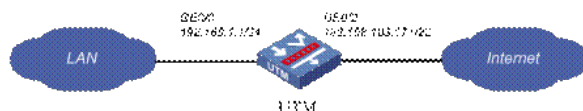


H3C UTM域间策略的典型配置

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	192.168.103.17	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。

接口编辑

接口名称：

GigabitEthernet0/0

接口类型：

不设置

VID：

MTU：

1500 (46~ 1500，缺省值= 1500)

TCP MSS：

1460 (128~ 2048，缺省值= 1460)

工作模式：

☐ 二层模式
☒ 三层模式

IP配置：

☐ 无IP配置
☒ 静态地址
☐ DHCP
☐ BOOTP
☐ PPP协商
☐ 借用地址

IP地址：

192.168.1.1

网络掩码：

24 (255.255.255.0)

其他接口：

GigabitEthernet0/2

确定

返回

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	192.168.103.17	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。

接口编辑

接口名称：

GigabitEthernet0/2

接口类型：

不设置

VID：

MTU：

1500

(46- 1500, 缺省值= 1500)

TCP MSS：

1460

(128- 2048, 缺省值= 1460)

工作模式：

二层模式

三层模式

IP配置：

无IP配置

静态地址

DHCP

BOOTP

PPP协商

借用地址

IP地址：

192.168.103.171

网络掩码：

22 (255.255.252.0)

其他接口：

GigabitEthernet0/0

确定

返回

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。

修改安全域

ID：

0

域名：

Trust

优先级：

85

(1- 100)

共享：

No

虚拟设备：

Root

子网地址：

多选

接口：

查询项：接口

关键字：

查询

接口	所属VLAN
☒ GigabitEthernet0/0	
☐ NULL0	
☒ Vlan-interface1000	
☒ GigabitEthernet0/1	1-4094
☒ GigabitEthernet0/1-50	1-4094

星号(*)为必填填写项

确定

取消

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。

修改安全域

ID:

域名:

优先级: (1~100)

共享:

虚拟设备:

子网地址:

接口: 接口 关键字: 查询

接口	所属VLAN
☒ GigabitEthernet0/2	
☐ NULL0	
☒ Vlan-interface60	
☒ GigabitEthernet0/1/60	1-4094
☒ GigabitEthernet0/3	1-4094
☒ GigabitEthernet0/4	1-4094

共6条, 每页 15 条 | 当前: 1/1页, 1~6条 | 首页 上一页 下一页 尾页 跳转

星号(*)为必填项

确定 取消

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 >。

ACL加速状态图标描述: ●已加速 ●未加速 ●部分加速

访问控制列表ID	类型	规则数量	匹配顺序	ACL加速管理	操作
3000	高级	1	用户配置	加速	

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

新建ACL

访问控制列表ID: 2000-2999 基本访问控制列表。
3000-3999 高级访问控制列表。
4000-4999 二层访问控制列表。

匹配规则:

星号(*)为必填项

确定 取消

点击ALC 2222栏中的 按钮。

ACL加速状态图标描述: ●已加速 ●未加速 ●部分加速

访问控制列表ID	类型	规则数量	匹配顺序	ACL加速管理	操作
2222	基本	0	用户配置	加速	
3000	高级	1	用户配置	加速	

新建

在出现的界面中点击< 新建 >。

基本ACL2222

规则ID	操作	描述	时间段	操作

新建 返回

在出现的界面中配置ACL规则。点击< 确定 >后返回基本ACL2222。

ACL=2222 新建基本规则

☐ 规则ID: (0-65534。如果不输入规则ID，系统将会自动指定一个。)

操作: 时间段:

☐ 分片报文 ☐ 记录日志

☒ 源IP地址: 源地址通配符:

VPN实例:

确定 取消

基本ACL2222

规则ID	操作	描述	时间段	操作
0	permit	source 192.168.1.0 0.0.0.255	无限制	

新建 返回

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”。

地址池

地址池索引	开始/IP地址	结束/IP地址	优先级	操作
新建				

地址转换关联

接口	ACL	地址池索引	地址转换方式	操作
新建				

在这个界面中，按照下图配置。点击< 确定 >返回主界面。

新建动态地址转换

接口：

GigabitEthernet0/2

ACL：

2222

（ 2000~ 3999 ）

地址转换方式：

Easy IP

地址池索引：

（ 0~ 31 ）

星号（*）为必须填写项

确定

取消

地址池

地址池索引	开始/IP地址	结束/IP地址	优先级	操作
新建				

地址转换关联

接口	ACL	地址池索引	地址转换方式	操作
GigabitEthernet0/2	2222		Easy IP	 

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 >

。

内部服务器转换

接口	VPN实例	外部/IP地址	外部端口	内部/IP地址	内部端口	协议类型	操作
新建							

配置下图所示的内部服务器：新建内部服务器

新建内部服务器

接口：

GigabitEthernet0/2

VPN实例：

1

协议类型：

6(TCP)

