SecPath UTM域间策略的典型配置

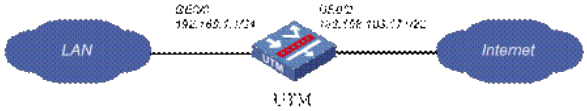
万欣 2009-06-07 发表

H3C UTM域间策略的典型配置

一．用户需求

某用户网络使用UTM来进行内网和外网之间的访问控制，其中高优先级用户可以访问低优先级网络资源，但反之则不允许。

二．组网图



三．配置步骤

1.配置接口GE0/0地址

在左侧导航栏中点击“设备管理 > 接口管理”。

名称	IP地址	网络掩码	安全域	状态	操作
GigabitEthernet0/0	192.168.1.1	255.255.255.0	Trust		
GigabitEthernet0/1			Trust		
GigabitEthernet0/2	192.168.103.171	255.255.252.0	Untrust		
GigabitEthernet0/3			Untrust		
GigabitEthernet0/4			Untrust		
GigabitEthernet0/1.50			Trust		
Vlan-interface1000	7.0.0.1	255.255.255.0	Trust		
NULL0			-		
Vlan-interface60	8.0.0.1	255.255.255.0	Untrust		
GigabitEthernet0/1.60			Untrust		

点击GE0/0栏中的 按钮，进入“接口编辑”界面。按照下图设置接口GE0/0，点击< 确定 >返回“接口管理”界面。

2.配置接口GE0/2地址

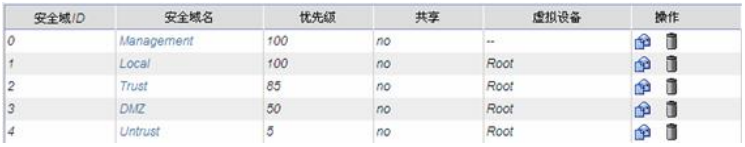
在左侧导航栏中点击“设备管理 > 接口管理”。

名称	IP地址	网络掩码	安全域	状态	操作
GigabitEthernet0/0	192.168.1.1	255.255.255.0	Trust		
GigabitEthernet0/1			Trust		
GigabitEthernet0/2	192.168.103.171	255.255.252.0	Untrust		
GigabitEthernet0/3			Untrust		
GigabitEthernet0/4			Untrust		
GigabitEthernet0/1.50			Trust		
Vlan-interface1000	7.0.0.1	255.255.255.0	Trust		
NULL0			-		
Vlan-interface60	8.0.0.1	255.255.255.0	Untrust		
GigabitEthernet0/1.60			Untrust		

点击G0/2栏中的 按钮，进入“接口编辑”界面。按照下图设置接口G0/2，点击< 确定 >返回“接口管理”界面。

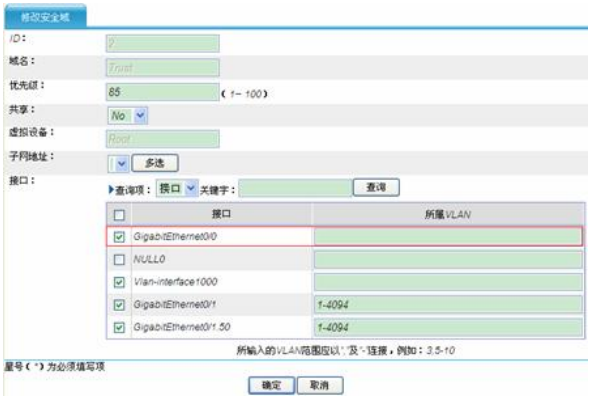
3.接口GE0/0加入Trust域

点击左侧导航栏“设备管理 > 安全域”。



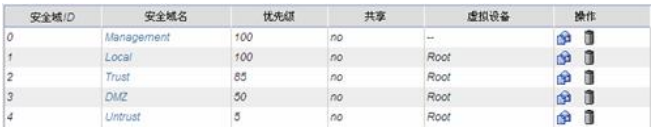
安全域ID	安全域名	优先级	共享	虚拟设备	操作
0	Management	100	no	--	
1	Local	100	no	Root	
2	Trust	85	no	Root	
3	DMZ	50	no	Root	
4	Untrust	5	no	Root	

