NETSCREEN NSRP 典型配置及维护

1、NSRP 工作原理

NSRP（NetScreen Redundant Protocol）是 Juniper 公司基于 VRRP 协议规范自行开发的设备冗余协议。防火墙作为企业核心网络中的关键设备，需要为所有进出网络的信息流提供安全保护，为满足客户不间断业务访问需求，要求防火墙设备必须具备高可靠性，能够在设备、链路及互连设备出现故障的情况下，提供网络访问路径无缝切换。NSRP 冗余协议提供复杂网络环境下的冗余路径保护机制。NSRP 主要功能有：

1、在高可用群组成员之间同步配置信息；

2、提供活动会话同步功能，以保证发生路径切换情况下不会中断网络连接；

3、采用高效的故障切换算法，能够在短短几秒内迅速完成故障检测和状态切换。

NSRP 集群两种工作模式：

一、 Active/Passive 模式：通过对一个冗余集群中的两台安全设备进行电缆连接和配置，使其中一台设备作为主用设备，另一台作为备用设备。主用设备负责处理所有网络信息流，备用设备处于在线备份状态。主设备将其网络和配置命令及当前会话信息传播到备用设备，备用设备始终保持与主用设备配置信息和会话连接信息的同步，并跟踪主用设备状态，一旦主设备出现故障，备份设备将在极短时间内晋升为主设备并接管信息流处理。

二、Active/Active 模式：在 NSRP 中创建两个虚拟安全设备（VSD）组，每个组都具有自己的虚拟安全接口(VSI)，通过 VSI 接口与网络进行通信。设备 A 充当 VSD 组 1 的主设备和 VSD 组 2 的备份设备。设备 B 充当 VSD 组 2 的主设备和 VSD 组 1 的备份设备。Active/Active 模式中两台防火墙同时进行信息流的处理并彼此互为备份。在双主动模式中不存在任何单一故障点。

NSRP 集群技术优势主要体现于：

1、消除防火墙及前后端设备单点故障，提供网络高可靠性。即使在骨干网络中两类核心设备同时出现故障，也能够保证业务安全可靠运行。

2、根据客户网络环境和业务可靠性需要，提供灵活多样的可靠组网方式。NSRP 双机集群能够提供 1、Active-Passive 模式 Layer2/3 多虚拟路由器多虚拟系统和口型/交叉型组网方式；2、Active-Active 模式 Layer2/3 多虚拟路由器多虚拟系统和口型/Fullmesh 交叉型组网方式。为用户提供灵活的组网选择。

3、NSRP 双机结构便于网络维护管理，通过将流量在双机间的灵活切换，在防火墙软件升级、前后端网络结构优化改造及故障排查时，双机结构均能够保证业务的不间断运行。

4、结合 Netscreen 虚拟系统和虚拟路由器技术，部署一对 NSRP 集群防火墙，可以为企业更多的应用提供灵活可靠的安全防护，减少企业防火墙部署数量和维护成本。

2、NSRP Active/Passive 模式配置

Active/Passive 模式也就是主/备模式，该组网模式是当前很多企业广泛采用的 HA 模式，该模式具有对网络环境要求不高，无需网络结构做较大调整，具有较好冗余性、便于管理维护等优点。缺点是 Netscreen 防火墙利用率不高，同一时间只有一台防火墙处理网络流量；冗余程度有限，仅在一侧链路和设备出现故障时提供冗余切换。但主/备模式具有较强冗余性、低端口成本和网络结构简单、便于维护管理等角度考虑，成为很多企业选用该组网模式的标准。

配置说明：两台 Netscreen 设备采用相同硬件型号和软件版本，组成 Active/Passive 冗余模式，两台防火墙均使用一致的 Ethernet 接口编号连接到网络。通过双 Ethernet 端口或将 1 个 Ethernet 接口放入 HA 区段，其中控制链路用于 NSRP 心跳信息、配置信息和 Session 会话同步，数据链路用于在两防火墙间必要时传输数据流量。

