

许先生，您好：

如刚才电话沟通，经您的同意，此 case 将做关闭处理，以下为案例总结，请您知悉：

Case No: CAS-07184-W0V1P6

问题描述：

=====

用户反馈无法关闭本地 MSTSC，请协助提供方案。

问题分析：

=====

经与用户沟通，在了解用户实际需求后，通过注册表添加键值，ipsec 禁用端口，禁用 netbios 协议等方式实现，具体步骤可参见历史邮件。

问题总结：

=====

经用户同意，此问题已解决，可以关闭此案例。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：4008180055
电子邮箱 Email: liqi@cmgos.com



发件人: Li Qi

发送时间: 2022 年 9 月 26 日 15:15

收件人: 'win10 技术支持' <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

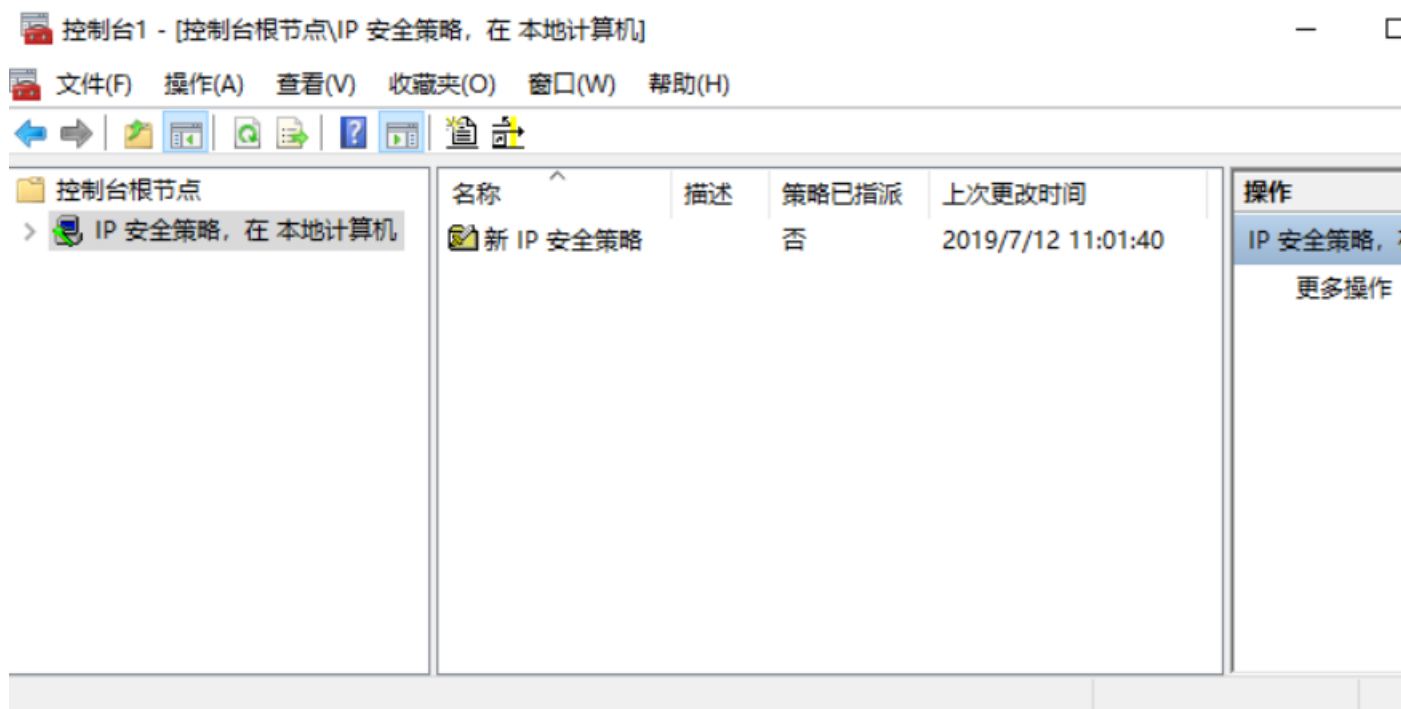
主题: 回复: 【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2|ICBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

许先生, 您好:

如刚才电话沟通, 请按如下步骤尝试使用 ipsec 对端口进行禁用。

操作步骤:


- 1.键入 Windows 键+R 键调出运行栏, 输入 mmc, 调出控制台
- 2.点击左上角“文件”-“添加/删除管理单元”, 添加 IP 安全策略管理



- 3.双击“新 IP 安全策略”, 在“新 IP 安全策略属性”下双击“新 IP 筛选器列表”, 在“编辑规则 属性”下双击打开“新 IP 筛选器列表”, 点击“添加”, 进行配置

规则

常规

和其他计算机通讯的安全规则

IP 安全规则(I):

IP 筛选器列表	筛选器操作	身份验证方法	隧道终结点
<input checked="" type="checkbox"/> 新 IP 筛选器列表	新筛选器操作	<无>	无
<input type="checkbox"/> <动态>	默认响应(仅限于 ...	Kerberos	<无>

<

>

添加(D)...

