



piccolo,
leggero,
efficace

brainwall



Il firewall intelligente



Il firewall intelligente

BrainWall non è solo un Firewall: gestisce NAT, IPSEC, Inbound Load Balancing, VPN, PPTP Server, DHCP, Dynamic DNS, e molto altro.

Una soluzione nuova, potente ed economica per la sicurezza della tua azienda: in pochi grammi, BrainWall garantisce la protezione alla tua rete.

Caratteristiche:

FIREWALL

- Filtraggio da sorgente e destinazione IP, protocollo IP, porta sorgente e destinazione per TCP e UDP traffic.
- Abilitazione dei limiti per connessioni simultanee su regole di base.
- BrainWall utilizza p0f, un'avanzata utility di rete per fingerprinting che abilita il filtraggio attraverso il sistema operativo all'inizio della connessione.
- Opzione di log su determinato tipo di traffico.
- Politiche di routing ad alta flessibilità per la selezione del gateway sulle regole di base per il bilanciamento di banda, failover, WAN multiple, backup su più ADSL, ecc...
- Possibilità di creazione Alias di gruppi di IP e nomi di IP, networks e porte. Queste caratteristiche aiutano a tenere la configurazione pulita e facile da comprendere, specialmente in configurazioni dove ci sono svariati IP pubblici e numerosi Server.
- Filtraggio trasparente Layer 2. Possibilità di effettuare bridge su interfacce e filtrare il traffico tra queste.
- Normalizzazione di pacchetto. Abilitato di default. È possibile disabilitarlo se necessario.
- Possibilità di disabilitare il filtraggio (firewalling) per utilizzare BrainWall come puro router.

STATE TABLE (TABELLA DI STATO)

- La tabella di stato del firewall mantiene informazioni sulle connessioni aperte. BrainWall è uno stateful firewall, per default tutte le regole sono stateful. Molti firewall non hanno la capacità di controllare la tabella degli stati. BrainWall ha numerose funzioni in grado di eseguire un controllo granulare della tabella dello stato, grazie alle caratteristiche di OpenBSD's pf.
- Regolazione della dimensione della tabella dello stato. Di default la tabella di stato varia in funzione della RAM installata nel sistema, ma può essere aumentata in tempo reale alla dimensione desiderata. Ciascuno stato occupa approssimativamente 1 KB di RAM, quindi questo parametro va tenuto a mente quando si va a dimensionare la memoria.

BrainWall offre numerose opzioni per la gestione dello stato.

- Keep state – Funziona con tutti i protocolli di default su tutte le regole.
- Modulate state – Lavora solo con TCP. BrainWall genererà dei ISNs (Initial Sequence Numbers) per conto dell'host.
- Synproxy state – i Proxy iniziano le connessioni TCP per aiutare i server da spoofed TCP SYN floods.
- None – Non viene tenuta nessuna voce sullo stato.

BrainWall offre quattro stati per l'ottimizzazione della tabella di stato.

- Normale – default
- Hight latency – usata per links ad alta latenza, come collegamenti satellitari
- Aggressive – scadenza dello stato di idle più veloce. Più efficiente usando più risorse hardware, ma può eliminare connessioni corrette
- Conservative – Cerca di evitare la cancellazione di connessioni corrette a scapito di un maggior utilizzo della CPU e RAM

NAT: NETWORK ADDRESS TRANSLATION

Il Port forwards include un range e uso di IP pubblici multipli:

- NAT 1:1 per IP individuali o intere subnet.
- Outband NAT, Impostato di default, tutto il traffico in uscita verso l'IP della WAN. In configurazioni con WAN multiple, verrà usato il traffico in uscita all'IP dell'interfaccia WAN.
- Advanced Outbound NAT.
- NAT Reflection – in qualche configurazione, NAT Reflection, è utilizzato per servizi che possono accedere con IP pubblici da reti interne.



RIDONDANZA

Il protocollo CARP da OpenBSD gestisce l'hardware failover. Due o più gruppi di firewall hardware possono essere configurati come un gruppo di failover. Se un'interfaccia si guasta sul dispositivo primario o il dispositivo primario va offline, il secondo si attiva. BrainWall include anche una capacità di sincronizzazione automatica tra il dispositivo primario ed il secondario. pfsync assicura che la tabella di stato del firewall sia replicata su tutti firewall inseriti nel failover. Questo significa che le connessioni esistenti saranno mantenute nel caso di failure va a dimensionare la memoria.

BILANCIAMENTO DEL CARICO

Bilanciamento di carico in uscita: (Outbound). Il load balancing in uscita è usato su WAN multiple per fornire il bilanciamento ed il failover. Il traffico è diretto verso un gateway designato o un pool di bilanciamento di carico definito nelle regole di base del firewall.

INBOUND LOAD BALANCING

Il bilanciamento di carico in ingresso è usato per distribuire il carico tra vari server. È comunemente usato per con server web, server di posta e altri. I server che non rispondono al ping o connessione TCP su porta definita saranno esclusi dal pool.

VPN

BrainWall offre tre tipologie per la connettività VPN, IPsec, OpenVPN, e PPTP.

IPsec

IPsec consente connettività con tutti i dispositivi che supportano lo standard IPsec. Questo è di uso comune nelle configurazioni site to site con altri dispositivi BrainWall . Altri firewall open source come m0n0wall e molti altri firewall commerciali come Cisco, Juniper, ecc... la implementano. È usata spesso anche nelle connessioni client mobile.

OpenVPN

OpenVPN è una flessibile, potente soluzione SSL VPN che supporta un ampia gamma di sistemi operativi client. Vedere il sito di OpenVPN per maggiori dettagli.

PPTP Server

PPTP è un sistema VPN molto popolare perché installato su quasi tutti i S.O. client inclusi tutti i sistemi operativi Windows a partire da Windows 95 OSR2. Il server **BrainWall** PPTP può usare un database locale o un RADIUS server per l'autenticazione. La compatibilità RADIUS è supportata.

PPPoE Server

BrainWall offre un server PPPoE. Per maggiori informazioni sul protocollo PPPoE, vedere la documentazione. Gli utenti locali del database posso essere usati per l'autenticazione e l'autenticazione RADIUS con opzioni di accounting è anche supportata.

Report e Monitoraggio

I grafici RRD in BrainWall forniscono le seguenti informazioni:

- Utilizzo della CPU.
- Traffico totale.
- Stato del firewall.
- Traffico individuale sulle interfacce.
- Packets per second rates per tutte le interfacce.
- Tempo di risposta al ping del gateway dell'interfaccia WAN.
- Code di traffic shaper sul sistema se il traffic shaper è abilitato.

REAL TIME INFORMATION

Le informazioni della storia del sistema sono importanti, ma qualche volta sono più importanti le informazioni real time. I grafici SVG mostrano il traffico in real time per tutte le interfacce. La pagina iniziale include grafici AJAX che mostrano il tempo reale il carico della CPU, memoria, swap e spazio disco usato e la tabella di stato.

DNS DINAMICO

Il client di DNS dinamico abilita alla registrazione mediante uno di questi servizi:

DynDNS, DHS, DNSexit, DyNS, EasyDNS, FreeDNS, HE.net, Loopia, Namecheap, No-IP, ODS.org, OpenDNS, ZoneEdit.



CAPTIVE PORTAL

Il captive portal permette di forzare l'autenticazione o ridirigere il traffico di rete ad una pagina di autenticazione di rete. Questo è comunemente usato nelle connessioni di rete hot spot, ma anche ampiamente usata per livelli di sicurezza aggiuntivi nell'accesso delle reti internet attraverso i sistemi wireless. Per maggiori informazioni sul Captive Portal si veda questa pagina. Quello che segue è una lista di funzioni e caratteristiche del Captive Portal:

- Connessioni massime concorrenti - Limita il numero delle connessioni concorrenti per ciascun IP client. Questa funzionalità previene gli attacchi DOS.
- Idle timeout – Disconnette i client che non effettuano connessioni per più di un certo numero di minuti.
- Hard timeout – Forza la disconnessione dei client connessi per più di un numero definito di minuti
- Pop up di logon – Opzione di pop up della finestra con pulsante di disconnessione
- URL Redirection – dopo l'autenticazione gli utenti possono essere rediretti verso una pagina di default definita.
- MAC Filtering – di default BrainWall usa il filtraggio indirizzi MAC.
- Opzioni di autenticazione – ci sono tre metodi di autenticazione:
 1. Nessuna autenticazione: abilita la navigazione senza l'inserimento di nessun dato.
 2. Utenti locali – il database degli utenti locali può essere configurato e usato per l'autenticazione.
 3. Autenticazione RADIUS – Questo è il metodo prediletto da aziende, enti ed ISP. Può essere usato con l'autenticazione di Microsoft Active Directory e numerosi altri server RADIUS.
- Capacità di RADIUS:
 1. Forzare la re-autenticazione.
 2. Abilitazione all'aggiornamento degli account.
 3. Autenticazione MAC RADIUS abilita il Captive Portal all'autenticazione dei client usando il MAC address e username e password.
 4. Accetta configurazioni ridondanti di RADIUS Server.
- http e HTTPS – La pagina del portale può essere configurata sia in http che in https.
- Pass-through MAC and IP addresses – Indirizzi MAC e IP possono essere inseriti in una white list bypassando il portale.
- File manager – Questo permette di caricare delle immagini che possono essere utilizzate nella pagina iniziale del captive portal.

DHCP Server & Relay

BrainWall include DHCP Server e funzionalità Relay.

BrainWall è basato su tecnologia pfSense®