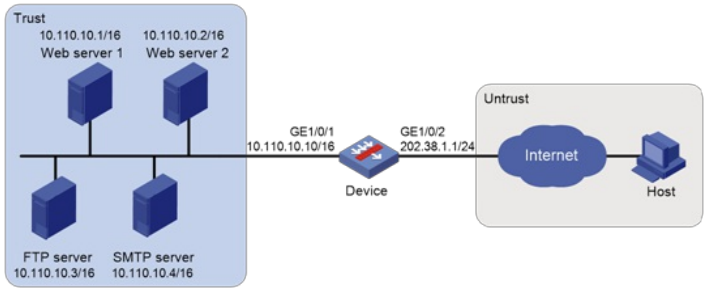
基于全局NAT策略实现内网用户使用公网地址访问内部服务器（NAT hairpin）

NAT 关萌 2021-05-29 发表

组网及说明

Nat44使用场景：内网用户通过nat44策略，通过访问202.38.1.1地址访问内网10.110.10.1，并将源ip地址转换为10.110.10.10防火墙上接口地址。



配置步骤

配置接口IP地址

根据组网图中规划的信息，配置各接口的IP地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.110.10.10 16
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的IP地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置安全策略

配置名称为untrust-trust的安全策略，保证trust安全域中的Host可以访问Trust安全域中的Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-trust
[Device-security-policy-ip-1-trust-trust] source-zone trust
[Device-security-policy-ip-1-trust-trust] destination-zone trust
[Device-security-policy-ip-1-trust-trust] action pass
[Device-security-policy-ip-1-trust-trust] quit
[Device-security-policy-ip] quit
```

(4) 配置NAT功能

配置服务对象组，提供Web服务。

```
[Device] object-group service service2
[Device-obj-grp-service-service2] service tcp destination eq 80
[Device-obj-grp-service-service2] quit
```

配置全局NAT规则，允许内网主机访问内网服务器。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] destination-ip host 202.38.1.1
[Device-nat-global-policy-rule-rule1] source-zone trust
[Device-nat-global-policy-rule-rule1] service service1
[Device-nat-global-policy-rule-rule1] action dnat ip-address 10.110.10.1 local-port 80
[Device-nat-global-policy-rule-rule1] action snat easy-ip
[Device-nat-global-policy-rule-rule1] quit
```

配置关键点

配置全局NAT规则，允许内网主机访问内网服务器。
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] destination-ip host 202.38.1.1
[Device-nat-global-policy-rule-rule1] source-zone trust
[Device-nat-global-policy-rule-rule1] service service1
[Device-nat-global-policy-rule-rule1] action dnat ip-address 10.110.10.1 local-port 80
[Device-nat-global-policy-rule-rule1] action snat easy-ip
[Device-nat-global-policy-rule-rule1] quit