Indice

Capitolo 1

Inquadramento del problema

La continua e sempre maggiore diffusione di Internet ha portato con sè la necessità di un incremento del grado di sicurezza dei computer di grandi società e importanti istituzioni accademiche con accesso alla rete esterna.

Negli ultimi anni, molte grandi aziende e molte grosse università hanno avuto almeno un computer fermo a cause di attacchi esterni ed è di soli pochi mesi fa la notizia di cinque studenti canadesi arrestati con l'accusa di aver bloccato per diverse ore il sito della CNN.

Le principali cose da proteggere su un server sono:

- dati
- risorse
- reputazione

Un attacco ai dati può avvenire con lo scopo di rubare importanti informazioni di tipo tecnologico a grandi aziende (spionaggio industriale) o con lo scopo di modificare i dati presenti su un server (bilanci bancari, votazione degli studenti).

Un attacco alle risorse avviene solitamente o con lo scopo di danneggiare una società concorrente o semplicemente per dimostrare le proprie capacità di pirata informatico. Questo tipo di attacco è stato molto utilizzato negli ultimi mesi del 1999 contro server ben protetti di grandi portali web, da parte di un gruppo di hacker che pensava di riuscire a mettere in luce le proprie capacità informatiche collezzionando le cadute dei server attaccati.

Un danneggiamento della reputazione di una società può avvenire mediante l'accesso di uno sconosciuto sulle macchine di tale azienda. Se l'intruso riesce a farsi identificare da tali macchine come un dipendente della società, egli ha a propria disposizione tutti i mezzi per far perdere di credibilità l'azienda nei confronti dei propri collaboratori, dei propri clienti e dei propri fornitori.

Le principali politiche di difesa sui server sono due: network-secuity e host-security.

Il modello network-security è molto diffuso nelle aziende ed ha lo scopo di delineare un perimetro al cui interno i dati sono da ritenersi fortemente sicuri. Questa politica di difesa, forza il passaggio dei pacchetti fluenti tra rete esterna e rete interna, ad attraversare un firewall. Il firewall è un dispositivo di sicurezza in grado di bloccare i pacchetti ritenuti pericolosi e in una politica network-security deve essere l'unico collegamento tra intranet ed Internet.

Il modello host-security viene utilizzato nelle grandi istituzioni accademiche dove possono esserci collaboratori esterni che hanno accesso ai server universitari e ricercatori che devono pubblicare le proprie ricerche. Questa politica di difesa ha lo scopo di limitare le risorse disponibili ai servizi attivi sui server, lasciando loro solamente quelle indispensabili per un corretto funzionamento.

Per incrementare ulteriormente il livello di sicurezza fornito da host-security o network-security, vengono utilizzate ulteriori politiche aggiuntive. Tali politiche sono specializzate, cioè difendono solamente da alcuni tipi di attacchi, e singolarmente non offrono un elevato livello di protezione, ma la loro combinazione porta ad un notevole incremento del livello di sicurezza.

Le principali politiche utilizzate per incrementare la sicurezza sono:

- deny of stance: tutto ciò che non è espressamente permesso sui server viene vietato
- weakest link: si pone come obiettivo di trovare il punto debole del server e lo elimina
- universal partecipation: tenta di diffondere nella società o nel gruppo di ricerca l'importanza della sicurezza e non permette la creazione di utenti privilegiati che possono accedere alla rete esterna attraverso una back-door
- diversity of difence: utilizza dispositivi di sicurezza di differenti fornitori, in modo da ridurre la probabilità di un bug comune
- defence in depth: utilizza meccanismi di sicurezza multipli, permettendo così una buona protezione anche in caso di mal funzionamento di qualche dispositivo di sicurezza
- fail-save stance: in caso di caduta del sistema nega l'accesso ad un eventuale attaccante

Capitolo 2

Identificazione dei problemi di sicurezza

2.1 Introduzione

Il crescente impatto delle applicazioni di rete sul mondo del lavoro ha favorito la crescita delle esigenze di sicurezza nel traffico dati. Le architetture hardware e sofware dedicate sono oggetto costante di studio e miglioramento. Da un lato si cerca di ottimizzare la velocita' di scansione dei dati in modo da garantire all'utenza un funzionamento il più possibile trasparente, dall'altro si cerca di introdurre algoritmi di individuazione del traffico malizioso sempre piu' selettivi ed intelligenti. Tali caratteristiche sono chiaramente in contrasto tra loro poichè uno studio approfondito dei dati in transito richiede un grande lavoro su ogni pacchetto e la ricostruzione opportuna dell'intero flusso dati. La ricostruzione di tali flussi e' in massima parte demandata all'implementazione ISO/OSI del sistema operativo e quindi può essere ragionevolmete considerata al limite dell'ottimizzazione ma la stessa analisi di quanto ottenuto non è un problema banale e viene risolto solitamente tramite algoritmi euristici. Tutti questi meccanismi rispondono in ultima analisi alla necessità di proteggere un certo numero di macchine appartenenti ad una rete privata -detta intranet o lan- dalle aggressioni provenienti da persone non autorizzate. La quantità di applicazioni operanti, ognuna con una propria implementazione, verso Internet effettivamente lascia supporre una grossa difficoltà nella gestione globale del problema.

Inoltre la rete è in continua evoluzione per cui di giorno in giorno nascono nuove falle nei sistemi di sicurezza dovute alla richiesta e aggiunta di nuove funzionalità. Un esempio su tutti è la realizzazione ad-hoc di applicativi java per l'aggiramento dei tipi più diffusi di firewall di cui apprezzeremo più avanti il funzionamento.

2.2 Problemi locali ed ambientali

Purtroppo l'esistenza della rete non mette le aziende al riparo da casi di spionaggio o sabotaggio interni. La condivisione delle risorse è oggi un'alleata del dinamismo ma anche la principale origine di situazioni pericolose. I servizi ed i dati importanti devono necessariamente essere seaparati dagli altri strumenti lavorativi e soltanto le persone strettamente autorizzate devono poter accedere alle risorse più critiche. L'accesso deve essere salvaguardato sia tramite opportuni sbarramenti in rete sia mediante la restrizione dell'accesso fisico alle console dei calcolatori. Buona parte dei sistemi informatici infatti vedono la propria console come un canale privilegiato: chi vi si siede viene investito di una fiducia a volte mal riposta a causa della necessaria presenza di procedure di recovery nel caso di malfunzionamento del sistema che devono essere effettuate localmente. Ovviamente gli stessi sistemi mettono a disposizione degli amministratori procedure di recovery dotate di chiavi di accesso che stabiliscano l'identità dell'operatore anche nei casi estremi di panico hardware. Ciò sposta l'attenzione su uno dei più grandi problemi nella gestione della sicurezza, ovvero l'amministratore. Un insieme di calcolatori di media dimensione e normalmente esposto verso la rete Internet ha assoluto bisogno di una figura dotata di un bagaglio culturale e di esperienza notevoli. Si pensi alla quantità dei sistemi di sicurezza esistenti. È evidente che in una rete le protezioni implementate dovranno essere diverse sia per provenienza sia per tipologia. Questo impedisce che un singolo errore di programmazione possa abbattere in un solo colpo tutte le difese. D'altro canto la gestione di una quantità di risorse, tutte diverse e tutte potenzialmente migliorabili, diviene talmente onerosa da poter essere considerata come una delle principali cause di insicurezza.

Si pensi alla gestione delle politiche di accesso. In genere si tende a negare tutto quello che non è espressamente consentito. Le autorizzazioni però dovrebbero essere rilasciate con grande oculatezza e dopo un'attenta valutazione dei problemi topologici della rete. Molto spesso infatti una struttura di sicurezza convive con lacune ben conosciute ma tollerate per il funzionamento di servizi accessori quando invece gli stessi servizi potrebbero essere eliminati o modificati opportunamente.

Nei casi in cui i dati sicuri e gli utenti normali convivano sulla stessa macchina il lavoro dell'amministratore è ulteriormente gravato in quanto è necessaria una grande tempestività di intervento laddove le applicazioni incaricate di vagliare euristicamente le azioni di tutti gli utenti -che possono essere centinaia- ravvedano un tentativo di attacco. Ovviamente le applicazioni di questo tipo hanno un grado di intelligenza limitato per cui il rilevamento dell'attacco deve avvenire tramite l'interpolazione di più parametri non completamente significativi come l'occupazione di cpu e memoria per cui i falsi allarmi sono all'ordine del giorno.

Tutto questo carico ha generalmente ripercussioni sull'aggiornamento degli strumenti di difesa e sulla soddisfazione degli utenti.

2.3 Attacchi esterni alla rete locale

Una buona parte degli attacchi verso una rete di calcolatori proviene da Internet. I sistemi di sicurezza vengono plasmati su questa consapevolezza in modo da garantire il massimo bloccaggio di qualsiasi dato sospetto da e verso la rete. Esistono vari tipologie di attacco che danno esito diverso a seconda del tipo di difese adottate e del livello di cura profuso nella configurazione di queste ultime.

Il sistema maggiormente subdolo è il furto di informazioni passivo detto "sniffing". Tale sistema di intrusione ha successo solo grazie ad eventali lacune del sistema attaccato e soprattutto non può essere rilevato poichè si limita all'ascolto del traffico dati transitante su di una linea accessiblie. L'attaccante puo' rilevare il passaggio delle password in chiaro durante l'autenticazione telnet o impossessarsi di interi file transitanti su NFS. Ecco perchè tutte le informazioni importanti dovrebbero essere protette anche durante il trasferimento in rete e non solo durante la loro custodia sul disco fisso. Il transito di dati potenzialmente pericolosi per la sicurezza in genere non può essere eliminato, vuoi per la necessità di autenticare utenti esterni per il lavoro su shell, vuoi per la necessità di unire sottoreti distanti tramite "tunnel" sulla rete pubblica -si parla di Virtual Private Network (VPN) riferendosi alle varie intranet unite da uno o più tunnel-. Per proteggere la trasmissione si può ricorrere a sistemi di crittazione più che collaudati come RSA e Rabin per i dati di dimensione limitata -tra cui le e-mail e la fase di scambio iniziale di chiavi segrete previsto da IPV6- e MD5 o simili per gestire grandi flussi tramite cifranti binarie. Già oggi esistono applicativi perfettamente funzionanti come SSH, il quale rimpiazza il telnet, e gateway cifranti per l'implementazione di VPN tra i firewall di intranet "amiche".

Un tipo di attacco maggiormente controllabile è lo spoofing. In questo caso l'attaccante tenta di introdursi nella rete locale attraverso Internet contando di sfruttare le relazioni di fiducia esistenti tra le macchine della stessa rete. A tale scopo la macchina dell'intruso deve spacciarsi per una macchina "amica" presentandosi con un indirizzo IP locale. Per un firewall qualsiasi è facilissimo rilevare la presenza di una macchina della rete interna fuori posizione i cui dati, arrivati attraverso Internet -e non dalla sua collocazione naturale sulla intranet-, vengono bloccati.

Un firewall dovrebbe limitare al massimo le possibilità di accesso degli utenti esterni alle macchine locali e dovrebbe proteggerle da eventuali attacchi miranti al blocco del sistema. Il primo limite aiuta l'amministratore del sistema, il quale non deve imporre agli utenti restrizioni sui software installabili -ed in particolare sui loro bachi- ma semplicemente evita che il mondo possa approfittare di essi accedendovi liberamente. Il secondo invece deve coprire le lacune di alcuni sistemi operativi nella gestione della rete. Purtroppo alcune particolari combinazioni di pacchetti malformati possono provocare il crash del sistema e in altri casi l'eccesiva frammentazione di pacchetti molto grandi ma legittimi può dare risultati simili. I sistemi di difesa come ipchains per linux danno garanzie totali su entrambi i fronti poichè i dati in arrivo vengono controllati alla ricerca di irregolarità di costruzione e, volendo, i pacchetti frammentati vengono ricostruiti interamente prima di essere girati al destinatario finale.

