17 常见 IPSG 操作

关于本章

介绍IPSG的常见操作。

17.1 配置 IP+VLAN 静态绑定

通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤，可以有效防止恶意主机盗用合法主机的IP地址仿冒合法主机非法访问网络。适用于局域网络中主机数较少，且主机使用静态配置IP地址的网络环境。

以添加源IP为192.168.2.1、VLAN ID为10的静态绑定表项，并在VLAN 10上使能IPSG功能为例，配置过程如下：

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 192.168.2.1 vlan 10
[HUAWEI] vlan 10
[HUAWEI-vlan10] ip source check user-bind enable
```

17.2 配置 IP+MAC 静态绑定

通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤，可以有效防止恶意主机盗用合法主机的IP地址仿冒合法主机非法访问网络。适用于局域网络中主机数较少，且主机使用静态配置IP地址的网络环境。

以添加源IP为192.168.2.1、源MAC为0002-0002-0002的静态绑定表项，并在VLAN 10上使能IPSG功能为例，配置过程如下：

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 192.168.2.1 mac-address 0002-0002-0002
[HUAWEI] vlan 10
[HUAWEI-vlan10] ip source check user-bind enable
```


17.3 配置 IP+MAC+接口静态绑定

通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤，可以有效防止恶意主机盗用合法主机的IP地址仿冒合法主机非法访问网络。适用于局域网络中主机数较少，且主机使用静态配置IP地址的网络环境。

以添加源IP为192.168.2.1、源MAC为0002-0002-0002、接口为GE0/0/1的静态绑定表项，并在VLAN 10上使能IPSG为例，配置过程如下：

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 192.168.2.1 mac-address 0002-0002-0002 interface
gigabitethernet 0/0/1
[HUAWEI] vlan 10
[HUAWEI-vlan10] ip source check user-bind enable
```

17.4 配置基于 DHCP Snooping 动态绑定表的 IPSG

通过配置基于DHCP Snooping动态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤控制，可以有效防止恶意主机盗用合法主机的IP地址来仿冒合法主机后非法访问网络。适用于局域网络中主机较多，且主机使用DHCP动态获取IP地址的网络环境。配置过程如下：

1. 配置DHCP Snooping，生成DHCP Snooping动态绑定表。
   a. 系统视图下执行命令**dhcp enable**，全局使能DHCP功能。
   b. 系统视图下执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。
   c. 接口或VLAN视图下执行命令**dhcp snooping enable**，使能接口或者VLAN的DHCP Snooping功能。
   d. 接口视图下执行**dhcp snooping trusted**或者VLAN视图下执行**dhcp snooping trusted interface** *interface-type interface-number*，配置信任接口。

      对于从信任接口收到的IP报文，IPSG不做匹配检查且允许通过。
2. 接口或者VLAN视图下执行命令**ip source check user-bind enable**，使能IPSG功能。

以下通过示例介绍如何配置基于DHCP Snooping动态绑定表的IPSG。

配置DHCP Snooping功能，指定GE1/0/1为信任接口，并在GE0/0/2上使能IPSG。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping trusted
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/2] ip source check user-bind enable
```

配置DHCP Snooping功能，指定GE1/0/1为信任接口，并在VLAN10上使能IPSG。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk
[HUAWEI-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
```



```
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping trusted interface gigabitethernet 1/0/1
[HUAWEI-vlan10] ip source check user-bind enable
```

17.5 删除静态绑定表项

当绑定表创建错误或者已绑定主机的网络权限变更时，需要执行命令**undo user-bind static** [{ { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *，删除静态绑定表项。

- 删除单条绑定表时，**undo**命令指定的参数必须和绑定表中表项完全匹配，才能删除成功。
- 支持批量删除绑定表项。例如：
  - 执行命令**undo user-bind static**，删除所有绑定表信息。
  - 执行命令**undo user-bind static interface gigabitethernet 1/0/1**，删除指定接口**GE1/0/1**的所有表项。
  - 执行命令**undo user-bind static vlan 10**，删除指定**VLAN10**的所有表项。

以下通过示例介绍如何删除静态绑定表项。

首先，通过命令**display dhcp static user-bind all**查看已存在的静态绑定表项。

```
<HUAWEI> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                      MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
192.168.1.1                     0001-0001-0001  --  /--  /--    --
192.168.1.2                     0002-0002-0002  --  /--  /--    GE1/0/2
192.168.2.1                     --              --  /--  /--    GE1/0/1
192.168.2.2                     --              --  /--  /--    GE1/0/1
192.168.2.3                     --              --  /--  /--    GE1/0/1
192.168.3.1                     0004-0004-0004  10  /--  /--    --
192.168.3.2                     0005-0005-0005  10  /--  /--    --
--------------------------------------------------------------------------------
Print count:          7          Total count:          7
```

删除IP地址为192.168.1.1的静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static ip-address 192.168.1.1 mac-address 0001-0001-0001
```

删除IP地址为192.168.1.2的静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static ip-address 192.168.1.2 mac-address 0002-0002-0002 interface
gigabitethernet 1/0/2
```

删除GE1/0/1接口的所有静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static interface gigabitethernet 1/0/1
```

删除VLAN10的所有静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static vlan 10
```

以上步骤顺序执行完后，所有绑定表项均被删除。

