



GUIA D'ADMINISTRACIÓ DE TALLAFOCS

Índex

3 . . . Qui fem aquesta guia

5 . . . Introducció

5 . . . Audiència

5 . . . Abast

5 . . . Aspectes legals i normatius

7 . . . Una visió general de l'arquitectura

**10 . . . Amenaces presents en l'ús
d'aquesta tecnologia**

10 . . . Errors de configuració

11 . . . Accés no autoritzat

12 . . . Recomanacions

12 . . . Recomanacions per prevenir
errors de configuració

13 . . . Recomanacions per prevenir
l'accés no autoritzat

14 . . . Conclusions

15 . . . Glossari

16 . . . Referències i enllaços web

16 . . . Eines

Qui fem aquesta guia

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
- Donar suport a la protecció de les infraestructures crítiques TIC nacionals
- Promocionar un teixit empresarial català sòlid en seguretat TIC
- Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

El contingut de la present guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecta a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà mitjançant la inclusió de la següent menció:



Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.


Llicenciada sota la llicència CC BY-NC-ND.

La present guia es publica sense cap garantia específica sobre el contingut.





L'esmentada llicència té les següents particularitats:


Vostè és lliure de:

 Copiar, distribuir i comunicar públicament la obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de la obra de la manera especificada per l'autor o el llicenciador (en tot cas no de manera que suggereixi que gaudeix del seu suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Respecte d'aquesta llicència caldrà tenir en compte el següent:

■ **Modificació:** Qualsevol de les condicions de la present llicència podrà ser modificada si vostè disposa de permisos del titular dels drets.

■ **Altres drets:** En cap cas els següents drets restaran afectats per la present llicència:.

■ Els drets del titular sobre els logots, marques o qualsevol altre element de propietat intel·lectual o industrial inclòs a les guies. Es permet tan sols l'ús d'aquests elements per a exercir els drets reconeguts a la llicència.

■ Els drets morals de l'autor.

■ Els drets que altres persones poden tenir sobre el contingut o respecte de com s'empra la obra, tals com drets de publicitat o de privacitat.

Avis: En reutilitzar o distribuir la obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.

El text complert de la llicència pot ser consultat a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>.

Introducció

Audiència

Aquesta guia està adreçada als administradors i responsables de sistemes d'Universitats i Centres de Recerca, Administracions públiques catalanes i PIME que utilitzen tallafocs a la seva xarxa.

De la mateixa manera, qualsevol organització que tingui en ment implantar un sistema de Gestió per a la Seguretat de la Informació trobarà interessant i útil el conjunt de bones pràctiques recollides en aquesta guia.

Abast

La finalitat d'aquest document és assolir unes bones pràctiques en seguretat de la informació aplicades a l'administració de tallafocs. Aquests dispositius protegeixen els serveis i usuaris de la xarxa, separen els diferents segments que la componen i representen un mur de contenció entre l'organització i Internet, per la qual cosa els tallafocs són la base de la seguretat perimetral i interna.

Aspectes legals i normatius

La present guia s'ha elaborat tenint en compte les recomanacions provinents de l'estàndard internacional ISO 17799, que queden recollides als controls següents:

- 6.1.3 Assignació de les responsabilitats en la Seguretat de la Informació.
- 10.1.2 Gestió dels canvis.
- 10.1.3 Segregació de funcions.
- 10.2.1 Prestació del servei.

- 10.5.1 Còpies de seguretat de la informació.
- 10.6.1 Controls de xarxa.
- 10.6.2 Seguretat dels serveis de xarxa.
- 11.4.1 Política d'ús dels serveis de xarxa.
- 11.4.6 Control de connexió a la xarxa.
- 11.5.1 Processos de connexió segurs.
- 11.6.1 Restricció d'accés a la informació.

Una visió general de l'arquitectura

Tant la natura com els éssers humans al llarg de la història han construït defenses per protegir els actius més valuosos, des de les costelles que protegeixen el cor i els pulmons dins del nostre cos, fins a les muralles que envoltaven i encara envolten algunes de les nostres ciutats.

En aquest sentit, no hi ha diferències dins el món de les tecnologies de la informació i les comunicacions, on aquestes defenses es reuneixen sota diverses formes i on els tallafocs són l'element principal que separa els actius més importants de les mans més malicioses.