命令模式配置说明如下：

NS-A（主用）：

```
Set hostname NS-A                          /***定义主机名***/
Set interface ethernet1 zone untrust
Set interface ethernet1 ip 100.1.1.4/29
Set interface ethernet1 route              /***配置接口：Untrust/Trust Layer3  路由模式***/
Set interface ethernet2 zone trust
Set interface ethernet2 ip 192.168.1.4/29
Set interface ethernet2 route
Set interface mgt ip 192.168.2.1/24        /***通过管理口远程管理 NS-A***/
Set interface ethernet3 zone HA
Set interface ethernet4 zone HA            /***Eth3 和 Eth4 口用于 HA 互连，用于同步配置文件、会话信息和跟踪设备状态信息***/

set nsrp cluster id 1
set nsrp rto-mirror sync
set nsrp vsd-group id 0 priority 50        /***缺省值为 100，低值优先成为主用设备***/
set nsrp monitor interface ethernet2
set nsrp monitor interface ethernet1       /***配置 NSRP：Vsd-group 缺省为 0，VSI 使用物理接口 IP 地址,非抢占模式***/
```

NS-B（备用）：

```
Set hostname NS-B                          /***定义主机名***/
Set interface ethernet1 zone Untrust
Set interface ethernet1 ip 100.1.1.4/29
Set interface ethernet1 route
Set interface ethernet2 zone trust
Set interface ethernet2 ip 192.168.1.4/29
```

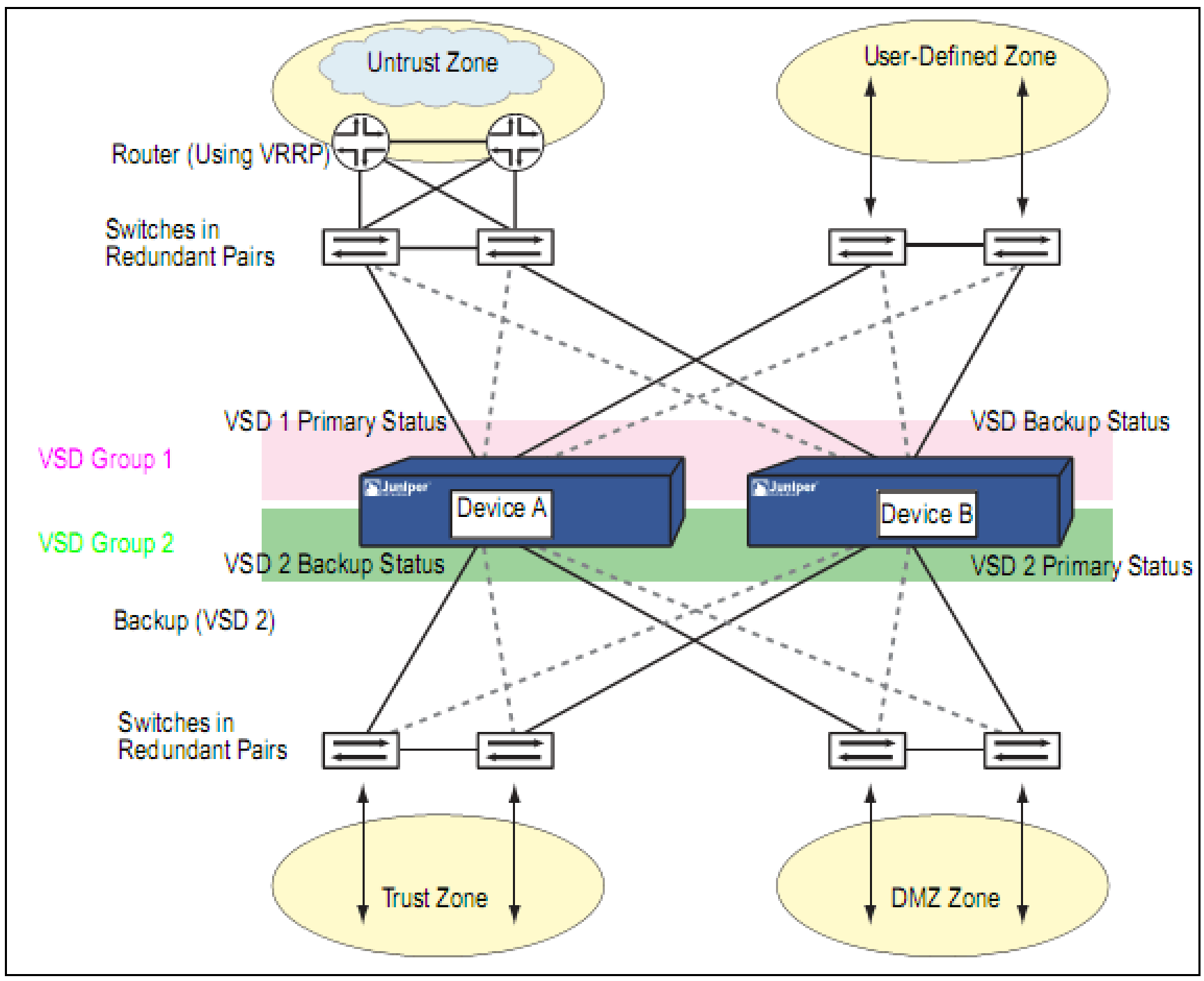
```
Set interface ethernet2 route                 /***配置接口：Untrust/Trust Layer3  路由模式***/
Set interface mgt ip 192.168.2.2/24           /***通过管理口远程管理 NS-A***/
Set interface ethernet3 zone HA
Set interface ethernet4 zone HA               /***Eth3 和 Eth4 口用于 HA 互连，用于同步配置文件、会话信息和跟踪设
备状态信息***/

set nsrp cluster id 1
set nsrp rto-mirror sync
set nsrp vsd-group id 0 priority 100
set nsrp monitor interface ethernet2
set nsrp monitor interface ethernet1          /***Vsd-group 缺省为 0，VSI 使用物理接口 IP 地址，备用设备：优先级 100，
成为非抢占模式***/
```

