ASA/PIX 7.x ：冗余或备份ISP链路的配置示例

目录

简介

静态路由存在一个问题，即没有任何内在机制可确定路由有效还是失效。即使下一跳网关不可用，路由表中也会保留该路由。只有在安全设备上的相关接口失效时，才会从路由表中删除静态路由。为了解决此问题，使用了一种静态路由跟踪功能以跟踪静态路由的可用性，如果该路由失败，则从路由表中将其删除，并将其替换为备份路由。

本文档提供一个示例，介绍如何在 PIX 500 系列安全设备或 ASA 5500 系列自适应安全设备上使用静态路由跟踪功能，以使设备可以使用冗余或备份 Internet 连接。在本示例中，通过静态路由跟踪，安全设备可以在主租用线路失效时使用辅助 Internet 服务提供商 (ISP) 的廉价连接。

为了实现此冗余，安全设备将静态路由与所定义的监控目标相关联。服务水平协议 (SLA) 操作定期采用 Internet 控制消息协议 (ICMP) 的回声请求监控目标。如果未收到回声应答，则将对象视为失效，并从路由表中删除相关路由，并用以前配置的备份路由代替所删除的路由。当使用备份路由时，SLA 监控操作不断尝试访问监控目标。目标再次可用后，将替换路由表中的第一个路由，并删除备份路由。

注意： 因为ASA/PIX，不支持在本文描述的配置不可能用于共享的负载均衡或的负载。此配置仅用于冗余或备份用途。传出流量使用主 ISP，如果主 ISP 失败，则使用辅助 ISP。主 ISP 故障会导致流量临时中断。

先决条件

要求

选择能回答ICMP echo请求的监听目标。目标可以是所选择的任何网络对象，但建议采用与 ISP 连接紧密联系的目标。下面列出了一些可能的监控目标：

- ISP 网关地址
- 由另一个 ISP 管理的地址
- 安全设备需要与之通信的另一个网络上的服务器（如 AAA 服务器）
- 另一个网络上的持久性网络对象（不宜选择晚间可能关闭的桌面或笔记本计算机）

本文档假设安全设备运行完全正常，并配置为允许 Cisco ASDM 对配置做出更改。

注意： 有关如何允许 ASDM 配置设备的信息，请参阅允许 ASDM 进行 HTTPS 访问。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为 7.2(1) 或更高版本的 Cisco PIX 安全设备 515E
- Cisco 自适应安全设备管理器 5.2(1) 或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

还可以将此配置用于 Cisco ASA 5500 系列安全设备版本 7.2(1)。

注意： 必须采用 **backup interface** 命令配置 ASA 5505 上的第四个接口。参考的备份接口欲知更多信息。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在本示例中，安全设备与 Internet 保持两个连接。第一个连接是通过主 ISP 提供的路由器访问的高速租用线路。第二个连接是通过辅助 ISP 提供的 DSL 调制解调器进行访问的低速数字用户线路 (DSL) 线路。

注意： 本示例中不进行负载均衡。

只要租用线路处于活动状态，并且主 ISP 网关可访问，DSL 连接就处于空闲。但是，如果与主 ISP

的连接失效，则安全设备将更改路由表，以便将流量定向到 DSL 连接。静态路由跟踪用于实现此冗余。

为安全设备配置了一条静态路由，用于将所有 Internet 流量定向到主 ISP。SLA 监控进程每 10 秒检查一次，确认主 ISP 网关可访问。如果 SLA 监控进程确定主 ISP 网关不可访问，则从路由表中删除将流量定向到该接口的静态路由。为替换该静态路由，安装了一条备用静态路由，用于将流量定向到辅助 ISP。此备用静态路由通过 DSL 调制解调器将流量定向到辅助 ISP，直到主 ISP 的链路可访问为止。

此配置提供一个相对廉价的方式，以确保安全设备后的用户仍可进行出站 Internet 访问。如本文档所述，此设置可能不适于对安全设备后的资源进行入站访问。需要高级联网技能才能实现无缝入站连接。本文档中不涉及这些技能。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 此配置中使用的 IP 地址不能在 Internet 上合法地路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- 命令行界面 (CLI)
- 自适应安全设备管理器 (ASDM)

