

邮件流配置

1、发送连接器配置

常规的发送连接器配置会分两种情况，一是扔给公网，二是扔给邮件网关（目前各种垃圾邮件盛行，在预算允许的情况下选择第二种方式）。

本次实验环境，是由2台邮箱角色服务器(ex01、ex02)+1台边缘传输服务器(edge)组成，边缘传输订阅成功后，会自动生成出站和入站两条传输策略。

如有第三方独立邮件网关，可以通过以下步骤添加；如使用边缘传输，以下步骤略过。



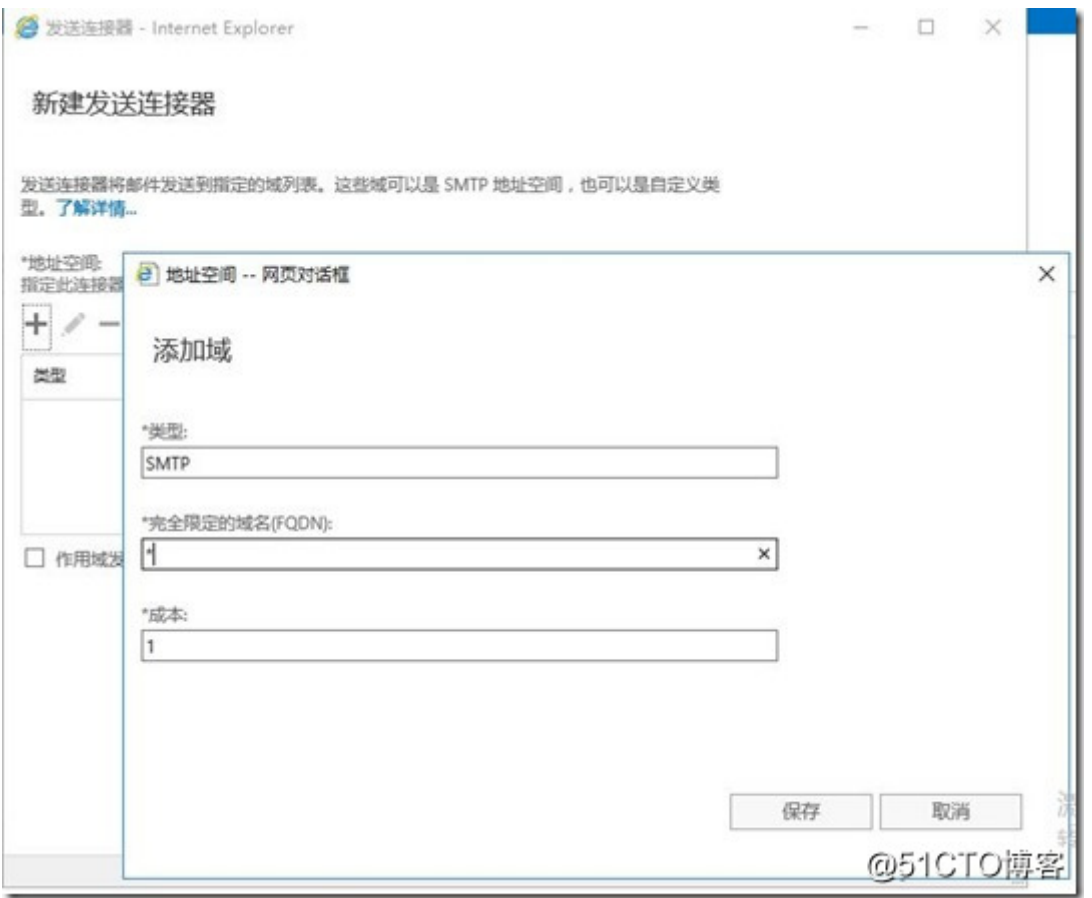
