配置冗余或备份ISP链路的ASA

目录

简介

本文描述如何配置Cisco ASA 5500系列可适应安全工具(ASA)为使用静态路由追踪功能为了使设备使用冗余或备份互联网连接。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 5555-X系列Cisco的ASA运行软件版本9.x或以上
- Cisco ASDM版本7.x或以上

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

您能以Cisco ASA 5500系列版本9.1(5)也使用此配置。

> **Note**:**backup interface命令**要求为了配置在5505系列的ASA的第四个接口。*参考Cisco安全设备命令参考的*备份接口部分，*版本7.2*欲知更多信息。

背景信息

此部分提供在本文描述静态路由追踪功能的概述，以及一些重要建议，在您开始前。

静态路由追踪功能概述

与使用的一问题静态路由是能确定的内在的机制不存在路由是否上上下下是。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，一个静态路由追踪功能用于为了跟踪静态路由的可用性。功能从路由表删除静态路由并且用备份路由替换它在失败。

在主要的租用的线路变得不可用情况下，静态路由追踪允许ASA使用对第二ISP的一低廉连接。为了达到此冗余， ASA连结静态路由与您定义了的监听目标。服务级别协议操作监控有定期ICMP echo请求的目标。如果echo replies没有接收，则对象考虑得下来，并且相关的路由从路由表删除。并用以前配置的备份路由代替所删除的路由。当备份路由是在使用中的时， SLA监视器操作继续其尝试到达监听目标。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。

在本文使用的示例中， ASA维护对互联网的两连接。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。通过第二ISP提供的DSL调制解调器访问的第二连接是更加低速的数字用户线路 DSL。

> **Note**:在本文描述的配置不可能用于共享的负载均衡或的负载，因为ASA不支持。此配置仅用于冗余或备份用途。如果主要的发生故障，出站流量使用主ISP然后第二ISP。主 ISP 故障会导致流量临时中断。

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。然而，如果对主ISP的连接断开， ASA更改路由表为了直接数据流对DSL连接。静态路由追踪用于为了达到此冗余。

ASA用处理所有互联网数据流对主ISP的静态路由配置。每十秒， SLA监视器过程检查为了确认主ISP网关可及的。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。

此配置提供一个比较便宜的方式保证出局的网络访问依然是可用对在ASA后的用户。正如本文所描述，此设置也许不适用于对资源的入站访问在ASA后。先进的联网技能要求为了达到无缝的Inbound连接。本文档中不涉及这些技能。

重要建议

在您尝试在本文描述的配置前，您必须选择能回答互联网控制消息协议(ICMP) ECHO请求的监听目标。目标可以是您选择的所有网络对象，但是紧密联系对您的互联网服务提供商连接推荐的目标。这是一些可能的监听目标：

- ISP 网关地址
- 由另一个 ISP 管理的地址
- 在另一网络的一个服务器，例如ASA必须联络的验证、授权和统计(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）

本文假设， ASA是完全能操作和已配置的为了允许Cisco Adaptive Security Device Manager (ASDM)做配置更改。

> **提示**：关于如何允许ASDM的信息配置设备，*参考CLI书1的*ASDM部分的*配置的HTTPS访问：思科ASA系列一般操作CLI配置指南， 9.1*。

配置

请使用在此部分描述为了配置ASA为使用静态路由追踪功能的信息。

> **Note**:请使用命令查找工具(仅限注册用户)为了得到关于在此部分使用的命令的更多信息。

> **Note**:在此配置方面使用的IP地址不是合法可路由的在互联网。他们是RFC 1918地址，用于实验室环境。

网络图

在此部分提供的示例使用此网络设置：

CLI 配置

请使用此信息为了通过CLI配置ASA ：

```
ASA# show running-config

ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0

!--- The interface attached to the Secondary ISP.
!--- "backup" was chosen here, but any name can be assigned.

!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone IND 5 30
object network Inside_Network
 subnet 192.168.10.0 255.255.255.0
object network inside_network
 subnet 192.168.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
```

```
no arp permit-nonconnected
!
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface

!--- NAT Configuration for Outside and Backup

route outside 0.0.0.0 0.0.0.0 203.0.113.2 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 0.0.0.0 198.51.100.2 254

!--- 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 pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00

sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 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.

crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
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 stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 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 rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
!
service-policy global_policy global
```

