

Disseny d'un sistema de regles

Enunciat

El cap de l'empresa TecnoHack us ha demanat que dissenyar un sistema de protecció eficaç per a la vostra empresa, i començarem pensant en protegir la xarxa local mitjançant un sistema de seguretat perimetral basat en firewalls.

La xarxa té actualment quatre servidors (tot i que potser en el futur en podem afegir algun de nou amb serveis addicionals):

- Un es fa servir per al correu electrònic, en el qual els usuaris llegeixen el correu mitjançant el protocol POP3 i envien els seus missatges a través del protocol SMTP (Si necessiteu aclaracions de com van aquests dos protocols, pregunteu-ho!!).
- Per altra banda també s'ofereix un servidor web (www.tecnohack.com) en el qual hi ha la informació comercial de l'empresa, que pot ser consultada per tots els usuaris.
- En tercer lloc existeix un servidor de transferència de fitxers (FTP) el qual únicament ha de ser accedit per als comercials exteriors per a deixar-hi informació temporal.
- I finalment tenen un servidor de bases de dades que conté tota la informació de facturació, clients i distribuïdors.
- Tots els usuaris han de poder utilitzar Internet lliurement.

Se us demana que dissenyeu l'arquitectura més adequada per a protegir aquesta xarxa. Per a dissenyar el sistema de seguretat idoni podeu utilitzar routers, firewalls i bastions amb el nombre d'interfícies de xarxa que vulgueu (Tenim molt de pressupost!!).

Parts de l'activitat:

1.- Un dibuix/esquema explicant on quedaran ubicats tots els elements, i com s'enllaçaran. (Podeu fer servir com a referència els dibuixos que hi ha a les transparències de teoria). També heu de descriure les diferents zones de protecció que tingueu.

2.- Explicar els adreçaments que tindreu, definiu les adreces a les diferents interfícies de les subxarxes, i si utilitzeu NAT expliqueu on es troba ubicat i quines adreces dóna.