Esistono infine debolezze insite nei servizi tradizionalmente presenti su Internet come l'FTP. Tale servizio di movimentazione file richiede nella forma più comune -detta "attiva"- che il client comunichi al server la porta locale sul quale effettuare la connessione. Il server, una volta ricevuto il numero di porta verso cui comunicare effettua una connessione e trasferisce i file. Questo è concettualmente sbagliato poichè da Internet nessuno dovrebbe poter stabilire di propria iniziativa una connessione verso l'interno della rete. La maggior parte dei firewall aggira il problema tenendo conto del messaggio iniziale del client nel quale si comunica il numero di porta al server. Purtroppo il firewall a volte non è molto "furbo" per cui se a generare il messaggio -PORT ###- è un'applicazione maliziosa ed il numero della porta è ad esempio il 23 è possibile che un utente non autorizzato possa tentare l'accesso tramite il telnet.

Ovviamente le applicazioni maliziose devono essere eseguite ma la grande diffusione dei virus tramite l'apertura incauta di messaggi e-mail ed il proliferare di applicazioni java per il web dovrebbero far suonare un campanello d'allarme. Fortunatamente va diffondendosi un diverso tipo di standard nella negoziazione della connessione FTP definito "passivo" perchè è il server a decidere la propria porta locale ed è il client questa volta ad avviare la connessione.

Capitolo 3

Metodi per garantire la sicurezza

3.1 Architetture tipiche di reti sicure

Il nome degli host, il loro indirizzo, i servizi da essi offerti, rappresentano l'immagine pubblica dei server e per questo sono i primi bersagli degli attaccanti. Solitamente, tale immagne viene fornita attraverso expandable hosts, cioè hosts esterni al firewall ma aventi una via di comunicazione preferenziale con le macchine collegate sulla intranet. Limitando il numero degli hosts esposti, facendo strategici settaggi sulle risorse disponibili sui server, si riesce a proteggere la rete locale dagli attacchi più comuni, mentre per difendersi dagli attacchi più complessi occore utilizzare apposite architetture.

A seconda del grado di sicurezza desiderato, a seconda dei servizi che si devono offrire, si hanno a disposizione differenti implementazioni di reti sicure che possono anche essere tra loro combinate con lo scopo di incrementare il livello di sicurezza della LAN.

Tali architetture sono divise in tre principali configurazioni:

- dual home
- bastion host
- perimeter network

3.1.1 Dual home

Una architettura dual home, è un sistema che ha almeno due sbocchi su reti differenti e per questo viene solitamente costruita attorno ad un dual host, ovvero attorno ad un insieme di computer che globalmente hanno due o più interfacce di rete (vedi fig 3.1 a pag 10).

Il dual home può fornire un elevato livello di controllo, ma per sfruttare al massimo le potenzialità del sistema occore una elevata quantità di risorse.

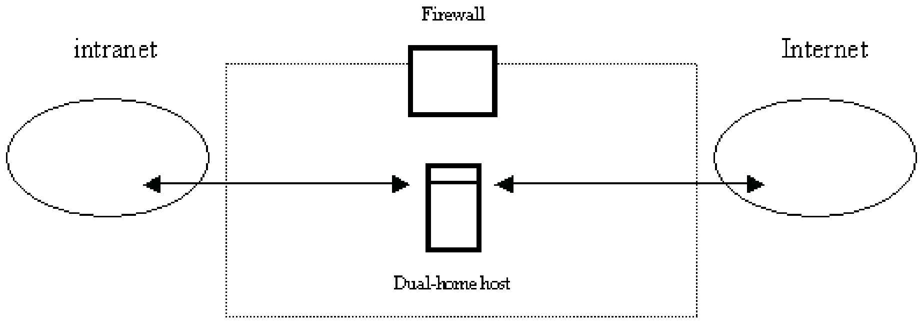

Figura 3.1: Architettura dual home

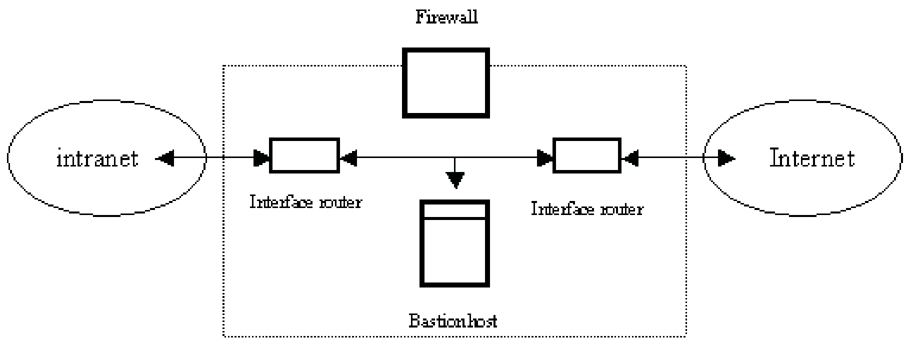

Figura 3.2: Architettura bastion host

3.1.2 Bastion host

Un bastion host è un sistema che permette ai suoi utenti di effettuare connessioni sicure sulla rete esterna rendendo però pubblica la propria presenza su Internet e diventando così il principale punto di attacco di hackers (vedi fig 3.2 a pag 10).

Il progetto di un bastion segue due principi di base: la semplicità ed il mantenimento dell'integrità della rete interna nel caso di violazione del bastion.

Un bastion host semplice, è sicuramente più sicuro di uno con configurazione complessa, in quanto la possibilità di errori di settaggio tendono a diminuire con l'incremento della semplicità del sistema. Su tali server devono funzionare solamente i servizi indispensabili con le risorse minime che richiedono: qualche programma potrebbe contenere dei bug riutilizzabili da un malintenzionato per accedere alla rete locale e provocare la caduta del bastion stesso. In caso di attacco riuscito, la caduta del bastion non deve

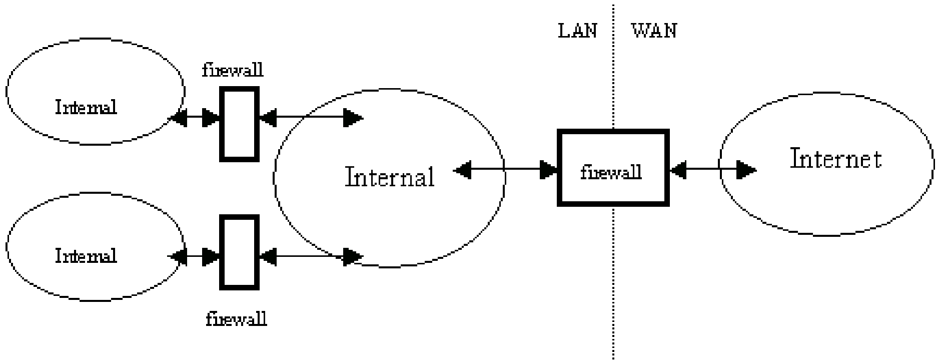

Figura 3.3: Architettura perimeter network

portare alla violazione di tutta la rete intranet, perciò le macchine principali non devono essere sotto il diretto controllo del bastion ed i servizi offerti devono avere solamente i privilegi necessari per il corretto funzionamento, mentre gli altri devono essere scrupolosamente negati.

Victim machine

Una particolare versione di bastion host è la victim machine. Su una macchina, detto appunto victim machine, vengono fatti girare servizi difficilmente implementabili in modo sicuro o che utilizzano nuovi programmi che potrebbero contenere dei bug. Tale macchina non deve in alcun modo accedere ad altri computer della rete interna, bensì, solo far girare il servizio insicuro. In tal modo, se anche un attaccante riuscisse a loggarsi su essa, i danni che potrebbe provocare rimarrebbero limitati alla victim machine ed i privilegi che avrebbe a disposizione sarebbero minimi. I servizi non necessari devono inderogabilmente essere disabilitati sul bastion, in modo da diminuire le possibili risorse a disposizione di un eventuale intruso; in pratica, i servizi che solitamente se non utilizzati devono essere disabilitati su un bastion host sono: FTP, HTTP, NTTP e Gopher.

3.1.3 Perimeter network

Per incrementare la sicurezza o per definire differenti livelli di sicurezza sulla rete interna, è possibile aggiungere dei firewall tra differenti gruppi di lavoro (vedi fig 3.3 a pag 11). In questo modo, un possibile intruso trova nuovi sbarramenti che gli negano una quantità di risorse più o meno grande e dipendente dalla politica di sicurezza scelta durante il posizionamento dei firewall aggiuntivi. Questa struttura viene solitamente utilizzata come seconda linea difensiva per architetture bastion host, ottenendo così un incremento della sicurezza in caso di caduta del bastion.

Attraverso una compartimentazione della LAN, effettuata tramite perimeter network, è anche possibile garantire il diritto di accesso ad alcuni dati e risorse sui server di una società, solamente ad un ristretto numero di dipendenti.

3.2 Tipi di firewall

Il firewall è un insieme di componenti messi tra due reti con lo scopo di far passare solamente in traffico autorizzato (definito autorizzato dalla politica di sicurezza scelta) ed impedire il passaggio di quello non autorizzato, bloccando anche tutto quello che cerca di bypassare il firewall stesso. I vantaggi derivanti dall'utilizzo di un firewall sono di tre tipi:

- diretti o principali
- secondari
- aggiuntivi

I vantaggi diretti sono un incremento del livello di sicurezza del sistema stesso, anche se non bisogna dimenticare che un utilizzo non corretto del firewall può comunque comportare l'accesso alla rete locale da parte di un intruso esterno.

I vantaggi secondari derivano dal fatto che il firewall diventa il punto centrale per l'amministrazione dei servizi mail e FTP. Nel considerare questo tipo di vantaggio, si ipotizza l'impossibilità di aprire una back-door tra la rete intranet e quella Internet. In quest'ottica, quando si vogliono studiare e risolvere problemi di sicurezza, si ha a che fare con un'unica macchina, differentemente da quanto capita quando ogni macchina comunica direttamente con la rete esterna per implementare i servizi mail e FTP. Utilizzando solo un server, risultata meno onerosa la protezione della intranet.

I motivi aggiuntivi sono legati alla necessità di avere un amministratore dei firewall. Tale amministratore, differentemente da quello di sistema, dedica tutto il suo tempo ai problemi di sicurezza, ha o viene ad avere una formazione dedicata su tale argomento e la sua presenza può diffondere tra gli utenti della rete, l'importanza della sicurezza dei dati, dei propri servizi e della propria immagine.

3.2.1 Packet filtering

Il packet filter fa passare selettivamente i pacchetti dagli hosts esterni verso quelli interni. La tecnica di bloccare certi tipi di pacchetti prende il nome di screening router. Ogni pacchetto ha una propria intestazione che permette di risalire all'indirizzo sorgente e di destinazione, al protocollo utilizzato, alla porta da cui arriva e alla porta di destinazione.

Il packet filter è il responsabile che deve segnalare l'arrivo di un incoming packet (pacchetto proveniente dall'esterno avente come destinazione l'intranet) che non ha corrispondenza con una richiesta interna. In questo modo si evitano gli attacchi frontali da parte di un malintenazionato che cerca di valicare la barriera di sicurezza della rete interna, spacciando la sua richiesta di apertura di una connessione verso l'esterno con una risposta esterna ad una precedente richiesta degli host interni. Osservando i dati che il packet filter ha a propria disposizione, indirizzi sorgente e destinazione, protocollo utilizzato, porte di partenza e di arrivo, e notando che l'ordine di arrivo dei pacchetti è praticamente random, si può concludere che la costruzione di tale filtro risulta molto complessa sebbene il suo utilizzo suo molto semplice. In aggiunta alla precedente considerazione c'è da sottolineare che il controllo di sicurezza viene fatto on fly evitando indesiderati tempi di latenza. Così operando, il packet filter non tiene conto dei pacchetti precedentemente arrivati, in caso contrario, esso avrebbe dovuto avere una prima fase di memorizzazione dei pacchetti, una seconda fase di ordinamento degli stessi e solamente in una terza fase avrebbe potuto eseguire un controllo della sicurezza.