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

CLI 配置

PIX

```
pix# show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
 nameif backup
!--- The interface attached to the Secondary ISP. !---
```

```
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging buffered debugging mtu outside 1500 mtu backup
1500 mtu inside 1500 no failover asdm image
flash:/asdm521.bin no asdm history enable arp timeout
14400 global (outside) 1 interface
global (backup) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0
!--- NAT Configuration for Outside and Backup route
outside 0.0.0.0 0.0.0.0 10.200.159.1 1 track 1
!--- Enter this command in order to track a static
route. !--- This is the static route to be installed in
the routing !--- table while the tracked object is
reachable. The value after !--- the keyword "track" is a
tracking ID you specify. route backup 0.0.0.0 0.0.0.0
10.250.250.1 254
!--- Define the backup route to use when the tracked
object is unavailable. !--- The administrative distance
of the backup route must be greater than !--- the
administrative distance of the tracked route. !--- If
the primary gateway is unreachable, that route is
removed !--- and the backup route is installed in the
routing table !--- instead of the tracked route. timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable http 172.22.1.0 255.255.255.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface
outside
 num-packets 3
 frequency 10
!--- Configure a new monitoring process with the ID 123.
Specify the !--- monitoring protocol and the target
network object whose availability the tracking !---
process monitors. Specify the number of packets to be
sent with each poll. !--- Specify the rate at which the
monitor process repeats (in seconds). sla monitor
schedule 123 life forever start-time now
!--- Schedule the monitoring process. In this case the
lifetime !--- of the process is specified to be forever.
The process is scheduled to begin !--- at the time this
command is entered. As configured, this command allows
the !--- monitoring configuration specified above to
determine how often the testing !--- occurs. However,
you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times. !
track 1 rtr 123 reachability
!--- Associate a tracked static route with the SLA
monitoring process. !--- The track ID corresponds to the
```

```
track ID given to the static route to monitor: !---
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1 !---
"rtr" = Response Time Reporter entry. 123 is the ID of
the SLA process !--- defined above.

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a4a0e9be4593ad43bc17a1cc25e32dc2
: end
```

ASDM 配置

要用 ASDM 应用程序配置冗余或备份 ISP 支持，请完成以下这些步骤：

1. 在 ASDM 应用程序中，单击 **Configuration**，然后单击 Interfaces。
2. 从 Interfaces 列表中，选择 **Ethernet0**，然后单击 Edit。此时显示以下对话框。
3. 选中 **Enable Interface** 复选框，并在 Interface Name、Security Level、IP Address 和 Subnet Mask 字段中输入值。
4. 单击 **OK** 关闭对话框。
5. 根据需要配置其他接口，然后单击 **Apply** 更新安全设备配置。
6. 单击 ASDM 应用程序左侧的 **Routing**。
7. 单击 **Add** 添加新的静态路由。此时显示以下对话框。
8. 从 Interface Name 下拉列表中选择路由所在的接口，然后配置到达网关的默认路由。在本示例中，10.0.0.1 为 ISP 的主网关，以及要用 ICMP 回声监控的对象。
9. 在 Options 区域中，单击 **Tracked** 单选按钮，并在 Track ID、SLA ID 和 Track IP Address 字段中输入值。
10. 单击 **Monitoring Options**。此时显示以下对话框。
11. 输入频率和其他监控选项的值，然后单击 **OK**。
12. 添加辅助 ISP 的另一个静态路由，以提供到达 Internet 的路由。要使其成为辅助路由，请用

较高的度量（如 254）配置此路由。如果主路由（主 ISP）失败，则从路由表中删除该路由。并在 PIX 路由表中安装此辅助路由（辅助 ISP）。

13. 单击 **OK** 关闭对话框。配置显示在 Interface 列表中。
14. 选择路由配置，然后单击 **Apply** 更新安全设备配置。

验证

使用本部分可确认配置能否正常运行。

确认配置完成

使用以下这些 **show** 命令验证配置是否完整。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show running-config sla monitor** — 显示配置中的 SLA 命令。`pix# show running-config sla monitor`

```
sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** — 显示操作的当前配置设置。`pix# show sla monitor configuration 123`