3、NSRP Active/Active Full-Mesh 模式配置

Fullmesh 连接组网使用全交叉网络连接模式，容许在同一设备上提供链路级冗余，发生链路故障时，由备用链路接管网络流量，防火墙间无需进行状态切换。仅在上行或下行两条链路同时发生故障情况下，防火墙才会进行状态切换，Fullmesh 连接进一步提高了业务的可靠性。该组网模式在提供设备冗余的同时提供链路级冗余，成为很多企业部署关键业务时的最佳选择。

典型拓扑如下：



Fullmesh 连接组网模结构提供了一种更为灵活的组网方式，在保证网络高可靠性的同时提升了网络的可用性。该结构中两台防火墙同时作为主用设备并提供互为在线备份，各自独立处理信息流量并共享连接会话信息。一旦发生设备故障另一台设备将负责处理所有进出网络流量。Fullmesh 组网模式对网络环境要求较高，该组网方式中两台防火墙为双 Active 状态，但要求网络维护人员具备较强技术能力，防火墙发生故障时，接管设备受单台设备容量限制，可能会导致会话连接信息丢失，采用 A/A fullmesh 模式组网时，建议每台防火墙负责处理的会话连接数量不超过单台设备容量的 50%，以确保故障切换时不会丢失会话连接。

配置说明：定义 VSD0 和 VSD1 虚拟安全设备组 (创建 Cluster ID 时将自动创建 VSD0)，其中 NS-A 为 VSD0 主用设备和 VSD1 备用设备，NS-B 为 VSD1 主用设备和 VSD0 备用设备；创建冗余接口实现两物理接口动态冗余；配置交换机路由指向来引导网络流量经过哪个防火墙。