新建发送连接器，定义名称

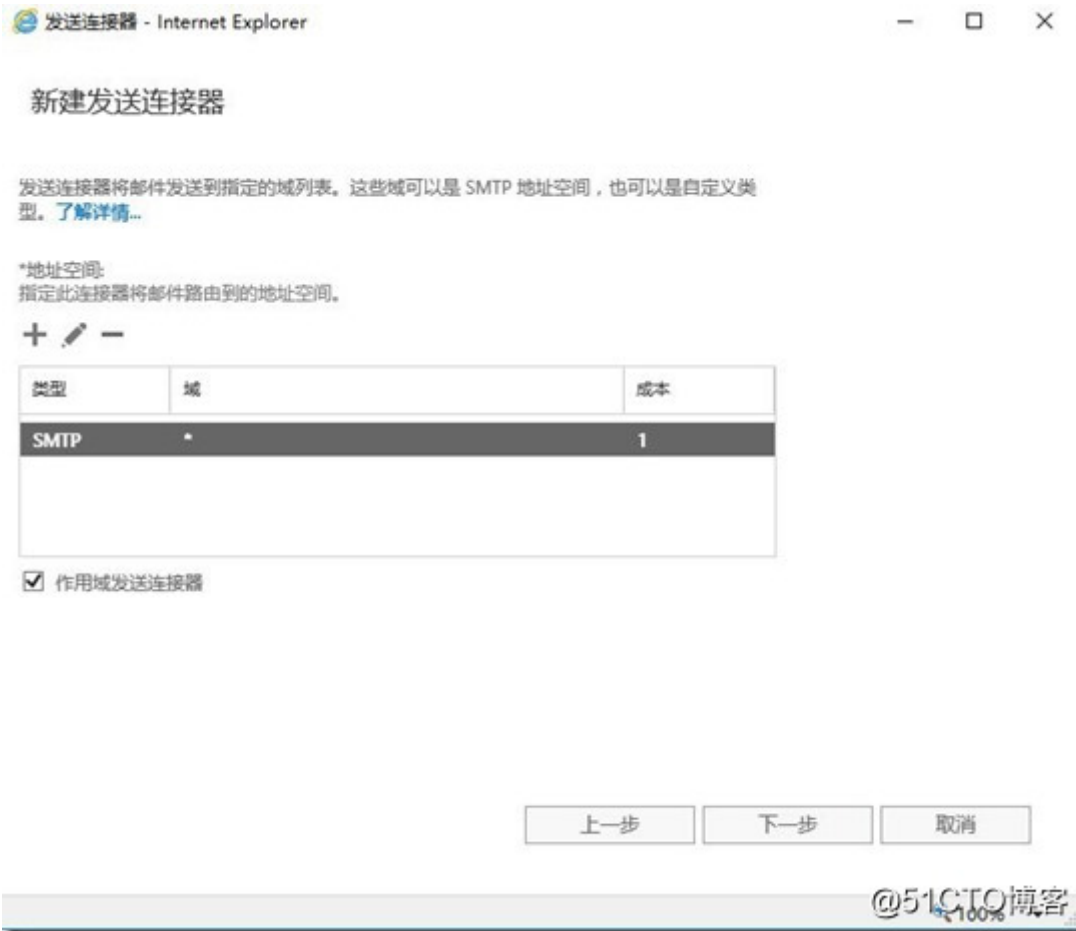


通过DNS路由，解析收件人关联的MX记录；或添加邮件网关。

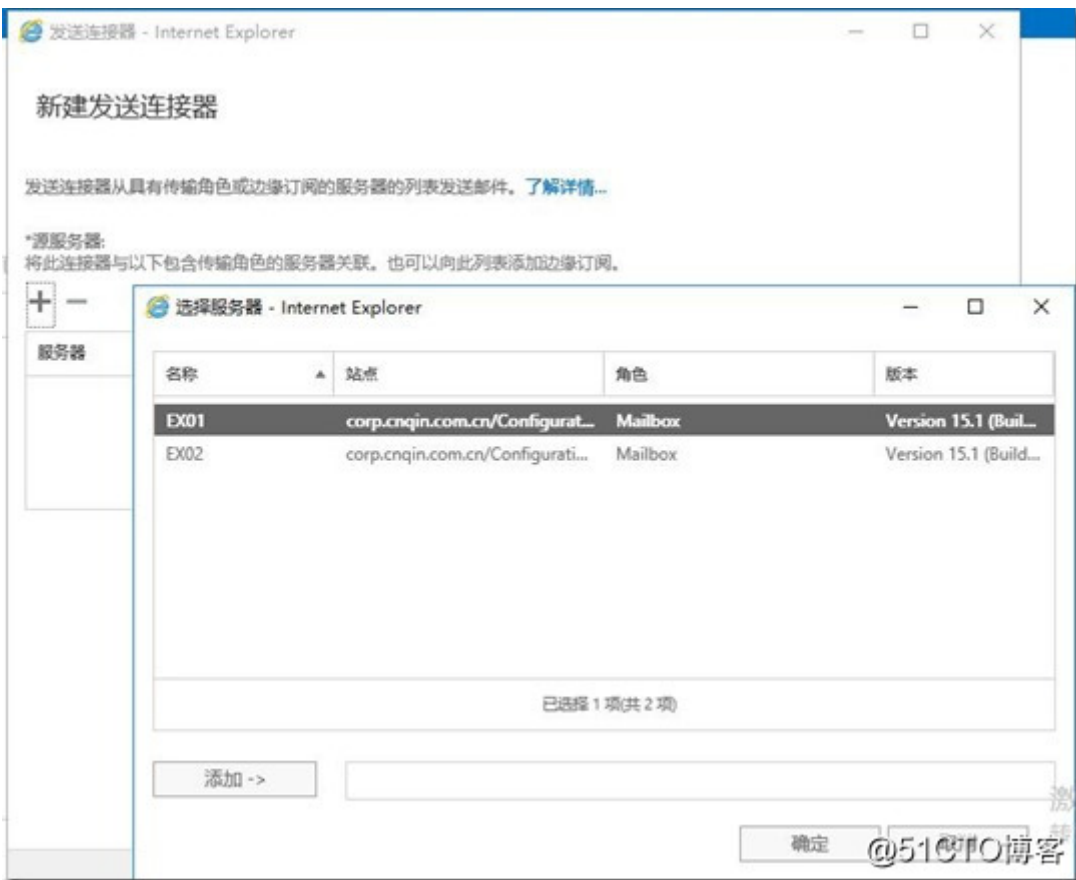


新建地址空间，类型为SMTP，FQDN为*，成本为1





选择添加源服务器





发送连接器配置完成



2、接收连接器配置

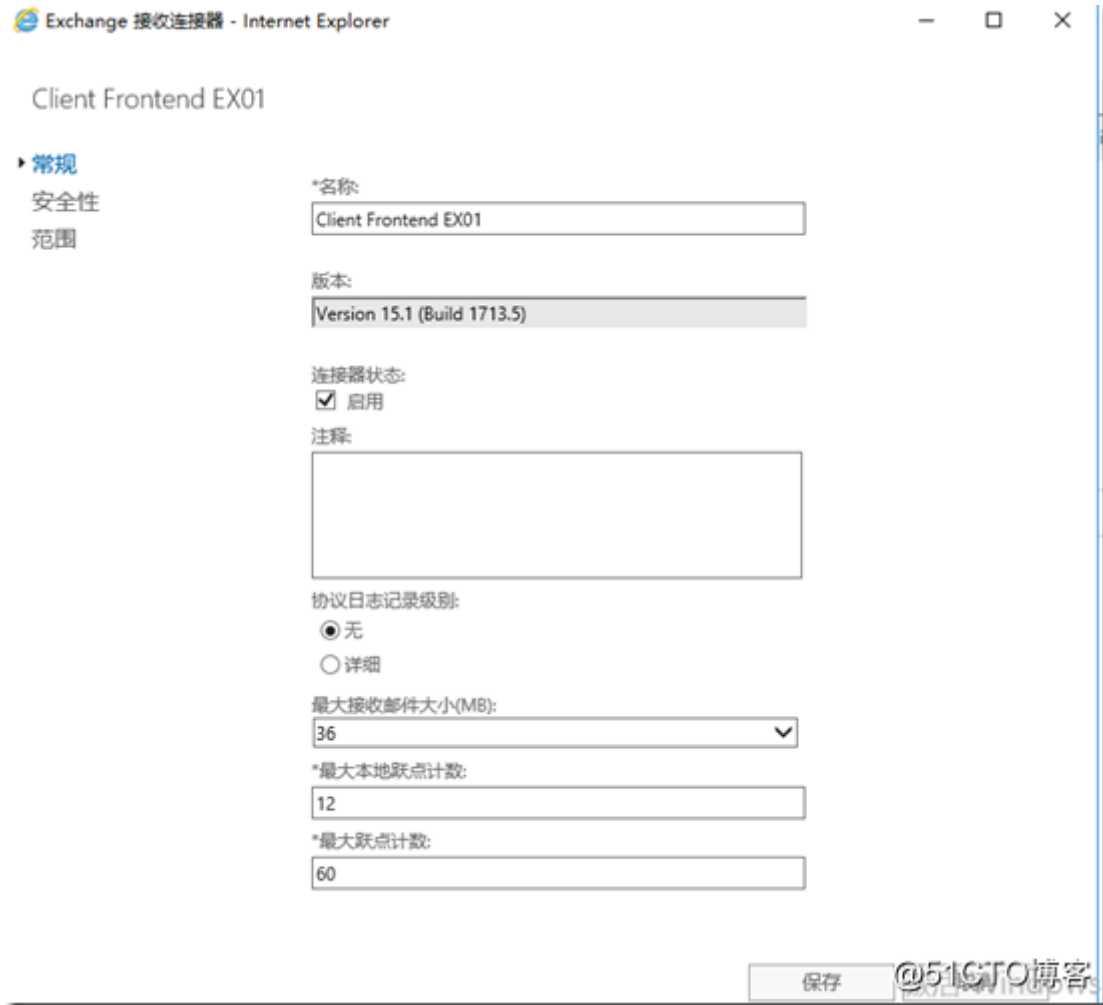