```
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.0.0.1
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

- **show sla monitor operational-state** — 显示 SLA 操作的运行统计信息。在主 ISP 发生故障之前，正常运行的状态如下：`pix# show sla monitor operational-state 123`

```
Entry number: 123
Modification time: 13:59:37.824 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 367
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
```

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 15:00:37.825 UTC Thu Oct 12 2006
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

在主 ISP 发生故障（和 ICMP 回声超时）之后，正常运行的状态如下：`pix# show sla monitor operational-state`

```
Entry number: 123
Modification time: 13:59:37.825 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 385
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 15:03:27.825 UTC Thu Oct 12 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

确认安装了备份路由（CLI 方法）

使用 **show route** 命令确定安装备份路由的时间。

- 在主 ISP 发生故障之前，路由表如下：`pix# show route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.200.159.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.200.159.1, outside
```

- 在主 ISP 发生故障之后，删除静态路由，然后安装备份路由，路由表如下：`pix(config)# show route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
```

```
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

确认安装了备份路由（ASDM 方法）

要用 ASDM 确认安装了备份路由，请完成以下这些步骤：

1. 单击 **Monitoring**，然后单击 Routing。
2. 从 Routing 树中，选择 **Routes**。在主 ISP 发生故障之前，路由表如下：DEFAULT 路由通过外部接口指向 10.0.0.2。在主 ISP 发生故障之后，删除该路由，然后安装备份路由。DEFAULT 路由现在通过备份接口指向 10.250.250.1。

故障排除

debug 命令

- **debug sla monitor trace** — 显示回声操作的进度。跟踪的对象（主 ISP 网关）有效，并且 ICMP 回声成功。`pix(config)# show route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

  跟踪的对象（主 ISP 网关）失效，并且 ICMP 回声失败。`pix(config)# show route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

- **debug sla monitor error** — 显示 SLA 监控进程遇到的错误。跟踪的对象（主 ISP 网关）有效，并且 ICMP 成功。`pix(config)# show route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

跟踪的对象（主 ISP 网关）失效，并且删除了所跟踪的路由。

```
%PIX-7-609001: Built local-host
NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:02
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:02
%PIX-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.200.159.1,
               distance 1, table Default-IP-Routing-Table, on interface
               outside
!--- 10.0.0.1 is unreachable, so the route to the Primary ISP is removed.
```

不必要地删除了所跟踪的路由

如果不必要地删除了所跟踪的路由，请确保监控目标始终可供接收回声请求。此外，请确保监控目标状态（即目标是否可访问）与主 ISP 连接的状态紧密相关。

如果选择的监控目标比 ISP 网关还要远，则沿该路由的另一条链路可能发生故障或另一个设备可能产生干扰。此配置可能造成 SLA 监控断定与主 ISP 的连接发生故障，并造成安全设备不必要地故障转移到辅助 ISP 链路。

例如，如果选择分支机构路由器作为监控目标，则 ISP 与分支机构的连接以及沿路的任何其他链路可能发生故障。监控操作发送的 ICMP 回声失败后，将删除所跟踪的主路由，即使主 ISP 链路仍有效也是如此。

在本示例中，用作监控目标的主 ISP 网关由 ISP 管理，并位于 ISP 链路的另一端。此配置可确保如果监控操作发送的 ICMP 回声失败，则 ISP 链路几乎无疑地处于失效状态。

ASA 上的 SLA 监控

问题：

ASA 升级到 8.0 版之后，SLA 监控不起作用。

解决方案：

问题可能是由于在 OUTSIDE 接口中配置了 **IP Reverse-Path** 命令。删除 ASA 中的该命令，并尝试检查 SLA 监控。

相关信息

- **配置静态路由跟踪**
- PIX/ASA 7.2 命令参考
- Cisco ASA 5500 系列安全设备
- Cisco PIX 500 系列安全设备
- 技术支持和文档 - Cisco Systems