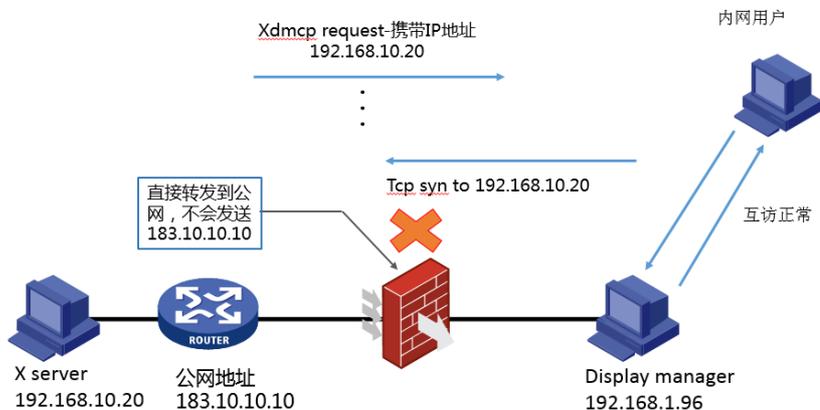


知 XDMCP业务跨防火墙不通，但是可以实现内网XDMCP业务互通

ALG 斑大人 2018-10-14 发表

组网及说明

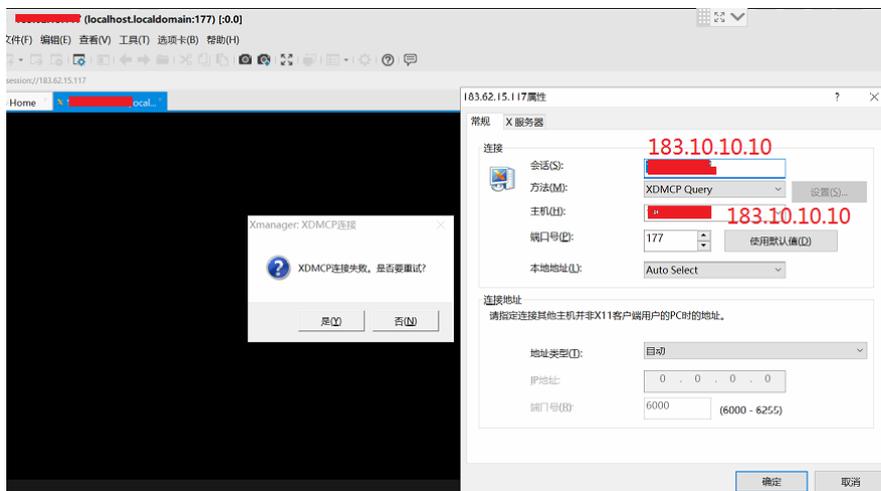
如图所示：



问题描述

防火墙上客户配置1对1静态映射静态映射183.10.10.10<--->192.168.1.96后，服务器192.168.1.96的其他端口均可从外网正常使用（比如22端口），但udp177不正常；UDP177内网用户使用正常当前公网地址在其他设备上使用UDP端口177正常。

XDMCP（X Display Manager Control Protocol）X显示监控协议，基于XDMCP的远程X是非常简单易用而且体现Unix/Linux长处一个网络应用，它是把整个X桌面输出到远端。xdmcp服务默认使用p177端口



过程分析

XDMCP协议在客户端（X server，在该问题中就是内网的192.168.1.92以及外网的183）发送给服务器（display manager，在这个问题中就是192.168.1.96这个被管理的centos虚拟机）的request报文中携带X server的IP地址，之后Display manager会向request中携带的IP的tcp 6000端口号发起tcp三次握手。

正常内网UDP177端口互访报文如下：

No.	Time	Source	Destination	Length	Protocol	Info
423	5.895306	183.10.10.10	192.168.1.96	60	XDMCP	Query
424	5.895917	192.168.1.96	183.10.10.10	75	XDMCP	Willing
491	6.656011	183.10.10.10	183.10.10.10	149	XDMCP	Request[Disse
492	6.656632	192.168.1.96	183.10.10.10	94	XDMCP	Accept
493	6.662778	183.10.10.10	192.168.1.96	64	XDMCP	Manage
584	8.661967	183.10.10.10	192.168.1.96	64	XDMCP	Manage
791	12.663733	183.10.10.10	192.168.1.96	64	XDMCP	Manage
1275	20.666514	183.10.10.10	192.168.1.96	64	XDMCP	Manage
10314	133.844054	192.168.1.96	183.10.10.10	85	XDMCP	Failed
16648	261.077955	192.168.1.96	183.10.10.10	85	XDMCP	Failed
16649	261.078217	192.168.1.96	183.10.10.10	60	XDMCP	Refuse
16650	261.078476	192.168.1.96	183.10.10.10	60	XDMCP	Refuse

跨防火墙UDP177端口访问不通的抓包：

No.	Time	Source	Destination	Length	Protocol	Info
423	5.895306	183.10.10.10	192.168.1.96	60	XDMCP	Query
424	5.895917	192.168.1.96	183.10.10.10	75	XDMCP	Willing
491	6.656011	183.10.10.10	183.10.10.10	149	XDMCP	Request[Dissector bug, protocol XDMCP: C:\buildbot\wireshark\wireshark-2.4-32\windows-2016-x86\build\epan\ tvb.c:532: failed assertion "tvb && tvb->len >= tvb->len"]
492	6.656632	192.168.1.96	183.10.10.10	94	XDMCP	Accept
493	6.662778	183.10.10.10	192.168.1.96	64	XDMCP	Manage
584	8.661967	183.10.10.10	192.168.1.96	64	XDMCP	Manage
791	12.663733	183.10.10.10	192.168.1.96	64	XDMCP	Manage
1275	20.666514	183.10.10.10	192.168.1.96	64	XDMCP	Manage
10314	133.844054	192.168.1.96	183.10.10.10	85	XDMCP	Failed
16648	261.077955	192.168.1.96	183.10.10.10	85	XDMCP	Failed
16649	261.078217	192.168.1.96	183.10.10.10	60	XDMCP	Refuse
16650	261.078476	192.168.1.96	183.10.10.10	60	XDMCP	Refuse

Request报文中携带的X server地址：

Display manager (192.168.1.96) 向X server (192.168.1.92) 发起tcp三次握手，建立成功之后使用x11协议初始化相关参数，之后远程控制建立成功。

192.168.1.92	192.168.1.96	357	XDMCP	Request[Dissector bug, protocol XDMCP: C:\buildbot\wireshark\wireshark-2.4-32\windows-2016-x86\build\epan\ tvb.c:532: failed assertion "tvb && tvb->len >= tvb->len"]
192.168.1.96	192.168.1.92	94	XDMCP	Accept
192.168.1.92	192.168.1.96	64	XDMCP	Manage
192.168.1.96	192.168.1.92	74	TCP	50146 → 6000 [SYN] Seq=0 Win=2 Len=0
192.168.1.92	192.168.1.96	66	TCP	6000 → 50146 [SYN, ACK] Seq=0 Win=0 Len=0
192.168.1.96	192.168.1.92	60	TCP	50146 → 6000 [ACK] Seq=1 Ack=1 Len=0
192.168.1.96	192.168.1.92	102	X11	Initial connection request
192.168.1.92	192.168.1.96	734	X11	Initial connection reply

上面是内网正常访问的报文，而外网访问异常时的xdmcp request报文中写携带的 x server地址还是私网地址 (192.168.10.20)：

之后display manager (192.168.1.96) 向192.168.10.20的tcp 6000端口发起三次握手：

192.168.1.96	192.168.10.20	74	TCP	51232 → 6000 [SYN] Seq=0 Win=29200 Len=0
192.168.1.96	192.168.10.20	74	TCP	[TCP Retransmission] 51232 → 6000 [SYN] Seq=0 Win=29200 Len=0

当然这个三次握手肯定建立失败，也就没有后续的x11初始化相关参数，远程管理自然失败。

解决方法

只要display manager收到的request报文里携带的X server地址是公网地址（183.10.10.10）就可以正常建立远程控制，对应用层中携带的地址/端口号进行转换需要ALG功能支持，开启nat alg xdmcp即可，而使用其他设备正常可能是因为很多厂家设备默认开启各项alg。

在我司的设备当中，nat alg xdmcp默认是disable状态

```
[M9006]display nat alg
```

NAT ALG:

```
DNS      : Enabled
FTP      : Enabled
H323     : Disabled
ICMP-ERROR : Enabled
ILS      : Disabled
MGCP     : Disabled
NBT      : Disabled
PPTP     : Enabled
RTSP     : Enabled
RSH      : Disabled
SCCP     : Disabled
SIP      : Disabled
SQLNET   : Disabled
TFTP     : Disabled
XDMCP    : Disabled
```

建议开启nat alg xdmcp功能

nat alg命令用来开启指定或所有协议类型的NAT ALG功能。

undo nat alg命令用来关闭指定或所有协议类型的NAT ALG功能。

【命令】

```
nat alg { all | dns | ftp | h323 | icmp-error | ils | mgcp | nbt | pptp | rsh | rtsp | sccp | sip | sqlnet | tftp | xdmcp }
```

```
undo nat alg { all | dns | ftp | h323 | icmp-error | ils | mgcp | nbt | pptp | rsh | rtsp | sccp | sip | sqlnet | tftp | xdmcp }
```