编辑(E)...

删除(R)

☒ 使用“添加向导”(W)

确定

取消

应用(A)

IP 筛选器列表

筛选器操作

身份验证方法

隧道设置

连接类型



所选的 IP 筛选器列表指定了哪个网络流量将受此规则影响。

IP 筛选器列表(L):

名称	描述
<input checked="" type="radio"/> 新 IP 筛选器列表	

添加(D)...

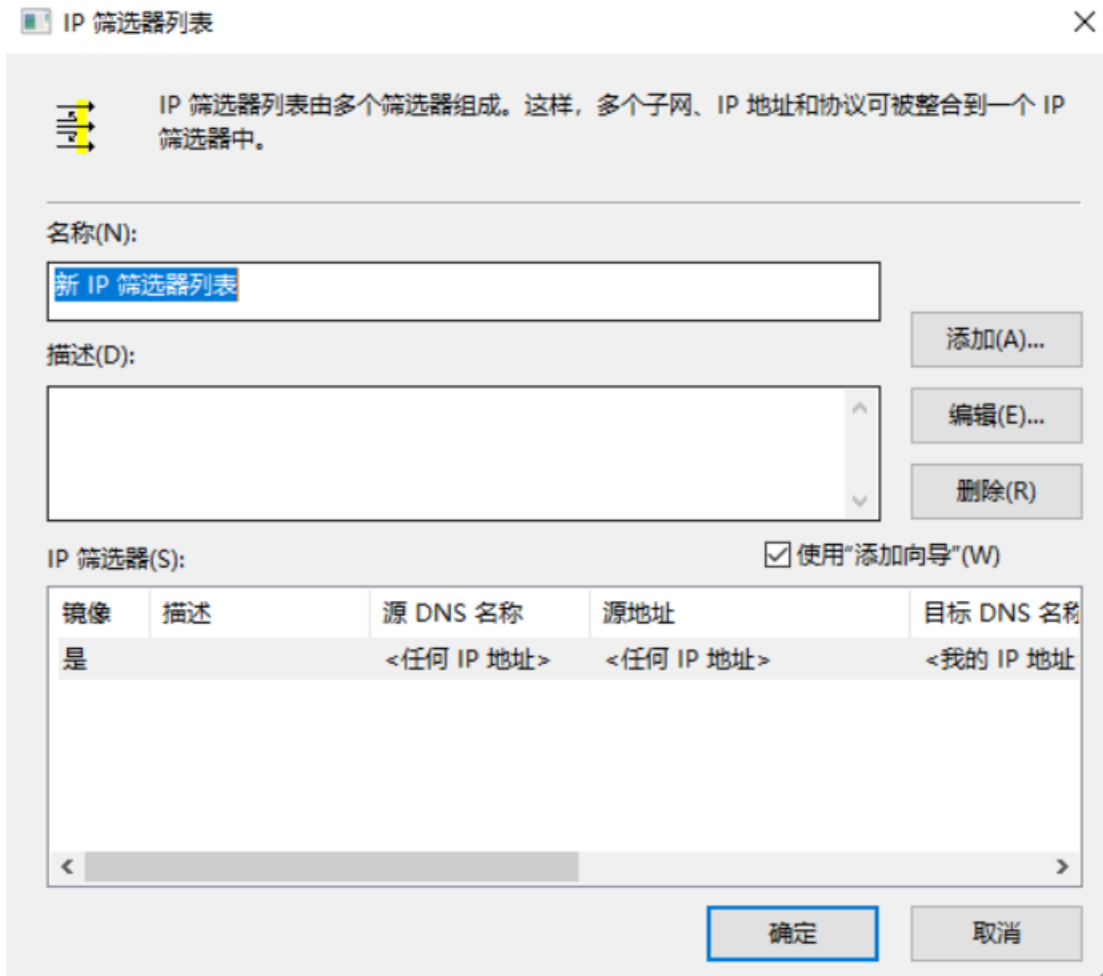
编辑(E)...

