Sicurezza nelle reti

Filtraggio dei contenuti

Filtri

- Filtri IP
  - Servono ad autorizzare o vietare dei link
- Filtri sui contenuti
  - Permettono di filtrare i contenuti
    - Permettono di limitare i comandi accettati (ad esempio impediscono i GET in FTP)
    - Permettono di limitare i materiali scaricati (ad esempio nessun file *.eml o *.nws)

SQUID

- Significa calamaro
- E' un proxy applicativo
- Scopo originario è gestire una cache per ridurre il traffico
- Permette di introdurre Access Control Lists per decidere cosa lasciar leggere ed a chi
- Permette di loggare l'attività fatta sul WEB

Installazione squid

- Si installa in qualsialsi distribuzione usando i sistemi automatici
  - SuSE / RedHat tramite rpm
  - Debian tramite apt-get

Configurazione Squid

- Si configura editando un solo file
  - File di testo
  - Normalmente /etc/squid/squid.conf
  - Esiste un manuale in italiano in http://merlino.merlinobbs.net/Squid-Book
  - Varie sezioni illustrate qui di seguito
  - Quella che segue è una guida per l'utente impaziente ricavata dal manuale di cui sopra

Opzioni di rete di squid

- TAG con i numeri di porta
  - http_port 3128
    - HTTP per le normali richieste
  - icp_port 3130
    - ICP per il coordinamento gerarchico di più cache
- Alternativache permette di specificare più indirizzi IP e numeri di porta
  - http_port 1.2.3.4:3128
  - http_port 1.2.3.5:8080

Controllo cache di Squid

- cache_peer proxy.dmn.com type 8088
  - Solo se ci si apppoggia ad un proxy esterno, type vale sybling o parent
- cache_mem x MB
  - quantità di memoria massima usata, non dovrebbe mai superare 1/4 della memoria fisica installata sulla macchina
- maximum_object_size yy Kb
  - Massima dimensione oggetto cacheato

Memorizzazione cache squid

- cache_dir ufs /path MB L1 L2
  - Definisce dov'è situata la cache (/path)
  - Definisce la dimensione (MB)
  - L1 = numero di cartelle di primo livello
  - L2 = numero di cartelle di secondo livello
- cache_dir ufs /ciccio 100 10 10

Log files di Squid

- cache_access_log /squid/logs/access.log
  - Transazioni effettuate dai client
- cache_log /squid/logs/cache.log
  - Informazioni sullo stato della cache
- cache_store_log /squid/logs/store.log
  - Attività storage manager di Squid

Opzioni di log di Squid

- emulate_httpd_log on
  - Permette di emulare un log http se lo squid è usato come un reverse proxy
- mime_table /squid/etc/mime.conf
  - percorso della tabella dei mime type, tale tabella contiene gli esempi standard di mime type nella formattazione più comune
- pid_filename /squid/logs/squid.pid
  - nome del file che contiene il numero di processo di Squid

Parametri amministrativi

- cache_mgr nmaster@dominio.com
  - indirizzo di posta elettronica dell'amministratore del proxy
- visible_hostname proxy1.dominio.com
  - nome dell'host visualizzato da Squid nel caso si incontri un messaggio di errore o di semplice messaggio amministrativo

Redirector

- redirect_program /bin/squid_redirect
  - è possibile specificare il percorso di un file eseguibile esterno a Squid al quale è possibile reindirizzare tutte le richieste HTTP
  - il programma esterno può funzionare anche da filtro facendo passare solo le richieste che soddisfino determinate regole
  - uno dei programmi redirector più famosi ed utilizzati è squidGuard.

Analisi del traffico

- Si può fare
  - Abilitando SNMP
  - Creando delle ACL in Squid
  - Attivando MRTG per produrre grafici del traffico
- E' spiegato nel manuale
  - Anche nelle sezioni di configurazione veloce

Controlli di accesso - ACL

- Le access control list vengono definite per impostare svariati livelli di controllo per l'accesso al proxy server Squid
- E' possibile impostare diversi tipi di acl
- Il formato utilizzato da Squid nella realizzazione delle acl è
  - acl nomeacl tipoacl stringa1 ...
  - acl nomeacl tipoacl "file" ...

