

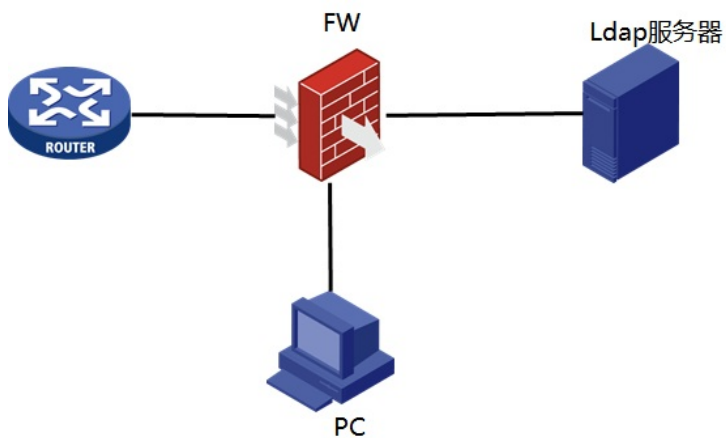
某局点sslvpn结合ldap认证不成功经验案例

SSL VPN

单畅 2020-04-30 发表

组网及说明

组网如下：



问题描述

sslvpn结合ldap认证，用iNode拨号认证不通过，把ldap相关配置删掉用本地认证测试认证成功。看设备配置没有问题，刚开始怀疑问题出在ldap服务器侧。检查ldap相关配置创建的用户也正常，查询路径也没问题。

#

ldap server ldapserver

login-dn cn=administrator,cn=users,dc=h3c,dc=com

search-base-dn dc=h3c,dc=com

ip 192.168.13.199

login-password cipher \$c\$3\$7oUQhFW3wfxOvS0nBwMHPCMJ02Y5QZYFNeo=

#

过程分析

收集debug信息：debug sslvpn和debug ldap

到查询报文后没有成功。

*Mar 4 16:48:04:728 2020 GDSD-SHDZ-FW LDAP/7/EVENT: -COntext=1;

PAM_LDAP:Keep state authentication searching for incomplete searching.

*Mar 4 16:48:12:937 2020 GDSD-SHDZ-FW LDAP/7/EVENT: -COntext=1;

PAM_LDAP:Get result message errno = -14

*Mar 4 16:48:12:937 2020 GDSD-SHDZ-FW LDAP/7/EVENT: -COntext=1;

PAM_LDAP:Get entry count is 0.

*Mar 4 16:48:12:937 2020 GDSD-SHDZ-FW LDAP/7/EVENT: -COntext=1;

PAM_LDAP:Keep state authentication searching for incomplete searching.

*Mar 4 16:48:26:937 2020 GDSD-SHDZ-FW LDAP/7/EVENT: -COntext=1;

PAM_LDAP:Get result message errno = -14

PAM_LDAP:Failed to find session (socketFd=53, msgId=19)

在设备到ldap侧的接口上抓包，发现服务器回复了查询报文就没有后续交互的报文，设备并没有回复查询是否成功。

No.	Time	Source	Destination	Protocol	Length	Sinfo
231	2019/3/1 15:06:07.1...	192.168.13.174	192.168.13.199	LDAP	150	searchRequest(24) "dc=h3c,dc=com" wholesubtree
232	2019/3/1 15:06:07.1...	192.168.13.199	192.168.13.174	LDAP	1719	searchResEntry(24) "Ch-zhangzhichao,CN=Users,DC=h3c,DC=com" searchResRef(24) searchResRef(24) s...

又在防火墙另外一个接口抓包，发现很奇怪的现象：设备向dns服务器发送的dns报文中，有包含请求解析h3c.com这个域名的报文。这个是ldap服务器用户所在的域。

line	Source	Destination	Protocol	Length	Info
60	2020/121 06:59:43.9...	192.168.1.2	DNS	82	Standard query 0xf59f A ForestDnsZones.h3c.com
61	2020/121 06:59:43.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
63	2020/121 06:59:45.9...	192.168.1.2	DNS	82	Standard query 0xd504 A ForestDnsZones.h3c.com
64	2020/121 06:59:45.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
67	2020/121 06:59:46.9...	192.168.1.2	DNS	82	Standard query 0xa072 AAAA ForestDnsZones.h3c.com
68	2020/121 06:59:46.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
69	2020/121 06:59:48.9...	192.168.1.2	DNS	82	Standard query 0xc9eb AAAA ForestDnsZones.h3c.com
70	2020/121 06:59:48.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
73	2020/121 06:59:49.9...	192.168.1.2	DNS	82	Standard query 0x07b2 A DomainDnsZones.h3c.com
74	2020/121 06:59:49.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
75	2020/121 06:59:51.9...	192.168.1.2	DNS	82	Standard query 0xaa08 A DomainDnsZones.h3c.com
76	2020/121 06:59:51.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
79	2020/121 06:59:52.9...	192.168.1.2	DNS	82	Standard query 0x6559 AAAA DomainDnsZones.h3c.com
80	2020/121 06:59:52.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
86	2020/121 06:59:54.9...	192.168.1.2	DNS	82	Standard query 0xb37e AAAA DomainDnsZones.h3c.com
87	2020/121 06:59:54.9...	192.168.1.1	ICMP	110	Destination unreachable (Port unreachable)
95	2020/121 06:59:55.9...	192.168.1.2	DNS	67	Standard query 0x1196 A h3c.com
96	2020/121 06:59:55.9...	192.168.1.1	ICMP	95	Destination unreachable (Port unreachable)

发现现场的配置里面有配置dns server 192.168.1.1。后面确认得知配置了dns server后会去查ldap.com的域名，因为这个域名不存在，所以就会超时。

解决方法

后续指导现场把dns server相关配置删掉问题解决。
在配置sslvpn结合ldap时需要注意，和接口上面配置dns server会和ldap域冲突，导致ldap认证时，会向dns服务器请求ldap.com的域名。