Le principali politiche che utilizzano packet filter sono:

- TCP request-response
- connection base UDP services
- NFS client filtering.

3.2.2 TCP Request-response

La politica request-response si basa sugli inbound packet, pacchetti provenienti dall'esterno, permettendo l'accesso alla LAN solo a quelli correlati ad una precendente richiesta interna. Così operando, si evita l'apertura di una possibile connessione da parte di un attaccante appartenente al mondo Internet. L'utilizzo di packet filter è il metodo migliore per attuare la politica sui protocolli TCP. Il fatto che un host interno alla intranet decide di stabilite una connessione TCP verso un host esterno, comprende un permesso implicito che permette gli host non della rete locale di spedire attraverso il firewall dei pacchetti. In pratica questa politica, che può essere attuata principalmente grazie all'uso di packet filter, permette agli host esterni di partecipare ad una connessione TCP stabilita da qualsiasi host sulla LAN, impedendo però a loro di iniziare una connessione verso l'interno grazie ad un filtraggio di tali richieste. Il filtraggio delle richieste di connessione arrivanti dall'esterno avviene usando lo standard SYN. La fase della connessione TCP ha tre modi di combinarsi:

- SYN
- ACK

- SYN+ACK.

La politica di filtraggio per porte TCP permette a tutti i pacchetti arrivanti dall'esterno di penetrare, fatta eccezione di quelli che vogliono iniziare una connessione, quindi in pratica viene lasciato passare solamente il modo SYN e non ACK. Il punto debole di questa politica è che permette facili attacchi che hanno lo scopo di negare alcuni servizi interni alla LAN.

3.2.3 Connection based UDP services

Un piccolo numero di applicazioni che utilizzando il protocollo UDP usano porte del server e del client ben conosciute. Questi protocolli vengono trattati come per la connessione TCP, ovvero creando un opportuno filtro che controlla gli indirizzi sorgente e destinazione, i relativi numeri di porta e il contenuto del pacchetto.

NFS client filtering

NFS client filtering utilizza la politica request-response, infatti il client NFS manda un richiesta RPC al server NFS ed esso risponderà in un secondo momento inviando indietro il dato precedentemente richiesto. La politica request-response deve permettere ad un utente fuori della LAN, con i diritti di fare un NFS mount da un NFS server esterno al firewall, di eseguire l'operazione di mount in modo trasparente. Come con un TCP, la politica request-response per un NFS viene realizzata tramite un filtro che non lascia passare i falsi pacchetti di risposta. Attualmente il processo di mount NFS richiede un dialogo iniziale con il demone di mount per ottenere un file-handle. Il demone di mount viene localizzato attraverso una richiesta RPC sul remote server portmapper. Per evitare problemi con UDP port mapping, viene spesso utilizzata una utility di mount modificata che permette la transazione RPC su TCP piuttosto che su UDP. I moderni client e server NFS sono configurati per funzionare su TCP, aumentando in questo modo la sicurezza della tecnica request-response. Sfortunatamente se le workstation hanno un sistema Unix con una implementazione NFS interna al kernel, la modifica di tale kernel per spostare le transazioni su TCP andrebbe a compromettere la facilità di installazzione del firewall, qualità essenziale per un'ottima politica di sicurezza.

3.2.4 Application level

Esistono categorie di applicativi che non possono essere ricondotte al paradigma di request-response. Per alcune di queste applicazioni critiche si fa ricorso a particolari applicazioni che hanno lo scopo di ovviare a questo problema garantendo un elevato livello di sicurezza. La più importante ed utilizzata in questa categoria di applicazioni è la connectionless UDP-based application.

Connectionless UDP-based application

Molti programmi non usano il socket UDP in modo tradizionale, quindi il packet filter non è sempre in grado di riconoscere i pacchetti di UDP response dai pacchetti di UDP request arrivanti da un host esterno. I pacchetti UDP response sono quelli che devono avere accesso alla rete locale perchè correlati ad una precedente richiesta di un host interno al firewall. I pacchetti UDP request sono quelli che non devono assolutamente valicare la barriera creata dal firewall perchè spediti da un possibile attaccante. Per valutare quando un inbound packet è certamente un valido UDP response, il packet filter ha bisogno di alcune risorse specifiche come ad esempio il DNS per mapping tra hostname e address. Sebbene il DNS permette l'utilizzo del paradigma request-response e può essere configurato per usare sia TCP che UDP, normalmente usa il protocollo UDP da una porta UDP arbitraria. L'uso del servizio DNS serve per forwardare, da un set di internal slave nameserver verso un filtro, tutte le richieste ricevute. Il packet filter utilizzato permette il traffico UDP tra porte DNS riservate (DNS reserved port) tra external host e nameserver. Questa struttura lavora in modo soddisfacente ed ultimamente ha dato degli ottimi risultati inaspettati, grazie alla cache interna dei nameserver.

Altre applicazioni che utilizzano in socket in modo differente possono essere bloccate o fatte girare su un external bastion host (talk, archie e reuser). Tale compromesso risulta poco pratico per gli utenti perchè devono avere anche una sessione aperta sull' external host per usufruire di determinati servizi, ma risulta molto efficiente dal punto di vista della sicurezza.

3.2.5 Circuit level Gateway

I proxy sono applicazioni specializzate che girano su un dual-home host. Questi programmi, in un primo tempo, prendono le richieste che gli utenti fanno verso il mondo Internet (FTP, telnet, HTTP) e le forwardano verso host esterni. In un secondo tempo fanno l'operazione inversa, forwardando la risposta giunta della rete WAN verso gli host della rete LAN. Durante le precedenti operazioni di forward, il proxy effettua controlli di sicurezza connessi alla politica del sistema. Queste applicazioni o dispositivi, visto che esistono sia in forma software che hardware ma la modalità di funzionamento è in linea di massima sempre la stessa, sono solitamente trasparenti agli utenti della rete locale ed ai servizi della rete esterna. La trasparenza è il loro miglior pregio perché dopo un primo settaggio iniziale, che solitamente viene fatto in maniera automatica dall'amministratore, possono essere utilizzati senza problemi aggiuntivi anche dagli utenti meno smaliziati. L'utente, infatti,

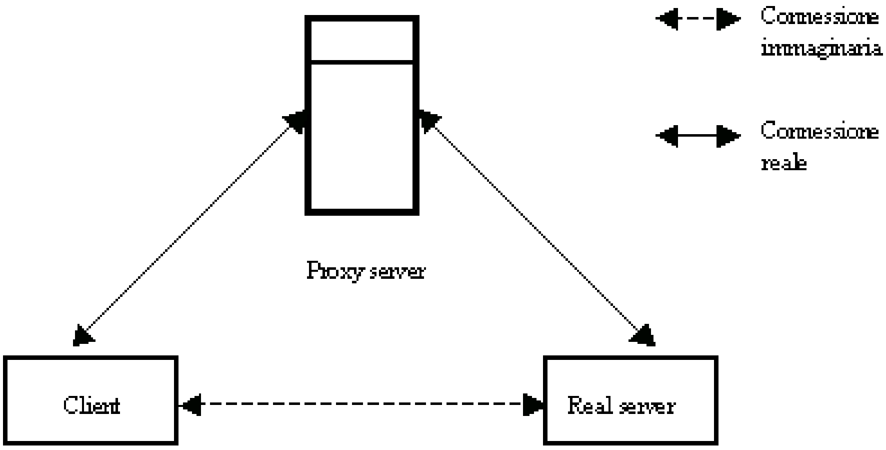

Figura 3.4: Connessione tramite proxy system

pur utilizzando il proxy, ha l'impressione di connettersi direttamente alla rete esterna, ma è solamente una illusione perché tale comunicazione passa appunto attraverso il proxy.

Queste applicazioni vengono utilizzate congiuntamente con altri dispositivi di sicurezza come packet filter e dual-home host.

Il proxy internamente, soprattutto nelle versioni hardware ma in linea teorica anche nelle versioni software, può essere scomposto in due dispositivi unidirezionali: il proxy server ed il proxy client. Il proxy server gira nel dual-home sull'interfaccia di rete dedicata ad Internet, mentre il proxy client gira sempre sullo stesso host ma sull'interfaccia di rete dedicata alla intranet. Così operando, la connessione tra LAN e WAN avviene tramite proxy client e proxy server, mentre svanisce la connessione diretta tra le due reti che è la principale fonte di problemi riguardanti la sicurezza del sistema.

I dettagli su come lavora un proxy dipendono dai servizi offerti. Esistono comunque alcuni svantaggi nell'utilizzo di tale applicativo:

- non è in grado di proteggere la rete interna da attacchi fatti con particolari protocolli, soprattutto se nuovi
- occorre almeno un iniziale settaggio delle applicazioni che precedentemente si connettevano direttamente sulla rete esterna
- non è in grado di lavorare con alcuni servizi

Sicuramente ci sono anche dei vantaggi:

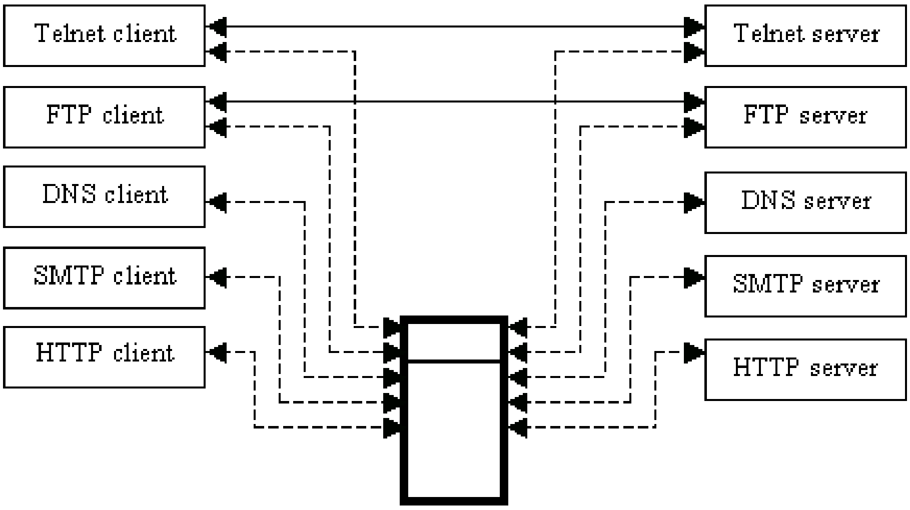

Figura 3.5: Proxy server utilizzato per differenti servizi

- un ottimo metodo di log (attraverso proxy si possono loggare anche solo i comandi in uscita del firewall e le risposte dei server, evitando così enormi file di log)
- non permette un accesso diretto sulla rete Internet

Un particolare utilizzo del proxy è nei proxies for reserved-channel services e serve per gestire tutte quelle applicazioni che richiedono un back-channel per un funzionamento corretto.

