Firewall

Motivazioni

Molte problematiche di sicurezza dei sistemi informatici ed in particolare delle reti nascono dalla necessita di proteggere:

- Dati
  - Privacy
  - Integrità
  - Disponibilità
- Risorse
  - Integrità hardware e software
  - Tempo di calcolo / memoria
- Reputazione
  - Furto di identità (es. accesso a chiavi private)
  - Catena di attacchi (mascheramento provenienza originaria)
  - Presenza materiale indesiderato in archivi pubblici
  - Web site defacement (modifica del contenuto di una pagina o di un sito web mediante l'introduzione illecita di testi)

Sicurezza delle reti

- Sicurezza a livello singola macchina (“host level”)
  - Ogni sistema e dotato di misure di protezione individuali `
  - Non scalabile e di difficile gestione
  - Schema soggetto ad errori
  - Non si adatta ad ambienti eterogenei per architetture e software
- Sicurezza a livello rete (“network level”)
  - Controllo d’accesso concentrato (hw/sw dedicato)
  - Scalabile, gestibile, adattabile
  - Minore flessibilità

Progetto di un sistema firewall

Definizioni

Firewall
Insieme di componenti che regola gli accessi ed il traffico tra due o più reti

Host bastione, single e dual-homed
Sistema la cui sicurezza deve essere salvaguardata in modo particolare, poiché esposto ad attacchi (es. fornisce servizi pubblicamente accessibili o rappresenta il punto di interfaccia tra la rete Internet ed una rete interna). Dual-homed se interfacciato a più di una rete (es. accessibile tanto da Internet quanto da una rete interna)

Router e router filtranti
Apparecchio che effettua l’instradamento del traffico tra due o più reti

Proxy server
Sistema che prende in carico richieste a server esterni per conto di client interni, filtrando eventualmente tali richieste

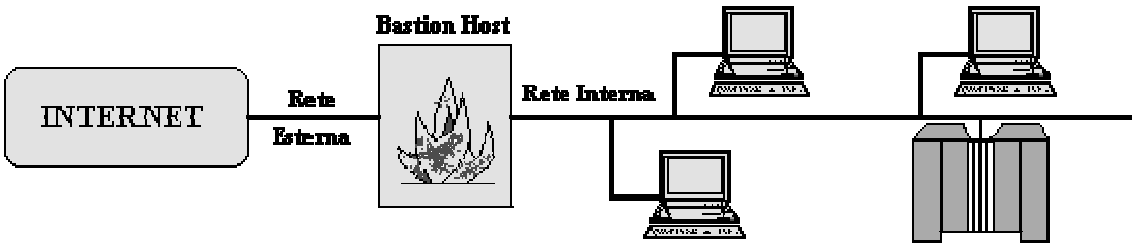
Firewall

Esistono diversi tipi di firewall che funzionano su diversi livelli del modello OSI. A seconda del tipo di servizio e della sicurezza necessari per la tua rete, devi scegliere il tipo giusto di firewall. Di seguito sono elencati sette diversi tipi di firewall che sono ampiamente utilizzati per la sicurezza della rete.

- Firewall host schermati
- Firewall di sottorete schermati
- Firewall di filtri a pacchetto
- Firewall di ispezione stateful
- Firewall ibridi
- Firewall server proxy
- Firewall di livello applicazione (gateway)

Bastion host

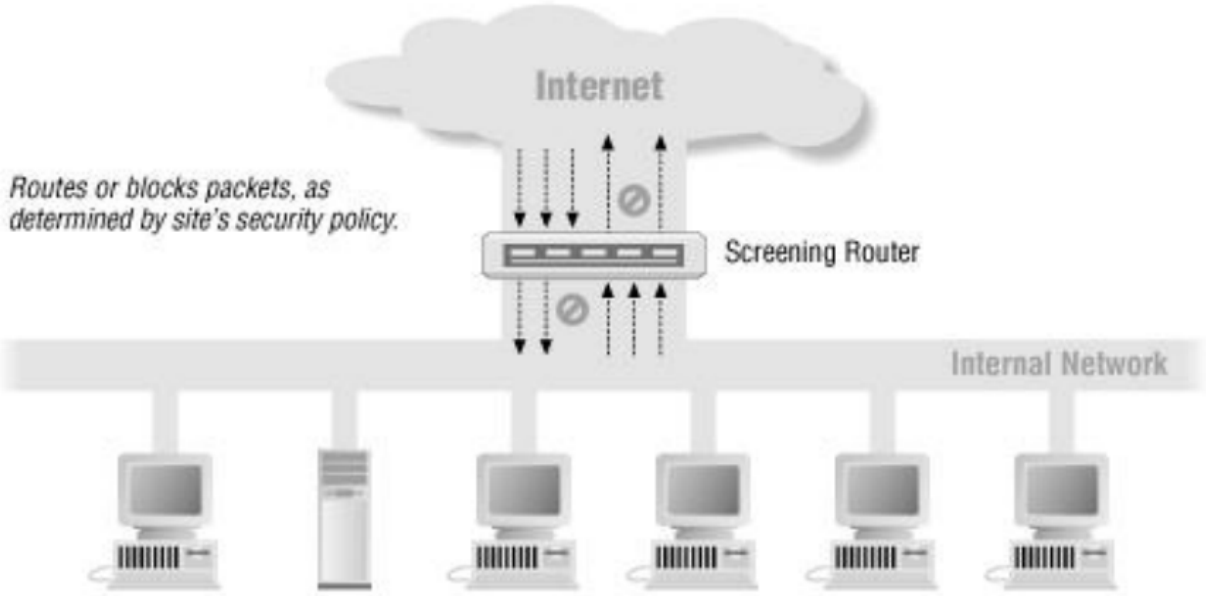
Parlando dei firewall, si incontrerà spesso il termine bastion host. Questo nome deriva dal termine bastione che nel medioevo indicava un particolare punto delle fortificazioni di un castello che aveva lo scopo di respingere gli attacchi nemici. Un bastion host è un computer della rete particolarmente preparato a respingere attacchi contro la rete stessa. I progettisti di reti posizionano il bastion host nella prima linea di difesa. Un bastion host costituisce un punto nevralgico per tutte le comunicazioni fra la rete e Internet. In altre parole, nessun computer della rete può accedere a Internet senza passare attraverso il bastion host e nessun computer di Internet può accedere alla rete senza passare attraverso il bastion host. Se si concentra ogni accesso alla rete in un unico computer, può essere molto facile gestire la sicurezza della rete. Inoltre, facendo in modo che una sola macchina possa accedere a Internet, è facile configurare il software in modo appropriato per proteggere la rete.
Con il termine bastion host si identificano tutti quei firewall host critici per la sicurezza della rete in questione; data la sua importanza nella sicurezza di rete, tale host deve essere ben fortificato e l'accesso diretto a tale host deve essere massimamente controllato. Il bastion host effettua la funzione di interfaccia tra la rete interna e quella esterna e per questo è spesso soggetto di attacchi dall'esterno ma del resto la sua più classica configurazione d'uso è quella di primo ed unico punto di contatto tra privato e pubblico dominio.



Le caratteristiche salienti di un bastion host possono essere riassunte come segue:

- unico calcolatore della nostra rete raggiungibile da Internet
- host massiciamente protetto
- sistema operativo sicuro
- rimozione software non necessario
- rimozione compilatori
- proxy server in ambiente isolato
- read-only file system
- process checker
- integrity file system checker
- numero minimo di servizi
- nessun account utente
- salvataggio e controllo del log
- eliminazione dei servizi non fidati
- disattivazione del source-routing.

Router filtrante (TCP/IP)

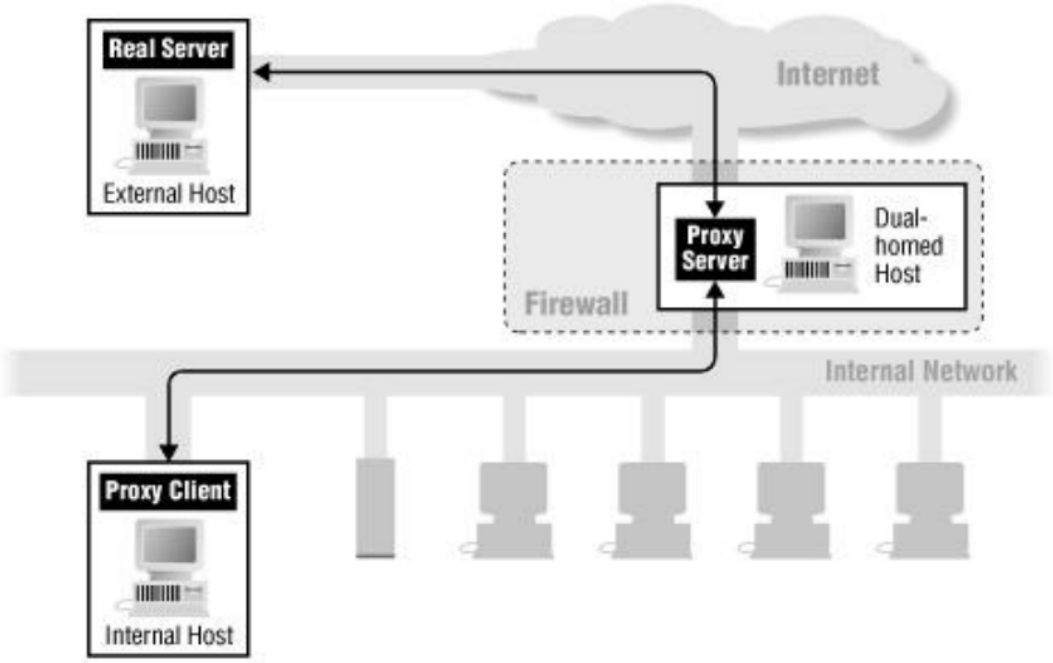


Filtraggio sulla base dell'informazione contenuta nel singolo pacchetto

- Indirizzo IP sorgente
- Indirizzo IP destinazione
- Tipo di protocollo di trasporto (TCP, UDP, ICMP, ...)
- Porta TCP/UDP sorgente
- Porta TCP/UDP destinazione
- Tipo di messaggio ICMP

Esempio: blocco connessioni entranti tranne quelle sulla porta 25/TCP dell'host mail-server e su 80/TCP dell'host www-server

Proxy server (Application gateway)

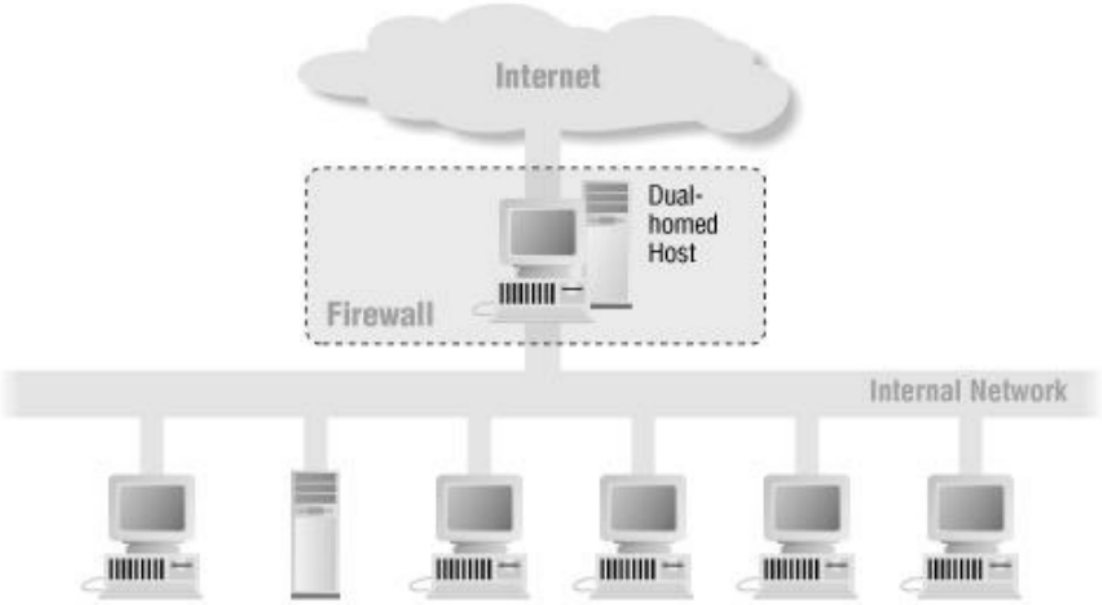


- Lavora a livello applicazione
- Funge da tramite fra client e server inoltrando le richieste e presentando le risposte
- Filtra le richieste in accordo con la policy di sicurezza
- Effettua funzioni di caching

Architetture

- Dual-homed host
- Screened host
- Screened subnet
- Architetture combinate
- DMZ

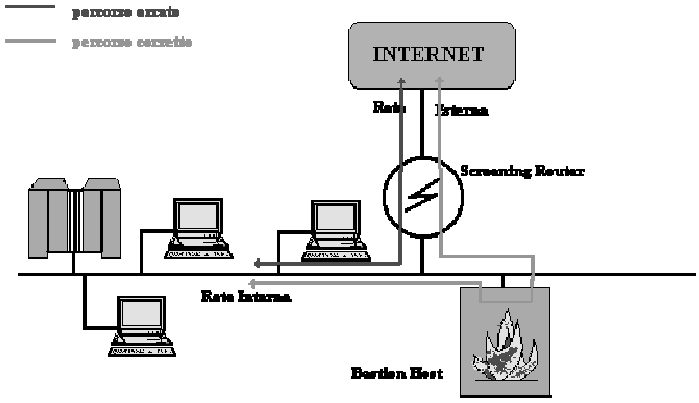
Architettura dual-homed host



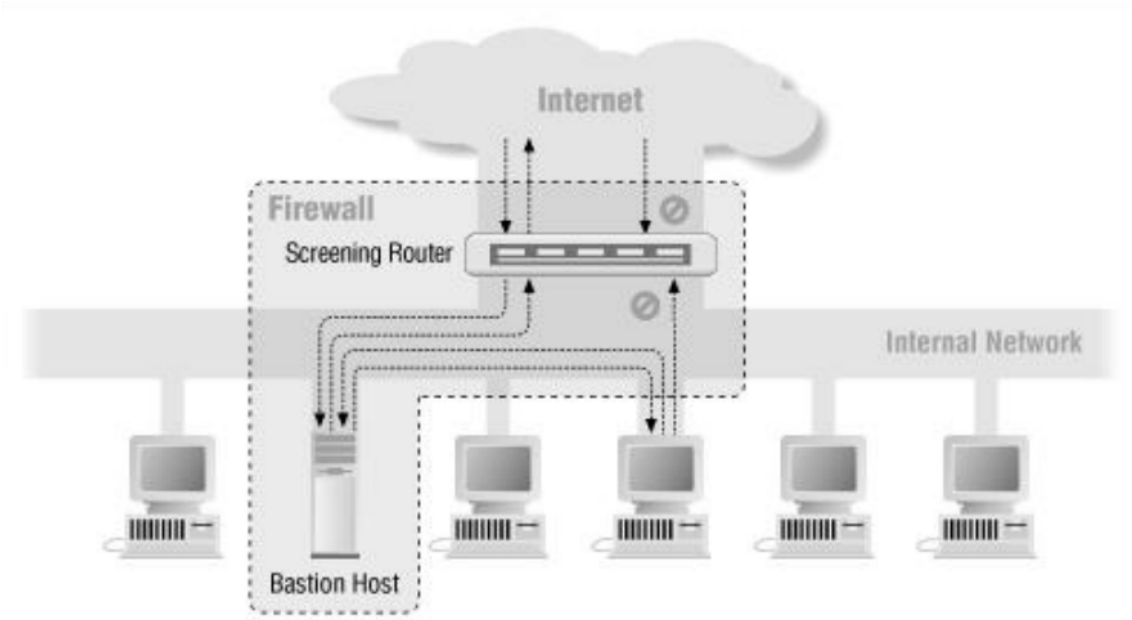
- No routing (traffico IP diretto non consentito)
  - Accesso solo mediante application gateway (HTTP, SMTP, ...)
  - Accesso mediante login esplicito (necessaria particolare attenzione agli account)
- Non adeguata a fornire servizi pubblicamente disponibili
  - Possibile compromissione diretta di host sulla rete interna

Architettura screened host

Data l'importanza del bastion host all'interno del sistema di sicurezza, spesso si pone una prima linea di difesa tra la rete esterna e quella interna dove il bastion host viene inserito; la prima linea di difesa può essere rappresentata da uno screening router opportunamente configurato secondo la politica di sicurezza scelta. Ovviamente tutti i pacchetti che ottengono il permesso di accesso alla rete interna devono essere diretti verso il bastion host. In questo modo un intruso che voglia entrare nella rete privata (o interna) dovrà prima eludere le regole di filtraggio dello screening router e quindi i controlli effettuati dal bastion host.
Questo usa le funzioni del livello di applicazione per capire se il pacchetto può essere inoltrato oppure no, eseguendo quindi un ulteriore controllo sugli header dei pacchetti.



Quindi, il ruolo delle tavole di filtraggio dello screening ruoter, risulta di fondamentale importanza; infatti, se vengono variati i campi relativi agli indirizzo di destinazione dei pacchetti da inoltrare, non solo lo screening router non svolgono più il ruolo per è impiegato, ma se viene settato un indirizzo di destinazione interno diverso dal bastion host, si viene a perdere anche la funzione di controllo di quest'ultimo in quanto viene completamente scavalcato. Le tabelle di filtraggio dovranno quindi essere memorizzate in un posto difficilmente accessibile a qualsiasi operatore esterno. Inoltre, generalmente i ruoters effettuano un aggiornamento delle loro tabelle (dynamic router) anche in base a dei pacchetti ICMP spediti da e verso altri router; tale funzione dovrà essere disabilitata all'interno dello screening router (static router), altrimenti potrebbero essere oggetto di falsi pacchetti ICMP spediti da parte di un intruder mascherato da router, inoltre le tabelle di instradamento saranno gestite staticamente dall'amministratore di rete senza aggiornamento dinamico (protocollo ARP). Ciò avviene impostando inizialmente le tabelle di instradamento (ARP table); in tale caso il router non si deve preoccupare di aggiornarle e quindi non comunica a nessuno il suo indirizzo fisico, senza il quale nessun host si può mascherare da router per spedirgli un pacchetto ICMP falso.



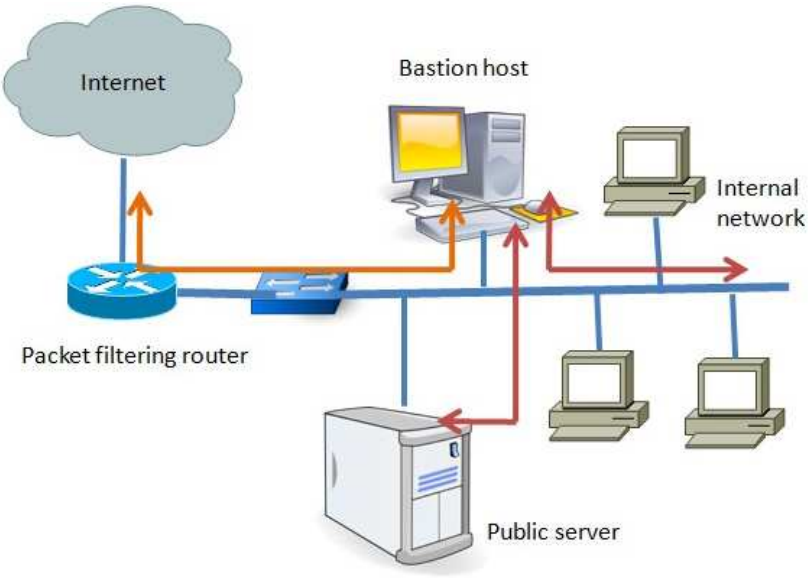
- Router filtrante + host bastione nella rete interna
- Servizi pubblicamente accessibili
    - Connessioni dall'esterno permesse verso il solo bastione per i protocolli ammessi
- Accesso esterno
    - Accesso diretto coi protocolli consentiti via packet filtering
    - Accesso indiretto mediante proxy sul bastione
- Debolezze
    - La compromissione del bastione implica la compromissione della rete interna (single point of failure)
    - Necessarie forti misure di sicurezza host level
    - La compromissione del router implica la compromissione della rete interna
- Vantaggi
    - Configurazione del router meno soggetta ad errori rispetto a quella del dual-homed host

Esistono due tipi di host schermati

1. host bastion single homed
2. host bastion dual homed

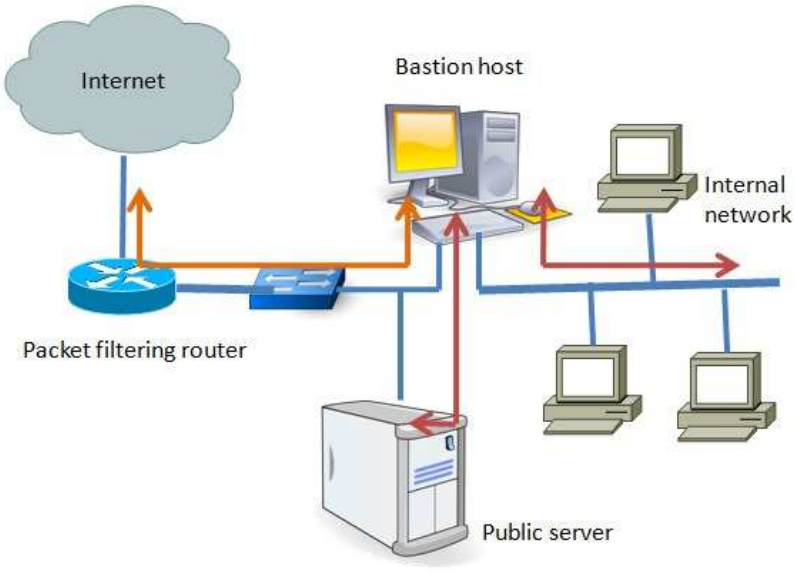
In caso di host bastion single-homed, il sistema firewall è costituito da un router per il filtraggio dei pacchetti e un host bastion. Un host bastion è fondamentalmente un singolo computer con configurazione ad alta sicurezza, che ha le seguenti caratteristiche:

- Il traffico da Internet può raggiungere solo l'host del bastione; non può raggiungere la rete interna.
- Il traffico con l'indirizzo IP dell'host del bastione può solo accedere a Internet. Nessun traffico dalla rete interna può andare su Internet.



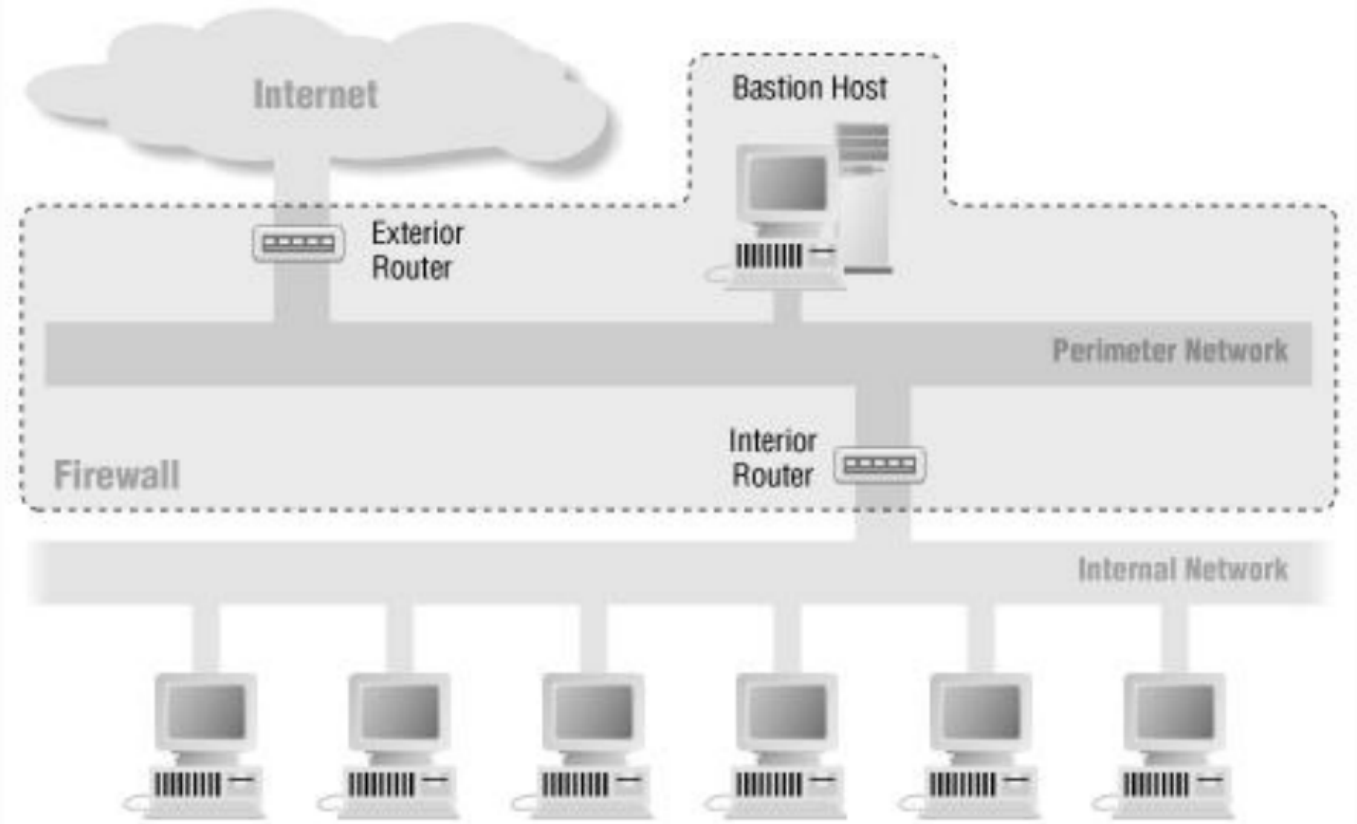
Screened host firewall (single-homed bastion host)

Questo tipo di configurazione può avere un server Web posizionato tra il router e l'host bastion per consentire al pubblico di accedere al server da Internet. Il problema principale con l'host bastion single-homed è che se la route del filtro dei pacchetti viene compromessa, l'intera rete verrà compromessa. Per eliminare questo inconveniente, è possibile utilizzare il sistema di firewall host bastion dual homed , in cui un host bastion dispone di due schede di rete, una per la connessione interna e la seconda per la connessione con il router. In questo caso, anche se il router viene compromesso, la rete interna rimarrà inalterata poiché si trova nella zona di rete separata.



Screened host firewall (Dual-homed bastion host)

Architettura screened subnet



- Rete perimetrale (DMZ, DeMilitarized Zone)
- L'intrusione sugli host bastione NON da accesso diretto alla rete interna (multiple points of failure)
- Possibilita strati multipli
    - Strati piu esterni: risorse più vulnerabili

- DMZ
    - Impossibilità di intercettare il traffico sulla rete interna
    - Possibile intercettazione del traffico Internet-rete interna e rete interna-bastione

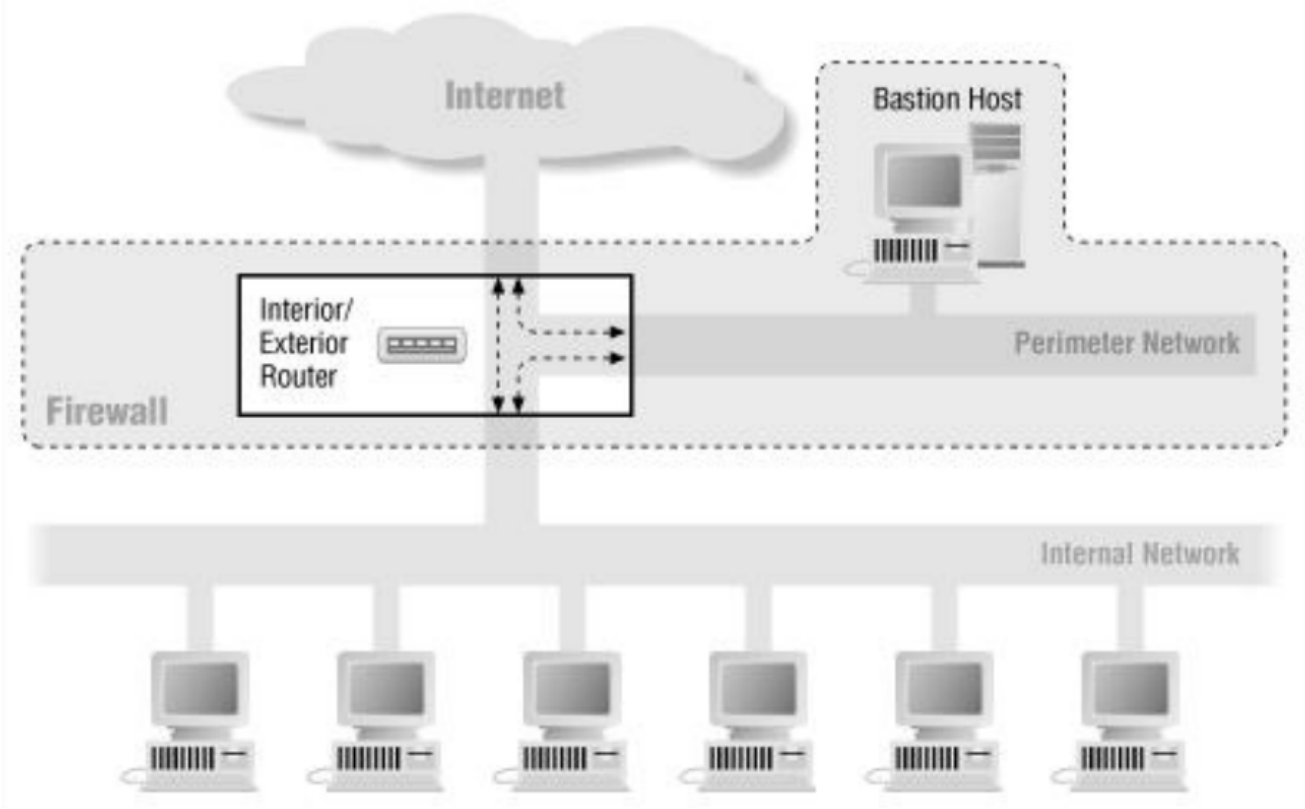
- Bastione
    - Fornisce i servizi esterni (HTTP, SMTP, ...)
    - Può agire da proxy per connessioni uscenti (altrimenti possibili attraverso packet forwarding)

- Router interno
    - Protezione dell'accesso alla rete interna dall'esterno e dalla DMZ
    - Importante. Ridurre al minimo il livello di fiducia della rete interna nei confronti del bastione
        - No possibilità di connessione ai servizi interni
        - No possibilità di uso di risorse interne (es. file system condivisi)

- Router esterno
    - Protezione della DMZ e filtraggio ridondante dell'accesso alla rete interna
    - Prevenzione IP spoofing (falsificazione del proprio indirizzo IP, username, ...)

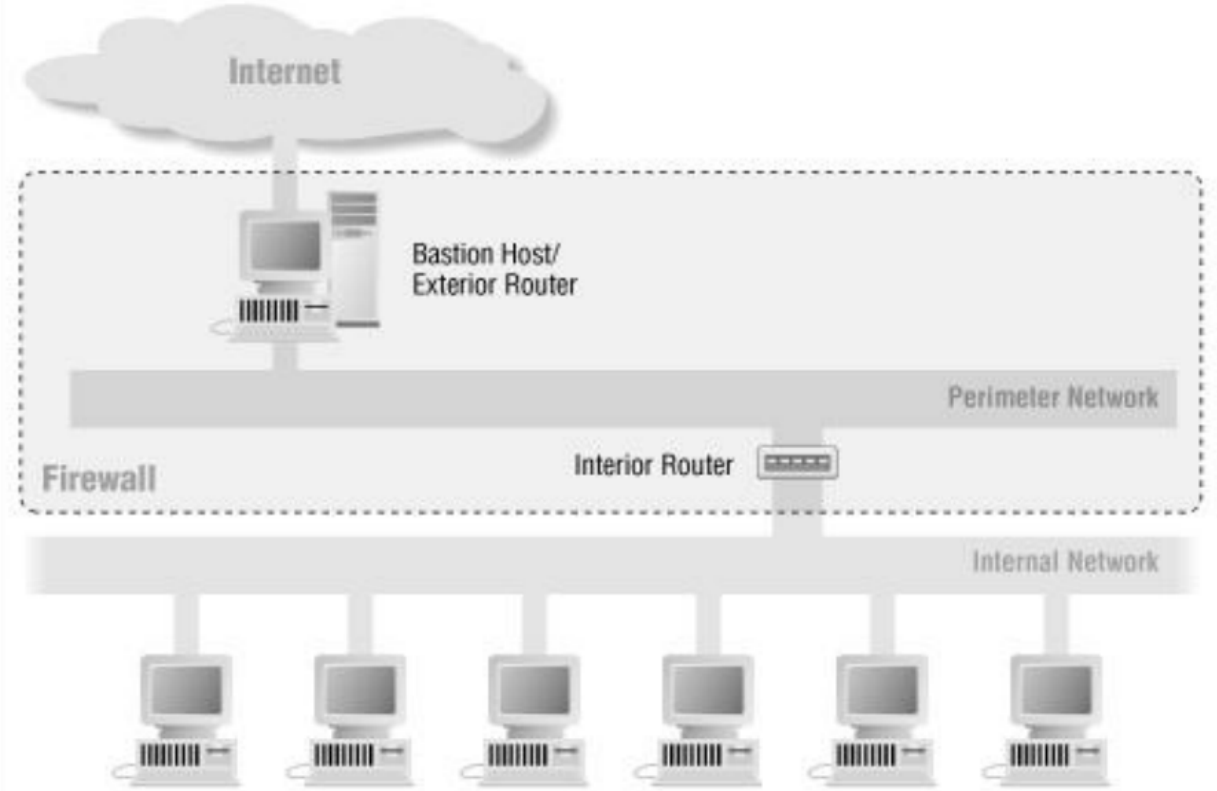
Varianti

- **Router unico**



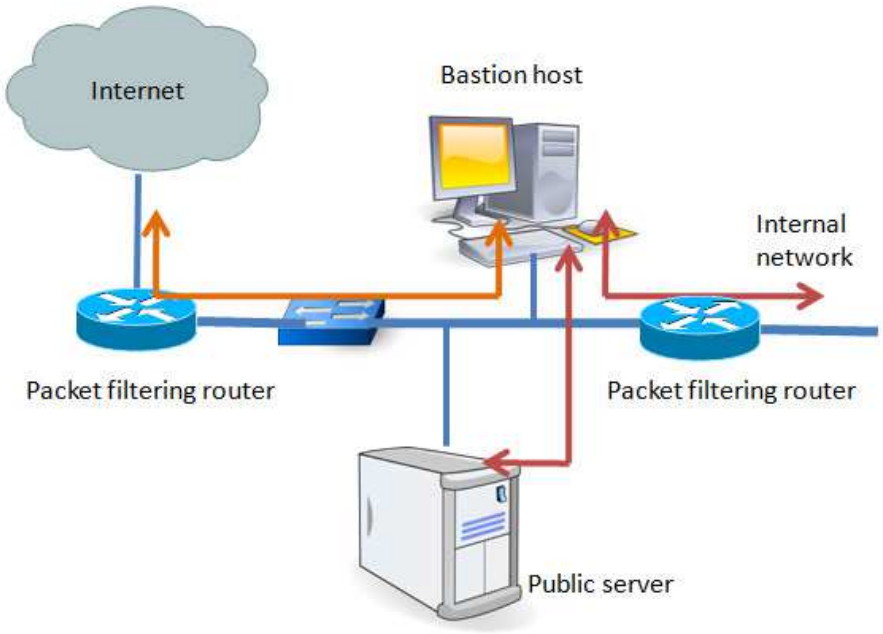
Maggiore complessita del router

- **Router e host bastione combinati**



• Bastion tra due router

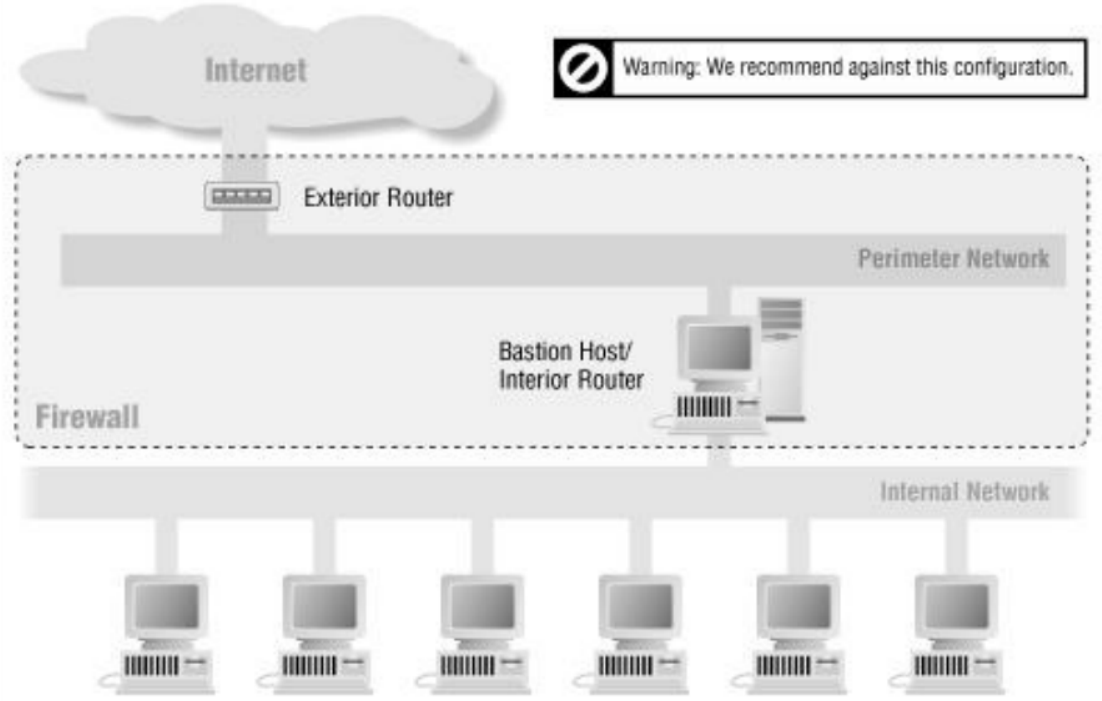
Questa è una delle configurazioni firewall più sicure. In questa configurazione, vengono utilizzati due router di filtraggio dei pacchetti e l'host del bastion è posizionato tra i due router. In un caso tipico, sia Internet che gli utenti interni hanno accesso alla sottorete schermata, ma il flusso di traffico tra le due sottoreti (uno è dall'host del bastione alla rete interna e l'altro è la sottorete tra i due router) è bloccato.



Screened subnet firewall

Varianti pericolose

• Combinazione di bastione e router interno



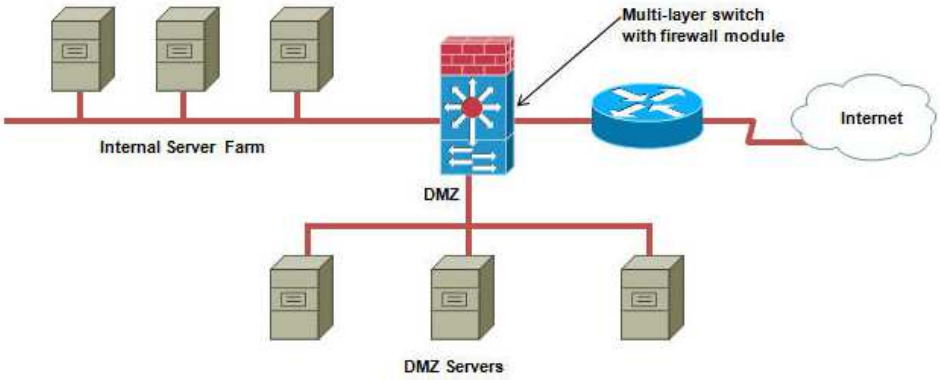
Espone la rete interna se il bastione è compromesso
Le regole di filtraggio del router possono venir modificate

DMZ

Dividere la rete interna in zone è una tecnica che aumenta notevolmente la sicurezza. DMZ è una zona delicata ed importante per i processi di sicurezza; l'acronimo significa "zona demilitarizzata".
La sicurezza perimetrale si occupa di proteggere una rete nei punti in cui essa è a contatto con il mondo esterno. In base al tipo di traffico e alla funzione si possono identificare diverse zone.

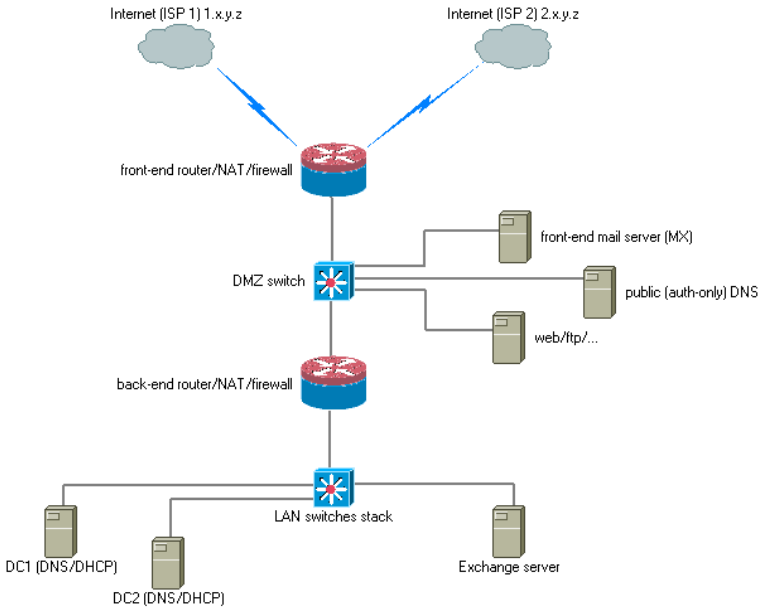
1) Nei casi più semplici le uniche due zone, LAN e WAN, sono attestate sui due lati del router/firewall, senza DMZ. Il lato LAN (local area network) è il segmento privato e protetto, e ad esso appartengono tutti gli host ed i server i cui servizi sono riservati all'uso interno.
La zona WAN (wide area network) è la parte esterna, e ad essa appartengono uno o più apparati di routing che sostengono il traffico da e per la rete locale, sia verso internet che verso eventuali sedi remote dell'azienda.

2) Non appena l'architettura della rete comincia ad evolversi, ci si trova nella necessità di esporre all'esterno alcuni servizi. In questo caso è fortemente consigliata la creazione di una terza zona: la DMZ. Essa è un'area in cui sia il traffico WAN che quello LAN sono fortemente limitati e controllati; in pratica, si tratta di una zona "cuscinetto" tra interno ed esterno, che viene attestata su una ulteriore interfaccia di rete del router/firewall, come negli schemi qui sotto.

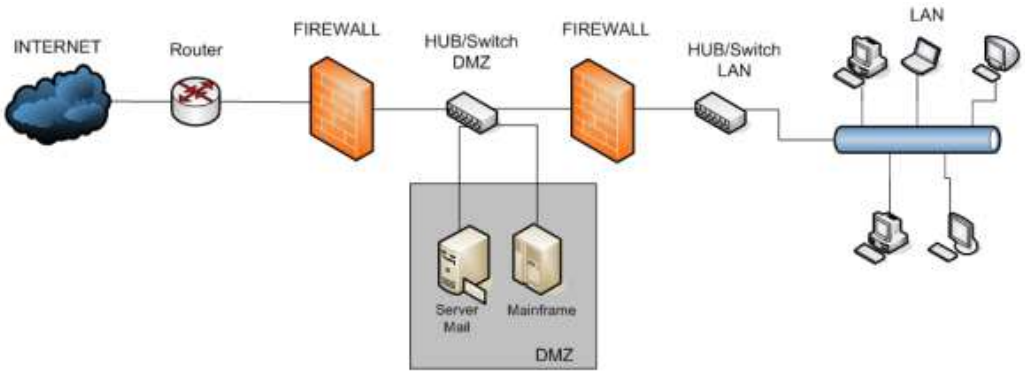


3) Generalmente però si installano in DMZ i server detti front-end, a cui corrispondono i relativi back-end in LAN, protetti non con un solo firewall, ma con più **firewall**.

Esempio 1



Esempio 2



Altre situazioni

Firewall di filtraggio dei pacchetti

Questo tipo di firewall è il più comune e facile da implementare in una rete di piccole dimensioni. Un router funziona come un firewall esaminando ogni pacchetto che passa attraverso la rete. In base all'elenco di controllo degli accessi, il router inoltra o rilascia i pacchetti. Normalmente, l'indirizzo IP di origine e destinazione, il numero di porta e il tipo di traffico vengono presi in considerazione quando il router elabora ogni pacchetto di dati. Poiché un router non può controllare il pacchetto nel livello applicazione, questo tipo di firewall non può difendere gli attacchi che utilizzano le vulnerabilità dei livelli dell'applicazione. Inoltre non riescono a combattere attacchi di spoofing. È possibile utilizzare questa configurazione se è necessaria una maggiore velocità di rete e sono necessari capacità di accesso e autenticazione limitate.

Ispezione di stato

Il firewall di ispezione stateful funziona a livello di rete nel modello OSI . Controlla sia l'intestazione che i contenuti del traffico. La principale differenza tra il filtraggio dei pacchetti e l'ispezione stateful è che quest'ultimo analizza non solo le intestazioni dei pacchetti, ma controlla anche lo stato dei pacchetti e fornisce servizi proxy. I firewall di ispezione stateful mantengono una tabella di stato e un set di istruzioni per ispezionare ciascun pacchetto e archiviare le informazioni in base al tipo di traffico. Controlla inoltre ogni connessione TCP e ricorda quali porte vengono utilizzate da quella connessione. Se c'è una qualsiasi porta non richiesta dalla connessione, quella porta viene chiusa.

Firewall ibridi

Funzionano quasi allo stesso modo dei firewall di tipo stateful inspection, il che significa che possono funzionare sia in rete che a livello di applicazione. Normalmente, in un sistema ibrido alcuni host risiedono all'interno del firewall mentre gli altri risiedono all'esterno del firewall. Per comunicare con la macchina all'esterno della rete centrale vengono utilizzati i tunnel IPsec. Un esempio in cui questo tipo di configurazione è adatto è un sito principale collegato con i suoi siti di filiali tramite VPN. Una caratteristica distinta di questa configurazione è l'amministrazione del firewall sul sito principale che distribuisce la politica di sicurezza al proprio sito di succursale in modo da mantenere una sicurezza uniforme in tutta l'organizzazione.

Firewall server proxy

Il proxy consente agli utenti di eseguire servizi specifici (FTP, TELNET, HTTP ecc.) O il tipo di connessione applicando l'autenticazione, il filtraggio e la registrazione. Per il servizio specifico ci sarà un proxy specifico. Ad esempio, se si desidera consentire solo la connessione HTTP a Internet per gli utenti della rete interna, è necessario consentire solo il proxy HTTP, nient'altro. Gli utenti che devono accedere a Internet creano un circuito virtuale con il server proxy e il server proxy invia la richiesta per connettersi a un sito specifico per conto di quel particolare utente. Il server proxy modifica l'IP della richiesta in modo che Internet o il mondo esterno possano vedere solo l'IP del server proxy. Quindi il server proxy nasconde la rete interna dietro di esso. Quando un proxy riceve i dati da Internet, restituisce i dati all'utente intenzionale interno tramite il circuito virtuale. Il vantaggio principale dell'utilizzo del proxy è che è pienamente consapevole del tipo di dati che gestisce e può proteggerli. Uno svantaggio del proxy è che se è presente un aggiornamento del protocollo utilizzato da Internet, anche il software proxy deve essere aggiornato per consentire un servizio specifico relativo a tale protocollo.

Sommario