配置安全策略（针对穿越流量）

2016年6月9日　17:26

安全策略的功能
阻止流量或放行流量

白名单模式：
阻止所有，允许个别

Juniper SRX默认的策略是：阻止所有流量穿越、到达
所以针对Juniper SRX的设置就是放行流量

Cisco ASA对于流量的默认策略
高安全级别--->低安全级别　是放行
低安全级别--->高安全级别　是阻止

root# run show security policies detail
Default policy: deny-all

Juniper对于穿越设备的流量：zone间的流量
在设置穿越流量的时候，设置从哪个zone到哪个zone
set security policies from-zone 源zone to-zone 目标zone

每个策略都需要一个名称
set security policies from-zone 源zone to-zone 目标zone policy 策略名称

策略元素
1、源IP、目标IP
2、源端口、目标端口
3、执行动作：permit（允许）、deny（拒绝）、reject、tunnel

对于源IP和目标IP，可以设置address-book，然后再调用到策略中去匹配
在设置address-book的时候，一定要指明这个地址（段）属于哪个zone

设置address-book的命令：
set security zones security-zone 区域名称 address-book address 地址簿的名称 地址段

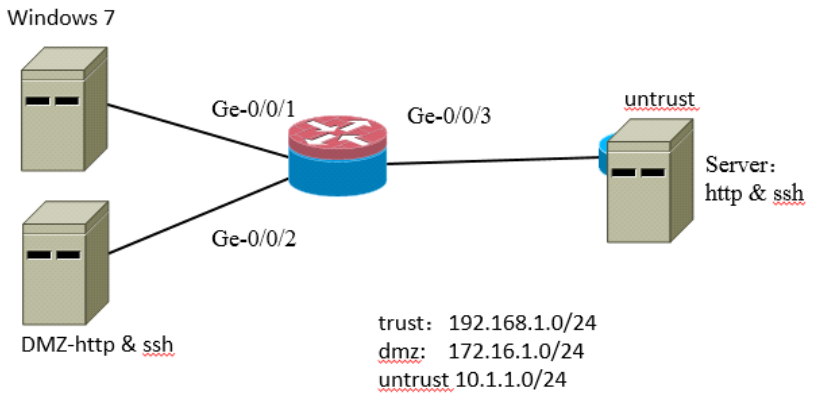
源端口和目标端口，可以通过设置application，再调用到策略中去匹配
set applications application 名称 protocol TCP/UDP destination-port 目标端口号

把设置好的address-book和application调用到策略中
set security policies from-zone 源zone to-zone 目标zone policy 策略名称 match source-address 源IP地址的地址薄名称
set security policies from-zone 源zone to-zone 目标zone policy 策略名称 match destination-address 目标IP地址的地址簿
set security policies from-zone 源zone to-zone 目标zone policy 策略名称 match application 应用名称
set security policies from-zone 源zone to-zone 目标zone policy 策略名称 then 允许就是Permit，拒绝就是deny

如果觉得命令太长，可以进行简化
edit security policies from-zone 源zone to-zone 目标zone policy
set policy 策略名称 match source-address 源IP地址的地址薄名称
set policy 策略名称 match destination-address 目标IP地址的地址簿
set policy 策略名称 match application 应用名称
set policy 策略名称 then 允许就是Permit，拒绝就是deny

※如果你的地址对象或者端口对象是所有，则不需要地址簿或应用程序簿

放行trust到untrust的所有流量
set security policies from-zone trust to-zone untrust policy PERMITANY match source-address any
set security policies from-zone trust to-zone untrust policy PERMITANY match destination-address any
set security policies from-zone trust to-zone untrust policy PERMITANY match application any
set security policies from-zone trust to-zone untrust policy PERMITANY then permit



需求描述1：
禁止trust区域中的192.168.1.2主机访问172.16.1.2的http服务，允许其他主机访问
允许trust区域中的192.168.1.2主机访问172.16.1.2的ssh服务，禁止其他主机访问

设置地址簿，本案例中源IP是192.168.1.2/32，目标IP是172.16.1.2/32
由于对象只针对单个IP，所以子网掩码用/32

设置针对源IP的address-book，源IP位于trust区域，address-book的名称设置为192.168.1.2
匹配的IP地址是192.168.1.2/32
set security zones security-zone trust address-book address 192.168.1.2 192.168.1.2/32

设置针对目标IP的address-book，目标IP位于dmz区域，address-book的名称设置为172.16.1.2
匹配的IP地址是172.16.1.2/32
set security zones security-zone dmz address-book address 172.16.1.2 172.16.1.2/32

设置针对TCP 80端口的application
set applications application TCP-80 protocol tcp
set applications application TCP-80 destination-port 80

设置策略，名称为DENY-HTTP
set security policies from-zone trust to-zone dmz policy DENY-HTTP match source-address 192.168.1.2
set security policies from-zone trust to-zone dmz policy DENY-HTTP match destination-address 172.16.1.2
set security policies from-zone trust to-zone dmz policy DENY-HTTP match application TCP-80
set security policies from-zone trust to-zone dmz policy DENY-HTTP then deny

允许SSH服务，新增一个针对TCP 22的application
set applications application TCP-22 protocol tcp
set applications application TCP-22 destination-port 22

设置策略，名称为PERMIT-SSH
set security policies from-zone trust to-zone dmz policy PERMIT-SSH match source-address 192.168.1.2
set security policies from-zone trust to-zone dmz policy PERMIT-SSH match destination-address 172.16.1.2
set security policies from-zone trust to-zone dmz policy PERMIT-SSH match application TCP-22
set security policies from-zone trust to-zone dmz policy PERMIT-SSH then permit

把主机IP改成192.168.1.20，还是访问不了172.16.1.2的http，是因为Juniper的默认策略是拒绝所有
设置一个针对192.168.1.0/24网段的地址簿
set security zones security-zone trust address-book address 192.168.1.0/24 192.168.1.0/24

设置放行192.168.1.0/24网段到达172.16.1.2 http服务的策略
set security policies from-zone trust to-zone dmz policy QITA-HTTP match source-address 192.168.1.0/24
set security policies from-zone trust to-zone dmz policy QITA-HTTP match destination-address 172.16.1.2
set security policies from-zone trust to-zone dmz policy QITA-HTTP match application TCP-80
set security policies from-zone trust to-zone dmz policy QITA-HTTP then permit

先设置拒绝针对个别的地址的策略，再设置允许所有地址的策略

如果要是配置允许个别的策略，则不需要配置拒绝所有的策略，因为Juniper默认就是拒绝所有