接收连接器默认有5条策略，分属2种角色，

前端传输 (FrontendTransport) : Client Frontend EX01、Default Frontend EX01、Outbound Proxy Frontend EX01;

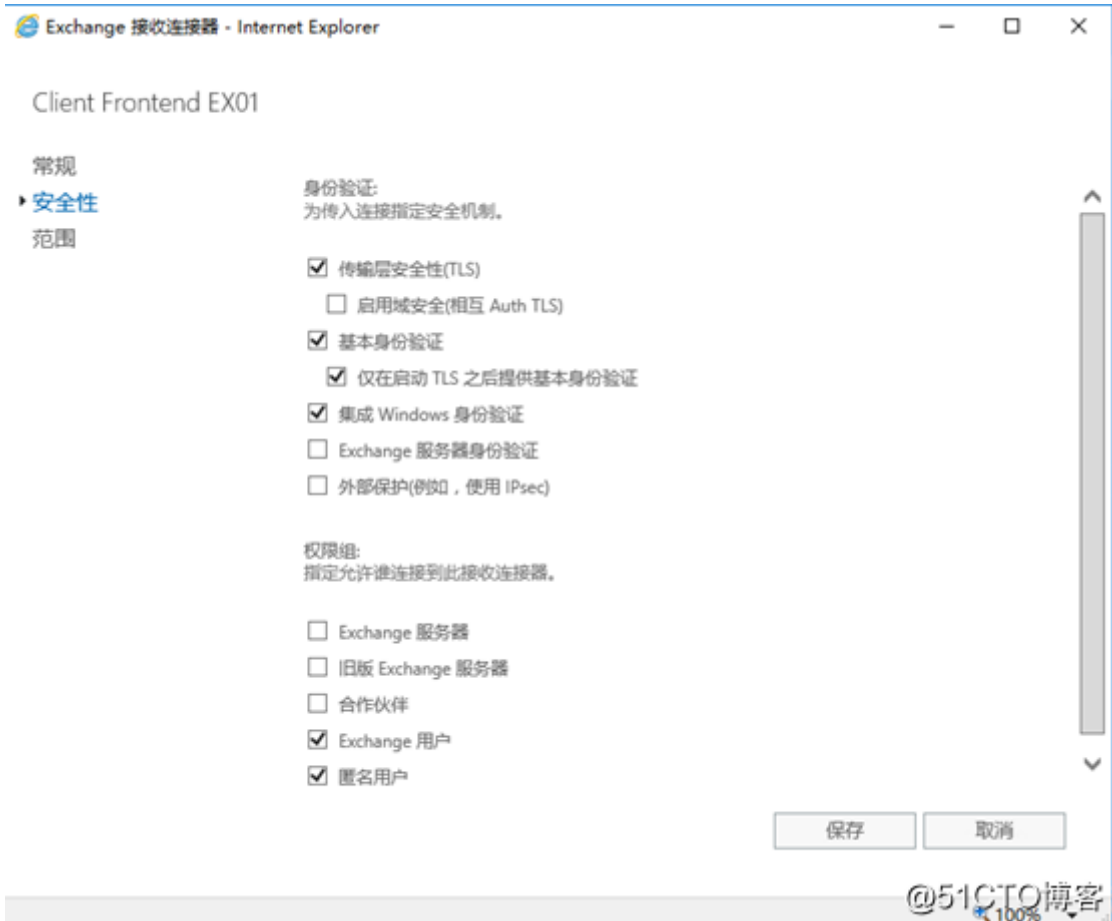
集线器传输 (HubTransport) : Client Proxy EX01、Default EX01;