Els tallafocs són uns dispositius que controlen les comunicacions que flueixen a través seu i que permeten segmentar la xarxa i aplicar la política de seguretat més enllà dels equips, tot arribant als fluxos d'informació entre els sistemes interns i vers Internet. Parlem, doncs, d'un element clau en la defensa perimetral de la nostra xarxa, perquè ens permetrà controlar com accedim a la resta de xarxes internes -especialment als sistemes crítics-, a Internet i, alhora, ens ajudarà a defensar els nostres serveis de qui intenti accedir-hi il·legítimament des de l'exterior.

Les característiques més rellevants per a un tallafocs són les que permeten les funcionalitats següents:

- **Filtratge de paquets entrants i sortints:** aquesta és sens dubte la característica principal dels tallafocs i consisteix en l'aplicació de regles de filtratge on, en funció del tipus de trànsit que estigui creuant el dis-

positiu, s'aplicarà una política de seguretat o una altra. Uns exemples en serien els següents:

- Permetre l'entrada de paquets al nostre servidor Web mitjançant el protocol HTTP.
- Denegar l'entrada de paquets des de l'exterior a qualsevol altre port del servidor Web.
- Denegar la sortida de paquets cap a Internet si no es realitza pels ports 80 (HTTP) o 443 (HTTPS).

■ **Invisibilitat:** la invisibilitat és la capacitat de fer indetectables els actius que hi ha presents dins la xarxa interna de l'organització, gràcies a la presència del tallafocs entre la part més externa de la xarxa interna i la sortida a Internet, que bloqueja els paquets de trànsit destinats a originar una resposta dels diferents actius i, així, saber que existeixen.

■ **DMZ:** una altra funcionalitat que proporciona un tallafocs és la creació d'una DMZ o Zona Desmilitaritzada (Demilitarized Zone) on ubicar els actius i serveis de l'organització que cal que siguin visibles des d'Internet, però que, al mateix temps, han de disposar d'una protecció bàsica per evitar que algú extern a l'organització en pugui fer un mal ús.

■ **NAT (Network Address Translation):** conversió d'adreces IP públiques en adreces IP privades de manera que molts actius d'una organització, mitjançant la compartició d'IP públiques, puguin accedir a Internet i, així, reduir el cost de l'organització en l'adquisició d'IP públiques per al seu ús. Aquesta característica també facilita el control del trànsit exterior

cap a la xarxa interna, ja que permet bloquejar totes les connexions entrants cap a IP internes no autoritzades explícitament.

■ **Encaminament:** readreçament intern intencionat de les comunicacions que traspassen els tallafocs cap a destí, d'acord amb la configuració de regles que l'organització hagi aplicat al dispositiu. Així s'aconsegueix controlar les rutes per on viatgen els paquets entre les diferents xarxes i subxarxes internes i, alhora, es facilita l'aïllament dels actius considerats crítics per l'ens respecte d'altres menys importants com podrien ser les estacions de treball dels usuaris.

■ **Monitoratge:** els tallafocs disposen de registres on consultar com es comporta el trànsit que els travessa, facilitant així les tasques d'auditoria, manteniment i millora de la seguretat proporcionada pel tallafocs.

La complexitat de la seguretat a les xarxes provoca que els tallafocs, per poder oferir una defensa coherent i completa, hagin de comptar paral·lelament amb elements addicionals com detectors i previsors d'intrusions, interceptors de codi maliciós i correu brossa, etc., la qual cosa va fer sorgir els primers dispositius anomenats UTM (de l'anglès Unified Threat Management), que inclouen tot un seguit de complements com els esmentats que acompanyen les funcions tradicionals del tallafocs.

Aquesta visió dels tallafocs ha evolucionat en els darrers anys cap al concepte de "tallafocs de nova generació", que es basa en poder aplicar les polítiques de seguretat

de xarxa, no només als paquets, ports i IP, sinó a aplicacions i usuaris concrets.

Exemple de regla en un tallafocs tradicional:

- L'adreça IP 192.168.0.5 no ha de poder comunicar-se amb el servidor xx.xx.xx.xx pel port 80.

Independentment del model, l'administració dels tallafocs ha de permetre assolir les directrius i polítiques de seguretat internes marcades per la pròpia organització, amb l'objectiu de defensar-la de les amenaces existents.

Amenaces presents en l'ús d'aquesta tecnologia

Errors de configuració

Segons Gartner^[1], la probabilitat d'una incidència als nostres sistemes depèn fonamentalment dels errors humans en les configuracions (40%).

Un tallafocs és un dispositiu de seguretat perimetral, la primera línia de defensa. Donada la seva funció, l'organització ha de minimitzar el risc que es produeixin errors de configuració directament vinculats a aquests tipus de dispositius, ja que podrien comprometre l'aïllament de la xarxa interna, d'altres subxarxes i d'Internet.

