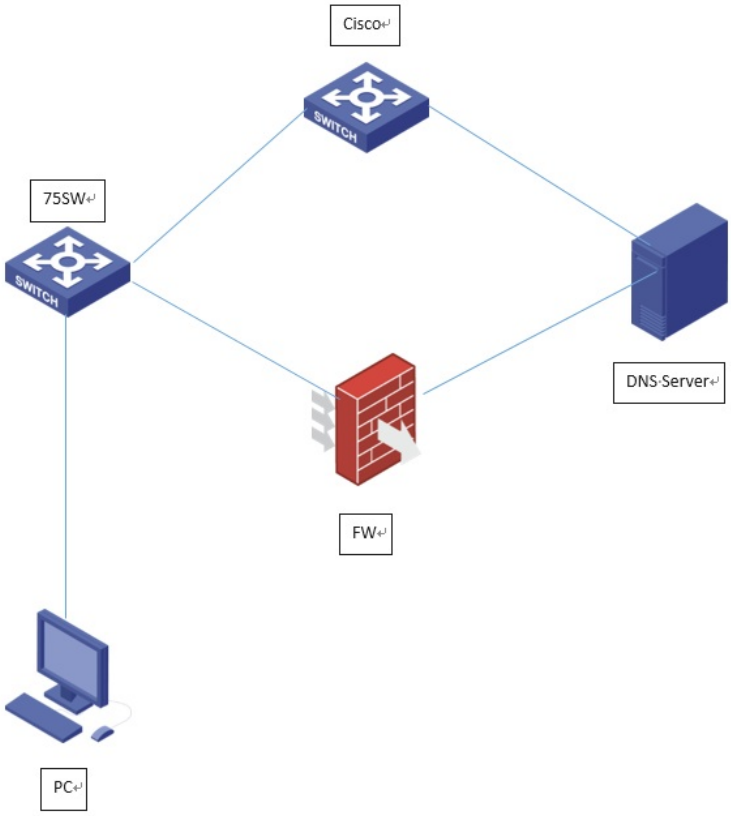
某局点SecBlade FW插卡替换思科交换机域名解析业务异常问题案例分析

DNS　尤良柱　2018-06-29 发表

组网及说明



1、现场内网一台DNS服务器，网关设在cisco交换机上，客户端PC通过我司75交换机将报文转发至cisco交换机，完成与DNS服务器的交互，实现域名解析；
2、在75交换机上部署两块防火墙插卡SecBlade FW，将DNS服务器网关更改设置到FW上，并在75交换机上关闭到cisco交换机端口，客户端流量走75交换机内联口上到防火墙板卡，再转发到DNS服务器，完成与DNS服务器的交互，实现域名解析。

问题描述

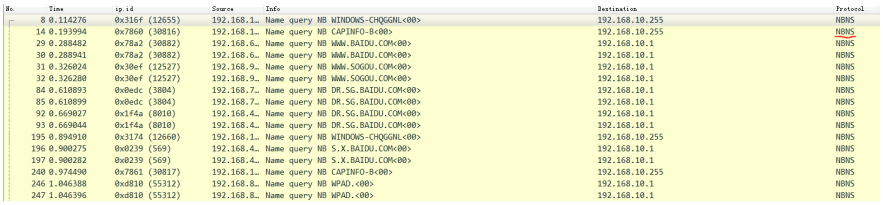
现场防火墙板卡上线之后，发现大部分主机业务域名无法访问，域名解析异常，但是客户端可以ping通域名服务器地址，且防火墙策略是全通的。

过程分析

1、在防火墙上查看配置，只是对报文简单的转发，不涉及nat，查看会话，发现有udp53端口的会话，说明策略也没有阻断；
2、在客户端抓包，发现和业务域名相关的很少又udp 53端口的报文，由于是内网环境，一些公网的域名解析是失败时正常情况，分析报文，发现有很多NBNS协议的报文，开始排查现场的组网和域名解析机制；
DNS报文：

