流量。风暴控制分为 Flood、multicast 和 broadcast 模式如下：

- ✧ Flood 模式可以对未知单播和未知组播报文进行抑制。
- ✧ multicast 模式只对已知组播抑制。
- ✧ broadcast 模式只对广播抑制。

6.9 可靠性保护

MC-LAG

MCLAG（Multichassis Link Aggregation Group）即跨设备链路聚合组，一方面可以起到负载分担流量的作用，另一方面可以起到备份保护的作用。在两台交换机之间部署 MC-LAG，既可以实现冗余备份同时又提高链路的利用率，从而实现交换机的双归接入。这样

两台交换机间形成负载分担，共同进行流量转发，当其中一台设备发生故障时，流量可以快速切换到另一台设备，保证业务的正常运行。

Warm Reboot

Warm Reboot 热启动相比于 Fast Reboot 和 Reboot 可以实现重启的过程中二三层转发不丢包，对业务的影响最低。

重启类型	重启速度	业务影响
Warm Reboot	快	二三层转发不丢包
Fast Reboot	快	丢包
Reboot	慢	丢包

7 安全发布

参考《浪潮产品安全白皮书》，践行浪潮端到端的产品安全保障。

《浪潮产品安全白皮书》官网地址：
https://www.inspur.com/lcjtww/psirt/whitepaper/index.html