大亚湾核电站Internet防火墙剖析

广东核电合营有限公司　　俞玉存

▲ 本文介绍了大亚湾核电站(GNPJVC)Internet 系统的安全核心PIX 防火墙，围绕防火墙的安全策略，具体介绍了PIX 防火墙的战略地位与参数配置，并对重点、难点技术参数作出分析。同时，简单地介绍了一下Internet 系统的架构和其主要的组成部分如PROXY、DNS和Mail服务器等。

1. GNPJVC防火墙的战略地位

PIX 防火墙处于Internet、公司网页与企业内网之间，具有重要的战略地位(见图1)。

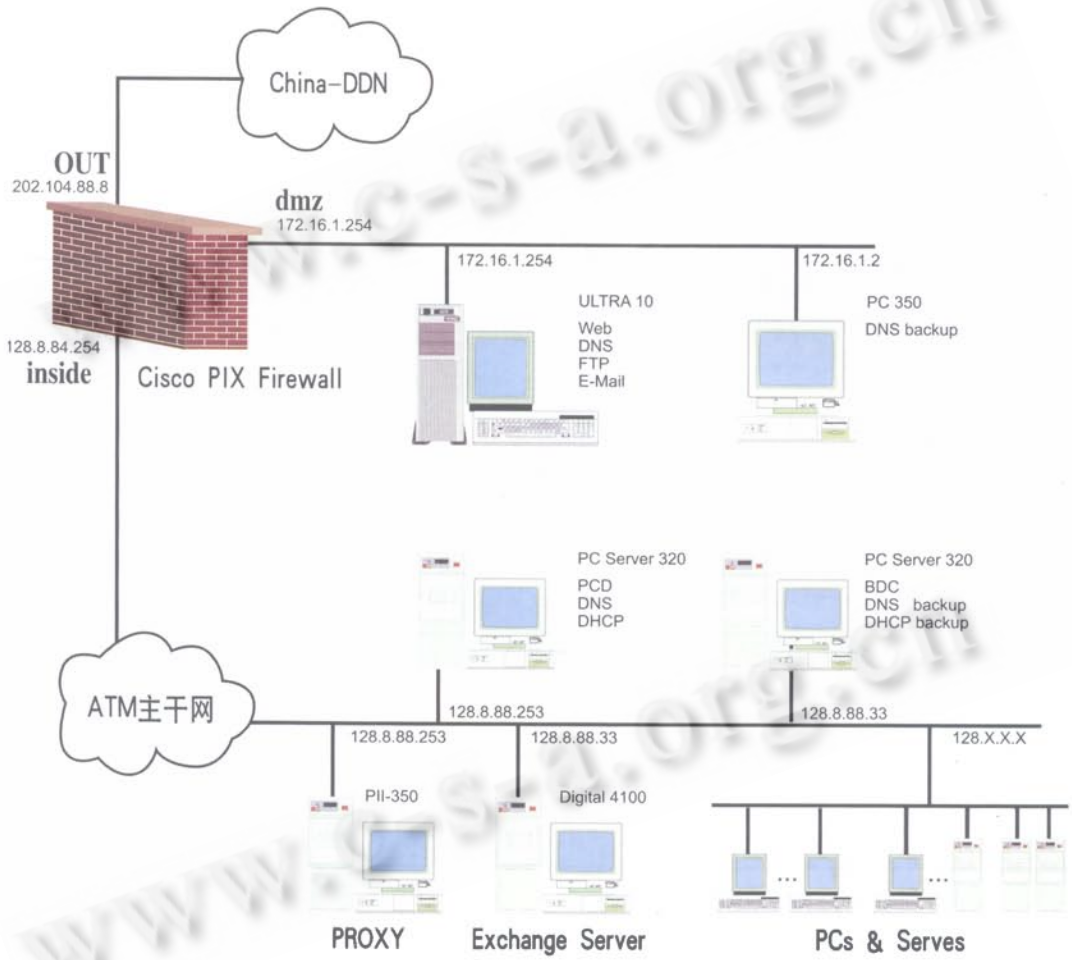

图 1　PIX 防火墙在Internet 系统中的战略位置

PIX 防火墙具有三块网卡，分别取名为out 、dmz和 inside，各自连接到对应的网段，我们称之为out网段、dmz网段和inside网段。通过对三块网卡的合理控制，实现内网用户方便使用Internet、公司主页访问畅通和充分保障内网安全的目标。

inside 网段就是GNPJVC 的企业内部网。包括30多台服务器和上千台PC 机，更有三十多个应用系统和相应的数据库，是GNPJVC宝贵的信息财富。因此，保卫inside 网段是我们最重要的目标。