删除(R)

确定

取消

应用(A)



4.添加新的规则，对此规则进行描述，源地址选择“任何 IP 地址”，目标地址选择“我的 IP 地址”，根据禁用的端口属性，选择协议类型，测试中使用的是 445 端口，协议选择 TCP

IP 筛选器描述和镜像属性

使用此描述字段来指定 IP 筛选器的名称或详细解释。

选择“镜像”复选框来为每一个方向指定一个筛选器。

描述(D):

禁用端口

☒ 镜像(M)。与源地址和目标地址正好相反的数据包相匹配。

< 上一步(B)

下一步(N) >

取消

IP 协议类型

选择 IP 协议类型。如果类型是 TCP 或 UDP，你将同时指定源和目标端口。

选择协议类型(S):

TCP ▾

6 ▲
▼

100%

< 上一步(B)

下一步(N) >

取消

IP 筛选器向导

×

IP 协议端口
许多 TCP/IP 应用程序协议建立在常用的 TCP 或 UDP 端口上。

设置 IP 协议端口:

☒ 从任意端口(F)

☐ 从此端口(R):

445

☐ 到任意端口(T)

☒ 到此端口(O):

445

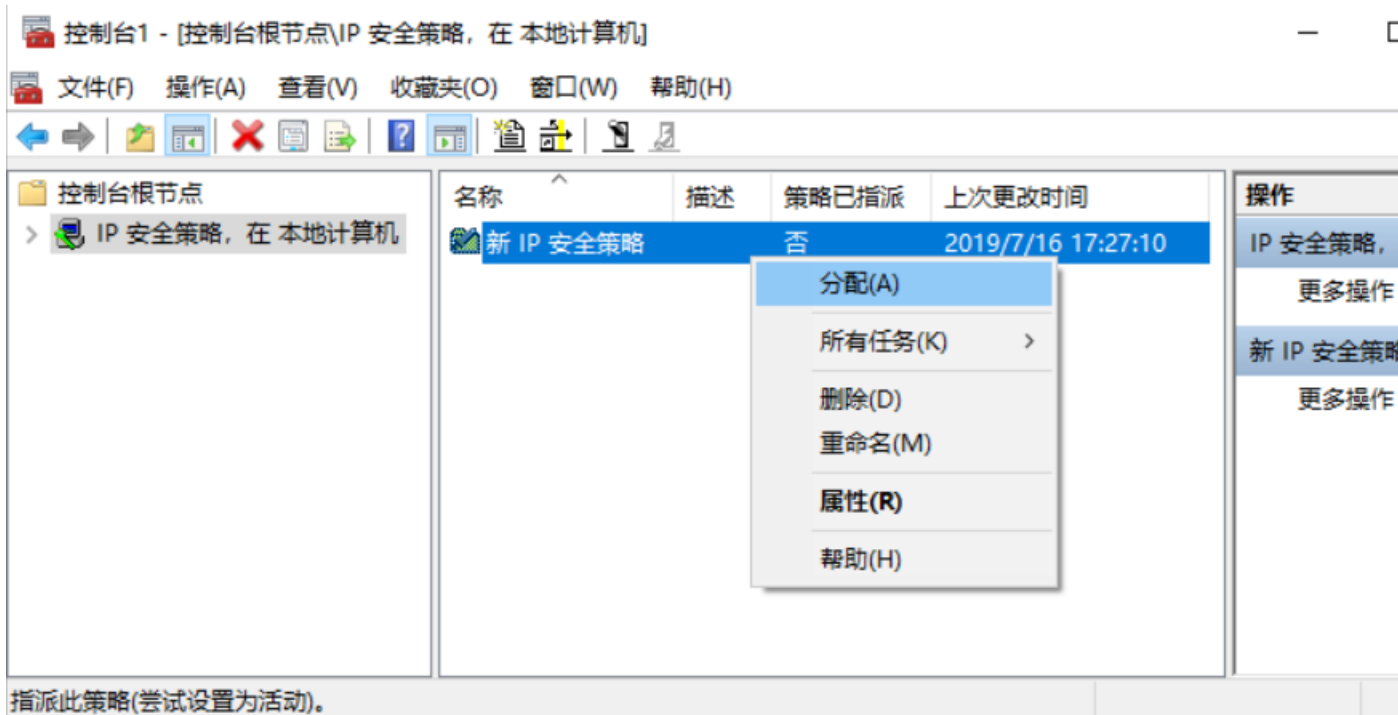
100%

< 上一步(B)

下一步(N) >

取消

5.完成设置后，在控制台下对新 IP 安全策略进行分配，右键点击该 IP 安全策略，选择“分配”，分配完成后，禁用端口成功



6.使用 powershell 进行连通测试，确认是否禁用

分配前（禁用端口前）：

```
PS C:\Windows\system32> test-netconnection -computername 10.0.18.125 -port 445

ComputerName      : 10.0.18.125
RemoteAddress     : 10.0.18.125
RemotePort        : 445
InterfaceAlias    : 以太网
SourceAddress     : 10.0.18.97
TcpTestSucceeded  : True
```

分配后（禁用端口后）：

```
PS C:\Windows\system32> test-netconnection -computername 10.0.18.125 -port 445
警告: TCP connect to (10.0.18.125 : 445) failed

ComputerName      : 10.0.18.125
RemoteAddress     : 10.0.18.125
RemotePort        : 445
InterfaceAlias    : 以太网
SourceAddress     : 10.0.18.97
PingSucceeded     : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : False
```

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co.,Ltd.

服务支持电话： 4008180055

电子邮箱 Email: liqi@cmgos.com



发件人: Li Qi

发送时间: 2022 年 9 月 26 日 14:46

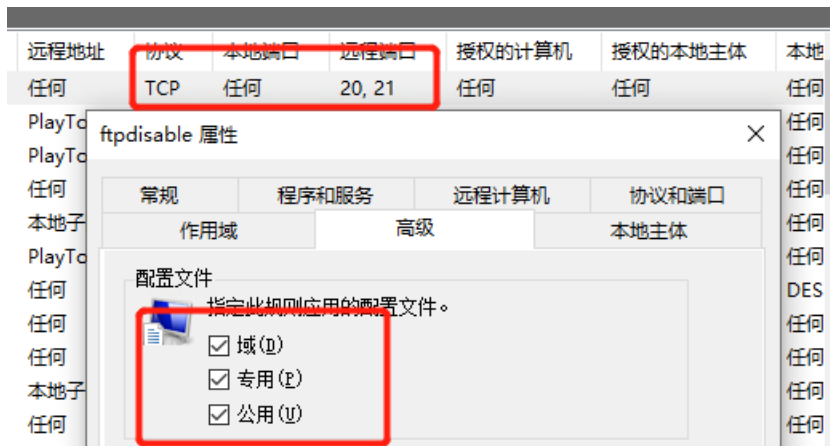
收件人: 'win10 技术支持' <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: 【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2|ICBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

许先生, 您好:

常用的 ftp 端口为 20 和 21, 您可以把这两个端口都禁用后再尝试访问看看。



网络访问依据您的访问方式不同, 涉及到的网络协议不同, “网络”中的计算机发现是 netbios 协议。“\\IP\sharefolder”是 SMB 协议。根据与您的沟通, 请确保如下设置后查看效果:

关闭网络发现: (注意选择对应的网络配置文件)

网络发现和文件共享

网络发现

如果已启用网络发现，则这台计算机可以发现网络上的其他计算机和设备，而且其他网络计算机也可以发现这台计算机。

☐ 启用网络发现

☒ 启用网络连接设备的自动设置。

☒ 关闭网络发现

文件和打印机共享

启用文件和打印机共享时，网络上的用户可以访问通过此计算机共享的文件和打印机。

☐ 启用文件和打印机共享

☒ 关闭文件和打印机共享

来宾或公用

所有网络

禁用 NetBios:

IP 设置 DNS WINS

WINS 地址，按使用排序(W):

添加(A)... 编辑(E)... 删除(V)

如果启用 LMHOSTS 查找，它将应用于所有启用 TCP/IP 的连接。

☒ 启用 LMHOSTS 查找(L) 导入 LMHOSTS(M)...

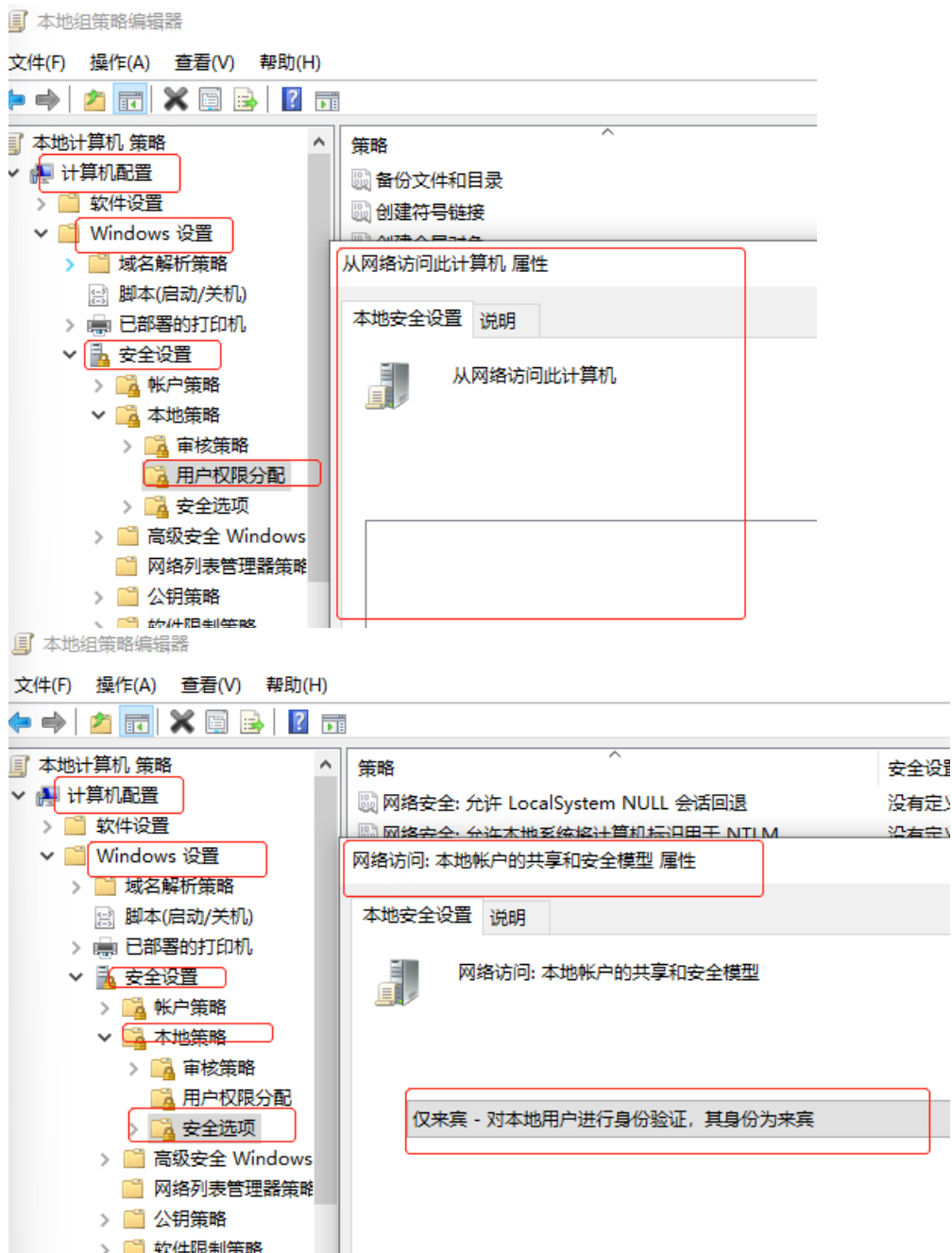
NetBIOS 设置

☐ 默认(F):
从 DHCP 服务器使用 NetBIOS 设置。如果使用静态 IP 地址或 DHCP 服务器不提供 NetBIOS 设置，则启用 TCP/IP 上的 NetBIOS。

☐ 启用 TCP/IP 上的 NetBIOS(N)

☒ 禁用 TCP/IP 上的 NetBIOS(S)

如下组策略设置：



另外，需要提醒的是，从以往经验，SMB 文件共享访问受网络环境，访问端及被访问端的操作系统版本，用户权限设置等影响，效果不同。因此需要具体问题具体分析，如设置后仍未达成您的需求，请结合实际情形向我们提交案例以具体分析，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055

电子邮箱 Email: liqi@cmgos.com



发件人: win10 技术支持 <win10sup@cdc.icbc.com.cn>

发送时间: 2022 年 9 月 26 日 10:29

收件人: Li Qi <liqi@cmgos.com>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: 回复: 【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2||CBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

FTP 关了 21 端口后还是可以访问, 请问还有别的方法么, 网络共享关了后还是可以在网络上发现共享文件。

高级安全 Windows 防火墙

文件(F) 操作(A) 查看(V) 帮助(H)