外部/IP地址：

☐ 指定/IP地址：

☒ 使用接口的/IP地址：

当前接口

外部端口：

☒ 21

（ 0~ 65535, 0表示任意端口 ）

☐

（ 1~ 65535 ）

内部/IP地址：

192.168.1.11

内部端口：

☐

（ 0~ 65535, 0表示任意端口 ）

☒ 21

（ 0~ 65535, 0表示任意端口 ）

星号（*）为必须填写项

确定

取消

点击< 确定 >返回主界面。

内部服务器转换

接口	VPN实例	外部/IP地址	外部端口	内部/IP地址	内部端口	协议类型	操作
GigabitEthernet0/2		192.168.103.171	21	192.168.1.11	21	6(TCP)	 

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 >

。

主机地址 范围地址 子网地址

查询项：

名称

关键字：

查询

☐	名称	子网	排除地址	描述	状态	操作
新建 删除选中 导入 导出						

如下配置一个子网地址，点击< 确定 >返回主界面。

主机地址

范围地址

子网地址

名称

public

(1-31字符, 1个汉字占2个字符)

描述

(1-31字符, 1个汉字占2个字符)

IP地址/掩码

192.168.100.0

/0.0.3.255

*IP地址通配符需要配置为反掩码方式

排除地址

可以输入多个IP地址, 以半角逗号(,)分隔。

星号(*)为必填填写项

确定

取消

主机地址

范围地址

子网地址

查询项: 名称

关键字:

查询

	名称	子网	排除地址	描述	状态	操作
☐	private	192.168.1.0/0.0.0.255			未使用	
☐	public	192.168.100.0/0.0.3.255			未使用	

新建

删除选中

导入

导出

(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 >。

主机地址

范围地址

子网地址

查询项: 名称

关键字:

查询

	名称	IP地址/域名	描述	状态	操作
☐					

新建

删除选中

导入

导出

进行如下配置，点击< 确定 >返回主界面。

主机地址

范围地址

子网地址

☒ IP地址

☐ 域名

名称

PrivateFTPServer

(1-31字符, 1个汉字占2个字符)

描述

(1-31字符, 1个汉字占2个字符)

IP地址列表

192.168.1.11

添加

192.168.1.11

删除

IP地址

星号(*)为必填填写项

确定

取消

主机地址

范围地址

子网地址

查询项: 名称

关键字:

查询

	名称	IP地址/域名	描述	状态	操作
☐	ftpserv	192.168.100.10		未使用	
☐	privateftpserv	192.168.1.11		未使用	

新建

删除选中

导入

导出

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 >。

查询项: 源域

关键字:

查询

	源域	目的域	规则ID	VPN实例	源IP地址	目的IP地址	服务	时间段	过滤动作	描述	启用选项	日志功能	源MAC地址	目的MAC地址	操作
☐															

新建

删除选中

导入

导出

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。

新建访问控制列表规则

源域: Untrust

目的域: Trust

规则ID: 1 (0-65534)

描述: (1-31字符)

VPN实例: 1

源IP地址: 新建IP地址 / 源IP地址: public 多选

目的IP地址: 新建IP地址 / 目的IP地址: privateftoserver 多选

服务: 名称: (Multiple) 多选

过滤动作: Permit

时间段: 1

☐ 启用MAC匹配

☐ 启用Syslog日志功能 ☒ 启用规则 确定后继续添加下一条规则 ☒

星号(*)为必填项

确定 取消

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：

引用资源

服务: ftp, ftp-get, ftp-put

可用的服务: any_service, bgp, chargen, cmd, daytime, dhcp-relay, discard_tcp, finger, ftp, ftp-get, ftp-put, gopher, http, https, icmp-address-mask

添加 删除

确定 取消

点击<确定>，返回。

域间策略为：

查询项: 源域 关键字: 查询

源域	目的域	规则ID	VPN实例	源IP地址	目的IP地址	服务	时间段	过滤动作	描述	启用选项	日志功能	源MAC地址	目的MAC地址	操作
Untrust	Trust	1		public	privateftoserver	ftp		Permit		☒	未开启			

新建 批量选中 导入 导出

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：

☐	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
☐	192.168.100.22.138	192.168.103.255.138	---	192.168.103.255.138	192.168.100.22.138	---	UDP	UDP-OPEN	3	
☐	192.168.100.130.137	192.168.103.255.137	---	192.168.103.255.137	192.168.100.130.137	---	UDP	UDP-OPEN	14	
☐	192.168.96.11.2669	192.168.103.171.80	---	192.168.103.171.80	192.168.96.11.2669	---	TCP	TCP-EST	3600	
☐	192.168.96.11.2048	192.168.103.171.3480	---	192.168.103.171.0	192.168.96.11.3480	---	ICMP	ICMP-OPEN	47	
☐	192.168.100.14.138	192.168.103.255.138	---	192.168.103.255.138	192.168.100.14.138	---	UDP	UDP-OPEN	3	
☒	192.168.1.2.2631	192.168.100.10.80	---	192.168.100.10.80	192.168.103.171.1026	---	TCP	TCP-EST	3487	

(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	 