Els elements de seguretat funcionen millor i estan més optimitzats si es configuren com a conjunt i no com a elements inconnexos. Per aquest motiu, és important que tota organització defineixi una Política de Seguretat com a marc de treball on s'estableixi quin és el nivell de seguretat que es vol assolir i com els tallafocs, com a elements de seguretat que són, han de contribuir a assolir aquest nivell de seguretat en conjunt.

La complexitat de les regles que es poden configurar en un tallafocs pot ser elevada i pot provocar conflictes que dificultin la identificació posterior de l'origen d'algun problema, sobretot quan s'han dut a terme modificacions en les configuracions del dispositiu —ja siguin programades o accidentals, per haver accedit al sistema amb permisos totals, en lloc d'operar amb un identificador amb menys permisos—, o producte de peticions internes de les quals no es manté un registre i control que permeti analitzar-ne la compatibilitat tant amb

la Política de Seguretat vigent a l'organització com amb l'actual configuració dels sistemes d'informació en xarxa.

Igual d'important és tenir la capacitat de tornar l'actiu a l'últim estat estable si pateix una contingència, ja sigui per un mal funcionament, per algun tipus d'error humà, etc. Com més completes siguin les còpies de seguretat de què disposa l'organització, més ràpid es disposarà de nou de l'actiu a producció.

Aquest dispositiu es pot proporcionar al client amb una instal·lació per defecte. És important recordar que les configuracions de fàbrica no es poden considerar segures, doncs sovint:

- No disposen dels últims pegats de seguretat proporcionats pel fabricant: el sistema està exposat a vulnerabilitats conegudes i explotables per tercers.
- Hi ha configurats comptes d'accés al sistema amb identificadors i contrasenyes per defecte, coneguts i difosos a través d'Internet.

Accés no autoritzat

Els tallafocs són la base sobre la qual una organització construeix la seva seguretat. Per tant, aquests actius es converteixen en crítics per a l'organització on es troben.

Un dels principals riscos als quals es troba subjecte tot actiu important d'una organització és el fet que algú vulgui accedir-hi, tot i no estar-hi autoritzat.

Si a l'organització s'utilitzen contrasenyes febles, és

a dir, contrasenyes construïdes amb pocs caràcters o basades en paraules que podem trobar en diccionaris (amb independència de l'idioma utilitzat) es facilita que puguin ser descobertes i utilitzades per tercers que vulguin accedir al sistema. El mateix succeeix si per construir la contrasenya utilitzem sèries lògiques i comunes, com per exemple, "abcdefg", "12345678", "abc123", etc.

Intercanviar contrasenyes robustes mitjançant canals de comunicació no segurs també en facilita el descobriment. Per exemple, si utilitzem serveis d'administració que utilitzen comunicacions no encriptades, com pot ser obrir sessions FTP o Telnet, en lloc d'utilitzar els seus homònims encriptats (SFTP i SSH, respectivament), o bé utilitzar formularis d'autenticació web sense mecanismes d'encriptació (utilitzar HTTP en comptes de HTTPS). Igualment, es facilita l'accés no autoritzat al tallafocs si la interfície de gestió és la mateixa que la interfície de producció.

Recomanacions

Aquest seguit d'amenaçes, si es materialitzen al llarg del temps, en major o menor mesura, tindran efectes perjudicials per a l'organització a la qual pertanyen. Per tal d'evitar que això succeeixi o minimitzar-ne l'efecte, si és que l'amenaça no pot evitar-se totalment, a continuació es proporcionen tot un conjunt de recomanacions dirigides als responsables i administradors de tallafocs.

Recomanacions per prevenir errors de configuració

És durant la instal·lació i configuració dels tallafocs que poden aparèixer les primeres amenaces. Per això, la persona responsable de la instal·lació i posada en servei del sistema ha de tenir en compte les recomanacions següents:

- Adequar la configuració de les regles del tallafocs a la Política de Seguretat interna de l'organització.
- Aplicar regularment les actualitzacions i els pegats de seguretat que publiquen els fabricants.
- Personalitzar les configuracions per defecte. Principalment, cal canviar la contrasenya per una de personalitzada als comptes d'accés que es configuren automàticament durant la instal·lació del producte.
- Accedir al sistema amb un identificador personal i no com a administrador o usuari primari (root).
- Sol·licitar autoritzacions formals dels responsables corresponents sempre que s'hagin de fer canvis en les regles de seguretat dels tallafocs o quan aquests hagin de ser retirats de l'entorn de producció.