Esempi di ACL (1)

- acl SSL_ports port 443 563
  - Porte gestite con SSL
- acl Safe_ports port 80 21 443 563 70 210 1025-65535
  - Porte utilizzabili

Esempi di ACL (2)

- acl localhost src 127.0.0.1/255.255.255.255
  - query in locale
- acl allowed_hosts src 192.168.0.0/255.255.255.0
  - Host della rete locale
- acl all src 0.0.0.0/0.0.0.0
  - Tutti gli host possibili ed immaginabili

Esempi di ACL (3)

- icp_access allow allowed_hosts
- icp_access deny all
  - Le due ACL qui sopra
    - permettono l'accesso alle funzionalità del proxy agli allowed_hosts definiti nella slide precedente
    - Negano l'accesso a qualunque altro host usando il nomeacl all definito nella slide precedente

Esempi di ACL (4)

- acl manager proto cache_object
  - Protocollo di gestione degli oggetti (ICP)
- acl CONNECT method CONNECT
  - Metodo connect (usato da SSL) (è uno dei metodi HTTP assieme a GET/PUT….)

Esempi di ACL (5)

- http_access allow allowed_hosts
  - Si a tutti gli host della rete locale (definiti prima)
- http_access deny manager all
  - No al manager da qualunque parte lo si chieda
- http_access deny all
  - No al caching da tutti (meno a quelli precedentemente garantiti)

Esempi di ACL (6)

- http_access deny !Safe_ports
  - Nessun accesso a quelle che sono porte non sicure (definite in una slide precedente)
- http_access deny CONNECT !SSL_ports
  - Non si permette il metodo Connect a meno che non arrivi con un collegamento SSL

Esempi di ACL (7)

- acl work_time time MTWHF 08:00-17:30
  - Definisce il work_time
- http_access allow work_time
  - questi due TAG del tipo acl ed http_access rappresentano un esempio di restrizione che può essere impostato per autorizzare gli accessi al proxy server nei soli giorni festivi e nelle sole ore lavorative

Esempi di ACL (8)

- acl password proxy_auth REQUIRED
  - Definisce una richiesta di password
  - Dev'essere definito uno schema di autenticazione per poter usare questa acl
- http_access allow password
  - Consente l'accesso a chi inserisce la password

Elementi delle ACL (1)

- src: sorgente (client) IP addresses
- dst: destinazione (server) IP addresses
- myip: l'indirizzo IP locale di una macchina che esegue una connessione client
- srcdomain: il nome di dominio sorgente (client)
- dstdomain: il nome di dominio di destinatizione (server)

Elementi delle ACL (2)

- srcdom_regex: espressione regolare che identifica un pattern contenuto in un indirizzo sorgente (client)
- dstdom_regex: espressione regolare che identifica un pattern contenuto in un indirizzo di destinazione (server)
- time: orario per giorno o giorno della settimana

Elementi delle ACL (3)

- url_regex: espressione regolare che identifica una URL
- urlpath_regex: espressione regolare che identifica una URL-path, non viene specificato il protocollo e l'eventuale hostname
- port: seleziona e specifica il numero di porta per il server di destinazione (server)

Elementi delle ACL (4)

- myport: seleziona e specifica il numero di porta che il client utilizza per connettersi a
- proto: protocollo di trasferimento (http, ftp, ecc.)
- method: metodo di richiesta HTTP (get, post, ecc.)