在Internet 系统中，Inside 网段有两个很重要的角色：DNS 服务器和PROXY 服务器。DNS服务器起着内网IP地址解析的作用，其中包括对Internet IP地址路由效果，加快地址寻找速度、减少网络风暴，从而提高网络效率。PROXY服务器把访问过的信息存到自己的硬盘中，而在下一位客户访问同一URL时，PROXY服务器就把硬盘中已存的信息直接送给该用户，极大地提高了速度。而在同一个企业中，访问同一 URL 的机率是很高的，因此，良好的PROXY服务器的设立将使用户端速度提高几倍。PROXY服务器自身有一

套刷新机制，以保证信息的新鲜程度和提高命中率。PROXY服务器本身的速度、硬盘容量及其组合配置将起到决定性的效果。PROXY 服务器是内网 Internet 用户对PIX 防火墙的唯一出入口，也具有软件防火墙的作用。PROXY 服务器起到协议口定义、Internet 资源缓存、对用户身份验证、网段隔离等作用，在一般的小企业中，PROXY 服务器往往是Internet 系统仅有的防火墙。也正是PROXY服务器与PIX 防火墙的复合技术，大大提高了GNPJVC内网的安全性。

2. 参数配置

PIX 防火墙的配置犹如一篇优美的文章，前后连贯，一气呵成

数设定往往为

笔

认端口号，具备Internet 的通用性。也可以设为其他的端口号，理论上具有一定的加密效果，但可能会给以后维护带来诸多不便。下面第一条语句解析为：ftp服务设定为第21端口。

fixup protocol ftp 21

fixup protocol http 80

fixup protocol smtp 25

(3)跟踪PIX 防火墙的重要信息

logging 命令可以使PIX 防火墙

有关资料信息传送到控制

件或者 SNMP

以从

(5)在内部网段建立路由信息协议

在内部网段建立路由信息协议rip (route information protocol)，以加快IP信息的识别速度。rip 命令保证路由信息表的更新，如下面前两条命令。route 命令则指明了默认的外部及内部路由器地址，可以加快IP地址的转发，如下面后两条命令

rip

.104.88.17 1

28.1.3.1 1

网段作

定将是

外访

议、

O

设为sec

其中 secu

最高。若不

认的访问权

任何主机可以

段的任何主机，

常使用，必须合

。

下面命令设定

防火墙各块网卡的安全等级，并起了名称，方便以后使用。第一条语句解析为：第0块以太网卡取名为out，安全等级为security0。

nameif ethernet0 out security0

nameif ethernet1 inside security100

nameif ethernet2 dmz security50

(2)设定各应用协议的端口号

应用协议的端口号一般设定为默

段访问安全等

，需要进行地址转换，使

安全等级网段的用户不能真正看到高安全等级网段的用户的IP地址，从而起到保护高安全等级网段的作用。

的

申请的Internet

nternet IP地址的唯一性；

side 地址为公司企业内网的合法地址；dmz 地址为 dmz 网段的合法地址。各地址在各自网段都具有重要的窗口地位。下面第一条语句解析为：名称为out 的接口卡的IP 地址为202.104.88.8，掩码为 255.255.255.240。

ip address out 202.104.88.8 255.255.255.240

ip address inside 128.8.84.254 255.255.0.0

ip address dmz 172.16.1.254 255.255.0.0

与Internet 连接时，nat (Network Address Translation) 命令通过IP地址表，把内网IP地址转换为Internet地址，从而使Internet 网用户只能看到访问者的经转换后的Internet 地址，而不是访问者真正的在企业内网中的IP地址，使Internet 黑客无从猜测内网IP地址的可能性。在下面命令中，分net_id 为30和20两组 net group，每一组为一独立的地址对应设定。

在net_id为30的一组里表示：inside地址 (nat) 中的128.1.x.x 网段将转换为相应的out网段 (global) 中的

202.104.88.20–202.104.88.28 地址或202.104.88.19地址。同时，Inside网段(nat) 128.1.x.x 地址将对应到 dmz网段(global)中的172.16.2.0–172.16.254.254地址。它们按一定的算法进行转换，是多对多的随机地址对应关系。

global (out) 30 202.104.88.20–202.104.88.28 netmask 255.255.255.240

global (out) 30 202.104.88.19–202.104.88.19 netmask 255.255.255.240

global (dmz) 30 172.16.2.0–172.16.254.254 netmask 255.255.0.0

nat (inside) 30 128.1.0.0 255.255.0.0 0 0

同样，在net_id 为20的一组里表示：dmz网段 (nat) 中的172.16.x.x地址将转换为相应的out网段 (global) 中的202.104.88.29–202.104.88.30 地址。

global (out) 20 202.104.88.29–202.104.88.30 netmask 255.255.255.240

nat (dmz) 20 172.16.0.0 255.255.0.0 0 0

与下面的 static、conduit 命令的区别为，这里是地址池(address pool)对地址池的转换，符合广大内网用户访问广阔Internet 网站的特点。

(7)outbound 与 apply 的配合，真正实现从高到低访问的许可

是否允许内部用户建立与外部Internet 的联接；是否允许内部用户访问特殊的Internet服务器；允许内部用户用何种服务去访问外部服务器；是否允许内部用户在内网执行Java applets来支持外部Internet 服务等，都可以通过outbound命令设定。并由 apply 命令来确定outbound命令描述的主机IP 地址表是针对企业内网的还是Internet 网的。

下面命令中，第一行定义了该主机可以通过udp(User Datagram Protocol)协议的 domain (53) 口访问外部主机；第二行定义了该主机可以通过任何协议的 POP3 (110) 口访问外部主机；第三行定义了该主机可以使用任何协议、任何口去访问外部主机；第四行定义了任何主机都禁止访问任何外部主机，该语句确保了除许可主机外，任何内网主机禁止去任何地方，避免了Internet网络资源的滥用。第五行apply 语句则表示上面的outbound 语句定义的是针对内部网络(inside)地址的。

outbound 1 permit 128.8.88.30 255.255.255.255 53 udp

outbound 1 permit 128.8.88.33 255.255.255.255 110 0

outbound 1 permit 128.8.88.51 255.255.255.255 0 0

outbound 1 deny 0.0.0.0 0.0.0.0 0 0

apply (inside) 1 outgoing_src

(8)static 与conduit 配合，实现从低到高的访问

实现从低安全等级网段到高安全等级网段的访问，同样需要建立地址的转换和设定访问许可。

建立dmz、inside网段的地址与out网段的Internet 地址之间的IP 静态影射关系，功能类似nat、global的设定，区别为static、conduit是一对一的清晰的地址影射关系，适用外部网络客户访问少量的内网主机。下面第一个语句表示：dmz 网段的172.16.1.1 地址将影射到out 网段的202.104.88.30 地址，或者说，对out网段的202.104.88.30主机的任何许可的访问就是对dmz 网段的172.16.1.1主机的访问。对外来的连接，conduit 语句对许可的协议、端口号进行了定义，只允许外部Internet用户使用特定的服务来访问特定的内网主机，也明确了内网的可能的安全性缺口。下面第三个语句表示为：允许任何外部地址通过tcp/ip 协议的 www端口访问其Internet 地址为202.104.88.30的内部主机。

static (dmz,out) 202.104.88.30 172.16.1.1 netmask 255.255.255.255 0 0

static (inside,out) 202.104.88.28 128.8.88.33 netmask 255.255.255.255 0 0

conduit permit tcp host 202.104.88.30 eq www any

(9)限制用户访问不良站点

禁止内部用户访问某些反动或不健康的Internet站点，既可以主动阻断源头也可以节约Internet网络资源。下面前二个语句定义了禁止用80口(http服务)访问二台假定的不良站点，第三个语句表示上面二句设定主机的IP地址是针对外部Internet地址的。

outbound 3 deny 202.1.19.130 255.255.255.255 80 tcp

outbound 3 deny 214.17.119.10 255.255.255.255 80 0

apply (out) 3 outgoing_dest

另外，配合PROXY服务器的使用，可以统计出每个人访问过的站点及次数，清楚考究任何用户访问过的站点

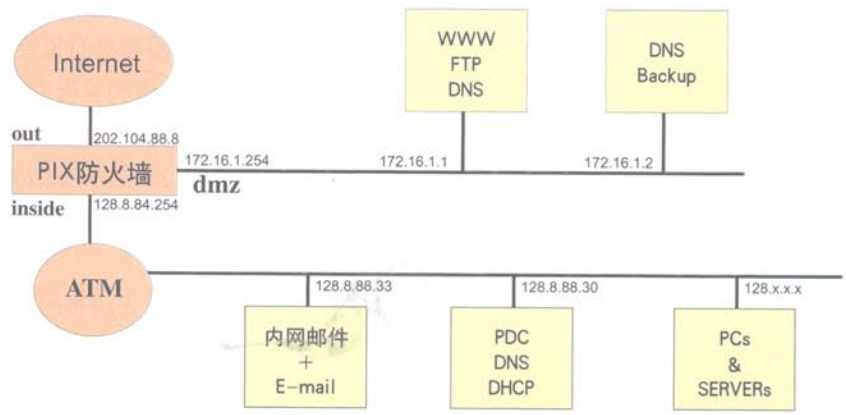

图 2 把E-mail 服务移到内网EXCHANGE服务器上的配置示意图

的情况。

(10)周期性验证口令

一个有用的参数，使用户不需要周期性验证口令，如第一条命令所设。但，在需要防范他人乘机使用Internet的情况时，则可以使用第二条命令，该命令将使用户每隔15分钟重新进行一次口令验证；而第三条命令，则将使用户在对一次URL(universal resource locator)访问结束并空闲10分钟后，需要重新进行一次口令验证；以确保非法用户的不能继续使用，保护合法用户的权益。

```
timeout uauth 0:00:00 absolute
timeout uauth 0:15:00 absolute
timeout uauth 0:10:00 inactivity
```