ASDM 配置

完成这些步骤为了配置与ASDM应用程序的冗余或备份ISP支持：

1. 在ASDM应用程序内，请点击**配置**，然后单击**接口**。

2. 选择从接口列表的**GigabitEthernet0/1**，然后单击**编辑**。 此对话框出现：

3. 在*接口名称*、*安全等级*、*IP地址*和*子网掩码*字段检查**Enable (event)接口检查**复选框，并且输入适当的值。

4. 单击 **OK** 关闭对话框。

5. 配置其他接口当必要时，然后单击**应用**为了更新ASA配置：

6. 选择**路由**并且点击在ASDM应用程序的左边查找的**静态路由**：

7. 单击 **Add** 添加新的静态路由。此对话框出现：

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。在本例中， **203.0.113.2**是主ISP网关，并且**4.2.2.2**是监控的对象与ICMP回音。

9. 在选项地区中，请在*跟踪ID*、*SLA ID*和*跟踪IP地址*字段点击**被跟踪的**单选按钮并且输入适当的值。

10. 单击 **Monitoring Options**。此对话框出现：

11. 输入频率和其他监听选项的适当的值，然后点击OK键。

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。此辅助路由(第二ISP)在专用互联网交换(PIX)路由表里安装。

13. 点击OK键为了关闭对话框：

    配置在接口列表出现：

14. 选择路由配置，然后单击**应用**为了更新ASA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

> **Note**:命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

请使用这些**显示**命令为了验证您的配置完成：

- **show running-config sla监视器**–此命令输出显示SLA in命令配置。

```
ASA# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **显示sla监视器配置**–此命令输出显示操作的当前配置设置。

```
ASA# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 4.2.2.2
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data&colon; 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:
```

- **显示sla监视器操作状态**–此命令输出显示SLA操作的可操作的统计信息。

在主 ISP 发生故障之前，正常运行的状态如下：

```
ASA# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:30:40.672 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 46
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: 13:38:10.672 IND Sun Jan 4 2015
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回音超时)后，这是操作状态：

```
ASA# show sla monitor operational-state
Entry number: 123
Modification time: 13:30:40.671 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 57
```

```
    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: 13:40:00.672 IND Sun Jan 4 2015
    Latest operation return code: Timeout
    RTT Values:
    RTTAvg: 0       RTTMin: 0       RTTMax: 0
    NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

确认备份路由安装(CLI方法)

输入**show route命令**为了确认备份路由安装。

在主ISP发生故障前，路由表看起来与此相似：

```
ASA# 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 203.0.113.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

在主ISP发生故障后，静态路由删除，并且备份路由安装，路由表看起来与此相似：

```
ASA# 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 198.51.100.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

确认备份路由安装(ASDM方法)

为了确认备份路由通过ASDM安装，请导航对**路由的Monitoring>**，从路径选择树然后选择**路由**。

在主ISP发生故障前，路由表看起来与在下镜像显示的那相似。注意**默认路由**指向203.0.113.2通过**外部接口**：

在主ISP发生故障后，路由删除，并且备份路由安装。**默认路由**当前指向198.51.100.2通过**备份接口**：

故障排除

此部分提供一些有用的调试指令并且描述如何排除故障被跟踪的路由不必要地删除的问题。

debug 命令

您能使用这些调试指令为了排除故障您的配置问题：

- **调试sla监视器trace** –此命令输出显示响应操作的进度。

  如果被跟踪的对象(主ISP网关)启用和ICMP回音成功，输出看起来与此相似：

```
ASA# 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 198.51.100.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

  如果被跟踪的对象(主ISP网关)发生故障和ICMP回音发生故障，输出看起来与此相似：

```
ASA# 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 198.51.100.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

- **调试sla监视器错误**–此命令输出显示SLA监视器进程遇到的所有错误。

如果被跟踪的对象(主ISP网关)启用和ICMP成功，输出看起来与此相似：

```
ASA# 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 198.51.100.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

如果被跟踪的对象(主ISP网关)发生故障和被跟踪的路由删除，输出看起来与此相似：

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside

!--- 4.2.2.2 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。

如果选择比ISP网关离开的监听目标，沿该路由的另一条链路也许发生故障或另一个设备也许干涉。此配置也许造成SLA监视器认为，对主ISP的连接失败和造成ASA不必要地故障切换到第二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。一旦由监视操作失败发送的ICMP回音，主要的被跟踪的路由删除，即使主ISP链路是活跃的。

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。此配置保证，如果由监视操作失败发送的ICMP回音， ISP链路几乎肯定是下来。

相关信息

- Cisco ASA 5500-X系列下一代防火墙
- 技术支持和文档 - Cisco Systems