- Establir un sistema de gestió del canvi per tal que quedi constància de tota modificació i baixa de dispositius de seguretat, com són els tallafocs. Un bon sistema de gestió del canvi haurà de tenir present:

- Documentar la informació següent per cada canvi que es porti a terme: data, hora, qui ho sol·licita, qui ho aprova, motiu del canvi, risc, impacte i com desfer els canvis si no proporcionen els resultats esperats.
- Ser útil a l'hora d'identificar si un canvi recent pot ser el causant d'un funcionament anòmal del dispositiu.

- Establir una Política de Còpies de Seguretat[3] per a la informació corporativa d'acord amb els diferents nivells de criticitat de la informació.

- Establir una Política de Recuperació de la Informació[3] per tal de garantir la correcta recuperació de la informació perduda, així com el correcte estat i manteniment de les còpies de seguretat i els suports físics utilitzats.

Altres recomanacions que cal tenir en compte per tal de preservar la seguretat en els accessos al sistema són les següents:

- A causa de la naturalesa del dispositiu, no accedir-hi utilitzant protocols de comunicacions no segurs. En lloc d'això, utilitzar protocols estàndard o propietaris que utilitzin mecanismes d'encriptació.

- Sempre que sigui possible, utilitzar la consola de gestió per a les tasques administratives. Si no es disposa de consola de gestió, utilitzar una interfície dedicada a l'administració que sigui diferent de les interfícies utilitzades per donar servei (interfícies productives).

- Fer un ús adequat dels usuaris, grups i permisos dels usuaris i grups sobre els fitxers de configuració per tal de mantenir la confidencialitat i integritat de les dades.

Recomanacions per prevenir l'accés no autoritzat

En primer lloc, cal implementar una **política de contrasenyes coherent i robusta**, preservar la privacitat de les contrasenyes i controlar-ne la vigència. La guia publicada pel CESICAT "Guia per gestionar les contrasenyes"^[2] és una bona referència en aquest sentit, però no es tracta d'una guia de màxims. És a dir, segons la importància que tingui l'actiu per a l'organització on es troba, es pot implementar una política encara més estricta que la recomanada a la guia esmentada anteriorment.

Conclusions

La seguretat és una cadena tan forta com l'esglaó més feble.

Els tallafocs són un element clau per a una infraestructura de xarxa segura, una part de l'engranatge que fa funcionar amb garanties els diferents processos de l'organització, però s'ha de tenir present que només amb la seva presència i un manteniment adequat no s'assoleix un nivell òptim de seguretat.

Hem vist que, per tal que aquest engranatge funcioni, cal cuidar-ne la configuració i el manteniment, tot establint uns criteris marc de seguretat corporatius, aplicant regularment les actualitzacions recomanades pels fabricants, i eliminant totes aquelles configuracions no personalitzades pel propi equip tècnic de l'ens.

Disposar d'una Política de Seguretat permetrà establir les bases de coses tan importants com:

- Regular quins seran els serveis de xarxa que hauran d'estar disponibles per als diferents col·lectius d'usuaris, ja siguin propis de l'organització, subcontractats o usuaris d'Internet.
- Qui haurà de tenir capacitat per accedir als tallafocs i amb quin nivell de privilegis.
- Quina política de seguretat és la més adequada per a dispositius com els tallafocs.
- Quina política de contrasenyes és la més adequada per a dispositius com els tallafocs.
- Quina política per gestionar els canvis de configuració és la més adequada per a dispositius com els tallafocs.

- Quina política de revisió i actualització del dispositiu és la més adequada per a aquest tipus de dispositius.
- Quan és imprescindible utilitzar protocols de comunicació xifrats i quan no és necessari.
- Etc.

També cal tenir present que les coses més simples són les que millor funcionen. Per tant, no per tenir moltes regles configurades en un tallafocs estarem més protegits. El que cal és que aquestes regles s'adeqüin als nostres serveis de xarxa i regulin allò que realment és imprescindible controlar i/o aïllar.

Glosari de termes

HTTP: el protocol de transferència d'hipertext o HTTP (Hypertext Transfer Protocol) estableix el protocol per a l'intercanvi de documents d'hipertext i multimèdia al web.

HTTPS: Hypertext Transfer Protocol sobre Secure Socket Layer és la capçalera utilitzada per a indicar una connexió segura HTTP. És sintàcticament idèntica a la capçalera `http://`, normalment utilitzada en l'accés de recursos fent servir HTTP. Utilitzar `https:` indica que s'utilitzarà HTTP, però amb un port TCP predeterminat diferent (el 443) i una capa d'encriptació/autenticació entre HTTP i TCP.