命令配置说明如下：

NS-A(Active)：

```
Set hostname NS-A                          /***定义主机名***/
Set interface mgt ip 192.168.2.1/24        /***通过管理口远程管理 NS-A***/
set interface redundant1 zone Untrust      /***创建冗余接口 1，用于 Untrust 接口冗余***/
set interface redundant1 ip 100.1.1.4/29   /***创建冗余接口管理地址***/
Set interface ethernet 1 zone null         /***默认为 Null***/
Set interface ethernet 2 zone null
Set interface ethernet 3 zone null
Set interface ethernet 4 zone null
set interface ethernet1 group redundant1   /***将物理接口加入冗余接口 1***/
set interface ethernet2 group redundant1
set interface redundant2 zone trust        /***创建冗余接口 2，用于 trust 接口冗余***/
set interface redundant2 ip 192.168.1.4/29
set interface redundant2 manage-ip 192.168.2.1
set interface ethernet3 group redundant2
set interface ethernet4 group redundant2
set interface redundant1:1 ip 100.1.1.5/29     /***配置冗余接口、定义 Vsd0 接口 IP 地址***/
set interface redundant2:1 ip 192.168.1.5/29   /***VSD1 的 VSI 接口需手动配置 IP 地址，冒号后面的 1 表示该接口属于 VSD1 的 VSI***/
set interface ethernet7 zone ha
set interface ethernet8 zone ha
set nsrp cluster id 1
set nsrp vsd-group id 0 priority 50
set nsrp vsd-group id 1                    /*** VSD1 使用缺省配置，优先级为 100***/
set nsrp rto-mirror sync
set nsrp monitor interface redundant1
set nsrp monitor interface redundant2
set nsrp secondary-path ethernet2/1        /***定义 NSRP 备用心跳接口，保证心跳连接信息不会丢失***/
```

set arp always-on-dest /***强制采用基于 ARP 表而不是会话表中的 MAC 地址转发封包***/
set vrouter trust-vr route 0.0.0.0/0 interface redundant1 gateway 100.1.1.1
set vrouter trust-vr route 0.0.0.0/0 interface redundant1:1 gateway 100.1.1.1

NS-B(Active)：

set interface redundant1 zone Untrust
set interface redundant1 ip 100.1.1.4/29
set interface ethernet1 group redundant1 /***VSD0 的 VSI 接口使用物理接口 IP 地址***/
set interface ethernet2 group redundant1
set interface redundant2 zone trust
set interface redundant2 ip 192.168.1.4/29
set interface redundant2 manage-ip 192.168.2.2
set interface ethernet3 group redundant2
set interface ethernet4 group redundant2 /***配置冗余接口、定义 Vsd0 接口 IP 地址***/
set interface redundant1:1 ip 100.1.1.5/29
set interface redundant2:1 ip 192.168.1.5/29
set interface ethernet7 zone ha
set interface ethernet8 zone ha
set nsrp cluster id 1 /***定义一致的 Cluster ID，自动启用采用缺省配置的 VSD0***/
set nsrp rto-mirror sync
set nsrp vsd-group id 1 priority 50
set nsrp monitor interface redundant1
set nsrp monitor interface redundant2
set nsrp secondary-path ethernet2/1 /***定义 NSRP 备用心跳接口，保证心跳连接信息不会丢失***/
set arp always-on-dest /***强制采用基于 ARP 表而不是会话中的 MAC 地址转发封包***/
set vrouter trust-vr route 0.0.0.0/0 interface redundant1 gateway 100.1.1.1
set vrouter trust-vr route 0.0.0.0/0 interface redundant1:1 gateway 100.1.1.1

4、NSRP 常用维护命令

1、get license-key

查看防火墙支持的 feature，其中 NSRPA/A 模式包含了 A/P 模式，A/P 模式不支持 A/A 模式。Lite 版本是简化版，支持设备和链路冗余切换，不支持配置和会话同步。

