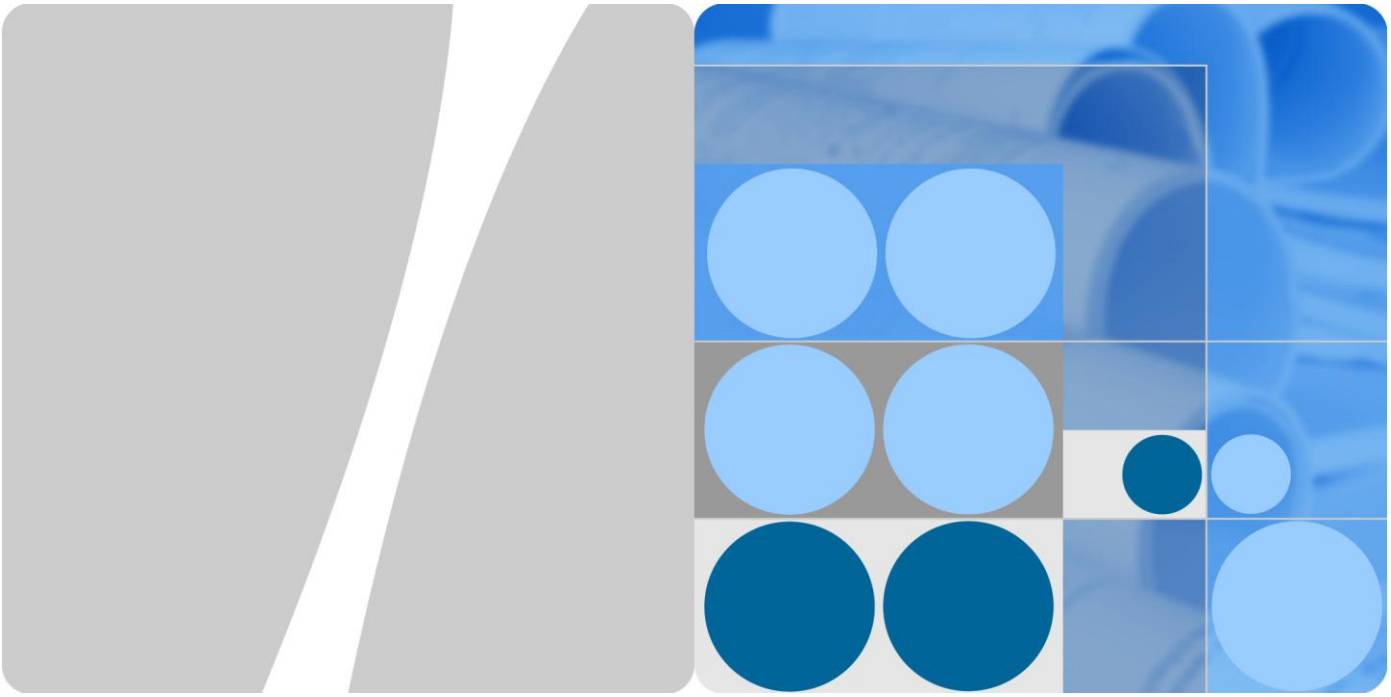


技术白皮书-IPSG

文档版本 01

发布日期 2012-09-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 IPSG

关于本章

1.1 介绍

定义

IPSG 是 IP Source Guard 的简称。IPSG 可以防范针对源 IP 地址进行欺骗的攻击行为。

目的

随着网络规模越来越大，基于源 IP 的攻击也逐渐增多。一些攻击者利用欺骗的手段获取到网络资源，取得合法使用网络资源的权限，甚至造成被欺骗者无法访问网络，或者信息泄露。IP Source Guard 针对基于源 IP 的攻击提供了一种防御机制，可以有效的防止基于源地址欺骗的网络攻击行为。

受益

防御网络上的 IP 源攻击，降低对 IP 源攻击的维护成本。

更安全的网络环境，更稳定的网络服务。

1.2 参考标准和协议

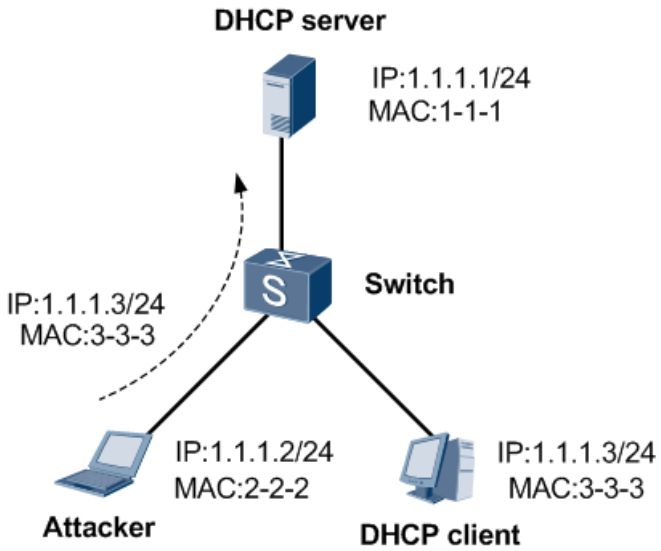
无。

1.3 原理描述

IP Source Guard 功能是基于绑定表对 IP 报文进行匹配检查。当设备在转发 IP 报文时，将此 IP 报文中的源 IP、源 MAC、端口、VLAN 信息和绑定表的信息进行比较，如果信息匹配，表明是合法用户，则允许此报文正常转发，否则认为是攻击报文，并丢弃该 IP 报文。

