**【标题】**

TrustMore配置示例V1.0

**可信接入**

**中宇万通**

**2015年6月**

**文档声明**

Copyright©2005~2014 by ZHYU Technologies Co., Ltd. All Rights Reserved.

中宇万通，版权所有。

未经中宇万通书面许可，不得使用任何形式或任何途径，包括使用影印、录制在内的电子或机械手段、其他信息储存和恢复系统等对本文任何部分进行复制或传播。

本文中表达的观点权属于中宇万通。

本文的解释权归中宇万通。

中宇万通

**版本声明**

**文档适用范围**

* 研发人员
* 技术人员
* 管理人员
* 其他人员

**文档变更声明**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 撰写人 | 部门 | 时间 | 备注 |
| 1 | 姓名 | 工作部门 | 撰写或修订时间 | 内容 |
| 2 | 郑泷浩 | 技术部 | 2015年6月 |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

目录

[文档声明 i](#_Toc387313724)

[版本声明 ii](#_Toc387313725)

[1 NTML 1](#_Toc387313726)

[1.1IIS设置 1](#_Toc387313727)

[1.2配置TSG管理端 3](#_Toc387313728)

[1.3用户登录TSG安全网关验证 6](#_Toc387313729)

[2 FORM 8](#_Toc387313730)

[2.1 验证应用可用性 8](#_Toc387313731)

[2.2配置TSG管理端 8](#_Toc387313732)

[2.3用户登录TSG安全网关验证 14](#_Toc387313733)

[3 HTML 15](#_Toc387313734)

[3.1 验证应用可用性 15](#_Toc387313735)

[3.2配置TSG管理端 15](#_Toc387313736)

[4 BASIC 20](#_Toc387313737)

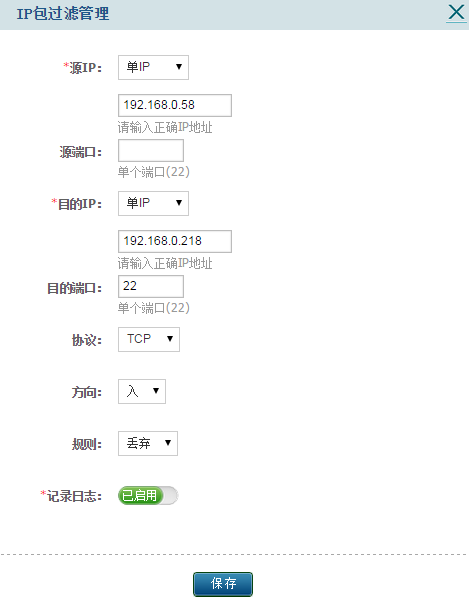
[4.1Tomcat配置 20](#_Toc387313738)

[4.2配置TSG管理端 21](#_Toc387313739)

[4.3用户登录TSG安全网关验证 25](#_Toc387313740)

# 网络防火墙

## IP包过滤



实例：0.58我的PC 0.218 网关

注释：我要访问0.218这个网关，比如是通过ssh访问，要禁止访问的话，那么就需要禁22端口，则目的端口需要配置为22，ssh是tcp协议就选tcp规则是丢弃，则配置好后保存开启，然后ssh 192.168.0.218 看是否能连上，若不能则证明成功（生效前ssh测试看是否连接，若能连接则进行测试）

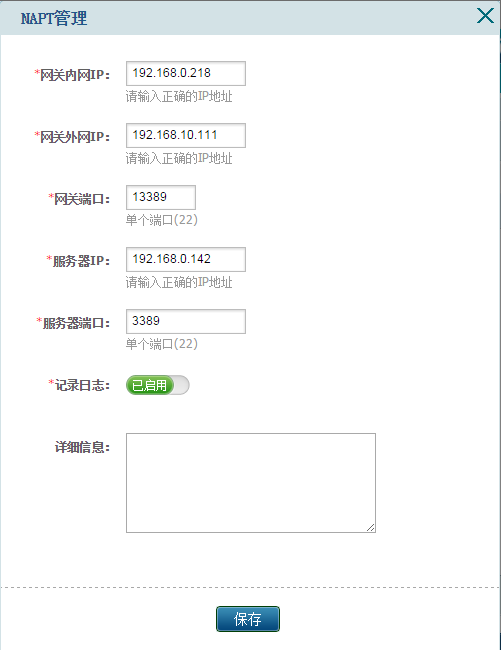
其他情况测试跟这个类似

## 端口映射

端口映射就是将外网主机的IP地址的一个端口映射到内网中一台机器，提供相应的服务。当用户访问该IP的这个端口时，服务器自动将请求映射到对应局域网内部的机器上**。**