点击Trust栏中的 按钮，进入“修改安全域”界面。按照下图将接口G0/0加入Trust域，点击< 确定 >返回“安全域”界面。



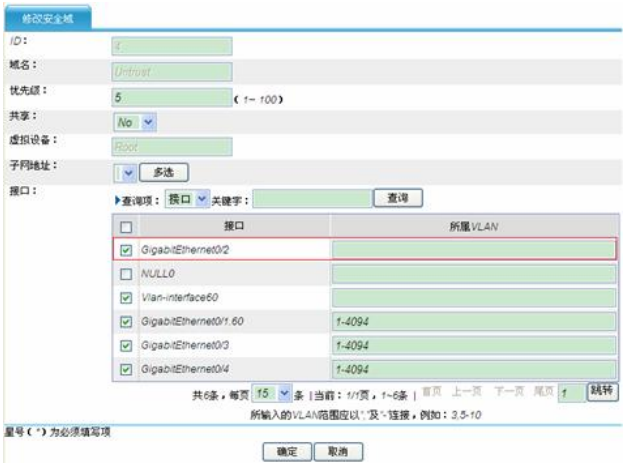
4.接口GE0/2加入Untrust域

点击左侧导航栏“设备管理 > 安全域”。



安全域ID	安全域名	优先级	共享	虚拟设备	操作
0	Management	100	no	--	
1	Local	100	no	Root	
2	Trust	85	no	Root	
3	DMZ	50	no	Root	
4	Untrust	5	no	Root	

点击Untrust栏中的 按钮，进入“修改安全域”界面。按照下图将接口GE0/2加入Untrust域，点击< 确定 >返回“安全域”界面。



5.配置用于NAT的ACL 2222

点击左侧导航栏“防火墙 > ACL”，在出现的界面中点击< 新建 >。

在出现的界面中，输入ID为2222，其余选择默认值。点击< 确定 >回到ACL主界面，新建ACL

点击ALC 2222栏中的 按钮。

在出现的界面中点击< 新建 >。

在出现的界面中配置ACL规则。点击< 确定 >后返回基本ACL2222。

6.在外网口接口G0/2上配置NAT

点击左侧导航栏“防火墙 > NAT > 动态地址转换”。在“地址转换关联”中，点击< 新建 >，出现“新建地址动态转换”。

在这个界面中，按照下图配置。点击< 确定 >返回主界面。

7.配置内网NAT Server

点击左侧导航栏“防火墙 > NAT > 内部服务器”，在出现的界面中点击“内部服务器转换”下的< 新建 >。

配置下图所示的内部服务器：新建内部服务器

点击< 确定 >返回主界面。

8.配置地址对象

（1）配置子网地址对象

点击左侧导航栏“资源管理 > 地址 > IP地址”界面，选择“子网地址”页签，在出现的界面中点击< 新建 >。

如下配置一个子网地址，点击< 确定 >返回主界面。

（2）配置主机地址对象

点击左侧导航栏“资源管理 > 地址 > IP地址”，选择“主机地址”页签，在出现的界面中点击< 新建 >。

进行如下配置，点击< 确定 >返回主界面。

9.配置域间策略

（1）配置高级别安全区域访问低级别安全区域

高级别区域，默认就可以访问低级别区域，不需要设置域间策略。

（2）配置低级别安全区域访问高级别安全区域

点击左侧导航栏“防火墙 > 安全策略 > 域间策略”页签，在出现的界面中点击< 新建 >。

如下配置一条域间策略，用于低级别区域（192.168.100.0/22）的主机可以访问高级别区域（192.168.1.11）这台FTP服务器的FTP服务。

上图中的服务（红色框内）配置如下：点击< 多选 >按钮，在出现的“服务”如下选择，点击< 确定 >，返回“新建域间策略配置”界面。

引用资源为：

点击<确定>，返回。

域间策略为：

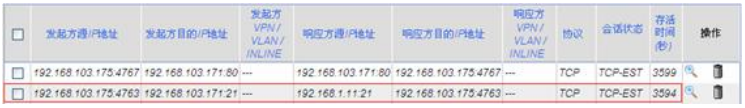
四．验证结果

（1）高级别区域访问低级别区域，默认就可以访问。

从内网发起向internet的访问，例如192.168.1.2对192.168.100.10发起http访问。点击左侧导航栏“防火墙 > 会话管理 > 会话列表”，能看到相关的会话信息：

（2）低级别区域访问高级别区域

从外网一台PC，访问内网FTP服务器，可以进行FTP操作。例如从192.168.103.175访问内网FTP Server 192.168.1.11，查看“会话列表”，可以看到相关会话信息：



	发起方源IP地址	发起方目的IP地址	发起方 VPN / VLAN / INLINE	响应方源IP地址	响应方目的IP地址	响应方 VPN / VLAN / INLINE	协议	会话状态	存活时间(秒)	操作
☐	192.168.103.175:4767	192.168.103.171:80	---	192.168.103.171:80	192.168.103.175:4767	---	TCP	TCP-EST	3599	
☐	192.168.103.175:4763	192.168.103.171:21	---	192.168.1.11:21	192.168.103.175:4763	---	TCP	TCP-EST	3594	