Elementi delle ACL (5)

- browser: espressione regolare che identifica una richiesta che viene effettuata da un browser web specifico
- ident: stringa che si combina con un nome utente
- ident_regex: espressione regolare che identifica uno user name specifico

Elementi delle ACL (6)

- src_as: numero di un Sistema Autonomo sorgente (client)
- dst_as: numero di un Sistema Autonomo di destinazione (server)
- proxy_auth: autenticazione degli utenti attraverso un processo esterno
- proxy_auth_regex: autenticazione degli utenti attraverso un processo esterno

Elementi delle ACL (7)

- snmp_community: definizione di una SNMP community string
- maxconn: un limite al numero massimo di connessioni che arrivano da un singono indirizzo IP
- req_mime_type: espressione regolare che identifica un header del tipo content-type incluso in una richiesta

Elementi delle ACL (8)

- arp: comparazione con un Ethernet (MAC) addres
- rep_mime_type: espressione regolare che identifica un pattern che viene inviato come risposta (downloaded content) all'intestazione del tipo content-type. Questo tipo di ACL può essere utilizzato unicamente nelle direttive http_reply_access ma non nelle direttive http_access

Elementi delle ACL (9)

- external: esegue il lookup ricorrendo a degli acl helper esterni che sono stati definiti da delle ACL del tipo external_acl_type

Autenticazione (1)

- Lo schema di autenticazione basic utilizza i seguenti parametri
  - auth_param basic program cmdline
  - auth_param basic children numberofchildren
  - auth_param basic realm realmstring
  - auth_param basic credentialsttl timetolive

Autenticazione (2)

- auth_param basic program cmdline
  - Specifica il comando che avvia il programma utenticatore esterno.
  - Tale programma legge una riga da stdin contenente "username password" e risponde con "OK" o "ERR" in un loop senza fine.
  - Come default, lo schema di autenticazione basic non viene attivato, a meno che non venga specificato un programma che si occupa di eseguire l'autenticazione

Autenticazione (3)

- Esempio:
  - auth_param basic program /usr/local/squid/libexec/ncsa_auth \ /usr/local/squid/etc/passwd

Autenticazione (4)

- auth_param basic children NN
  - Indica quante istanze del programma di autenticazione devono essere eseguite contemporaneamente.
  - Se viene configurato un numero di autenticatori troppo basso, Squid potrebbe essere costretto ad attendere un autenticatore libero, rallentando la navigazione.
  - Il valore predefinito è 5

Autenticazione (5)

- auth_param basic realm realmstring
  - Specifica il nome realm che viene fornito ai client per lo schema di autenticazione Basic (Il testo che l'utente vedrà nella dialog box di autenticazione del browser).
  - Il valore predefinito è "Squid proxy-caching web server"
  - auth_param basic realm Squid proxy-caching web server

Autenticazione (6)

- auth_param basic credentialsttl timetolive
  - Specifica il tempo di vita (Time To Live o TTL) di una coppia username:password che viene validata esternamente.
  - In altre parole, quanto spesso un programma helper debba validare nuovamente le credenziali per un dato utente.
  - Il valore predefinito é due ore
  - auth_param basic credentialsttl 2 hours

Autenticazione (7)

- E'sempre possibile testare il corretto funzionamento di un helper per la Basic authentication semplicemente eseguendolo con la stessa riga comandi specificata in squid.conf e verificando che, immettendo delle coppie username:password, si ottengano le risposte "OK" o "ERR" previste.

Helper NCSA

- auth_param basic program /usr/local/squid/libexec/ncsa_auth \
- /usr/local/squid/etc/passwd
- auth_param basic children 10
- auth_param basic realm Squid proxy-caching web server
- auth_param basic credentialsttl 30 minutes

Inserire gli utenti

```
# htpasswd -c /etc/squid/passwd stefano
New password:
Re-type new password:
Adding password for user stefano
```

Bloccare alcuni download

- ACL per bloccare il download di alcuni file
  - acl ftpblock url_regex -i \.mp3$ \.asx$ \.avi$ \.mpeg$ \.mpg$ \.qt$ \.ram$ \.rm$ \.iso$ \.wav$
- Applicare la ACL
  - http_access deny ftpblock