

在Sx500系列可堆叠交换机的IP源防护约束数据库的配置

客观

IP源防护是能提供防止导致的数据流攻击的安全功能，当主机设法使用一台相邻的主机时的IP地址。当IP源防护是启用的时，交换机只传输客户端IP数据流对在DHCP监听的约束数据库包含的IP地址。如果主机发送匹配在数据库的一个条目的信息包，交换机转发信息包。如果信息包不匹配在数据库的一个条目，被丢弃。

在一个实时方案中，IP源防护使用的一种方式将帮助防止不信任的第三方尝试伪装一个真正用户的中间人攻击。基于在IP源防护约束数据库被配置的地址，只有从客户端的数据流用该IP地址允许和信息包的其余丢弃。

Note: 监听的DHCP应该是启用的为了IP源防护能作用。为了获得关于怎样的更多详细资料对请监听enable (event)的DHCP请参见 [在Sx500系列可堆叠交换机的条款DHCP监听的约束数据库配置](#)。配置约束数据库指定也是必要的哪些IP地址允许。

此条款说明如何配置IP源防护的约束数据库在Sx500系列可堆叠交换机。

可适用的设备

- Sx500系列可堆叠交换机

软件版本

- v1.2.7.76

IP源防护约束数据库的配置

约束数据库

步骤1. 登录到Web配置工具，并且选择**安全> IP源防护>约束数据库**。约束数据库页打开：

Binding Database

Supported IP Format: Version 4

TCAM Resources Consumed:

Insert Inactive: Retry Frequency Sec. (Range: 10 - 600, Default: 60)
 Never

Binding Database Table (DHCP Snooping Binding Database Table)

Filter: VLAN ID equals to (Range: 1 - 4094)
 MAC Address equals to
 IP Address equals to
 Interface equals to Unit/Slot Port LAG

VLAN ID	MAC Address	IP Address	Interface	Status	Type	Reason
0 results found.						

步骤2. 点击appropriate条目从在插入非激活领域的以下选项选择多频繁应该由交换机做非激活条目激活。DHCP监听的约束数据库使用得三重内容可编程址存储器维护数据库。

- 重试次数频率—产生TCAM资源被检查的频率。DEFAULT值是60。
- 分期付款请设法激活非激活地址。

步骤3. 点击适用更新运行配置文件。

添加约束数据库条目

步骤1. 登陆到Web配置工具，并且选择IP Configuration>打开DHCP监听的约束数据库页的DHCP > DHCP监听的约束数据库。

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: VLAN ID equals to (Range: 1 - 4094)
 MAC Address equals to
 IP Address equals to
 Interface equals to Unit/Slot Port LAG

<input type="checkbox"/>	VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	
							Status	Reason
0 results found.								

步骤2. 点击添加输入条目在添加DHCP监听的条目页。

Supported IP Format: Version 4

VLAN ID:

MAC Address:

IP Address:

Interface: Unit/Slot Port LAG

Type: Dynamic Static

Lease Time: Infinite User Defined Sec. (Range: 10 - 4294967294, Default: Infinite)

步骤3.从信息包在VLAN ID字段预计的下拉列表选择VLAN ID。

步骤4.输入在MAC Address字段将匹配的MAC地址。

步骤5.输入在IP Address字段将匹配的IP地址。

步骤6.是否从接口下拉列表选择接口显示显示信息包预计的端口或滞后。

Type: Dynamic Static

Lease Time: Infinite User Defined

步骤7.点击类型显示条目是否是动态或静态的在Type字段。

- 动态—条目有一个有限的租用时间。
- 静态配置静态条目。

步骤8.输入租用时间在租用时间字段。如果条目动态请输入条目将依然是活动的持续时间。如果没有租用时间然后点击无限。

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: VLAN ID equals to (Range: 1 - 4094)

MAC Address equals to

IP Address equals to

Interface equals to Unit/Slot Port LAG

VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard Status	Reason
1	00-b0-d0-86-d6-f7	192.0.2.2	GE1/1/1	Dynamic	3456	Inactive	No Snoop VLAN

原因，如果接口不是活跃的在Reason字段显示。原因可以如下：

- 没有问题—接口是活跃的。
- 没有监听VLAN —监听的DHCP在VLAN没有被启用。
- 可信的端口—端口委托。
- 资源问题— TCAM资源浪费。

第9.步。要看到条目的一子集，输入适当的查寻标准在约束数据库表里和点击去。过滤器复选框用于过滤从DHCP绑定数据库表的一个特定的条目。

第10.步(可选)取消被输入了和输入新的值的值，点击**清楚动态**。

步骤11.点击**适用更新运行配置文件**。