Proxies for Reversed-Channel Services

L'implementazione request-response non è attualmente in grado di gestire il controllo di sicurezza sui servizi che richiedono una connessione back-channel. Per esempio, un client FTP implementa la richiesta dir e get, creando un socket TCP, mandando un messaggio al server remoto chiedendo di avere come risposta il risultato attraverso la porta aperta a tale scopo (porta random che quindi sarà differente da collegamento a collegamento) e aspettando su di essa la risposta. La classica implementazione request-response blocca la connessione attraverso questa porta. Il problema del back channel sorge in differenti forme quando un utente all'interno del firewall cerca di lanciare un client X-window da un host esterno e di farlo apparire sul proprio monitor (logicamente esterno al firewall). Per connettersi, il client esterno deve stabilire una connessione TCP all'X-server interno al firewall, ma la politica request-reresponseponse non lo permette. Si potrebbe lasciare passare questa connessione attraverso il firewall e far affidamento sul X-server di rigettare le connessioni non autorizzate, purtroppo questo meccanismo non è applicabile su tutte le macchine. Sarebbe impensabile implementare tale sistema di autentificazione su tutti i potenziali client, inoltre senza un unico e sicuro meccanismo di autentificazione, sarebbe sicuramente facile saltare l'autentificazione del server.

Attualmente quando si vuole implementare un meccanismo che permetta connessioni arbitrarie che richiedono un X-server si può usare un proxy. Il proxy alloca semplicemente un nuovo display su un bastion-host e la richiesta all'X-server proveniente dall'esterno viene forwardata su tale bastion che a sua volta ha il compito di verificare l'autenticità ed i relativi permessi del client esterno ed eventualemte permettere l'X-window. Logicamente questa gestione attraverso il bastion host dovrebbe essere una soluzione temporanea in attesa di nuove implementazioni di sicurezza che riescano a gestire le richieste di back-channel.

Capitolo 4

Firewall attualmente utilizzati

4.1 Software

4.1.1 Introduzione: Open source e prodotti commerciali

La storia del software open source non può certo considerarsi recente. Già negli anni '70 e '80 si erano creati alcuni movimenti per lo sviluppo di software libero ed aperto alle modifiche e migliorie di tutta la comunità scientifica. All'inizio degli anni '90 la scommessa di uno studente ha portato alla creazione del primo kernel funzionante aderente alla licenza GNU -esempio di acronimo ricorsivo: "GNU's Not Unix"-. La versione originale di tale kernel non rappresentava certo una rivoluzione tecnologica ne una soluzione efficace. Essa implementava le funzionalità di un sistema operativo commerciale ormai relegato tra i ricordi, il MINIX, ma quel che piú conta è che permise di raggruppare tutto il codice scritto sotto licenza della Free Software Foundation dagli sviluppatori di tutto il mondo formando un sistema operativo completo. Tale sistema operativo prese il nome di "linux" ed è il punto di riferimento per tutti coloro i quali vogliano avvicinarsi al mondo unix in quanto dispone di manuali e supporti di vario genere veramente ineguagliabili ed a costo zero. L'enorme numero di installazioni, la mole di lavoro profusa nel perfezionamento del kernel e di tutte le parti di contorno vitali per un uso produttivo hanno permesso la nascita di una forma di sicurezza completamente nuova ed aborrita da tutte le ditte specializzate.

Si è passati da un tipo di sicurezza incentrato su "scatole nere" funzionanti grazie a meccanismi oscuri e possibilmente spacciati per magici dagli stessi produttori alla pubblicazione integrale del codice sorgente opportunamente commentato da parte degli autori principali per garantire la continuità dello sviluppo.

I prodotti commerciali, essendo "segreti", sono molto meno soggetti ad attacchi dovuti ad errori di programmazione dei corrispettivi gratuiti. Chi non conosce qualcosa difficilmente potrà sfruttarne le debolezze. Purtroppo questo approcio è pericoloso in quanto anche gli utenti autorizzati stentano a capire il prodotto da usare. Ne consegue una debolezza più profonda: se pochi sanno aggirare un sistema di sicurezza probabilmente gli ultimi a saperlo saranno gli acquirenti e gli sviluppatori del sistema stesso e questo accadrà solo dopo la perdita di sicurezza di molte installazioni poichè la diagnosi di un "baco" difensivo è difficoltosa. Considerando inoltre che la sicurezza in fin dei conti è un parametro fortemente legato alla volontà degli attaccanti di averla vinta possiamo dire che una fase di reverse engeneering su qualsiasi dispositivo di sicurezza è da mettere in conto e può annullare i vantaggi fin qui elencati per i tools commerciali.

I prodotti gratuiti invece partono dal presupposto base di qualsiasi sistema di crittografia serio. Un buon sistema cifrante deve essere giudicato sicuro per via analitica e non deve sembrarlo solo perchè non è ancora stato infranto. Allo stesso modo un sistema di sicurezza dovrebbe dimostrarsi sicuro studiando tutte le possibili interazioni effettuabili. Questo è impossibile per un programma di medie dimensioni per cui l'unica garanzia sta nell'uso quotidiano e controllato da parte degli sviluppatori e degli utenti finali. L'eliminazione progressiva dei cosiddetti bug avvicina i prodotti gratuiti alla perfezione almeno quanto non facciano i team di sviluppo delle aziende di software.

4.1.2 Esempio di implementazione gratuita di un firewall: IPCHAINS

L'uso del firewall su architetture unix-like è talmente naturale da essere implementabile nel kernel tra le funzionalità di base del sistema operativo. Questo è di fondamentale importanza perchè nei firewall a filtraggio di pacchetto è necessaria la minima elaborazione per ogni quanto di informazione vagliato. Applicare un firewall su sistemi operativi non predisposti impone due possibili approci:

- l'utilizzo dell'interfaccia di rete già presente nel sistema operativo, con il conseguente aggravio sulle prestazioni del sistema. E' la modalità di funzionamento dei proxy server.
- l'utilizzo di un'interfaccia verso la rete proprietaria e soltanto compatibile con quella originariamente presente all'interno del sistema operativo "ospite".

La prima soluzione è quasi del tutto improponibile laddove i carichi di lavoro impongano elevati flussi dati poichè tutte le informazioni devono risalire l'intera pila ISO/OSI per poi essere vagliate da un normale applicativo e quindi ridiscendere nuovamente verso la rete. La seconda viene invece implementata spesso nei sistemi non ricompilabili e consiste nella creazione di uno "strato di filtraggio" il più vicino possibile al livello fisico della rete, sicuro e costitutito completamente dal codice del firewall installato. In questo

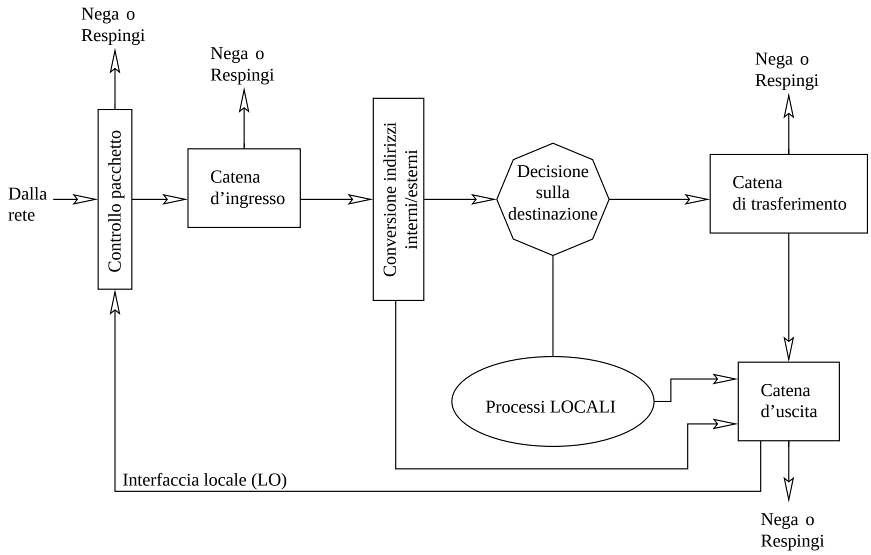

Figura 4.1: Struttura base di ipchains

modo il sistema operativo ospite viene protetto da qualsiasi attacco. Questo tipo di implementazione in effetti è piuttosto brutale e può degenerare nell'instabilità.

Struttura

Nel sistema gratuito linux le funzioni di firewall vengono svolte da due componenti distinte ed interagenti. Vi è il codice di packet-filtering implementato nel kernel ed un pacchetto di configurazione detto ipchains. Ipchains permette di configurare il kernel nel modo desiderato tramite un approcio flessibile e piuttosto semplice. Come vediamo in figura 4.1 il flusso dati transita attraverso alcuni stadi di confronto detti "catene". Ogni catena ha un'origine dalla quale attinge dati, una destinazione verso la quale i dati vengono indirizzati ed è composta da più anelli. Ogni anello è costituito da una regola imposta dall'utente. I dati vengono vagliati sequenzialmente e confrontati con tutte le regole della catena. Ogni regola specifica cosa fare di un certo tipo di pacchetto. Quest'ultimo può essere respinto verso l'origine, semplicemente distrutto, passato ad un'altra catena oppure sottoposto al vaglio della regola successiva.

Il flusso dati passa attraverso alcuni punti predefiniti dall'implementazione del kernel:

- Il controllo di validità del pacchetto. Esso verifica sia la corretta ricerzione sia la pericolosità di alcune sequenze che, a causa di errori di programmazione, possono insidiare la stabilità di vari sistemi operativi e lo stesso funzionamento delle regole di filtraggio.

- La catena di ingresso. Tutti i pacchetti dati ricevuti tramite la rete –compresi quelli generati dai processi locali– vengono vagliati da questo insieme di regole.

- La conversione degli indirizzi -NAT: network address translation-. La rete Internet adotta oggi lo standard Ipv4: esso è di facile implementazione ma ha problemi nel gestire il gran numero di host connessi nel mondo utilizzando soli 4 byte per l'identificazione univoca di ognuno di essi. Allo scopo di razionalizzare l'uso degli indirizzi disponibili si è fatta una distinzione tra indirizzi pubblici, conosciuti da tutta la Rete, e privati, volutamente ignorati dalla movimentazione dei dati pubblica e destinati alla connessione di più macchine in reti locali. Per garantire lo sbocco delle reti private verso Internet è necessario utilizzare un computer dotato di indirizzo pubblico -detto router, vedi figura 4.2 - come traslatore di indirizzi. Il router effettua sulla rete pubblica le richieste per conto dei computer appartenenti alla sua sottorete privata presentandosi col proprio IP pubblico e restituisce i risultati tramite opportune tabelle di corrispondenza generate automaticamente. La conversione degli indirizzi viene eseguita proprio sulla base di tali tabelle. È importante il fatto che la traslazione sia fatta prima del controllo sulle catene di forward e uscita poiché in questo modo, dove necessario, i controlli vengono effettuati sugli indirizzi reali e non su quanto il router ha opportunamente "mascherato".

- Decisione sulla destinazione. I pacchetti dati sopravvissuti fino a questo punto vengono spediti ai processi locali che ne avevano fatto richiesta oppure vengono instradati verso le catena di forward se la destinazione è esterna.

- Catena di forward. Tutti i pacchetti in arrivo dall'esterno del computer e destinati ad un'altro host attraversano questa catena.

- Catena di uscita. Tutti i pacchetti generati dalla macchina o transitanti attraverso essa attraversano questa catena.

