

ESW2-550X交换机上的IP源防护配置

目标

IP源防护是一种安全功能，可用于防止主机尝试使用相邻主机的IP地址时引起的流量攻击。启用IP源防护后，交换机只将客户端IP流量传输到DHCP监听绑定数据库中包含的IP地址。如果主机发送的数据包与数据库中的条目匹配，交换机将转发该数据包。如果数据包与数据库中的条目不匹配，则丢弃该数据包。

在实时场景中，使用IP源防护有助于防止中间人攻击，即不受信任的第三方试图伪装成正版用户。根据IP源防护绑定数据库中配置的地址，仅允许来自具有该IP地址的客户端的流量丢弃其余数据包。

注意：应启用DHCP监听，使IP源防护正常工作。要获取有关如何启用DHCP监听的更多详细信息，请参阅*ESW2-550X交换机上的DHCP属性配置*文章。还必须配置绑定数据库以指定允许哪些IP地址。有关此方面的详细信息，请参阅*ESW2-550X交换机上DHCP监听绑定数据库的配置*。

本文介绍如何在ESW2-550X可堆叠托管交换机上配置IP源防护。

适用设备

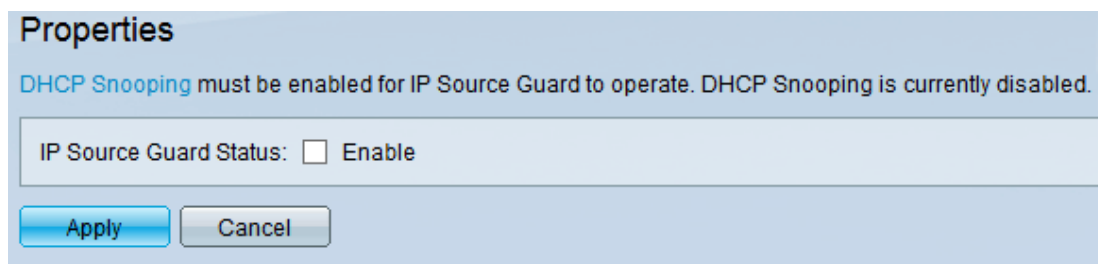
- ESW2-550X
- ESW2-550X-DC

软件版本

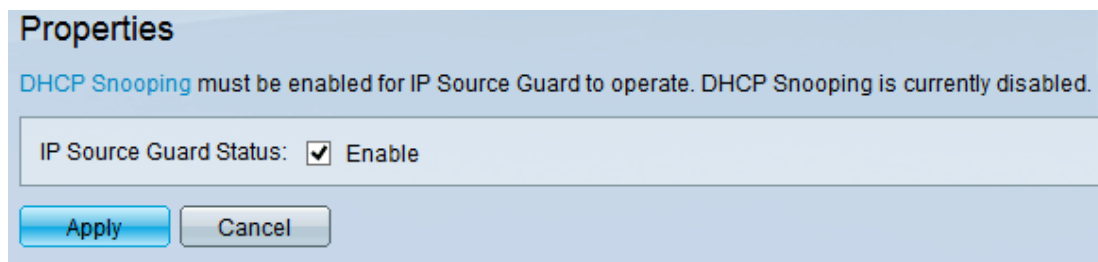
- v1.2.9.44

全局启用IP源防护设置

步骤1. 登录到Web配置实用程序，然后选择Security > IP Source Guard > Properties。“IP源防护属性”页打开：



The screenshot shows the 'Properties' configuration page for IP Source Guard. At the top, a message states: 'DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently disabled.' Below this, there is a section for 'IP Source Guard Status' with an unchecked checkbox and the label 'Enable'. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.



The screenshot shows the 'Properties' configuration page for IP Source Guard. At the top, a message states: 'DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently disabled.' Below this, there is a section for 'IP Source Guard Status' with a checked checkbox and the label 'Enable'. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

步骤2. 选中Enable复选框以全局启用IP源防护。

步骤3.单击“应用”以应用设置。

编辑IP源防护的接口设置

如果在不受信任的端口或LAG上启用IP源防护，则DHCP监听数据库允许传输的DHCP数据包。如果IP地址通过过滤器启用，则允许数据包传输，如下所示：

- IPv4流量 — 允许与源IP地址与特定端口关联的IPv4流量。
- 非IPv4流量 — 允许所有非IPv4流量。

步骤1.登录到Web配置实用程序，然后选择**Security > IP Source Guard > Interface Settings**。“接口设置”页打开：

Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1 GE1	No	No
<input type="radio"/>	2 GE2	No	No
<input type="radio"/>	3 GE3	No	No
<input type="radio"/>	4 GE4	No	No
<input type="radio"/>	5 GE5	No	No
<input type="radio"/>	6 GE6	No	No
<input type="radio"/>	7 GE7	No	No
<input type="radio"/>	8 GE8	No	No
<input type="radio"/>	9 GE9	No	No
<input type="radio"/>	10 GE10	No	No
<input type="radio"/>	11 GE11	No	No
<input type="radio"/>	12 GE12	No	No
<input type="radio"/>	13 GE13	No	No
<input type="radio"/>	14 GE14	No	No
<input type="radio"/>	15 GE15	No	No

接口设置表包含以下参数。

- 接口 — 显示应用IP源防护的接口。
- IP源防护 — 显示是否启用IP源防护。IP源防护可在单个接口上启用。
- DHCP监听受信任接口 — 显示它是否是DHCP受信任接口。受信任接口只能从网络内部接收流量。IP源防护通常在不受信任的DHCP接口上配置。不可信接口是配置为能够从网络外部接收消息的接口。