本次实验环境使用默认策略。

Client Frontend EX01, 角色FrontendTransport



允许匿名

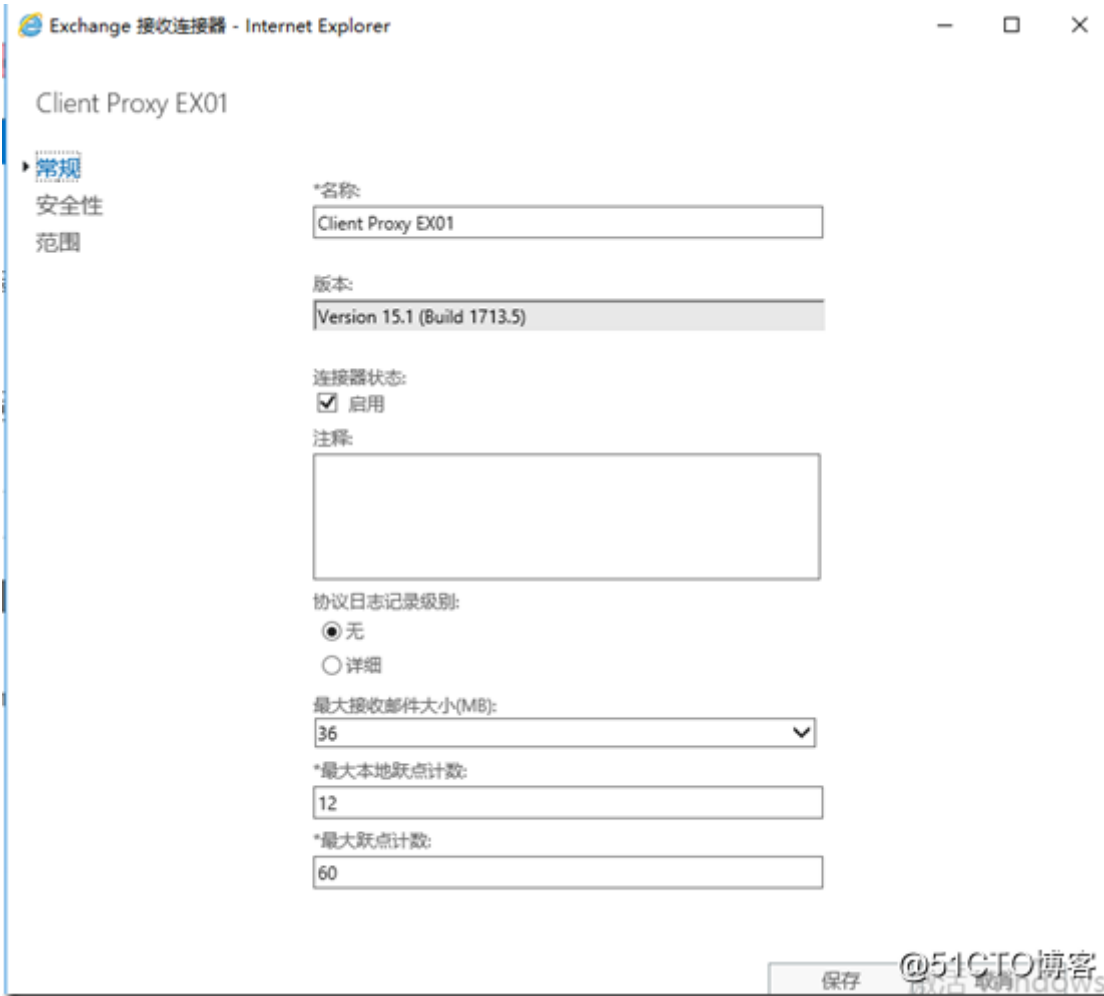


接收来自边缘传输服务器的邮件



其他4条策略默认。

Client Proxy EX01, 角色HubTransport



Exchange 接收连接器 - Internet Explorer

Client Proxy EX01

常规
安全性
范围

*远程网络设置:
接收来自具有下列远程 IP 地址的服务器的邮件。

+ -

IP 地址
0.0.0.0-255.255.255.255

*网络适配器绑定:
指定要绑定到接收连接器的网络适配器的 IP 地址和端口。

+ -

IP 地址	端口
(所有可用 IPv6)	465
(所有可用 IPv4)	465

FQDN:
指定此连接器将为响应 HELO 或 EHLO 提供的 FQDN。

EX01.corp.cnqin.com.cn

保存 @51CTO博客

Default EX01, 角色HubTransport

Exchange 接收连接器 - Internet Explorer

Default EX01

常规
安全性
范围

*名称:
Default EX01

版本:
Version 15.1 (Build 1713.5)

连接器状态:
 启用

注释:

协议日志记录级别:
 无
 详细

最大接收邮件大小(MB):
36

*最大本地跃点计数:
12

*最大跃点计数:
60

保存 @51CTO博客



Default Frontend EX01, 角色FrontendTransport

Exchange 接收连接器 - Internet Explorer

Default Frontend EX01

- 常规
- 安全性**
- 范围

*名称: Default Frontend EX01

版本: Version 15.1 (Build 1713.5)

连接器状态: 启用

注释:

协议日志记录级别:
 无
 详细

最大接收邮件大小(MB): 36

*最大本地跃点计数: 12

*最大跃点计数: 60

激溘存Vii@51GTO博客

Exchange 接收连接器 - Internet Explorer

Default Frontend EX01

- 常规
- 安全性**
- 范围

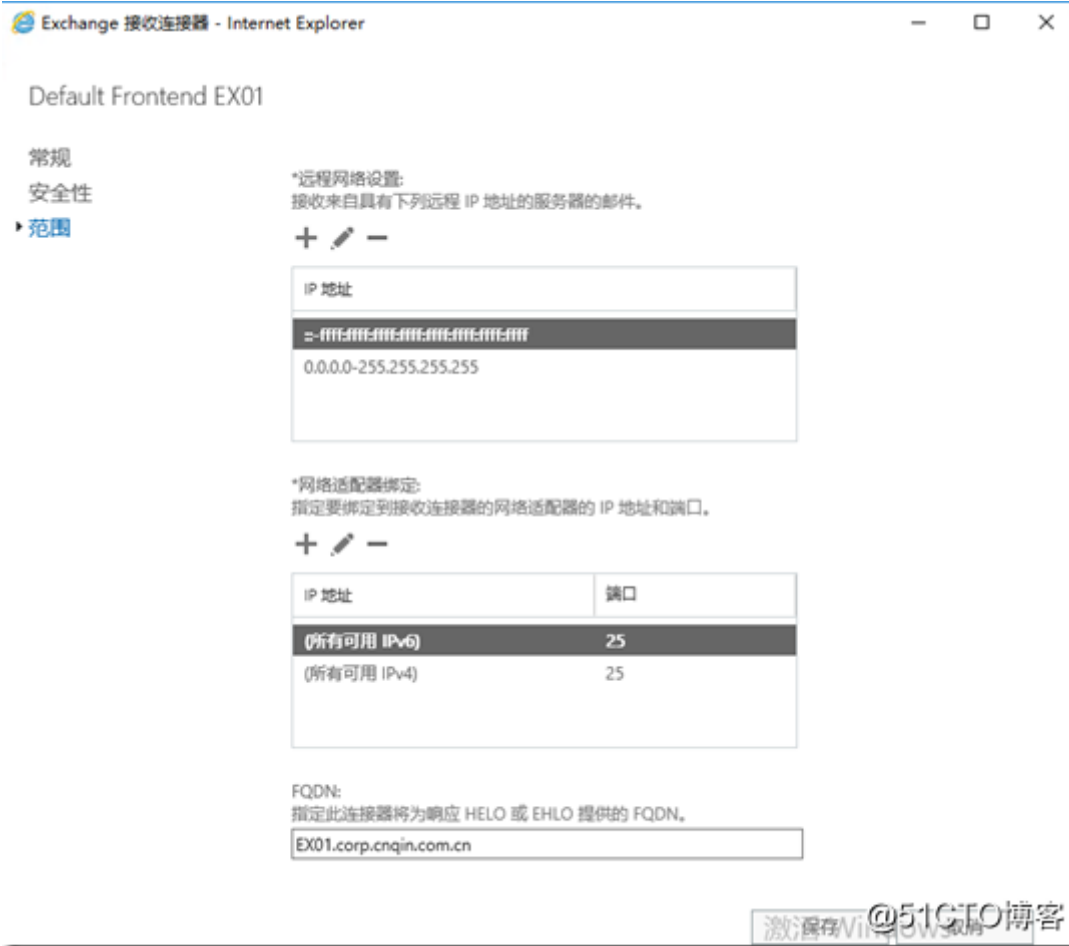
身份验证:
为传入连接指定安全机制。

- 传输层安全性(TLS)
 - 启用域安全(相互 Auth TLS)
- 基本身份验证
 - 仅在启动 TLS 之后提供基本身份验证
- 集成 Windows 身份验证
- Exchange 服务器身份验证
- 外部保护(例如, 使用 IPsec)