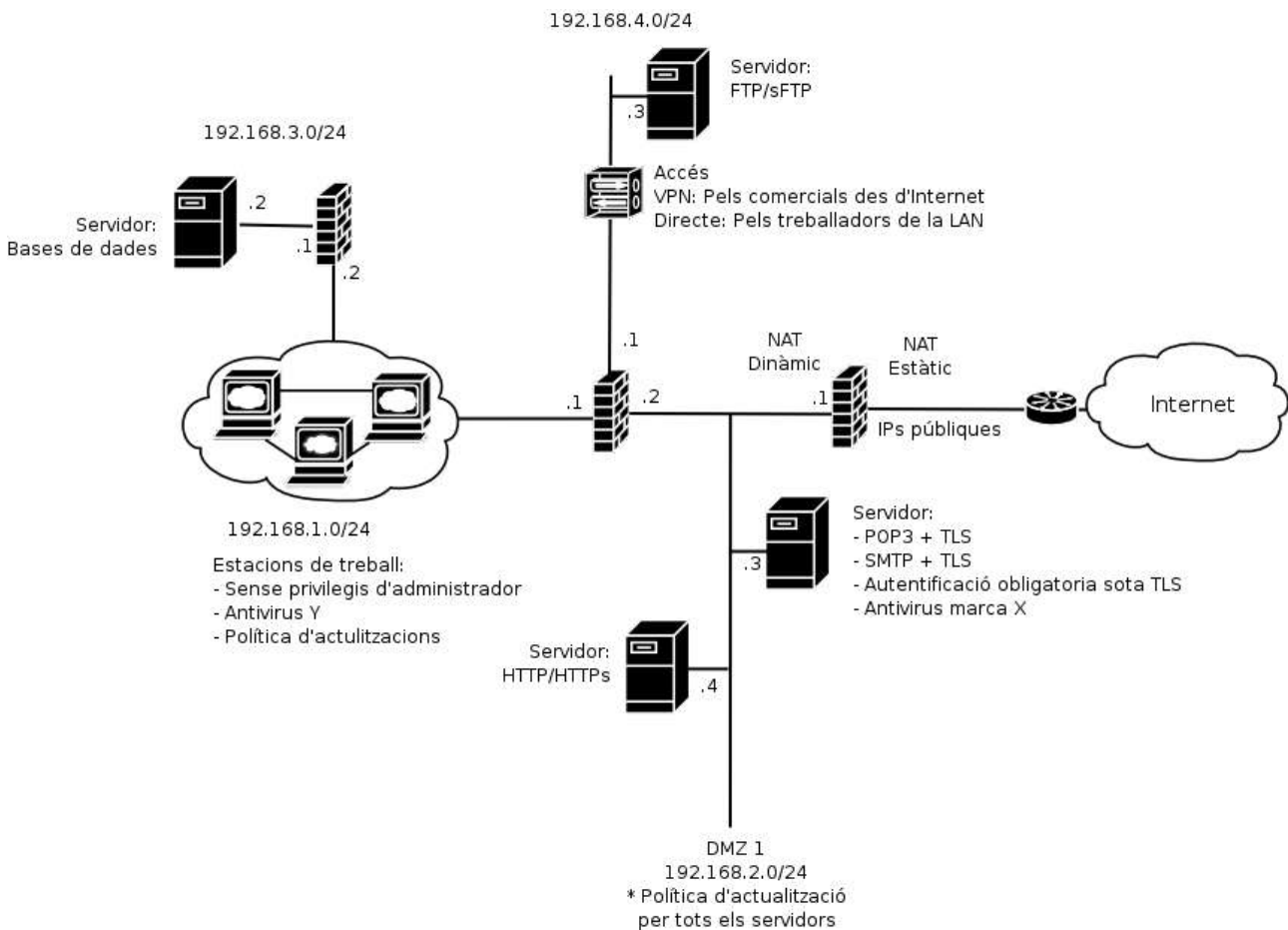
OPCIONAL: Si voleu completar més la informació podeu fins i tot afegir les taules de rutes dels elements.

3.- Per a tots els firewalls que utilitzeu, ompliu la corresponent taula de regles.

4.- Un cop definit tot el disseny, es hora d'introduir aquesta política dins de la taula de regles. Baixeu-vos el software de firewall builder, creeu un nou projecte i definiu les diferents regles, utilitzant els objectes, protocols i interfícies corresponents. Si teniu qualsevol dubte sobre aquest software, només cal que pregunteu a classe.

5.- OPCIONAL: Si voleu completar el treball, busqueu per Internet i dieu quina marca de firewall, bastion i/o routers utilitzaríeu per a portar a terme l'implantació d'aquest disseny. Valoreu la relació cost/prestacions...

1.- Dibuix/esquema explicant on quedaran ubicats tots els elements, i com s'enllaçaran.



L'arquitectura de seguretat perimetral per a la LAN corporativa es descriu gràficament en aquest esquema adjunt. En aquest primer apartat descriurem únicament l'arquitectura de la xarxa i no ens centrarem en les interfícies i els diferents adreçaments. Podem observar diferents elements de seguretat establerts en l'entorn. La connexió de l'exterior a la xarxa es reb per mitjà d'un border router que redirigeix tot el tràfic destinat a la xarxa corporativa de TecnoHack. Els diferents serveis que ha d'oferir l'empresa a l'exterior s'han situat en una subxarxa independent de la LAN corporativa per garantir la robustesa de l'entorn. És a dir, els serveis que ofereix l'empresa (mail i web) s'ubiquen en una subxarxa independent anomenada DMZ o "zona desmilitaritzada". Aquesta zona és accessible tant per qualsevol host de Internet com per qualsevol host de la LAN interna. Donat que aquests serveis seran accessibles per tothom, per això no s'han establert en la mateixa LAN, sinó que s'estableix un mur de seguretat entre ambdues subxarxes. La política de seguretat garantirà que des de la subxarxa DMZ no es pugui fer cap accés cap a la LAN o cap a l'exterior, a no ser paquets que siguin resposta a peticions rebudes. D'aquesta forma, ningú de l'exterior podrà accedir a la LAN per mitjà de la DMZ.

