安全防火墙设备做AFT转换时，域间策略（安全策略）实现流量控制方法

AFT 域间策略/安全域 **刘宏宇** 2019-10-29 发表

问题描述

安全防火墙设备做AFT转换时，域间策略（安全策略）实现流量控制方法

解决方法

众所周知，在安全设备中，对过设备流量只需要知道流量流经设备的源、目安全域，然后针对流量做相应源目安全域策略即可实现对流量的限制。
最近遇到有安全设备做AFT转换的流量限制问题，与我们通常认为实现方式不一致：

问题描述：
服务器（IPV6）----------（trust）防火墙（untrust，AFT）----------外网client（ipv4）

外网ipv4客户端需要访问内网ipv6服务器，按照通常理解，在防火墙上只需要放通untrust-trust域间策略即可放通外网访问内网服务器的流量即可。

指导客户完成配置后测试流量无法经过，通过和客户协商将所有的域间策略放通，测试流量可以经过。

建议通过debug packet-filter packet （客户域间策略调用的是ACL）发现，客户端访问服务的流量，在过AFT转换前后，匹配了两个域间策略：
AFT转换前： 匹配的是 untrust-local的域间策略
AFT转换后：匹配的是local-trust的域间策略

防火墙开启AFT相当于一个代理，外网访问内网开通ipv6侧需要从local-trust域做策略，而外网侧的ipv4需要从untrust-local做策略。