Processi locali. Tutti i pacchetti generati da processi locali e destinati ai medesimi attraversano la catena di uscita diretti verso l'interfaccia LO e tornano sulla catena di ingresso. La grande flessibilità di ipchains permette di definire catene aggiuntive che vanno ad affiancarsi alle catene di base sopra descritte (senza mai sostituirle però) permettendo all'utente di raggiungere livelli di ottimizzazione molto alti. Tramite l'uso delle catene aggiuntive infatti solo i pachetti aderenti alla descrizione fatta da una regola specifica –regola A in fig. 4.3– vengono confrontati con le ulteriori regole della nuova catena– . Dalla figura si evince anche che le catene di base sopra descritte non possono mai essere aggirate. Le catene aggiuntive non interrompono

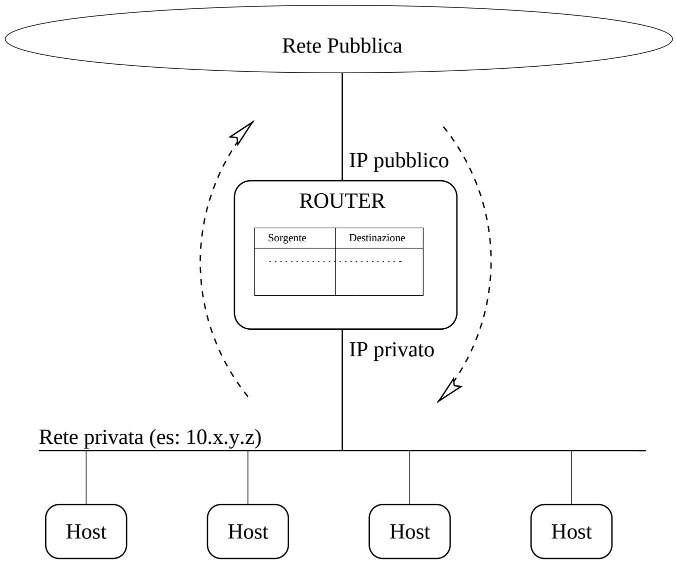

Figura 4.2: Conversione tra indirizzi pubblici e privati (NAT)

mai il flusso dei dati ma possono semplicemente allungarlo per poi tornare alla posizione di partenza.

Sintassi e funzionalità

La sintassi di ipchains è improntata all'aggiunta, cancellazione, manipolazione di catene aggiuntive così come di singole regole all'interno delle catene stesse. A differenza del suo predecessore ipfwadm, ipchains gestisce in modo flessibile le regole gestendo costrutti quali la negazione il riconoscimento delle porte TCP utilizzate tramite il riferimento al protocollo comunemente attestatovi.

Le regole permettono di discriminare sui parametri del pacchetto comprendenti IP e porta TCP sorgente, IP e porta TCP destinazione, interfaccia di rete su cui il pacchetto è arrivato. Allo scopo di eliminare certi tipi di connessione il ipchains può eliminare del tutto qualsiasi pacchetto destinato a tale connessione oppure può semplicemente eliminare il primo pacchetto inviato (un segnale di SYN). Questo rende comunque impossibile la connessione vera e propria per cui raggiunge lo scopo con il minimo sforzo. Per proteggere gli host da eventuali malformazioni dei pacchetti è presente il controllo di validità ma un attacante esperto potrebbe aggirare l'ostacolo segmentando le informazioni su più pacchetti. Il firewall agisce solo sul primo segmento che contiene i dati dell'intera ricostruzione mentre lascia passare gli altri. Per evitare l'eventualità di problemi su tali "segmenti vaganti" è possibile imporre al firewall la ricostruzione integrale dei dati intransito prima dell'inizio del processo di filtraggio. Per garantire la massima sicurezza

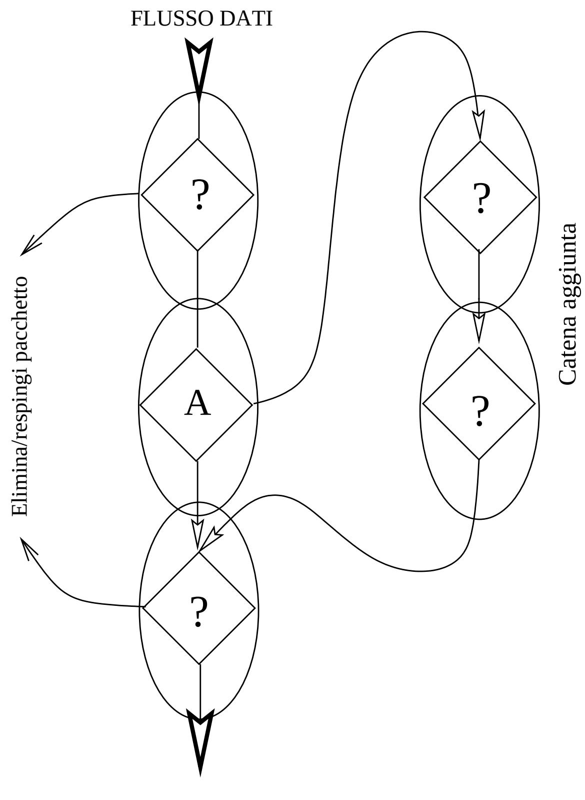

Figura 4.3: Esempio di percorso dei pacchetti sulle catene di ipchains

le connessioni FTP attive sono negate e solo l'installazione di una apposita patch può aggirare tale funzionalità.

Durante l'esame del pacchetto è possibile ridefinire alcuni parametri come i bit del "Type of service". Tali bit dovrebbero essere letti da tutti i router in modo da privilegiare nel modo più opportuno alcuni tipi di pacchetti appartenenti a servizi critici. Ad esempio è teoricamente possibile massimizzare la velocità di consegna di un pacchetto telnet o incrementare il flusso dati di una connessione ftp. Purtroppo l'instradamento dei dati su Internet è gestito da una tale quantità di hardware e software eterogeneo che l'utilizzo effettivo dei bit di "type of service" non è certo garantito.

Come detto in precedenza una delle funzionalità più comuni delegate al firewall è il NAT. Tale sistema permette ai computer di una intranet di presentarsi in rete tramite l'indirizzo IP del firewall che fa le richieste in loro vece. Tale sistema è quindi intrinsecamente sicuro poichè in primo luogo nasconde al mondo l'esistenza dell'intera intranet ed in secondo luogo protegge la stessa esponendosi agli attacchi -essendo comunque opportunamente pensato per resistervi-. Se i computer interni devono essere in qualche modo visibli al mondo il firewall può ridirigere le connessioni alle proprie porte TCP verso le porte TCP di un host specifico interno alla intranet. Tale sistema è definito PAT (Port Address Translation) ed è particolarmente utile per mantenere ad esempio server di posta o news presso macchine locali senza caricare ulteriormente il firewall. Per garantire un'ulteriore grado di sicurezza le macchine parzialmente visibili alla rete possono essere collocate su una LAN –demilitarizzata o DMZ– a bassa sicurezza e quindi opportunamente isolata.

Per proteggersi dagli attacchi "spoofing" non interviene il firewall ma è lo stesso motore di routing di linux ad implementare, nelle release più recenti l'opzione per rifiutare pacchetti originati da IP non appartenenti alla rete dalla quale sono arrivati. Nelle versioni precedenti le regole dovevano essere specificate al firewall per ogni interfaccia.

Si noti che il firewall, allo shutdown ed alla partenza del sistema, non salva ne recupera la configurazione impostata. Per mantenere la configurazione tra un arresto e l'altro è necessario inserire all'interno degli script di avvio le regole di filtraggio. Questo però deve essere fatto prima che i servizi di rete siano caricati in modo che in nessun istante il computer sia vulnerabile.

4.1.3 Esempio di firewall commerciale: Firewall One by Checkpoint

I firewall commerciali in generale offrono molte caratteristiche aggiuntive oltre al classico packet filtering. In effetti il semplice filtraggio di basso livello non offre garanzie illimitate e permette di raggiungere una certa sicurezza imponendo politiche di accesso restrittive. Chi paga decine –a volte centinaia– di milioni di lire per un applicativo commerciale ovviamente pretende qualcosa in più ed i produttori si sono orientati verso soluzioni sempre più intelligenti.

La soluzione proposta dalla Checkpoint è tra le più evolute in fatto di sicurezza e configurabilità del prodotto. Il pacchetto Firewall One è disponibile sia per la piattaforma windows NT che per la piattaforma unix -Solaris o HPUX-. Le prove effettuate in effetti dimostrano che le piattaforme unix offrono performance di un'ordine di grandezza maggiore rispetto a quelle windows in una prova basata su 32 client operanti ognuno 500 connessioni contemporanee con banda di circa 5Mb/s -somma delle connessioni del singolo client-.

L'anima del Firewall One è l'architettura "Stateful Inspection", la quale garantisce il massimo della protezione contro qualunque tipo di attacco conosciuto. Un modulo di sorveglianza viene integrato nel kernel del sistema ospite e filtra tutti i pacchetti passanti dal livello di rete, sopra al quale si attesta, verso il sistema operativo. Nessun pacchetto viene visto dal sistema operativo prima di aver subito il controllo del firewall. Il modulo di sorveglianza accede all'intera struttura dei dati analizzando il corpo dei pacchetti in transito. Oltre agli IP ed alle porte TCP il prodotto Cechkpoint può quindi ricostruire il contesto di tutte le transazioni eseguite da qualsiasi protocollo superiore conosciuto. I parametri di controllo sono:

- Informazioni istantanee su tutti e sette i livelli ISO/OSI delle comunicazioni in corso.

- Stato derivato dalle comunicazioni precedenti. Il firewall ricorda l'evoluzione delle connessioni precedenti ed autorizza eventualmente nuove connessioni di risposta come nel caso dell'ftp attivo.

- Stato derivato dalle applicazioni. Il firewall ricava informazioni dallo stato degli altri applicativi per trarre conclusioni sullo stato di sicurezza della connessione. Ad esempio un utente telnet o ssh potrà accedere agli altri protocolli autorizzati solo se l'autenticazione di terminale ha successo.

- Elaborazione dell'informazione. La creazione di regole derivanti da tutti i precedenti parametri.

Le connessioni possono essere bloccate durante la loro esecuzione in qualsiasi momento nel caso in cui il software rilevi un calo di sicurezza. La regola generale è sempre e comunque conservativa e prevede che tutto quello che non è esplicitamente concesso deve essere negato. Si noti che questo tipo di architettura coniuga le caratteristiche favorevoli del filtraggio di pacchetto, il quale è implementato, alle caratteristiche del proxy-firewall. Il proxy in effetti ha la spiacevole caratteristica di spezzare la connessione tra client e

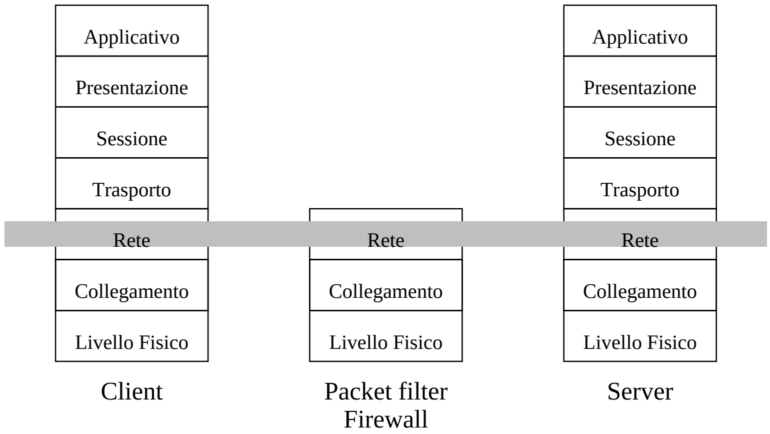

Figura 4.4: Firewall a filtraggio di pacchetto

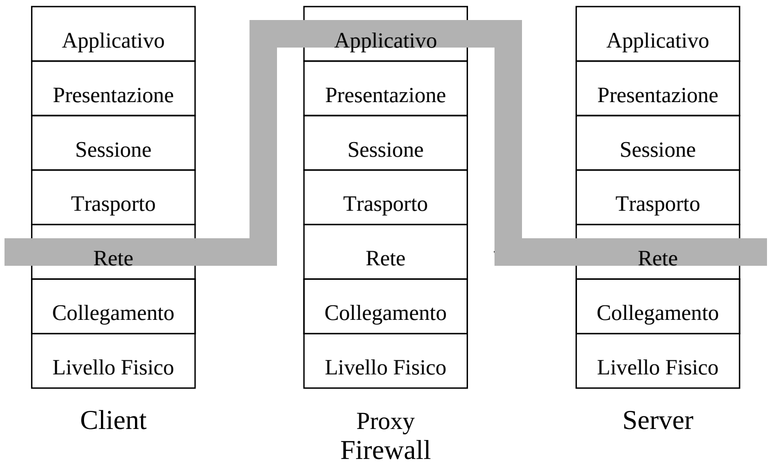

Figura 4.5: Proxy firewall

server insicuro in due tronconi mentre Firewall One lascia fluire i pacchetti pur mantenendo il pieno controllo sull'intera procedura di scambio dati. Nelle figure 4.4, 4.5 e 4.6 possiamo apprezzare i differenti percorsi dei dati.