3.配置片段示例

细心的读者可能会发现，在我们收发E-mail 的过程中，我们用的是dmz 网段的Mail服务器。那么，是不是可以在内网直接收发E-mail呢？其实，在PIX 防火墙只有二块接口卡的典型配置中，就是直接把E-mai 送入内网的，而且，具有同样的安全等级。下面将通过把E-mail服务移到内网的EXCHANGE 服务器上，既为大家提供一个解决方案，又为重要的参数配置作个小结。虽然在我们的Internet 系统中没有使用，但都是经过了我们开发组的理论和实验证明的、是有效的和具有实用价值的。

把E-mail服务移到EXCHANGE(128.8.88.33)服务器上的配置示意图(见图2)。

各网卡的基础参数设定如：速度、安全级别、名称、IP地址、路由等均与现实配置相同，而有关E-mail服务的功能配置需改变如下：

```
fixup protocol smtp 25
static (inside,out) 202.104.88.28 128.8.88.33 netmask 255.255.255.255 0 0
conduit permit tcp host 202.104.88.28 eq smtp any
global(out)30 202.104.88.19-202.104.88.21 netmask 255.255.255.240
nat (inside) 30 128.1.0.0 255.255.0.0 0 0
outbound 1 permit 128.8.88.33 255.255.255.255 109 0
outbound 1 permit 128.8.88.33 255.255.255.255 110 0
outbound 1 deny 0.0.0.0 0.0.0.0 0 0
apply (inside) 1 outgoing_src
```

第一句：指定smtp服务使用默认的第25端口号。

第二句：设定从低到高访问时的一对一的IP地址影射关系。

第三句：设定允许所有的外部Internet 客户通过smtp 服务访问202.104.88.28地址，而202.104.88.28地址对应的就是内网的128.8.88.33地址。也就是说，允许所有的外部Internet客户通过smtp 服务访问EXCHANGE 服务器。

第四句：设定从高到低访问时的地址池对地址池的IP地址影射关系。

第五句：设定允许所有的内部Internet 用户可以访问到任何外部Internet 主机。这里仅仅是地址网段的开放许可，能否真正访问，还需要下面outbound语句的协议许可。

第六、七句：设定允许EXCHANGE服务器用POP2、POP3端口访问任何外部Internet 主机。

第八句：设定禁止所有的内部Internet 主机用任何协议访问到任何外部Internet 主机。确保了除允许的主机用特定的协议、端口外，其他主机均被禁止。

第九句：设定上面outbound语句的定义是针对内部主机的IP地址。

从上面的具体语句设定可以看到，在外部Internet 用户访问内部E-mail服务(EXCHANGE服务器)时，仅允许通过smtp端口访问。据资料介绍，PIX 防火墙已经充分考虑到E-mail 协议的开放对内部网络影响的可能性，该端口只开放具有绝对安全性的七条命令，如：HELO,MAIL,RCPT,DATA,RSET,NOOP和QUIT。PIX 防火墙自身的严密保安也可见一斑。向外发信时，内部用户仅用POP2、POP3端口访问外部主机，如果开放更多的端口也只是涉及网络资源问题而没有内网安全问题。

很明显，如果把E-mail服务放在内网的EXCHANGE服务器上，在广大的客户端只需要一个Outlook软件就可以实现内部邮件与E-mail的收发，对维护与使用都是非常方便的。而放在dmz网段的理由是：dmz 网段极少需要维护，相对稳定，不会因为公司内网的检测、调整等影响到E-mail的接收，具有很好的对外服务，而且，在对外的任何活动中，公司形象的考虑往往是起主导地位的；从Internet 网络入侵的角度考虑，黑客有兴趣的往往是展示形象的公司网页或Mail服务器，把它们放在安全等级相对低的dmz网段，万一受到攻击，会给我们以警示，从而考虑进一步保护内网的非常手段。可以说，我们现在使用的方案是放弃了许多的方便而维护了更完美的形象。

参考文献

[1] http://www-china.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/archv42/pfmrn422.htm GNPJVC的PIX 防火墙型号的技术资料

[2]http://www.isi.edu/in-notes/iana/assignments/protocol-numbers协议名称与其对应的协议号

[3]http://www.isi.edu/in-notes/iana/assignments/port-numbers 协议的端口号与其对应的服务

[4]《因特网防火墙技术》刘渊、乐红兵等著 机械工业出版社出版 1998年8月