Per altra banda, el servidor de ftp no s'ha situat en la DMZ dels altres dos servidors, donat que el servidor de ftp no ha de ser accedit per qualsevol host d'Internet, sinó només per comercials de l'empresa, per la qual cosa s'utilitzarà, tal i com es comentarà posteriorment, una subxarxa addicional protegida per mitjà de VPN.

Pel que fa al servidor de bases de dades, aquest només ha de ser accedit per determinats usuaris de la LAN corporativa, la qual cosa implica que es situarà de forma que tingui accés exclusiu per a ús intern.

Els mecanismes per tal d'assegurar seguretat en aquest disseny són dos firewalls. El primer firewall s'encarrega de permetre l'accés a la DMZ a qualsevol usuari, però només als ports establerts, i de prohibir qualsevol accés a la xarxa interna per part de l'exterior, permetent això sí que els usuaris de la LAN corporativa tinguin ple accés a Internet.

El segon firewall s'ha decidit establir-lo com un element redundant de seguretat, per si hi hagués qualsevol possible fallida en el primer firewall. En aquest supòsit, es tindria ple accés als serveis de la DMZ des de l'exterior, però el segon firewall vetllaria per la seguretat dels hosts de la LAN interna. Aleshores, el funcionament del segon firewall es basa en permetre únicament que els usuaris de la xarxa interna puguin accedir tant a Internet com als serveis de la DMZ, però estigui prohibit qualsevol accés des de l'exterior cap a aquesta xarxa. Es sobreentén que el tràfic generat des de l'exterior en resposta a una petició de la xarxa interna sí s'accepta, el tràfic prohibit de l'exterior cap a la subxarxa s'entén que és el tràfic originat inicialment per peticions exteriors, a les quals no es permetrà cap concessió per tal de garantir la plena integritat de la LAN. Aquest segon firewall redirigeix a més el tràfic cap al servidor de ftp (per mitjà del VPN). A aquest destí ja s'aplica filtre des del primer firewall.

El tercer firewall garanteix l'accés exclusiu al servidor de bases de dades per part dels usuaris de la LAN, i només permetent el tràfic dirigit al port de la base de dades, així com exclouent tot aquell tràfic generat des del servidor en vers a la LAN que no sigui en resposta a una petició anterior. S'eviten doncs les intrusions a la LAN per totes les vies possibles.

Un element de seguretat addicional és el VPN (Virtual Private Network), aplicat arrel de la necessitat dels comercials de poder accedir a un servei (ftp) per a ús exclusiu dels treballadors interns de l'empresa, situats en la LAN corporativa. Cal tenir en compte que els comercials tindran molta mobilitat i no estaran situats en la LAN sinó que desitjaran accedir al servidor de FTP des de qualsevol punt d'Internet. El VPN proporciona doncs, l'accés virtual a una LAN protegida per mitjà de canal segur, emprant un canal no segur (Internet). Això és possible gràcies a l'establiment d'una connexió segura establerta inicialment amb autenticació i claus criptogràfiques, per la qual cosa una vegada configurat el tunel segur, els comercials podran accedir al servei de ftp com si fossin a la LAN interna de l'organització. En autenticar-se amb VPN, es pren ple control de tota la subxarxa, no només d'un host, motiu pel que s'ha situat el servidor de bases de dades en una altra subxarxa, per tal d'aplicar-hi VPN.

2.- Adreçaments, interfícies de xarxa i NAT.

En aquest segon apartat es defineixen en detall les diferents interfícies del sistema i els diferents mètodes emprats per fer l'enrutament d'informació entre els ordinadors de la xarxa interna i l'exterior.