Il modulo di sorveglianza deve essere configurato dall'utente ed allo scopo è stato concepito un linguaggio specifico detto "inspect language". Tale linguaggio permette di specificare regole di sicurezza riguardanti qualsiasi apetto dei dati in transito, dagli indirizzi di destinazione ad un particolare contenuto dei pacchetti stessi. Viene fornito anche un tool grafico che facilita il concepimento dello script di configurazione. Tale script inoltre è stato pensato per poter estendere in qualsiasi momento il campo di azione del firewall verso qualsiasi nuovo applicativo di rete e per offrire agli utenti politche di filtraggio sempre aggiornate tramite eventuali patch presenti sul sito del produttore.

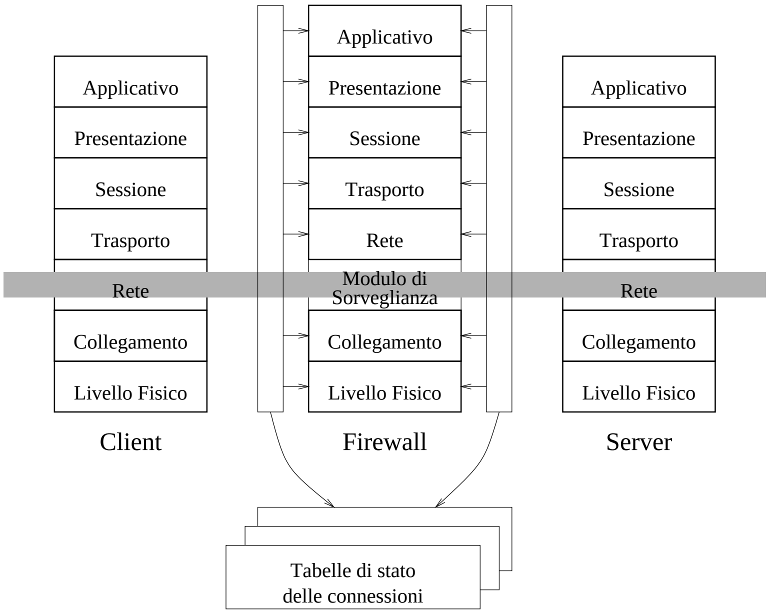

Figura 4.6: Firewall One

Altri software commerciali: principali caratteristiche

Il prodotto Checkpoint è uno dei riferimenti nel panorama commerciale per i software di sicurezza. Altre case hanno prodotti simili ed alcuni integrano ulteriori soluzioni per facilitare la vita dell'amministratore della sicurezza.

Uno dei difetti delle reti intranet sta nella necessità di mantenere due server DNS - domain name server-. Il primo, pubblico, deve risolvere gli indirizzi della rete pubblica mentre il secondo, appartenente alla rete interna ed irraggiungibile da Internet per mantenere oscure ad un'attaccante le risorse interne, deve fornire la risoluzione dei nomi per gli host interni. Alcuni prodotti come l'Altavista Software Firewall forniscono essi stessi un doppio server DNS attestato sulle interfaccie di rete opportune. Atri prodotti come il Labyrinth Firewall della CYCON integrano un sistema di load balancing -bilanciamento della banda- grazie al quale siti particolarmente "caricati" quali server web o ftp ad alto traffico possono funzionare senza la necessità di hardware stratosferici. In pratica il firewall provvede a redistribuire il carico convergente dalla rete su un unico indirizzo publico verso più indirizzi privati. Tali indirizzi privati devono corrispondere a computer, non necessariamente potentissimi, opportunamente configurati per rispondere tutti nello stesso modo alle richieste esterne.

Esistono infine un'infinità di altre varianti e migliorie, soprattutto a livello di interfaccia utente, introdotte da ogni singolo prodotto.

4.2 Hardware

In effetti la descrizione di architetture hardware specifiche per il firewalling non è facile poichè ogni produttore adotta in genere un'architettura specifica che indicativamente non si discosta granchè da quella di un qualsiasi PC ma che gode di una serie di ottimizzazioni hardware e software stupefacenti.

4.2.1 Router

In generale i router standard delle principali case costruttrici integrano alcune soluzioni di sicurezza di base quali NAT e PAT. Ultimamente si è assistito alla proliferazione di soluzioni basate sullo standard IPV6 le quali permettono ai router di stabilire connessioni VPN attraverso la rete pubblica in modo trasparente.

Eco alcune possibilità offerte dal software dei router Cisco (IOS).

- Controllo CBAC (Context-Based Access Control).Il motore CBAC di Cisco Secure IS fornisce controlli di accesso in base all'applicazione attraverso i perimetri della rete. CBAC migliora la sicurezza per le applicazioni di protocollo TCP e UDP che utilizzano porte conosciute, come FTP (File Transfer Protocol) e il traffico di posta elettronica, esaminando gli indirizzi di origine e di destinazione. Tale controllo consente agli amministratori di rete di implementare il firewall come parte di una soluzione unica integrata. Ad esempio, non sarà più necessario, per le sessioni in extranet che utilizzano applicazioni Internet, applicazioni multimediali o database Oracle, aprire una porta nella rete a cui è possibile accedere tramite punti deboli. Il controllo CBAC consente alle reti di eseguire il traffico applicativo di base attuale, così come le applicazioni avanzate, quali le applicazioni multimediali o le videoconferenze, attraverso un router, in maniera estremamente sicura. La verifica avviene su pacchetti TCP e UDP registrando lo stato degli stessi e della connessione. Durante l'inizializzazione della connessione, TCP passa attraverso diversi stati, o fasi, che sono facilmente identificabili tramite le intestazioni dei pacchetti–fase di triplo handshake, vedi pag. 13–. Gli elenchi ACL (Access Control List) standard ed estesi leggono gli stati dalle intestazione dei pacchetti per determinare se il traffico attraverso un determinato collegamento è autorizzato. Il controllo CBAC aggiunge alle funzionalità degli elenchi ACL una capacità di ispezione, leggendo l'intero pacchetto per esaminare le informazioni sullo stato dell'applicazione. Utilizzando queste informazioni, Esso crea una specifica voce ACL di sessione provvisoria, che consente il traffico di ritorno. Questo elenco ACL provvisorio apre una porta nel firewall. Quando una sessione scade o termina, la voce ACL sarà cancellata e la porta verrà chiusa ad ogni ulteriore traffico. Gli elenchi

ACL non possono creare voci di elenco temporanee, per cui sinora gli amministratori di rete sono stati costretti a soppesare il rapporto tra i rischi e l'esigenza di accesso alle informazioni. In passato, rendere sicure le applicazioni avanzate capaci di effettuare la selezione tra più canali per il traffico di ritorno usando gli elenchi ACL standard o estesi non si rivelava un'impresa facile. Prima dell'applicazione del controllo CBAC, gli amministratori potevano autorizzare il traffico applicativo avanzato solo redigendo degli elenchi ACL permanenti, il che, a conti fatti, equivaleva a lasciare le porte firewall aperte. Per questo la maggioranza degli amministratori in genere preferiva rifiutare questo tipo di traffico applicativo. Ora gli amministratori possono finalmente ammettere, senza rischi, il traffico multimediale e gli altri tipi di traffico applicativo, aprendo il firewall quando è necessario e tenendolo chiuso negli altri casi poiché è possibile valutare il tipo di applicazione per decidere se consentire una sessione attraverso il firewall adeguandosi alle selezioni di molteplici canali per il traffico di ritorno. Ad esempio, se CBAC è configurato per supportare Microsoft NetMeeting, quando un utente interno avvia una connessione, il firewall ammette il traffico di ritorno. Tuttavia, se una fonte NetMeeting esterna avvia una connessione con un utente interno, CBAC nega l'accesso e scarta i pacchetti.

- Rilevamento delle intrusioni. I sistemi IDS (Intrusion Detection Systems) forniscono un livello di protezione che va oltre il firewall, poiché protegge la rete da attacchi e minacce sia esterni che interni. La tecnologia IDS di Cisco Secure Integrated Software migliora la protezione firewall del perimetro intervenendo adeguatamente sui pacchetti e sui flussi che violano i criteri di sicurezza o costituiscono un'attività di rete ambigua.

- Rilevamento e risposta. La tecnologia IDS di Cisco Secure IS identifica i 59 più comuni attacchi per rilevare i motivi degli abusi nel traffico di rete assegnandogli una signature –o sigla–. Le sigle rappresentano importanti varchi nella sicurezza, i più comuni attacchi in rete e le scansioni della raccolta di informazioni. Cisco Secure IS opera come un sensore di rilevamento delle intrusioni in linea, controllando i pacchetti e le sessioni non appena questi fuoriescono dal router, analizzandone uno ad uno alla ricerca di sigle IDS. Quando rileva un'attività sospetta, reagisce prima che venga compromessa la sicurezza della rete e registra l'evento su syslog Cisco IOS. L'amministratore di rete può configurare il sistema IDS per scegliere il tipo di risposta adeguata alle minacce.Cisco ha sviluppato il software IOS basato sulle caratteristiche di rilevamento delle intrusioni nel Cisco Secure IS in maniera flessibile, in modo da consentire la disabilitazione di eventuali sigle individuali contraffatte. Inoltre, pur essendo preferibile abilitare entrambe le funzioni di firewall e di rilevamento delle intrusioni del motore CBAC di sicurezza per supportare correttamente i criteri di sicurezza di rete, ciascuna di queste funzioni può essere abilitata indipendentemente e su interfacce di router differenti. Tutte le piattaforme di router con Cisco Secure IS rilevano cinque tra i più comuni attacchi SMTP. Quando i pacchetti di una sessione identificano una sigla, il sistema ISD può essere configurato per:

  – Inviare un allarme a un server syslog o a un sistema Cisco Secure Intrusion Detection System (NetRanger) Director (interfaccia di gestione centralizzata)
  – Abbandonare il pacchetto
  – Riavviare la connessione TCP

- Proxy di autenticazione. Gli amministratori di rete possono creare specifiche regole di sicurezza per ciascun utente mediante l'autenticazione e l'autorizzazione dinamica, basata su LAN di Cisco Secure IS. In precedenza, l'identità e l'autorizzazione di accesso erano determinate da un dato indirizzo IP dell'utente oppure era necessario applicare un singolo criterio di sicurezza ad un intero gruppo di utenti o ad una rete secondaria. Oggi è possibile scaricare il criterio per l'utente nel router da un server di autenticazione TACACS+ o RADIUS utilizzando il software di autenticazione, autorizzazione e valutazione (AAA, Authentication, Authorization, and Accounting) Cisco IOS. Gli utenti possono effettuare la registrazione nella rete o su Internet mediante HTTP e i loro specifici profili d'accesso saranno scaricati automaticamente. I privilegi derivanti dall'accesso individuale dinamico proteggono la rete dai criteri più comunemente applicati ad un gruppo di utenti. L'autenticazione e l'autorizzazione possono essere applicate sul router in entrambe le direzioni per garantire la sicurezza delle extranet e delle intranet in entrata e in uscita, nonché dell'utilizzo di Internet.