Interface Settings Table					Showing 1-50 of 50	All	per page
Filter: Interface Type equals to					Port of Unit 2/1	Go	
Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface				
<input type="radio"/>	1	GE1	No	No			
<input type="radio"/>	2	GE2	No	No			
<input type="radio"/>	3	GE3	No	No			
<input type="radio"/>	4	GE4	No	No			
<input type="radio"/>	5	GE5	No	No			
<input checked="" type="radio"/>	6	GE6	No	No			
<input type="radio"/>	7	GE7	No	No			
<input type="radio"/>	8	GE8	No	No			
<input type="radio"/>	9	GE9	No	No			
<input type="radio"/>	10	GE10	No	No			
<input type="radio"/>	11	GE11	No	No			
<input type="radio"/>	12	GE12	No	No			
<input type="radio"/>	13	GE13	No	No			
<input type="radio"/>	14	GE14	No	No			
<input type="radio"/>	15	GE15	No	No			
Copy Settings...					Edit...		

步骤2. 向下滚动页面，然后点击与要编辑的接口对应的单选按钮。单击页面底部的**编辑**。系统将显示“**编辑接口设置**”窗口。

Interface: Unit/Slot 1/1 Port GE6 LAG 1

IP Source Guard: Enabled

步骤3. (可选) 要选择接口，请单击“接口”字段中的任一单选按钮。

·设备/插槽和端口 — 设备标识交换机是活动还是堆叠中的成员。单元1处于活动状态，单元2是成员。如果您不熟悉所用术语，请查看[思科业务：新术语表](#)。插槽标识交换机是ESW2-550还是ESW2-550X。插槽1是ESW2-550，插槽2是ESW2-550X。从Unit/Slot下拉列表中选择所需的选项，然后从Port下拉列表中选择所需的端口。

·LAG — 从LAG下拉列表中选择所需的LAG。链路聚合组(LAG)用于将多个端口链接在一起。LAG可增加带宽、提高端口灵活性，并在两台设备之间提供链路冗余以优化端口使用。

Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
1	GE1	No	No
2	GE2	No	No
3	GE3	No	No
4	GE4	No	No
5	GE5	No	No
6	GE6	No	No
7	GE7	No	No
8	GE8	No	No
9	GE9	No	No
10	GE10	No	No
11	GE11	No	No
12	GE12	No	No
13	GE13	No	No
14	GE14	No	No
15	GE15	No	No

步骤4. 选中IP Source Guard字段中的**Enabled**复选框，以在当前接口上启用IP Source Guard。

步骤5. 单击“应用”。

复制IP源防护的接口设置

步骤1. 登录到Web配置实用程序，然后选择**Security > IP Source Guard > Interface Settings**。“**接口设置**”页打开：

Interface Settings

DHCP Snooping must be enabled for IP Source Guard to operate. IP Source Guard operates only on DHCP Snooping untrusted interfaces.

Interface Settings Table					Showing 1-50 of 50	All	per page
Filter: Interface Type equals to					Port of Unit 2/1	Go	
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface			
<input type="radio"/>	1	GE1	No	No			
<input type="radio"/>	2	GE2	No	No			
<input type="radio"/>	3	GE3	No	No			
<input type="radio"/>	4	GE4	No	No			
<input type="radio"/>	5	GE5	No	No			
<input type="radio"/>	6	GE6	No	No			
<input type="radio"/>	7	GE7	No	No			
<input type="radio"/>	8	GE8	No	No			
<input type="radio"/>	9	GE9	No	No			
<input type="radio"/>	10	GE10	No	No			
<input type="radio"/>	11	GE11	No	No			
<input type="radio"/>	12	GE12	No	No			
<input type="radio"/>	13	GE13	No	No			
<input type="radio"/>	14	GE14	No	No			
<input type="radio"/>	15	GE15	No	No			

Copy Settings... Edit...

步骤2. 点击所需界面的单选按钮，然后向下滚动页面。

Interface Settings Table					Showing 1-50 of 50	All	per page
Filter: Interface Type equals to					Port of Unit 2/1	Go	
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface			
<input type="radio"/>	1	GE1	No	No			
<input type="radio"/>	2	GE2	No	No			
<input type="radio"/>	3	GE3	No	No			
<input type="radio"/>	4	GE4	No	No			
<input type="radio"/>	5	GE5	No	No			
<input checked="" type="radio"/>	6	GE6	No	No			
<input type="radio"/>	7	GE7	No	No			
<input type="radio"/>	8	GE8	No	No			
<input type="radio"/>	9	GE9	No	No			
<input type="radio"/>	10	GE10	No	No			
<input type="radio"/>	11	GE11	No	No			
<input type="radio"/>	12	GE12	No	No			
<input type="radio"/>	13	GE13	No	No			
<input type="radio"/>	14	GE14	No	No			
<input type="radio"/>	15	GE15	No	No			

Copy Settings... Edit...

步骤3. 单击“复制设置”。“复制设置”页打开：

Copy configuration from entry 6 (GE6)

to: (Example: 1,3,5-10 or: GE1,GE3-GE5)

Apply Close

Copy configuration from entry 6 (GE6)

to: (Example: 1,3,5-10 or: GE1,GE3-GE5)

步骤4.在提供的字段中输入所选条目需要复制到的接口。您可以按接口名称(GE1)或编号输入接口。您还可以提供一系列接口，例如GE30-GE37或30-40。

步骤5.单击“应用”。