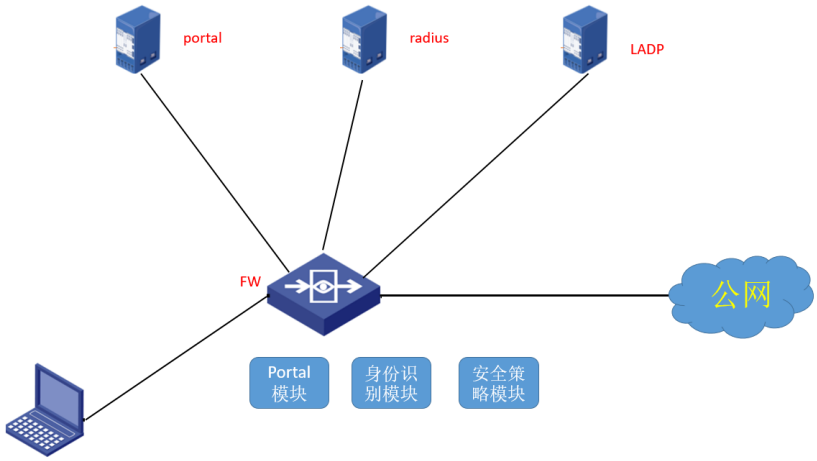
基于用户的安全策略生效的过程（以某局点不能生效为例解释）

域间策略/安全域　孔梦龙　2022-01-04 发表

组网及说明

如图所示，用户想做基于用户的安全策略，用户是用portal认证，用户存放于radius上。同时，radius上的用户在ladp上也有一份，FW通过用户导入将这部分的用户也在FW上保留了一份（此处如果没有LADP，那么用户可以自己在FW创建，总的来说，就是不管用户怎么来的，FW上必须有一份）



问题描述

假设上述的一份用户是：A/B/C三个用户，也就是说，radius上有ABC，本地也创建了三个用户ABC；
现场的配置是（以A用户为例）：

```
# local-user A class network
 authorization-attribute user-role network-operator
 identity-group KKK
#
# user-group KKK
  identity-member user A
#
```

安全策略中（想阻断这A用户）：

```
rule 2601 name MMM
source-zone DMZ
user-group KKK
```

过程分析

现场在接口下使能了portal，用户的输入是用inode的客户端。

（1）用户在inode中输入了A的用户名字

（2）FW收到报文以后直接转发portal服务器，portal认证服务器将这个用户的流量信息（证书、IP、MAC，用户名）加工成一个认证报文发给FW，

（3）FW收到认证报文以后转发给radius，radius认证用户名，名字认证成功就返回成功报文，不成功及返回不成功报文给FW。

（4）FW收到识别的结果转发给portal，portal转发给FW，然后FW再给终端，成功就上线，不成功就不能上线。

具体的过程可以参考配置指导的详细的解释。

现场当天在输入A用户的时候，勾线了证书，然会也是会上线成功，但是按照上面的安全策略的配置，应该是阻断上网的，但实际上没有阻断，正常上网。

分析原因：

上面的过程的细化：

（1）FW收到inode输入的流量以后，实际上FW的portal模块就打开了，当portal服务器发给FW经过加工以后的认证报文以后，这个用户的信息（证书、IP、MAC、用户名）就存在portal模块了。

（2）认证成功上线后，后续A的inode报文的流量过来以后。A用户的访问外网的流量，首先到达了FW，FW的用户识别模块会用poratl模块的数据和本地的用户对比（前面说过，本地的用户可以自己创建，也可以LADP上同步），如果比对成功，就会存在本地，生成一个表，说明这个是用户识别模块识别了的用户；然后这个表会被安全策略调用。有这个表策略才会能有调用的对象。

（3）现场不成功的原因是：流量中有证书，用户识别模块对比的时候，本地的用户只用用户名，没有证书的信息，所以失败。

解决方法

暂时不用勾选证书，后续版本优化。