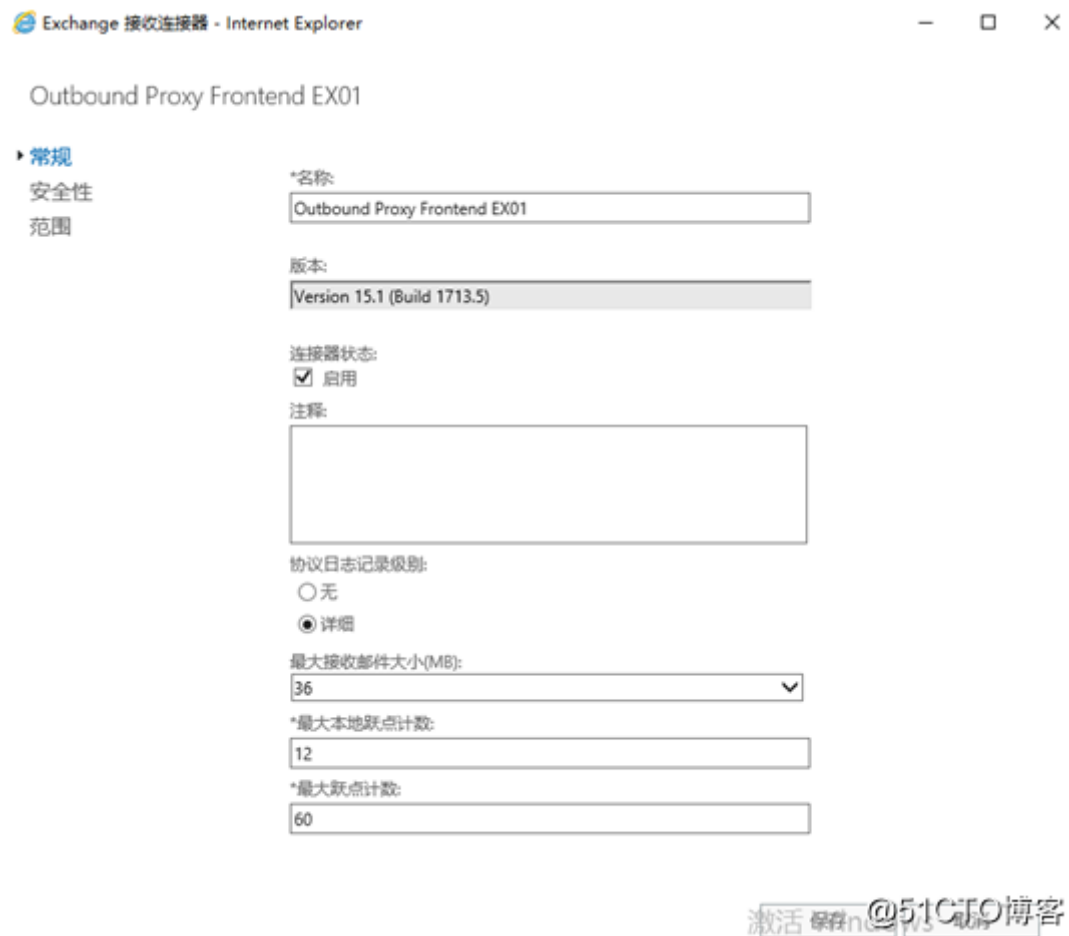
权限组:
指定允许谁连接到此接收连接器。

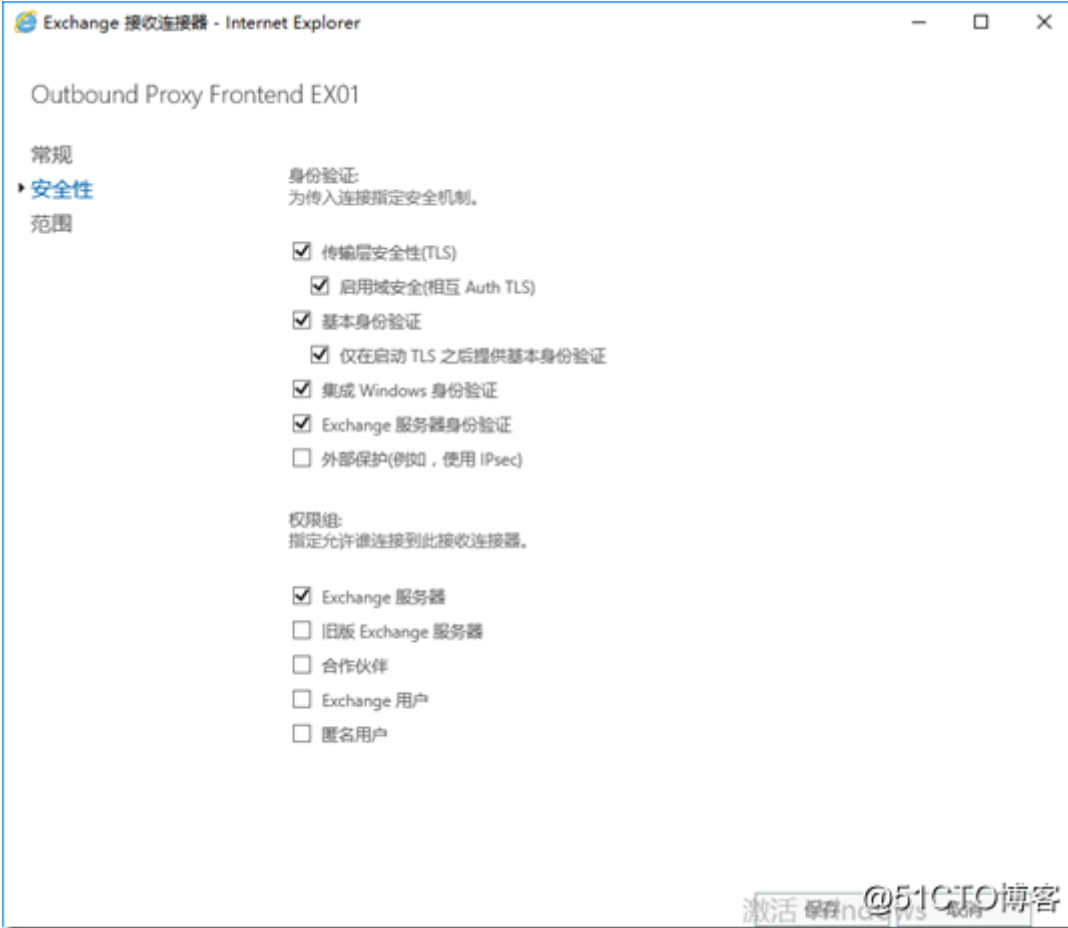
- Exchange 服务器
- 旧版 Exchange 服务器
- 合作伙伴
- Exchange 用户
- 匿名用户

激溘存Vii@51GTO博客



Outbound Proxy Frontend EX01, 角色FrontendTransport





3、订阅配置

登陆EDGE服务器, 打开EMS, 输入

[PS] C:\Windows\system32>New-EdgeSubscription -FileName C:\EdgeServerSubscription.xml

```
[PS] C:\Windows\system32>New-EdgeSubscription -FileName "c:\EdgeServerSubscription.xml"
确认
如果您创建边缘订阅,就可以通过 EdgeSync 复制来管理此边缘传输服务器。如此一来,系统将会删除以下任何手动创建的对象:
接受域、邮件分类、远程域和发送连接器。在创建边缘订阅后,您必须从组织内部管理这些对象,并且允许 EdgeSync
更新该边缘传输服务器。而且,在同步过程中,TransportConfig 对象的 InternalSMTPServers 列表将被覆盖。
EdgeSync 要求此边缘传输服务器能够解析订阅边缘传输服务器的 Active Directory 站点内部箱服务器的 FQDN。而这些邮箱服务器也必须能够解析此边缘传输服务器的
FQDN。您应该在启动帐户过期之前的“1440”分钟内,完成组织内的边缘订阅。
[Y] 是(Y) [A] 全是(A) [N] 否(N) [L] 全否(L) [S] 暂停(S) [?] 帮助 (默认值为“Y”): y
[PS] C:\Windows\system32>
```

@51CTO博客

生成订阅文件

[PS] C:\Windows\system32>New-EdgeSubscription -FileName "c:\EdgeServerSubscription.xml"

确认
如果您创建边缘订阅,就可以通过 EdgeSync 复制来管理此边缘传输服务器。如此一来,系统将会删除以下任何手动创建的对象:
接受域、邮件分类、远程域和发送连接器。在创建边缘订阅后,您必须从组织内部管理这些对象,并且允许 EdgeSync
更新该边缘传输服务器。而且,在同步过程中,TransportConfig 对象的 InternalSMTPServers 列表将被覆盖。
EdgeSync 要求此边缘传输服务器能够解析订阅边缘传输服务器的 Active Directory 站点内部箱服务器的 FQDN。而这些邮箱服务器也必须能够解析此边缘传输服务器的
FQDN。您应该在启动帐户过期之前的“1440”分钟内,完成组织内的边缘订阅。
[Y] 是(Y) [A] 全是(A) [N] 否(N) [L] 全否(L) [S] 暂停(S) [?] 帮助 (默认值为“Y”): y
[PS] C:\Windows\system32>

名称	修改日期	类型	大小
ExchangeSetupLogs	2019/6/14 11:47	文件夹	
inetpub	2019/6/14 10:31	文件夹	
PerfLogs	2019/6/6 16:59	文件夹	
Program Files	2019/6/14 11:47	文件夹	
Program Files (x86)	2016/7/16 21:23	文件夹	
Windows	2019/7/2 17:52	文件夹	
用户	2019/6/14 10:31	文件夹	
BitlockerActiveMonitoringLogs	2019/7/3 9:51	文件	1 KB
EdgeServerSubscription	2019/7/3 16:53	XML 文档	3 KB

@51CTO博客

拷贝订阅文件至邮箱角色服务器

192.168.20.233 - 远程桌面连接

名称	修改日期	类型	大小
ClusterStorage	2019/7/16 17:52	文件夹	
ExchangeSetupLogs	2019/7/2 9:58	文件夹	
inetpub	2019/6/13 9:29	文件夹	
PerfLogs	2019/6/6 14:53	文件夹	
Program Files	2019/6/13 18:13	文件夹	
Program Files (x86)	2016/7/16 21:23	文件夹	
root	2019/6/13 17:30	文件夹	
Windows	2019/7/16 17:50	文件夹	
用户	2019/6/13 9:28	文件夹	
BitlockerActiveMonitoringLogs	2019/7/16 18:33	文件	1 KB
EdgeServerSubscription.xml	2019/7/3 16:53	XML 文档	

@51CTO博客

在EX01上导入订阅文件,提示邮箱角色服务器能够解析到EDGE服务器和50636端口。

```
[PS] C:\Windows\system32>New-EdgeSubscription -FileData ([byte[]](Get-Content -Path "c:\EdgeServerSubscription.xml" -Encoding Byte -ReadCount 0)) -Site "Default-First-Site-Name"
```

Name	Site	Domain
EDGE	corp.cnqin.com.cn..	corp.cnqin.com.cn

警告: EdgeSync 要求 Active Directory 站点 Default-First-Site-Name 中的邮箱服务器能够解析 EDGE.corp.cnqin.com.cn 的 IP 地址, 并且能够在端口 50636 连接到该主机。

```
[PS] C:\Windows\system32>
```

@51CTO博客

在ex01 telnet edge服务器50636端口

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\administrator.CORP>telnet edge.corp.cnqin.com.cn 50636
```

@51CTO博客

```
Telnet edge.corp.cnqin.com.cn
```

@51CTO博客

邮箱角色服务器-发送连接器, 自动生成两条入站及出站策略

The screenshot shows the Exchange Management Center interface. On the left is a navigation pane with categories like '收件人', '权限', '合规性管理', '组织', '保护', '邮件流', '移动', '公用文件夹', '统一消息', '服务器', and '混合'. The main area is titled 'Exchange 管理中心' and contains tabs for '规则', '送达报告', '接受的域', '电子邮件地址策略', '接收连接器', and '发送连接器'. The '发送连接器' tab is active, showing a table of connectors:

名称	状态
EdgeSync - Default-First-Site-Name to Internet	已启用
EdgeSync - Inbound to Default-First-Site-Name	已启用
Mail To MG	已禁用

Red arrows point from the table to explanatory text:

- An arrow points to the first connector with the text: 出站: 从 Exchange 组织向 Internet 中继邮件的发送连接器
- An arrow points to the second connector with the text: 入站: 从边缘传输服务器向 Exchange 组织中继邮件的发送连接器

 On the right side of the interface, there is a detailed view for the selected connector, showing details like '上次修改时间: 2019/7/4 9:11:49', '连接器状态 - 已启用', '禁用', '日志记录 - 关闭', '打开', and '最大发送邮件大小(MB): 10'.

激活 Wi-Fi @51CTO博客

启用edge订阅

```
[PS] C:\Windows\system32>Start-EdgeSynchronization
```

```
RunspaceId      : 46541136-08ac-44fe-82a5-c5467f098cd2
Result          : Success
Type           : Recipients
Name           : EDGE
FailureDetails  :
StartUTC       : 2019/7/4 1:18:21
EndUTC         : 2019/7/4 1:18:21
Added          : 0
Deleted        : 0
Updated        : 0
Scanned        : 0
TargetScanned  : 0
```

```
RunspaceId      : 46541136-08ac-44fe-82a5-c5467f098cd2
Result          : Success
Type           : Configuration
Name           : EDGE
FailureDetails  :
StartUTC       : 2019/7/4 1:18:21
EndUTC         : 2019/7/4 1:18:21
Added          : 0
Deleted        : 0
Updated        : 0
Scanned        : 0
TargetScanned  : 0
```

```
[PS] C:\Windows\system32>_
```

@51CTO博客

测试edge订阅

```
[PS] C:\Windows\system32>Test-EdgeSynchronization
```

```
RunspaceId      : 46541136-08ac-44fe-82a5-c5467f098cd2
SyncStatus      : Normal
UtcNow          : 2019/7/4 1:20:01
Name            : EDGE
LeaseHolder     : CN=EX01,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=cnqin,CN=Microsoft Exchange,
                  CN=Services,CN=Configuration,DC=corp,DC=cnqin,DC=com,DC=cn
LeaseType       : Option
FailureDetail    :
LeaseExpiryUtc  : 2019/7/4 1:48:21
LastSynchronizedUtc : 2019/7/4 1:18:21
TransportServerStatus : Skipped
TransportConfigStatus : Skipped
AcceptedDomainStatus : Skipped
RemoteDomainStatus : Skipped
SendConnectorStatus : Skipped
MessageClassificationStatus : Skipped
RecipientStatus  : Skipped
CredentialRecords : Number of credentials 6
CookieRecords    : Number of cookies 2
```

激活 Windows

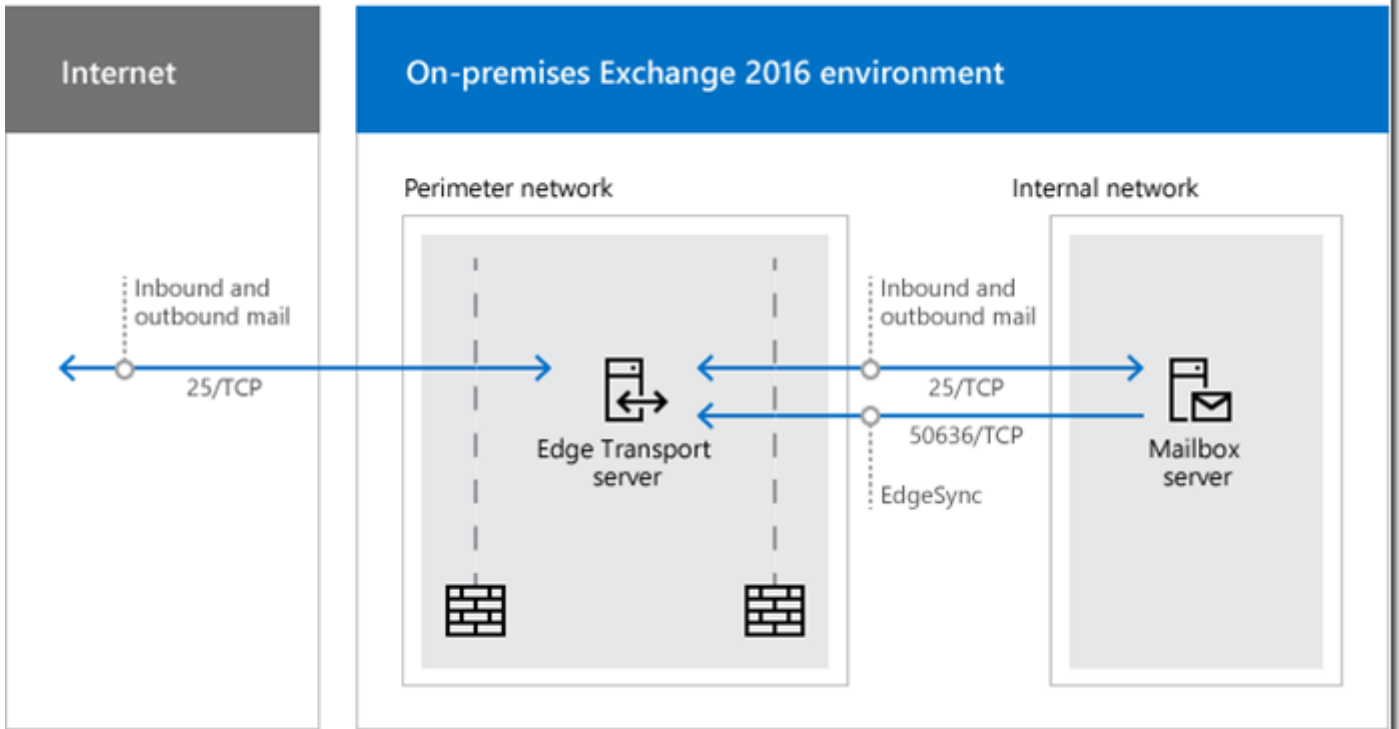
转到“设置”以激活 Windows。

@51CTO博客

```
[PS] C:\Windows\system32>
```

4、映射及解析配置

官方关于exchange2016所需的端口说明



@51CTO博客

用途	端口	源	目标	注释
入站邮件 - 从 Internet 到边缘传输服务器	25/TCP (SMTP)	Internet (任何)	边缘传输服务器	边缘传输服务器上名为“默认内部接收连接器_<边缘传输服务器>名称”的默认接收连接器会侦听端口25上的匿名 SMTP 邮件。
入站邮件 - 从边缘传输服务器到内部 Exchange 组织	25/TCP (SMTP)	边缘传输服务器	订阅的 Active Directory 站点中的邮箱服务器	名为“EdgeSync-入站到_<Active directory 站点名称>”的默认发送连接器会将端口25上的入站邮件中继到订阅的 Active Directory 站点中的任何邮箱服务器。有关详细信息,请参阅由边缘订阅自动创建的发送连接器。邮箱服务器上的前端传输服务中名为“默认前端_<邮箱服务器名称>_”的默认接收连接器会侦听所有入站邮件(包括来自 Exchange 2013 或更高版本传输服务器的邮件)端口25。
出站邮件 - 从内部 Exchange 组织到边缘传输服务器	25/TCP (SMTP)	订阅的 Active Directory 站点中的邮箱服务器	边缘传输服务器	出站邮件将始终通过邮箱服务器上的前端传输服务。邮件将从订阅的 Active Directory 站点中的任何邮箱服务器上的传输服务中继到边缘传输服务器,使用隐式和不可见的组织内部发送连接器,该连接器会自动在中 Exchange 服务器之间路由邮件。相同的组织。边缘传输服务器上名为“默认内部接收连接器_<边缘传输服务器>名称”的默认接收连接器会在已订阅的任何邮箱服务器上的传输服务中侦听端口25上的 SMTP 邮件。Active Directory 站点。
出站邮件-边缘传输服务器到 internet	25/TCP (SMTP)	边缘传输服务器	Internet (任何)	名为“EdgeSync- _<Active Directory 站点名称> _到 internet”的默认发送连接器会将端口25上的出站邮件从边缘传输服务器中继到 internet。
EdgeSync 同步	50636/TCP (安全 LDAP)	订阅的 Active Directory 站点中参与 EdgeSync 同步的邮箱服务器	边缘传输服务器	将边缘传输服务器订阅到 Active Directory 站点时,该站点中的所有邮箱服务器_参与 EdgeSync 同步时都存在。但是,稍后添加的任何邮箱服务器都不会自动_参与 EdgeSync 同步。
用于下一个邮件跃点的名称解析的 DNS (未显示在图中)	53/UDP、53/TCP (DNS)	边缘传输服务器	DNS 服务器	请参阅本主题后面的名称解析部分。
在发件人信誉中开放代理服务器检测 (不是图示)	请参阅注释	边缘传输服务器	Internet	默认情况下,发件人信誉(协议分析代理)将开放代理服务器检测作为用于计算源邮件服务器的发件人信誉级别(SRL)的条件之一。有关详细信息,请参阅发件人信誉和协议分析代理。开放代理服务器检测使用以下协议和 TCP 端口测试开放代理的源邮件服务器: <ul style="list-style-type: none"> • SOCKS4, SOCKS5: 1081, 1080 • Wingate, Telnet, Cisco:23 • HTTP CONNECT、HTTP POST: 6588、3128、80 此外,如果您的组织使用代理服务器控制出站 internet 流量,则需要定义发件人信誉在访问 internet 以实现开放代理服务器检测时所需的代理服务器名称、类型和 TCP 端口。或者,您可以在发件人信誉中禁用开放代理服务器检测。@51CTO博客 有关详细信息,请参阅发件人信誉过程。

阿里云配置域名解析, 省略, 结果如下

```
C:\Users\Administrator>nslookup mail.cnqin.com.cn
服务器: [redacted].com
Address: [redacted]

非权威应答:
名称: mail.cnqin.com.cn
Address: 1[redacted].148

C:\Users\Administrator>
```

@51CTO博客

在路由器上映射边缘传输服务器的25端口到外网

```
管理员: C:\Windows\system32\cmd.exe
220 EDGE.corp.cnqin.com.cn Microsoft ESMTPL MAIL Service ready at Wed, 17 Jul 2019 11:19:24 +0800
451 4.7.0 Timeout waiting for client input

遗失对主机的连接。

C:\Users\Administrator>telnet mail.cnqin.com.cn 25_
```

@51CTO博客

5、邮件测试

QQ邮箱收到exchange邮件;



exchange邮箱收到QQ邮箱邮件

The screenshot shows the Outlook '邮件' (Mail) interface. On the left is a navigation pane with folders like '收件箱' (Inbox) and 'du01'. The main area is divided into three panes: a list of emails, a selected email's header, and the email body. The selected email is a reply from 'Jiang <329913593@qq.com>' to 'du01' with subject '2019-07-17-001'. The body contains a quoted original email from 'du01' with subject '2019-07-17-001 test'. A red box highlights the sender information in the header. The bottom right corner features the '@51CTO博客' watermark.