2、exec nsrp sync global-config check-sum

检查双机配置命令是否同步

3、exec nsrp sync global-config save

如双机配置信息没有自动同步，请手动执行此同步命令，需重启系统。

4、get nsrp

查看 NSRP 集群中设备状态、主备关系、会话同步以及参数开关信息。

5、Exec nsrp sync rto all from peer

手动执行 RTO 信息同步，使双机保持会话信息一致

6、exec nsrp vsd-group 0 mode backup

手动进行主备状态切换时，在主用设备上执行该切换命令，此时该主用设备没有启用抢占模式。

7、exec nsrp vsd-group 0 mode ineligible

手动进行主备状态切换时，在主用设备上执行该切换命令，此时该主用设备已启用抢占模式。

8、get alarm event

检查设备告警信息，其中将包含 NSRP 状态切换信息

其它命令常用

1、清空备机配置命令

Unset all

"Erase all system config, are you sure y / [n]?" Y

Reset

"Configuration modified, save? [y] / n" N

"System reset, are you sure? y / [n]" Y

2、系统重新启动后配置命令

Set hostname xxxxxx

Set interface mgt ip x.x.x.x/x

Set nsrp cluster id 1

Exec nsrp sync file

Exec nsrp sync global-config run

/***适应于 5.1 以上版本，5.0 中使用 Exec nsrp sync global-config save 命令，需要重启设备***/

Set nsrp rto-mirror sync

Save all

3、检查设备状态

Nsrp：get nsrp

接口：Get interface

路由：get route

会话：get session

附录一 NSRP 缺省设置值

1、VSD 组信息

VSD group ID:0

Device priority in the VSD group:100

Preempt option:disable

Preempt hold-down time:0 second

Initial state hold-down time:5 second

Heartbeat interval:1000 milliseconds

Lost heartbeat threshold:3

Master (Primary) always exist:no

2、RTO 镜像信息

RTO synchronization:disable

Heartbeat interval:4 second

Lost heartbeat threshold:16

3、NSRP 链接信息

Number of gratuitous ARPs:4

NSRP encryption:disable

NSRP authentication:disable

Track IP:none

Interfaces monitored:none

Secondary path:none

HA link probe:none

Interval:15

Threshold:5

备注：

unset interface e4 ip　　将 e4 的 ip 地址删除

set interface e4 zone ha　　将 e4 和 HA 区域绑定一起

SSG550-> set nsrp cluster id 1　　设置 cluster 组号

SSG550(M)-> set nsrp vsd id 0　　设置 VSD 的组号,这条命令可以不用输入，因为 Netscreen 防火墙的默认的虚拟安全数据库（VSD）的值是 0。

SSG550(M)-> set nsrp vsd-group id 0 priority 50　　设置 NSRP 主设备的优先权值，priority 值越小，优先权越高。

SSG550(M)-> set　nsrp rto syn　设置配置同步

SSG550(M)-> set nsrp vsd-group id 0 monitor interface ethernet3　　设置防火墙监控的端口，假设端口 3 出现故障或所连接的交换机出现故障，防火墙的工作状态将切换到备份防火墙上。

SSG550(M)-> set nsrp　vsd-group id 0 monitor interface ethernet1　　设置防火墙监控的端口，假设端口 1 出现故障或所连接的交换机出现故障，防火墙的工作状态将切换到备份防火墙上。

注：如没有监控端口 2，端口 2 出现故障或连接网络出现故障，将不会激活防火墙工作状态切换

get nsrp　查看冗余状态

SSG550(M)-> set nsrp vsd-group hb-interval 200　　设置心跳信息每隔 200 秒将发出问候信息

SSG550(M)-> set nsrp vsd-group hb-threshold 3　　设置心跳信息总共发出 3 次问候信息

ISG1000-> set nsrp cluster id 1　　设置 cluster 组号

ISG1000(B)-> set nsrp vsd id 0　　设置 VSD 的组号,这条命令可以不用输入，因为 Netscreen 防火墙的默认的虚拟安全数据库（VSD）的值是 0。

ISG1000(B)-> set nsrp vsd-group id 0 priority 100　　设置 NSRP 主设备的优先权值，priority 值越小，优先权越高。

ISG1000(B)-> set　nsrp rto syn　设置配置同步

ISG1000(B)-> set nsrp vsd-group id 0 monitor interface ethernet3　　设置防火墙监控的端口，假设端口 3 出现故障或所连接的交换机出现故障，防火墙的工作状态将切换到备份防火墙上。

ISG1000(B)-> set nsrp vsd-group id 0 monitor interface ethernet1　　设置防火墙监控的端口，假设端口 1 出现故障或所连接的交换机出现故障，防火墙的工作状态将切换到备份防火墙上。

ISG1000(B)-> set nsrp vsd-group hb-interval 200　　设置心跳信息每隔 200 秒将发出问候信息

ISG1000(B)-> set nsrp vsd-group hb-threshold 3　　设置心跳信息总共发出 3 次问候信息

ISG1000(B)-> save

在备机上同步配置

NS-A(B)-> exec nsrp sync global-config check-sum　（将两台设备的配置进行校检，如有不同，备份的设备将会在重启后把主设备上的配置导入备份主机中）

NS-A (B)-> exec nsrp sync global-config save　（如有不同，备份的设备将会在重启后把主设备上的配置导入备份主机中）