- Rilevamento e prevenzione della negazione di servizio. Una migliorata capacità di rilevamento e prevenzione della negazione di servizi consente di difendere le reti dalle più comuni modalità di attacco, quali SYN (SYNchronize/start), scansioni della porta e infezioni dei pacchetti, ispezionando le sequenze numeriche dei pacchetti nelle connessioni TCP. Se i numeri non rientrano nella gamma prevista, il router scarta i pacchetti sospetti. Quando il router rileva un'inusuale quantità di nuove connessioni, invia un messaggio di allarme, quindi scarta la connessione TCP attiva per prevenire l'esaurimento delle risorse di sistema. Quando Cisco Secure IS rileva un eventuale attacco, traccia l'accesso utente in base all'indirizzo di origine e di destinazione e le coppie di porte. Inoltre esegue il dettaglio della transazione, creando un procedimento di verifica.

- Mappatura dinamica di porta. La mappatura di porta flessibile, per applicazione, consente di eseguire le applicazioni supportate da CBAC su porte non standard. Questa funzione permette agli amministratori di rete di personalizzare il controllo per applicazioni e servizi specifici al fine di soddisfare le esigenze locali delle proprie reti.

- Bloccaggio delle applet Java. Con il proliferare delle applet Java disponibili su Internet, la protezione della rete contro i pericoli eventualmente associati a queste applicazioni è diventata una grossa preoccupazione per i responsabili di rete. Il bloccaggio Java può essere configurato in modo da filtrare o rifiutare completamente l'accesso alle applet Java che non siano memorizzate in un archivio o compresse in file.

- VPN, Cifratura IPSec e supporto QoS –Quality of Service–. Combinato con la tecnologia IPSec di Cisco, Cisco Secure IS fornisce funzioni integrate VPN (vedi figura 4.7). Le VPN si stanno sviluppando velocemente per eseguire il trasferimento di dati sicuro sulle linee pubbliche (come Internet); riducono i costi relativi alle telecomunicazioni e di gestione per gli utenti remoti, le filiali e le extranet; inoltre, stanno potenziando l'affidabilità. Per garantire la sicurezza delle VPN, Cisco Secure IS interagisce con la cifratura e il tunneling del software Cisco IOS. Le caratteristiche di cifratura in rete consentono di prevenire l'intercettazione o la corruzione dei dati durante la trasmissione. Cisco Secure IS consente di cifrare dati per comunicazioni private su reti non conosciute mediante gli standard di cifratura del protocollo di sicurezza di Internet (IPSec, Internet Protocol Security), sia a 56 bit (DES) che a 168 bit (3DES). Per la massima interazione, il software Cisco IOS supporta vari protocolli di tunneling standard che lavorano con incapsulamento di instradamento generico (GRE, Generic Routing Encapsulation), invio Layer 2 (L2F) e protocollo di tunneling Layer 2 (L2TP). Le funzioni QoS classificano il traffico, gestiscono la congestione e distribuiscono le applicazioni secondo la priorità richiesta. Cisco Secure IS può essere implementato con piattaforme VPN Cisco, in particolare i router Cisco serie 1720, 2600, 3600 e 7100, che estendono una rete esistente a livello di rete privata virtuale. Le soluzioni VPN devono fornire tunnel di cifratura assolutamente sicuri sulle strutture delle reti pubbliche. Devono inoltre garantire una consegna dei dati tempestiva ed affidabile, nonché fornire un elevato livello di sicurezza perimetrale per il portale delle aziende sulla rete pubblica.

- Allarmi in tempo reale, controllo e registrazione degli eventi. Gli allarmi in tempo reale inviano messaggi di errore syslog alla console di

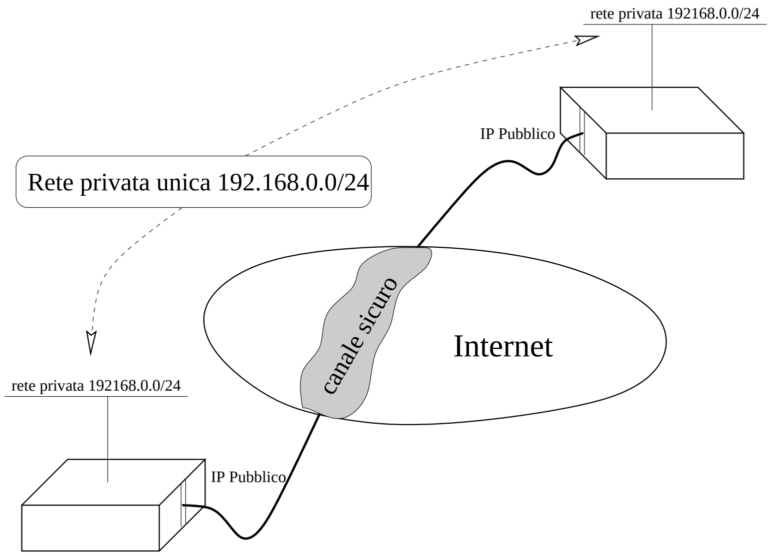

Figura 4.7: Rete privata virtuale (VPN)

gestione centrale dopo il rilevamento di attività sospette, consentendo ai gestori della rete di rispondere immediatamente alle intrusioni. Le migliorate funzioni di controllo utilizzano syslog per tenere traccia di tutte le transazioni, la registrazione di data e ora, l'host di origine, l'host di destinazione, le porte utilizzate, la durata della sessione ed il numero totale dei byte trasmessi per un reporting avanzato della sessione. Ora è possibile configurare gli allarmi e le funzioni di verifica di Cisco Secure IS, consentendo in questo modo un reporting più flessibile e la traccia degli errori. Le funzioni di controllo configurabili supportano tracce modulari di specifiche applicazioni supportate da CBAC e bloccaggio Java. Sia la funzione di allarmi in tempo reale che quella di controllo sono supportate da una serie di strumenti di reporting. Quando si verifica un evento di rete, invia un allarme all'host di registrazione mediante il meccanismo syslog del software Cisco IOS. Consente agli amministratori di individuare in tempo reale eventuali intrusioni o altre attività non standard, registrando i messaggi di errore di sistema su un terminale di consolle o un server syslog, impostando il livello di gravità della violazione e registrando anche altri parametri.

4.2.2 Architetture specifiche

Esistono architetture ultra-dedicate al firewalling come il WatchGuard Firebox o i Cisco della serie PIX -vedi figura 4.8-. In questi casi

l'hardware è quasi completamente realizzato "su misura" per cui la comprensione del contenuto di queste scatole preziosissime -nell'ordine di diverse

Figura 4.8: Firewall PIX Cisco

decine di milioni- è concesso esclusivamente a pochi. Il PIX è un prodotto che si pone ai vertici della categoria per sicurezza, scalbilità e soluzioni implementabili. Esso richiede una configurazione di base che può essere eseguita da console e un affinamento ulteriore tramite tool grafici (PIX firewall manager). Anche senza una configurazione precisa il PIX ricava informazioni dal traffico dati e pubblicizza se stesso come gateway predefinito su tutte le reti su cui si attesta iniziando a ruotare pacchetti con la massima sicurezza in base alla provenienza. Il cablaggio deve essere eseguito ina base ai criteri descritti più avanti. Ovviamente il firewall pubblicizza solo se stesso e non trasmette altri dati circa le sue reti. PIX può montare al massimo quattro interfaccie di rete, siano esse token ring o lan 100Mb/s, oppure può utilizzare le interfaccie per reti private virtuali -Private Link Card-. Il minimo numero di interfaccie è due per garantire la separazione tra rete sicura e rete insicura. Le ulteriori due interfaccie vengono definite dal firewall come "reti perimetrali" a sicurezza diversa l'una dall'altra. Il livello di sicurezza accordato ad ogni rete è uno dei parametri decisionali per lo smistamento dei pacchetti. Un pacchetto proveniente da una rete non può transitare verso una rete a sicurezza più elevata senza una specifica richiesta precedente inoltrata dall'interno della rete di destinazione o una specifica regola impostata dall'amministratore –vedi figura 4.9–. I pacchetti entranti vengono prima di tutto esaminati tramite l'algoritmo ASA discusso più avanti. Se sopravvive all'esame il pacchetto viene confrontato con le connessioni precedenti per capire se si tratta di una nuova connessione o meno. In quest'ultimo caso il firewall crea uno slot di traslazione in cui salva ip sorgente e destinazione, indirizzo di NAT e altri parametri. A questo punto viene eseguito il NAT –ove richiesto– e il pacchetto lascia il firewall. I pacchetti di ritorno devono sottostare alle regole preimpostate dopodiché vengono confrontati con gli slot attivi per accettare solo quanto richiesto. In figura 4.10 vediamo una tipica applicazione firewall.

Non mancano soluzioni per aumentare la banda gestibile tramite l'accoppiamento di più firewall e la presenza di un'opzione failover: tramite tale

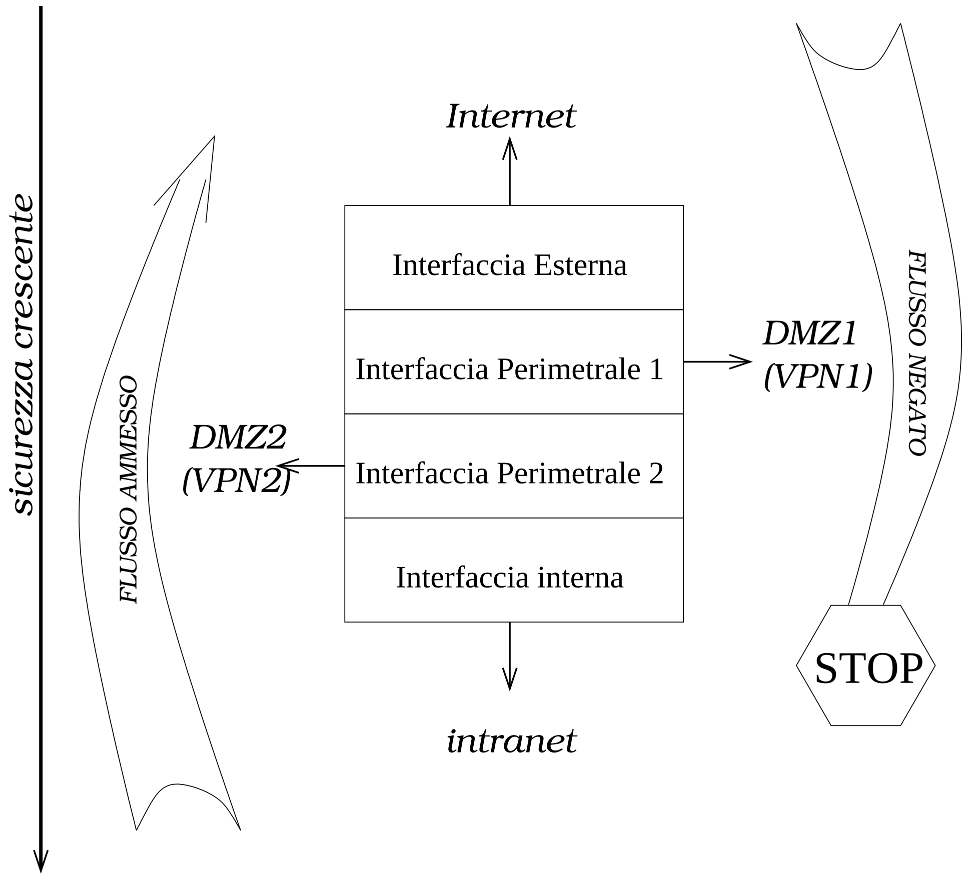

Figura 4.9: Politca di sicurezza sulle interfacce del PIX

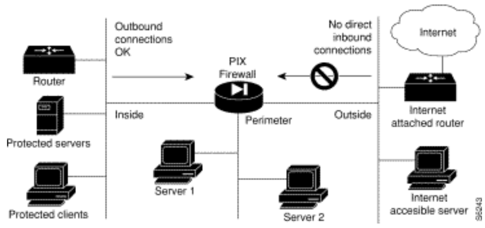

Figura 4.10: Esempio di rete dotata di firewall PIX

funzionalità, duplicando tutti gli apparati, è possibile gestire la partenza a caldo di un firewall di riserva qualora il suo corrispettivo vada in avaria –il tutto il un massimo di quarantacinque secondi–. La situazione di avaria, anche senza la presenza di un "gemello" pronto ad intervenire, è gestita in modo da mantenere il massimo livello di sicurezza. Tutti gli accessi vengono bloccati e tutte le sessioni telnet vengono reimpostate durante la fase di reboot automatica del router.