78	0.544294	0x3de9 (15849)	192.168.1…	Standard query 0xb21b A 1.xt-banben.com	202.12.27.33	DNS
79	0.544317	0x3dea (15850)	192.168.1…	Standard query 0x8da3 A www.baidu.com	202.12.27.33	DNS
80	0.544341	0x3deb (15851)	192.168.1…	Standard query 0x73f5 A armmf.adobe.com	202.12.27.33	DNS
81	0.544365	0x3dec (15852)	192.168.1…	Standard query 0x5a9e A teredo.ipv6.microsoft.com	202.12.27.33	DNS
82	0.544387	0x3ded (15853)	192.168.1…	Standard query 0x4a16 A swupmf.adobe.com	202.12.27.33	DNS
83	0.579533	0x1177 (4471)	192.168.6…	50610→3389 [ACK] Seq=108 Ack=6404 Win=256 Len=0	192.168.10.1	TCP
84	0.610893	0x0edc (3804)	192.168.7…	Name query NB DR.SG.BAIDU.COM<00>	192.168.10.1	NBNS
85	0.610899	0x0edc (3804)	192.168.7…	Name query NB DR.SG.BAIDU.COM<00>	192.168.10.1	NBNS
86	0.615168	0x3be3 (15331)	192.168.1…	Standard query 0xc108 AAAA capinfo-b	224.0.0.252	LLMNR
87	0.615227	0x3be4 (15332)	192.168.1…	Standard query 0xf0fc A capinfo-b	224.0.0.252	LLMNR
88	0.615589		CiscoInc_…	Who has 192.168.10.34? Tell 192.168.10.253	Broadcast	ARP
89	0.632117	0x33a3 (13219)	192.168.1…	Standard query 0x3f03 A teredo.ipv6.microsoft.com	192.168.10.1	DNS
90	0.632212	0x3dee (15854)	192.168.1…	Standard query 0xfd5e A teredo.ipv6.microsoft.com	192.36.148.17	DNS

NBNS报文：



No.	Time	ip.id	Source	Info	Destination	Protocol
8	0.114276	0x316f (12655)	192.168.1…	Name query NB WINDOWS-CHQGGNL<00>	192.168.10.255	NBNS
14	0.193994	0x7860 (30816)	192.168.1…	Name query NB CAPINFO-B<00>	192.168.10.255	NBNS
29	0.288482	0x78a2 (30882)	192.168.6…	Name query NB WWW.BAIDU.COM<00>	192.168.10.1	NBNS
30	0.288941	0x78a2 (30882)	192.168.6…	Name query NB WWW.BAIDU.COM<00>	192.168.10.1	NBNS
31	0.326024	0x30ef (12527)	192.168.9…	Name query NB WWW.SOGOU.COM<00>	192.168.10.1	NBNS
32	0.326280	0x30ef (12527)	192.168.9…	Name query NB WWW.SOGOU.COM<00>	192.168.10.1	NBNS
84	0.610893	0x0edc (3804)	192.168.7…	Name query NB DR.SG.BAIDU.COM<00>	192.168.10.1	NBNS
85	0.610899	0x0edc (3804)	192.168.7…	Name query NB DR.SG.BAIDU.COM<00>	192.168.10.1	NBNS
92	0.669027	0x1f4a (8010)	192.168.4…	Name query NB DR.SG.BAIDU.COM<00>	192.168.10.1	NBNS
93	0.669044	0x1f4a (8010)	192.168.4…	Name query NB DR.SG.BAIDU.COM<00>	192.168.10.1	NBNS
195	0.894910	0x3174 (12660)	192.168.1…	Name query NB WINDOWS-CHQGGNL<00>	192.168.10.255	NBNS
196	0.900275	0x0239 (569)	192.168.4…	Name query NB S.X.BAIDU.COM<00>	192.168.10.1	NBNS
197	0.900282	0x0239 (569)	192.168.4…	Name query NB S.X.BAIDU.COM<00>	192.168.10.1	NBNS
240	0.974490	0x7861 (30817)	192.168.1…	Name query NB CAPINFO-B<00>	192.168.10.255	NBNS
246	1.046388	0xd810 (55312)	192.168.8…	Name query NB WPAD.<00>	192.168.10.1	NBNS
247	1.046396	0xd810 (55312)	192.168.8…	Name query NB WPAD.<00>	192.168.10.1	NBNS

3、经过与现场沟通确认，发现现场有AD域，使用的业务软件在未加域业务终端上直接通过NBNS协议广播请求主机名对应IP地址，由对应的服务器单播响应；在加域的电脑上业务软件通过DNS解析请求完整域名对应的IP来访问。

4、此时业务流经过cisco交换机可以正常交互，检查cisco交换机配置，发现cisco交换机配置有ip helper命令将广播报文转为单播的配置，将NBNS协议的广播报文转到对应的服务器完成主机名对应IP地址的获取，而防火墙板卡上却没有同步此配置，无法将NBNS协议报文转到对应的服务器。

ip helper-address 192.168.x.x

ip helper-address 192.168.x.x

ip helper-address 192.168.x.x

ip helper-address 192.168.x.x

ip helper-address 192.168.x.x

解决方法

在FW上增加udp-helper配置：

udp-helper port 137 （NBNS协议端口）

udp-helper server x.x.x.x （相关主机名业务服务器地址）

对未加域终端发送的广播NBNS报文转换为单播报文发送到相关主机名业务服务器处理，服务器将主机名对应IP单播返回客户终端。