如图 1-1 所示，攻击者伪造合法用户报文，篡改了设备 MAC 表的出接口信息，使服务器回复的报文被发送给攻击者。

图1-1 IP/MAC 欺骗攻击示意图



为了防止此类攻击，可以在设备上配置 IP Source Guard 功能，对进入接口的 IP 报文进行绑定表匹配检查，报文的信息和绑定表一致，允许其通过，否则丢弃报文。

IPSG 检查项

IP Source Guard 功能是基于绑定表对 IP 报文进行检查，检查内容包括：源 IP 地址、源 MAC 地址、VLAN 和接口。设备支持的 IP Source Guard 可以对这几项的任意组合进行检查。

在接口视图下：

- 接口+IP
- 接口+MAC
- 接口+IP+MAC
- 接口+IP+VLAN
- 接口+MAC+VLAN
- 接口+IP+MAC+VLAN

在 VLAN 视图下：

- VLAN+IP
- VLAN+MAC
- VLAN+IP+MAC
- VLAN+IP+Interface
- VLAN+MAC+Interface
- VLAN+IP+MAC+Interface

1. 配置基于 VLAN 的 IP Source Guard：

1）. 使能IP报文检查功能。

```
[Switch] vlan 100
[Switch-vlan100] ip source check user-bind enable
```

2）. 配置IP报文检查项。
#配置检查IP报文的源IP地址和源MAC地址是否匹配绑定表

```
[Switch-vlan100] ip source check user-bind check-item ip-address mac-address
[Switch-vlan100] quit
```

3）. 使用 **display ip source check user-bind** 命令用来查看 IP 报文检查功能的配置信息。

```
[Switch] display ip source check user-bind
  ------------------------------------------------------------

  IPSG VLAN ID        : 100
  IPSG check items    : IP | MAC
```

其中 IP | MAC 表示 IP 报文检查项为源 IP 地址和源 MAC 地址。

2. 配置基于接口的 IP Source Guard：

1）. 使能IP报文检查功能。

```
[Switch] interface gigabitethernet 1/0/1
[Switch- GigabitEthernet1/0/1] ip source check user-bind enable
```

2）. 配置IP报文检查项。
#配置检查IP报文的源IP地址和源MAC地址是否匹配绑定表

```
[Switch- GigabitEthernet1/0/1] ip source check user-bind check-item ip-address mac-address
[Switch-vlan100] quit
```

3）. 使用 **display ip source check user-bind** 命令用来查看 IP 报文检查功能的配置信息。

```
[Switch] display ip source check user-bind
  ------------------------------------------------------------

  IPSG interface      : GigabitEthernet1/0/2
  IPSG check items    : IP | MAC
```

```
IPSG alarm          : Enable
IPSG alarm threshold : 360
```

其中 IP | MAC 表示 IP 报文检查项为源 IP 地址和源 MAC 地址。

IPSG 绑定机制

IP Source Guard 支持的绑定表包括：

- 对于 DHCP 动态用户，当使能 DHCP Snooping 功能后会动态生成绑定表。
- 对于静态配置用户，需要手动配置静态绑定表。

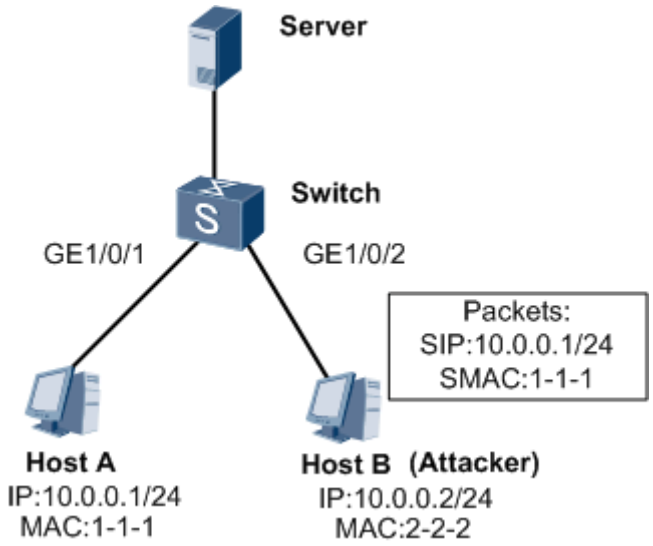
1.4 应用

1.4.1 IPSG 的典型组网应用

如图 1-2 所示，HostA 与 HostB 分别与 Switch 的 GE1/0/1 和 GE1/0/2 接口相连。用户的 IP 地址是静态分配的，要求使 HostB 不能仿冒 HostA 的 IP 和 MAC 欺骗服务器，保证 HostA 的 IP 报文能正常上送。

企业需要在 Switch 的两个接口上使能 IP 报文检查功能，并配置 HostA 的静态绑定表。

图1-2 配置 IP Source Guard 组网图



Switch 的配置文件

```
#
 user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
GigabitEthernet 1/0/1 vlan 10
#
```

```
interface GigabitEthernet 1/0/1
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
interface GigabitEthernet 1/0/2
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
return
```