FTP (File Transfer Protocol): el protocol de transferència de fitxers o FTP és un programari estandarditzat per enviar fitxers entre ordinadors amb qualsevol sistema operatiu. Forma part de la capa d'aplicació del model TCP/IP.

SFTP (SSH File Transfer Protocol): SFTP és un protocol de xarxa que proporciona la funcionalitat necessària per a la transferència i manipulació d'arxius sobre un flux de dades de confiança. S'utilitza habitualment amb SSH per proporcionar seguretat a les dades, tot i que es pot usar amb altres protocols de seguretat. La seguretat, doncs, no és inherent al protocol SFTP, sinó a SSH o el protocol que s'utilitzi amb aquesta fi.

SSH (Secure Shell): programari que permet establir una sessió amb un equip remot i administrar-lo mitjançant un indicador d'ordres. Encrypta la comunicació entre el client i el servidor per evitar que sigui desxifrada si s'intercepta.

TELNET: protocol que proporciona l'habilitat d'executar ordres d'usuari en un equip de forma remota.

Aquest protocol és insegur perquè envia tant l'autenticació de l'usuari com les ordres en text net per la xarxa.

Referències i enllaços web

S'han utilitzat com a referència en l'elaboració d'aquesta guia:

GE-GUI21-02 Administració de tallafocs al nus corporatiu de la Generalitat de Catalunya, del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI).

[2] **Guia per gestionar les contrasenyes**, CESICAT, febrer de 2010.

[PDF] <http://www.cesicat.cat>

[3] **Guia de còpies de seguretat**, CESICAT, febrer de 2010.

[PDF] <http://www.cesicat.cat>

A Internet s'hi pot trobar informació rellevant, relacionada amb la matèria desenvolupada en aquesta guia:

[1] **High Availability Q&A: Failures, Standards and Metrics**, Gartner, juliol de 1998

<http://www.gartner.com/webletter/ibmglobal/edition2/article5/article5.html>

Firewall Best Practices, by Kevin Beaver CISSP, 2009

[PDF] http://www.principlelogic.com/docs/Firewall_Best_Practices.pdf

Magic Quadrant for Enterprise Network Firewalls,

GARTNER, març de 2010

[PDF] http://www.vadition.com/pdf/Gartner_Magic_Quadrant_Firewalls_2010.pdf

Security Guide: Firewall Best Practices, Steven Warren, MCSE, MCDBA, març de 2002

<http://www.zdnet.com.au/security-guide-firewall-best-practice-120263895.htm>

Eines

Eines comercials

Check Point Software Technologies

Líder del mercat dels tallafocs empresarials, CheckPoint ofereix una gran varietat de plataformes amb la flexibilitat dels Software Blades per implementar sistemes UTM a mida.

<http://www.checkpoint.com/>

Juniper Networks

Els tallafocs de Juniper Networks són els principals competidors del mercat, compten amb característiques UTM i estan representats en diverses famílies, com ara els SRX o els SSG.

<http://www.juniper.net/es/es/products-services/security/>

Cisco

La família Adaptive Security Appliance (ASA) de Cisco és l'aposta principal en el camp dels tallafocs d'aquest líder mundial de les comunicacions de xarxa. La integració amb xarxes Cisco és una de les seves principals virtuts, a banda de poder incorporar funcionalitats com SSL VPN i IPS.

<http://www.cisco.com/go/asa>

Fortinet

Els productes FortiGate de Fortinet són tallafocs de tipus UTM amb tecnologia d'altres prestacions basada en ASIC. Pot incloure: IPS, Antivirus/Antispyware/Antimalware, AntiSpam, filtratge web, IPSEC VPN, inspecció SSL, optimització WAN, control d'aplicacions i d'altres.

<http://www.fortinet.com/products/fortigate/>

Paloalto Networks

Tallafocs de nova generació especialitzat en la identificació i el filtratge d'aplicacions, usuaris i amenaces. Ha revolucionat el mercat tradicional dels tallafocs.

<http://www.paloaltonetworks.com/>

Eines gratuïtes

Netfilter/Iptables

Netfilter/Iptables és un tallafocs que incorpora Linux en al nucli per realitzar funcions de filtratge, traducció d'adreces (NAT), qualitat de servei i encaminament, entre d'altres.

<http://www.netfilter.org/>



Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat