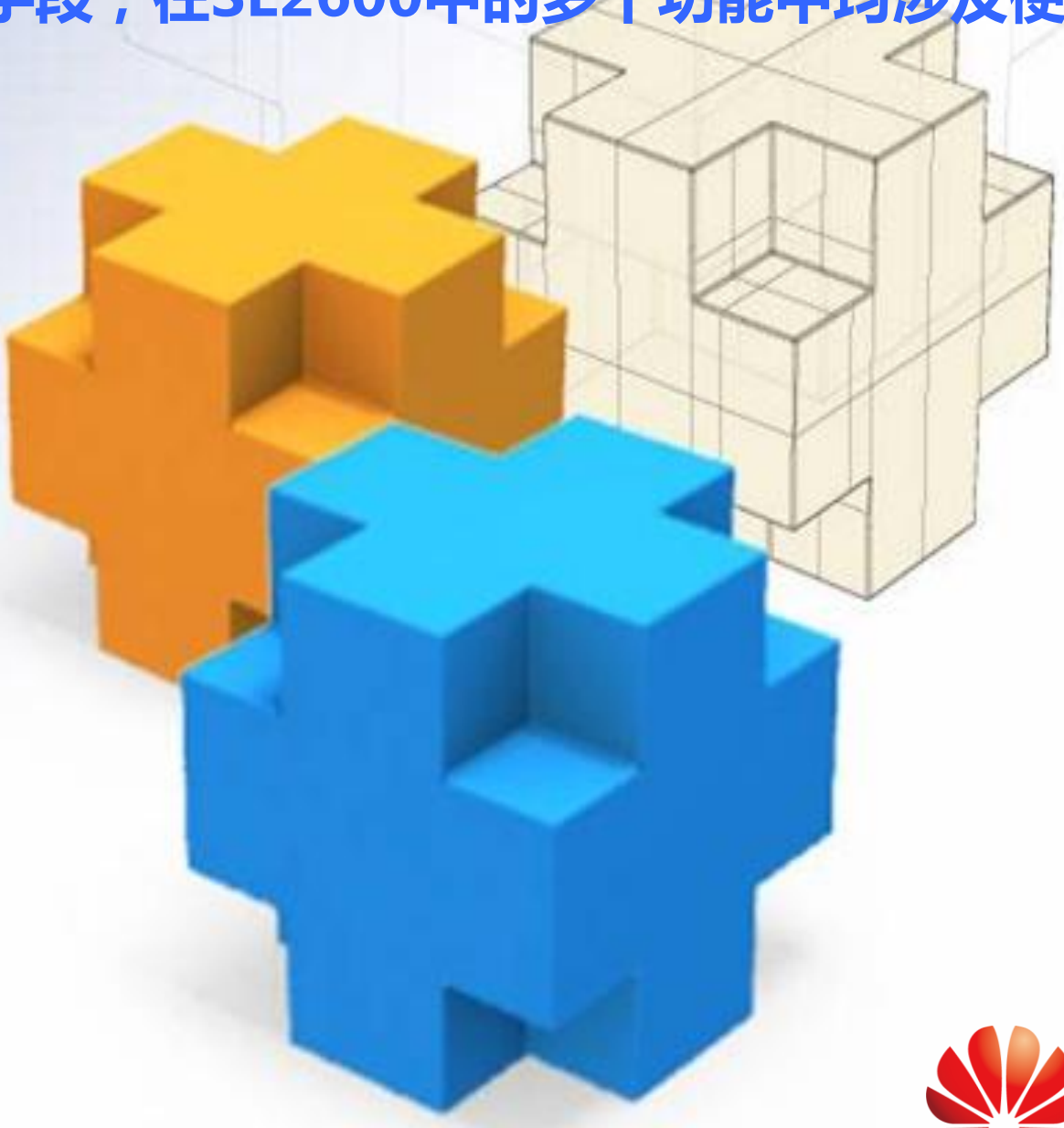
SBC资料直通车

第2期
2014年

核心网资料部　　主编

ACL知多少

----ACL(Access Control List) 是提供网络安全访问的基本手段，在SE2600中的多个功能中均涉及使用到ACL



HUAWEI

ACL是SE2600实现网络安全防护的主要手段之一，但是……

您真的了解ACL生效规律和细节么？

SE2600中又有哪些功能用到ACL呢？

本期将为您介绍ACL实现的关键细节，以及ACL在SE2600中的应用。

1 ACL分类

2 ACL匹配

3 ACL应用

ACL分类 - 选择的困惑

ACL规则有哪些类型？配置时该如何选择？

ACL规则分为**基本ACL**和**高级ACL**，区别是

过滤报文的条件不同

基本ACL规则

高级ACL规则

只通过最基本的条件过滤报文

通过复杂精细的条件过滤报文

ACL匹配 – 报文去哪儿了

我新增了一个允许报文通过的规则，为什么满足这个规则的报文还是被丢弃了？

这是由规则**匹配的顺序决定**的，一定是报文先匹配到了拒绝该报文通过的规则。

规律一：先来后到

在配置ACL规则时，规则会按照配置的先后顺序排列在ACL中保存。

规律二：先到先得

当收到的报文与ACL规则进行匹配时，是按照ACL中保存的顺序逐条匹配，一旦与一条规则匹配成功，则按照此条规则的配置处理报文（允许/拒绝），不再与后续规则进行对比。

了解上述原则后，我们来看看报文去哪儿了？

ACL应用 – 无处不在

SE2600中到底有哪些功能会用到ACL呢？它在各功能中又起到怎样的作用呢？

ACL在SE2600的多个功能中使用，其本质作用是**对报文进行分类识别**，达到**访问控制**的目的。下面对各功能进行介绍。

以太网接口上的流分类

作用：在SE2600流量策略功能中作为一种流分类的规则，对业务板接口上收发的报文进行过滤或流量监管。

搜索关键字：配置ACL规则、配置包过滤、激活基于复杂流分类的流量策略、激活基于复杂流分类的流量监管、配置URPF功能

远程登录访问控制

作用：限制远程登录SE2600的维护终端的IP地址，提高远程登录的安全性。

搜索关键字：配置用户接入IP地址限制

FTP访问控制

作用：限制以FTP方式登录SE2600的FTP客户端的IP地址，提高FTP登录的安全性。

搜索关键字：配置SE2600作为FTP服务器

SNMPv3访问控制

作用：限制使用SNMPv3与SE2600通信的网管的IP地址，提高网管访问的安全性。

搜索关键字：配置SNMPv3安全管理

NTP访问控制

作用：限制对SE2600上NTP服务的访问控制权限，提高NTP服务访问控制的安全性。

搜索关键字：激活NTP

IPSec隧道互通

作用：在IPSec隧道互通特性中，用于指定IPSec安全策略能够生效的报文类型。

搜索关键字：配置IPSec安全策略

在SE2600产品手册中搜索各功能的搜索关键字，详细了解ACL应用。

❶ Support网站

登录http://support.huawei.com/support 后点击“网站意见反馈”，反馈您的宝贵意见。
也可以在您下载SBC CPI页面中的“感谢您对我们的资料提出宝贵意见”一栏中反馈。

❷ HedEx Lite

在HedEX主窗口中，点击“反馈...”，反馈您的宝贵意见。

❸ Email

也可以将您对SBC产品资料的意见或者建议反馈至Support@huawei.com。我们将在两天内与您联系，将我们的解决方案、发布计划等反馈给您。