La xarxa global es troba dividida en 4 subxarxes:

- 192.168.2.0/24: DMZ a on es situen els servidors públics. Accessible des d'Internet i des de la LAN de treballadors, no es permetran connexions en sentit contrari.
- 192.168.4.0/24: DMZ a on es situa el servidor FTP. Accessible des de la LAN de treballadors sense necessitat de VPN i accessible des d'Internet establint un canal amb el VPN (Virtual Private Network). Com no podem fer un filtratge per IP dels comercials externs per la seva mobilitat, la millor opció es utilitzar un VPN i així garantim un accés autenticat i xifrat.

- 192.168.3.0/24: Subxarxa a on es situa el servidor de bases de dades. Es troba darrera d'un firewall per augmentar el nivell de seguretat respecte als propis usuaris de la LAN de treballadors, es possible que tinguem treballadors temporals o persones de poca confiança accedint directament a la LAN i es convenient protegir mínimament el servidor de bases de dades.
- 192.168.1.0/24: LAN dels treballadors, aquí es situen totes les estacions de treball.

El firewall que es troba directament connectat al router que té accés a Internet es qui s'encarrega de fer el NAT (Network Address Translation), donat que és l'últim element que disposa de IP pública, i per tant tradueix les adreces locals dels hosts de la LAN corporativa a l'adreça pública:

- NAT Dinàmic: Permetrà que les estacions de treball de la nostra LAN amb adreces IP privades puguin establir connexions amb servidors d'Internet, encarregant-se de la traducció d'IP per connexió establerta. Aleshores, s'utilitza NAT Dinàmic per fer la traducció d'adreces de la LAN Corporativa (on s'empren adreces privades) cap a l'exterior, on només s'empra una única adreça pública. El concepte de NAT Dinàmic fa referència al fet de què cal traduir múltiples adreces de una LAN privada per mitjà d'una única adreça pública, pel que caldrà tenir cura d'emmagatzemar l'origen privat de cada paquet que surt a l'exterior, per tal de poder retornar la resposta al host concret de la LAN privada que ha originat la petició. Tots els hosts de la LAN traduiràn la seva adreça privada per mitjà d'una única adreça pública.
- NAT Estàtic: Quan rebí la petició d'establir una connexió a una adreça IP pública determinada, aquesta serà redirigida al servidor corresponent sempre i quan es compleixin les regles de filtratge. El NAT Estàtic s'aplica en el cas de tenir el mateix nombre de hosts interns com d'adreces públiques, amb el que únicament es fa una regla d'enrutament per a cada element i cada adreça pública. Tindrem doncs adreces públiques per als tres serveis als que es permet accés extern (Web i Mail des de la DMZ, i VPN per accedir al FTP des de la xarxa separada de la DMZ).

3.- Taules de regles.

Suposem que les respostes a connexions ja establertes són permeses automàticament. Es a dir, si el firewall 1 permet establir connexió al servidor web, la resposta en sentit contrari es acceptada sense haver de ficar una regla específica.

Firewall 1

eth0: IP pública

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	INBOUND	Drop	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	0	0.0.0.0	0	ALL	IPs reservades	
1	INBOUND	Forward 192.168.2.4:80	0.0.0.0	0	IP pública	80	TCP	Servidor web	
2	INBOUND	Forward 192.168.2.4:443	0.0.0.0	0	IP pública	443	TCP	Servidor HTTPS	
3	INBOUND	Forward 192.168.4.3:VPN	0.0.0.0	0	IP pública	VPN	TCP	Servidor VPN	
4	INBOUND	Forward 192.168.2.3:25	0.0.0.0	0	IP pública	25	TCP	Servidor SMTP	
5	INBOUND	Forward 192.168.2.3:110	0.0.0.0	0	IP pública	110	TCP	Servidor POP3	

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
6	OUTBOUND	Allow	IP públiques	0	!10.0.0.0/8 !172.16.0.0/12 !192.168.0.0/16	0	ALL	LAN a Internet	
7	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

NOTA 1: La regla 0 impedeix que es rebí tràfic amb adreces origen privades per una interfície en la que només esperem rebre paquets amb adreces font públiques. Així evitem que es puguin fer atacs en que es modifiqui l'adreça IP font per fer veure que prové d'un host de la LAN privada, amb la conseqüent possible fallida de seguretat si intentessin accedir amb aquests paquets modificats a serveis com la base de dades privada. Aquesta regla no es estrictament necessari però dona major robustesa.