Ecco le caratteristiche più comuni per la serie PIX:

- Utilizzi di access list centralizzate (AAA). Si veda quanto detto a pagina 29 per il Context-Based Access Control.

- Algoritmo ASA. Garantisce la sicurezza costante di tutte le sessioni TCP/IP per proteggere le risorse private e critiche. Esso stabilisce che nessun pacchetto possa attraversare il firewall senza una connessione in corso ed uno stato assegnato. Tutte le connessioni uscenti -dove per "uscenti" si intendono le connessioni da interfaccie ad alta sicurezza verso interfaccie a sicurezza minore- sono autorizzate tranne quelle specificatamente negate dalla configurazione. Tutte le connessioni entranti invece sono negate a meno di istruzioni contrarie nella configurazione. Tutti i pacchetti che violano queste regole sono distrutti. I pacchetti ICMP sono distrutti anch'essi a meno di non autorizzarli espressamente. In realtà è bene autorizzare alcuni tipi di pacchetto ICMP.

- Proxy cut-through. Fornisce prestazioni di autenticazione al livello più elevato che oggi sia possibile raggiungere. Come nei proxy la sicurezza dei dati viene gestita su tutti i sette livelli ISO/OSI senza aggravi in termini di velocità e permette di autenticare il singolo utente sulle connessioni che effettua.

- Sistema incorporato sicuro e in tempo reale. Consente una maggiore sicurezza rispetto ai sistemi operativi aperti di tipo standard, come UNIX e NT Workstation.

- Schede di interfaccia di rete multiple. Massima sicurezza per il server Web e per tutti gli altri server ad accesso pubblico –da attestare su una DMZ–; collegamenti extranet multipli con partner diversi; server di registrazione e filtraggio URL protetti ed altro ancora.

- Prevenzione degli attacchi contro il servizio negato. Difende il firewall nonché i server e i client ad esso collegati da eventuali intrusioni dall'esterno; protegge inoltre tutte le operazioni e i servizi dagli attacchi contro il servizio negato. Gli attacchi di tipo SYN-flood vengono bloccati monitorando tutte le richieste di connessione verso gli host protetti. Il router verifica l'esistenza e la consistenza del richiedente in prima persona dopodiché avvia una richiesta verso l'host protetto riallacciando la connessione. Inoltre è possibile specificare il massimo numero di connessioni gestibili dagli host per cui il meccanismo di sicurezza entra in gioco anche in caso di impennate improvvise nelle richieste e permette di evitare gli attacchi di tipo "denial of service".

- Supporto fino a 256.000 connessioni contemporanee con 128Mb di ram e licenza software opportuna. Risultati nettamente superiori a quelli dei server proxy; è possibile utilizzare un numero inferiore di firewall a parità di banda gestibile.

- Filtraggio URL. Consente di controllare quali sono i siti Web frequentati dagli utenti, nonché di generare un rapporto di attività a fini contabili. In realtà questa funzione rallenta le prestazioni del PIX per cui, ove essa sia necessaria, è d'obbligo una configurazione dotata di un numero adeguato di firewall.

- Filtri per applet Java. Consente al firewall di bloccare le applicazioni Java potenzialmente pericolose operando a livello di singolo client o singolo indirizzo IP.

- Mail Guard. Elimina la necessità di un'applicazione di relay di posta esterna sul perimetro di rete, eliminando così gli attacchi contro il servizio negato su relay di posta esterna.

- Supporto per applicazioni multimediali.

- Traduzione NAT (Network Address Translation).

- PIX Private Link Card. La scheda di cifratura Cisco PIX Private Link consente di ottenere maggiori ritorni sugli investimenti effettuati per i collegamenti Internet, poiché trasforma la rete mondiale in una rete privata virtuale (VPN, figura 4.7) di lunga portata, solida e ben innervata. Mentre Cisco PIX Firewall protegge i dati e i sistemi LAN dalle intrusioni via Internet, le schede di cifratura Cisco PIX Private Link trasformano Internet in un canale sicuro per le comunicazioni private, collegando più PIX Firewall in una VPN. PIX utilizza la cifratura dei dati su base DES e tecnologie di base standard, grazie all'integrazione dei protocolli IETF Authentication Header/Encapsulating Security Payload (AH/ESP) (RFCS 1826 e1827, rispettivamente). La gestione principale è fornita mediante un massimo di sette chiavi precondivise, che possono essere modificate in momenti prestabiliti.

Capitolo 5

Prospettive future

La sempre maggiore diffusione di Internet porterà con se, dicono gli esperti, un sempre maggiore utilizzo di firewall nonchè l'assunzione da parte di grandi aziende, di personale che dovrà garantire la sicurezza della intranet aziendale. Qualcuno pensa che nasceranno scuole dedicate alla formazione culturare di questi amministratori di rete, ma già tutt'oggi vediamo nelle principali università la nascita di gruppi di ricerca legate alle problematiche di sicurezza delle reti.

Un elevato numero di esperti sarebbe propenso nel concedere l'accesso alla rete agli utenti solo attraverso un apposito identificativo. In tal modo, sarebbe più facile risalire agli attaccanti che tentano di violare un sistema e limiterebbe la voglia di alcuni hacker di mettere alla prova le proprie capacità informatiche. Se essi per testare le proprie conoscenze provassero ad attaccare un qualsiasi server web, pur poco protetto e quindi riuscissero nel loro intento di violazione dell'host, sarebbero facilmente rintracciabili ed eventualmente perseguiti legalmente. Purtroppo, attualmente, questa politica di assegnare una "carta di identità multimediale" ai vari utenti richiederebbe un enorme supplemento di lavoro alle compagnie che gestiscono l'accesso alla rete. Si presuppone, però, che in un futuro non troppo distante: quando molti utenti avranno un collegamento permanente su Internet 24 ore su 24, la precedente proposta verrà esaminata seriamente e forse messa in pratica.

Infine, per quanto riguarda l'utilizzo di firewall hardware e software, commerciali e gratuiti, si pensa che ci sarà una divisione del mercato. Indubbiamente, si pensa che i grandi portali web che fatturano parecchi miliardi di lire al mese si sposteranno verso soluzioni hardware commerciali, mentre le piccole aziende con sbocco sulla rete ed i piccoli siti web si dirigeranno verso soluzioni molto più economiche: software o hardware di bassa fascia. Tutto ciò è comunque vincolato al fatto che difficilmente una home-page o una piccola società possa essere l'obiettivo principale di possibili attaccanti. Discorso a parte va fatto per le università, dove si pensa che una soluzione commerciale verrà affiancata da un progetto di incremento della sicurezza portato avanti da appositi gruppi di ricerca.

Capitolo 6

Glossario

RPC: Remote Procedure Call

RPC, acronimo di Remote Procedure Call, è un meccanismo generale per la gestione di applicazioni client-server. Il sistema si basa su un demone, il portmapper, e un file che elenca i servizi disponibili associati al relativo demone. Il portmapper è un classico esempio di un programma che gestisce un servizio di rete in modo autonomo, cioè senza essere controllato da inetd.

6.0.3 RPC in generale

Semplificando in modo estremo il funzionamento delle RPC, si può dire che si tratta di un meccanismo attraverso cui si possono eseguire delle elaborazioni remote. Dal lato server si trova il portmapper in ascolto sulla porta 111, dal lato client ci sono una serie di programmi che, per un qualunque servizio RPC, devono prima interpellare il portmapper remoto. Il portmapper remoto fornisce a questi programmi le informazioni necessarie a stabilire una connessione con il demone competente. Per questo motivo, le chiamate RPC contengono l'indicazione di un numero di programma, attraverso il quale il portmapper remoto è in grado di rispondere informando il client sul numero di porta da utilizzare per quel programma.

Portmap

È il demone che si occupa di attivare i servizi RPC. Potrebbe anche chiamarsi rpc.portmap.Viene avviato di norma durante la procedura di inizializzazione del sistema, in modo indipendente dal controllo di inetd.

Rpcinfo

Rpcinfo permette di interrogare un portmapper. L'utilità di questo programma sta quindi nella possibilità di conoscere quali servizi RPC sono disponibili all'interno di un certo nodo e nella possibilità di verificare che questi siano

Figura 6.1: Pila ISO/OSI

effettivamente in funzione. Rpcinfo può, utilizzando protocollo UDP o il protocollo TCP, eseguire una chiamata RCP circolare (broadcast) a tutti i nodi in grado di riceverla ed il risultato viene emesso attraverso lo standard output.

6.1 Il modello ISO/OSI

Il protocollo OSI è organizzato in sette strati e schematizza quello che normalmente accade durante un processo di comunicazione via cavo. I sette strati, visualizzati in figura 6.1 sono i seguenti:

- strato 1, o strato fisico, che definisce le caratteristiche del segnale che deve essere trasferito tramite il canale. In questo strato sono definite caratteristiche quali l'ampiezza dell'impulso, la codifica della linea, la velocità di trasmissione, il tipo di connettore e quant'altro sia necessario alla trasmissione in maniera soddisfacente di un segnale digitale;

- strato 2, o strato di collegamento, che racchiude le istruzioni per il raggruppamento delle informazioni binarie. Si occupa della rilevazione e della correzione degli errori, racchiudendo i bit in frame. Attualmente tutti i formati di questo strato derivano da uno standard conosciuto come HDLC (High-level Data Link Control);

- strato 3, o strato di rete, che assicura il corretto indirizzamento dei messaggi verso la destinazione appropriata, e che inoltre provvede al meccanismo che assicura il controllo dei messaggi di conferma da parte dei destinatari;

- strato 4, o strato di trasporto, che collega i due terminali: i dati possono essere trasferiti da un terminale all'altro utilizzando vari formati degli strati 1, 2 e 3 (ad esempio tramite una LAN e ISDN), ma i terminali debbono ricevere le informazioni con le velocità appropriate;

- strato 5, o strato di sessione, che definisce il modo in cui gli applicativi ai due estremi del collegamento interagiscono fra loro, incluso il metodo di chiamata, di coordinazione delle loro attività durante la sessione di lavoro e di chiusura del collegamento;

- strato 6, o strato di presentazione, che stabilisce i formati usati da entrambi i terminali per rappresentare i dati ed i metodi per la loro gestione;

- strato 7, o strato dell'applicazione, che è in pratica l'operazione da compiere, ad esempio il trasferimento di un documento o la consultazione di un catalogo o di un orario.

Steven M. Bellovin and William R. Cheswick, *Network Firewall*

Bibliografia

[1] Michael Greenwald, Sandeep K. Singhal, Jonathan R. Stone, David R. Cheriton, *Designing an Accademic Firewall: Policy, Practice, and Experience whit SURF*

[2] Wolfgang Weber, *Firewall Basics*

[3] J.P. Anderson, S. Brand, L. Gong, T. Haigh, *Firewalls: an expert roundtable*

[4] David M. Martin, Aviel D. Rubin, Sivaramakrishnan Rajagopalan, *Blocking Java Applets at the Firewall*

[5] Chris Herringshaw, *Detecting Attacks on Networks*

[6] Rolf Oppliger, *Security at the Internet Layer*

[7] Sito Cisco: *www.cisco.com*

[8] Marcus Goncalves. *Firewalls complete*