本地计算机上的高级安全 Windows 防火墙

入站规则

出站规则

连接安全规则

监视

入站规则

名称	组	配置文件
360ent.exe		域
360ent.exe		域
AsiaInfo OfficeScan Listener		所有
Control Center		域
Control Center		域
Control Center UDP Port		域
desktop cloud tcp		所有
desktop cloud tcp 28511		专用
desktop cloud tcp 28511		域
desktop cloud tcp 28512		域
desktop cloud tcp 28512		专用
desktop cloud tcp 28521		域
desktop cloud tcp 28521		专用
desktop cloud tcp 28522		专用
desktop cloud tcp 28522		域
desktop cloud udp		所有
desktop cloud udp 28511		专用
desktop cloud udp 28511		域
desktop cloud udp 28512		域
desktop cloud udp 28512		专用
desktop cloud udp 6020		专用
desktop cloud udp 6020		域
desktop cloud udp 6021		域
desktop cloud udp 6021		专用
desktop cloud udp 6040		专用
desktop cloud udp 6040		域
desktop cloud udp 6041		专用
desktop cloud udp 6041		域
FTP端口		所有
ICMP Allow incoming V4 echo request		所有
ICMP Allow incoming V4 echo request		所有
ICMP Allow incoming V4 echo request		所有
ICMP Allow incoming V4 echo request		所有
ICMP Allow incoming V4 echo request		所有
scclient		所有
scclient64		所有
sccltui		所有
scupclt		所有
Sogou Pinyin Service		专用
Soqou Pinyin Service		专用

高级安全 Windows 防火墙

文件(F) 操作(A) 查看(V) 帮助(H)



本地计算机上的高级安全 Windows 防火墙

入站规则

出站规则

连接安全规则

监视

出站规则

名称	组	配置文件
FTP端口		所有
scclient		所有
scclient64		所有
sccltui		所有
scupclt		所有
Svctrl		所有
BranchCache 对等机发现(WSD-Out)	BranchCache - 对等机发现...	所有
BranchCache 内容检索(HTTP-Out)	BranchCache - 内容检索(...	所有
BranchCache 托管缓存服务器(HTTP-O...	BranchCache - 托管缓存服...	所有
BranchCache 托管缓存客户端(HTTP-O...	BranchCache - 托管缓存客...	所有
iSCSI 服务(TCP-Out)	iSCSI 服务	域
iSCSI 服务(TCP-Out)	iSCSI 服务	专用, 公用
Media Center Extender - qWave (TCP...	Media Center Extender	所有
Media Center Extender - qWave (UD...	Media Center Extender	所有
Media Center Extender - RTSP (TCP-...	Media Center Extender	所有
Media Center Extender - SSDP (UDP-...	Media Center Extender	所有
Media Center Extender - UPnP (TCP-...	Media Center Extender	所有
Media Center Extender - WMDRM-N...	Media Center Extender	所有
Media Center Extender - 服务(TCP-O...	Media Center Extender	所有
Media Center Extender - 媒体流(TCP-...	Media Center Extender	所有
Media Center Extender - 媒体流(UDP-...	Media Center Extender	所有
Media Center Extender - 设备配置(TC...	Media Center Extender	所有
Media Center Extender - 设备验证(TC...	Media Center Extender	所有
Windows Management Instrumentati...	Windows Management In...	域
Windows Management Instrumentati...	Windows Management In...	专用, 公用
Windows Media Player (TCP-Out)	Windows Media Player	所有
Windows Media Player (UDP-Out)	Windows Media Player	所有
Windows Media Player x86 (TCP-Out)	Windows Media Player	所有
Windows Media Player x86 (UDP-Out)	Windows Media Player	所有
Windows Media Player 网络共享服务(...	Windows Media Player 网...	专用, 公用
Windows Media Player 网络共享服务(...	Windows Media Player 网...	域
Windows Media Player 网络共享服务(...	Windows Media Player 网...	域
Windows Media Player 网络共享服务(...	Windows Media Player 网...	专用, 公用
Windows Media Player 网络共享服务(...	Windows Media Player 网...	域
Windows Media Player 网络共享服务(...	Windows Media Player 网...	专用, 公用
Windows Media Player 网络共享服务(...	Windows Media Player 网...	域
Windows Media Player 网络共享服务(...	Windows Media Player 网...	所有
Windows Media Player 网络共享服务(...	Windows Media Player 网...	专用, 公用
Windows Media Player 网络共享服务(...	Windows Media Player 网...	域
Windows Media Player 网络共享服务(...	Windows Media Player 网...	专用, 公用
Windows Media Player 网络共享服务(...	Windows Media Player 网...	域

C:\Windows\system32\cmd.exe - ftp 122.21.29.21

122.21.29.21 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间<以毫秒为单位>:
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\kfzx-hjwh2>ftp 122.21.29.21

连接到 122.21.29.21。

220

220-ATTENTION:Please quit if maintainancing this system isnot
220-Your duty,thank you!

220-警告:本计算机系统,包括网络及数据,只有经过本系统所有者授
220-权的人员和程序才能访问。任何其他方式的访问是被禁止的并且
220-是违反相关法律法规规定的,如果你是非授权用户,请不要继续进行
220-操作。任何非授权的访问将被记录下来并作为法律起诉的一部分!

220

220

用户<122.21.29.21:(none)>: 登录失败。

^C

C:\Users\kfzx-hjwh2>

C:\Users\kfzx-hjwh2>ftp 122.21.29.21

连接到 122.21.29.21。

220

220-ATTENTION:Please quit if maintainancing this system isnot
220-Your duty,thank you!

220-警告:本计算机系统,包括网络及数据,只有经过本系统所有者授
220-权的人员和程序才能访问。任何其他方式的访问是被禁止的并且
220-是违反相关法律法规规定的,如果你是非授权用户,请不要继续进行
220-操作。任何非授权的访问将被记录下来并作为法律起诉的一部分!

220

220

用户<122.21.29.21:(none)>: ^Z登录失败。

^C

C:\Users\kfzx-hjwh2>

C:\Users\kfzx-hjwh2>ftp 122.21.29.21

连接到 122.21.29.21。

220

220-ATTENTION:Please quit if maintainancing this system isnot
220-Your duty,thank you!

220-警告:本计算机系统,包括网络及数据,只有经过本系统所有者授
220-权的人员和程序才能访问。任何其他方式的访问是被禁止的并且
220-是违反相关法律法规规定的,如果你是非授权用户,请不要继续进行
220-操作。任何非授权的访问将被记录下来并作为法律起诉的一部分!

220

220

用户<122.21.29.21:(none)>:

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心(珠海)

许翔

系统一部

电话: 17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人: "Li Qi" <liqi@cmgos.com>

发送时间: 2022-09-23 11:25:08

收件人: "Windows Server 技术支持" <[windowsserver 技术支持.软件开发中心系统一部@工商银行.icbc](mailto:windowsserver技术支持.软件开发中心系统一部@工商银行.icbc)>

抄送: "ICBC_Notification" <icbc_notification@cmgos.com>

主题: 回复:【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2|ICBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

许先生, 您好:

请将附件注册表键值导入系统中可禁用 mstsc 应用, 您可以尝试一下, 是否满足您的需求, 有问题可随时和我联系, 谢谢。

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co.,Ltd.

服务支持电话: 4008180055

电子邮箱 Email: liqi@cmgos.com



神州网信
C M I T

发件人: Li Qi

发送时间: 2022 年 9 月 23 日 9:47

收件人: 'Windows Server 技术支持' <windowsserversupport@sdic.icbc.com.cn>

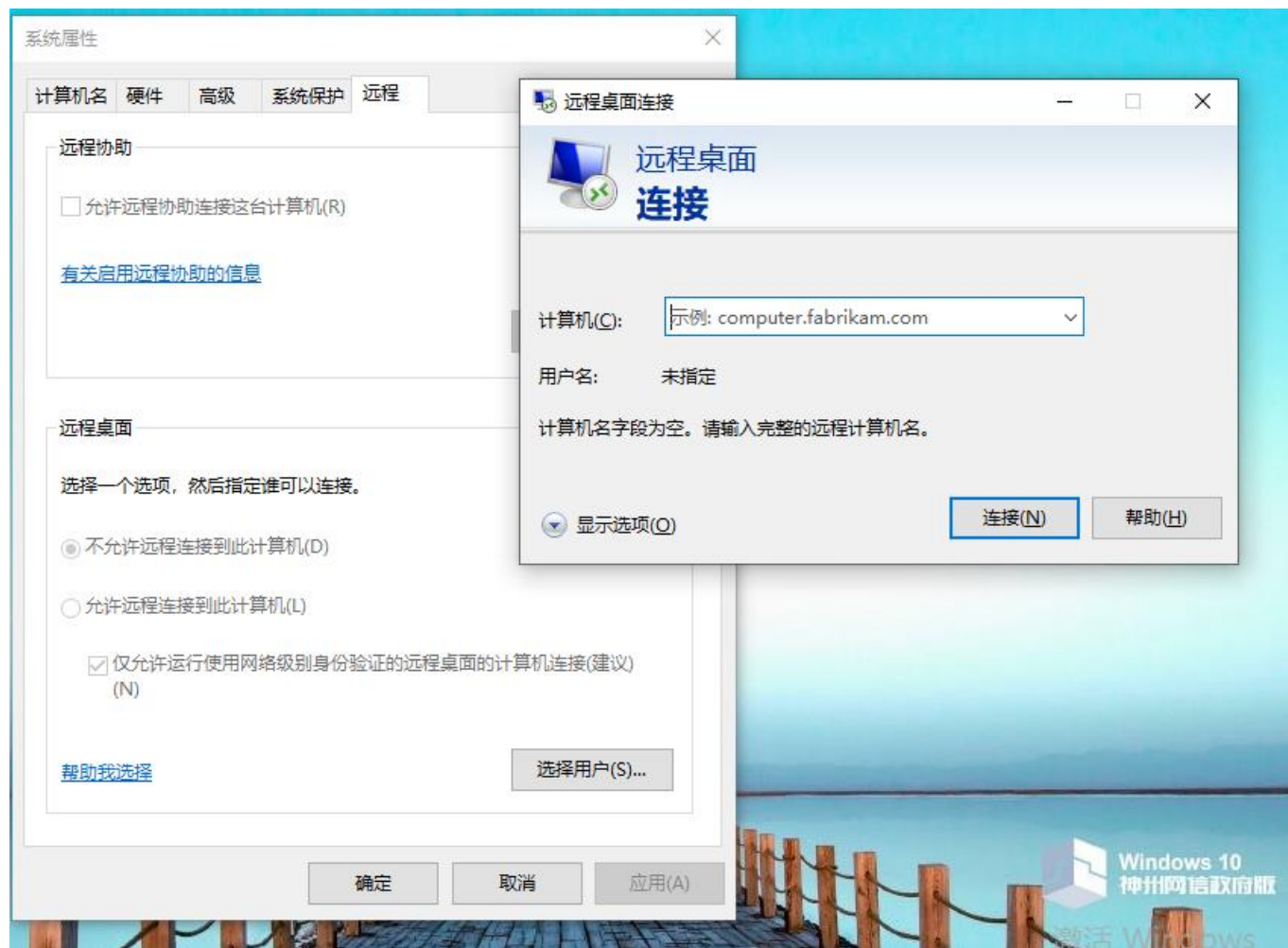
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: 【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2|ICBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

许先生, 您好:

请问附件邮件的步骤是否操作?

请您提供您的组策略设置截图, 另外您希望实现的效果是其他人无法远程桌面连接这台计算机? 还是这台计算机单纯无法运行“远程桌面连接”这个应用呢? 我的本地测试是如下图的, 不允许他人连接此计算机, 但本机可以正常运行“远程桌面连接”这个程序。



李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话: 4008180055
电子邮箱 Email: liqi@cmgos.com



神州网信
C M I T

发件人: Windows Server 技术支持 <windowsserversupport@sdicbc.com.cn>
发送时间: 2022 年 9 月 23 日 9:00
收件人: Li Qi <liqi@cmgos.com>
抄送: Li Qi <liqi@cmgos.com>
主题: 回复: 【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2|ICBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

在组策略中加入不可运行的程序 mstsc.exe 后还是可以打开远程连接工具。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心 (珠海)

许 翔

系统一部

电话: 17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人: "Li Qi" <liqi@cmgos.com>
发送时间: 2022-09-22 15:52:23
收件人: "Windows Server 技术支持" <[windowsserver 技术支持.软件开发中心系统一部@工商银行.icbc](mailto:windowsserver技术支持.软件开发中心系统一部@工商银行.icbc)>
抄送: "Li Qi" <liqi@cmgos.com>
主题: 【外来邮件, 注意核实】[案例号: CAS-07184-W0V1P6] % |P2|ICBC|工行用户反馈无法关闭本地 MSTSC 问题 % 初次响应 CMIT:0001158

许翔 先生/女士, 您好!

感谢您联系神州网信技术支持中心。我是技术支持工程师 李琦 。很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-07184-W0V1P6 与我联系。

如果您有任何其他疑问, 请随时与我联系。

此致,

敬礼

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中,您可以选择“全部回复”。

—

此邮件信息仅供收件人查阅, 所含任何评论、陈述或数据仅供收件人参考, 若有改动, 恕可能不另行通知。未经中国工商银行书面许可, 请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件, 敬请及时通知发件人, 并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.

—

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.