NOTA 2: La regla 6 suposa que prèviament s'ha realitzat el NAT i per tant l'adreça font ja no correspon a una IP privada de la LAN sinó a una IP pública.

eth1: 192.168.2.1

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	INBOUND	NAT	192.168.1.0	0	!10.0.0.0/8 !172.16.0.0/12 !192.168.0.0/16	0	ALL	NAT Dinàmic	
1	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

NOTA: El símbol ! s'ha d'interpretar com una negació (NOT).

Firewall 2

eth0: 192.168.2.2

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	INBOUND	Allow	0.0.0.0	0	192.168.4.3	VPN	TCP	Servidor VPN	
1	OUTBOUND	Allow	192.168.1.0	0	!10.0.0.0/8 !172.16.0.0/12 !192.168.0.0/16	0	ALL	LAN a Internet	
2	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

eth1: 192.168.4.1

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

eth2: 192.168.1.1

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	OUTBOUND	Allow	192.168.1.0	0	!10.0.0.0/8 !172.16.0.0/12 !192.168.0.0/16	0	ALL	Lan a Internet	
1	INBOUND	Allow	192.168.1.0	0	192.168.2.4	80	TCP	Servidor web	
2	INBOUND	Allow	192.168.1.0	0	192.168.2.4	443	TCP	Servidor HTTPS	
3	INBOUND	Allow	192.168.1.0	0	192.168.4.3	21 20	TCP	Servidor FTP	
4	INBOUND	Allow	192.168.1.0	0	192.168.2.3	25	TCP	Servidor SMTP	

Num regla	Direccio	Accio	Origen	Port orig.	Destí	Port destí	Protocol	Descripció	Logs
5	INBOUND	Allow	192.168.1.0	0	192.168.2.3	110	TCP	Servidor POP3	
6	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

Firewall 3

eth0: 192.168.3.2

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	INBOUND	Allow	192.168.1.0	0	192.168.3.0	3306	TCP	Servidor MySQL	
1	INBOUND	Allow	192.168.1.0	0	192.168.3.0	3306	UDP	Servidor MySQL	
2	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

eth1: 192.168.3.1

Num regla	Direccio	Accio	Origen	Port orig	Destí	Port destí	Protocol	Descripció	Logs
0	ALL	Drop	0.0.0.0	0	0.0.0.0	0	ALL	Prohibit altres	

4.- Firewall builder.

Veure fitxer adjunt.

5.- Marques de firewall/routers.

Es important que hi hagi diversitat a la xarxa, hauriem de tindre firewalls, routers i servidors amb diferents sistemes operatius i marques. D'aquesta forma si apareix una vulnerabilitat per a un sistema concret, no ens veurem afectats massivament.

Configuració d'exemple:

Servidor FTP: OpenBSD + proftpd
 Servidor Mail: GNU/Linux + exim + qpopper
 Servidor Web: FreeBSD + Apache
 Servidor Bases de dades: NetBSD + MySQL

Firewall 1:

Zyxel ZyWALL 100



<http://www.zyxel.com/product/model.php?indexcate=1022045333&indexcate1=1085450410&indexFlagvalue=1021873683>

Firewall 2:

Cisco PIX 535



<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2119/index.html>

Firewall 3:

Fortinet FortiGate-500



<http://www.fortinet.com/products/enterprise.html>

VPN:

SonicWALL's PRO 3060/4060



<http://www.sonicwall.com/industries/enterprise.html>

Autors:

Francisco José Aguilar Celdrán.

Sergio Blanco Cuaresma.

Tarragona, 15 d'Octubre de 2004.