**2.1添加端口映射**





上图解释：

1. 网关内网IP\网关外网IP：

这里咱们是想直接通过访问网关来访问应用，所以网关要配置外网地址与内网地址，外网地址是外部访问网关的地址，内网地址是与应用连通（在同一网段）的网关地址；

1. 网关端口：

通过网关的哪一个端口来访问网关；

1. 服务器ip：

代表要访问的应用的IP，

1. 服务器端口：

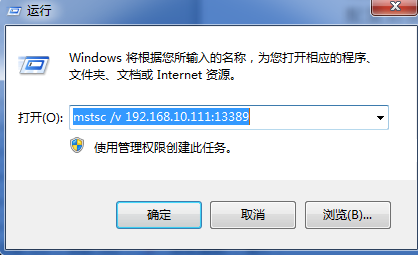
代表访问的应用对外开放的端口；

1. 记录日志：

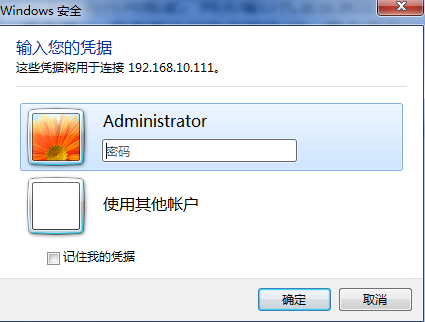
代表是否开启审计；

**2.2测试是否成功**

比如我上面的配置是想通过端口映射远程登录192.168.0.142这台机器，这样配置后我就可以执行win+R



即可远程登录到192.168.0.142这台主机

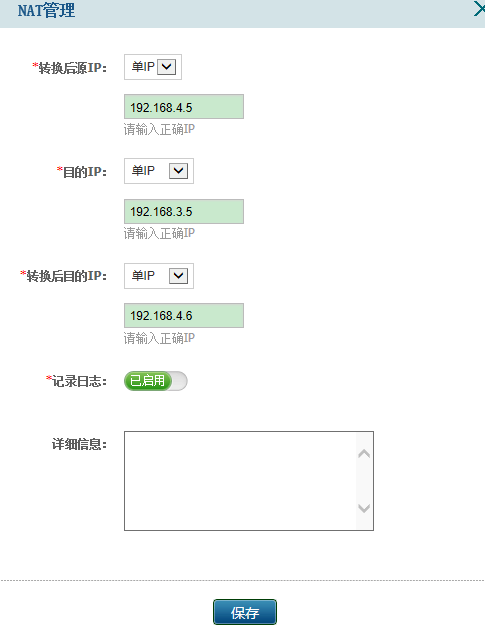


输入用户名口令登录即可

## 地址转换

地址转换(NAT)：路由器将私有地址转换为公有地址使数据包能够发到因特网上，同时从因特网上接收数据包时，将公用地址转换为私有地址。 在计算机网络中，网络地址转换（Network Address Translation或简称NAT，也叫做网络掩蔽或者IP掩蔽）是一种在IP数据包通过路由器或防火墙时重写源IP地址或/和目的IP地址的技术





## 都是固定IP

**客户端ip 192.168.3.4**

**网关ip是192.168.3.5和192.168.4.5**

**应用地址：192.168.4.6**

**转换之前，对于客户端来说目的地址就是网关地址也就是3.5即上图的目的IP配置，但是转换后源IP就是网关的地址（这里是相对于应用来说源IP所以这里是4.5）这样转换后目的地址也就变成4.6应用的IP地址。**

**最后测试是否成功，没有转换之前访问的是3.5，转换之后访问4.5，若是成功访问那么代表地址转换成功。**

## 其他类情况

**同上，只是是控制的一个ip段，但是访问的时候只要在这个段里面，访问就会直接访问转后后目的地址所代表的应用。**