Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Demilitarized Zone e Firewall con Intrusion Prevention System a protezione dei servizi web ICAR Sede di Napoli

Angelo Esposito[1], Giampiero Lago[1]

[1]Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche (ICAR-CNR)
Via Pietro Castellino, 111 – 80131 Napoli

angelo.esposito@icar.cnr.it
giampiero.lago@icar.cnr.it

Versione 1.0

RT-ICAR-NA-2024-07 **Dicembre 2024**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) Sede di Napoli, Via P. Castellino 111, I-80131 Napoli, Tel: +39-0816139508, Fax: +39-0816139531, e-mail: napoli@icar.cnr.it, URL: www.icar.cnr.it

Demilitarized Zone e Firewall con Intrusion Prevention System a protezione dei servizi web ICAR Sede di Napoli

Angelo Esposito[1], Giampiero Lago[1]

[1]Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche (ICAR-CNR) Via Pietro Castellino, 111 – 80131 Napoli

angelo.esposito@icar.cnr.it, giampiero.lago@icar.cnr.it,

Abstract

Questo lavoro descrive l'insieme delle misure di sicurezza informatica implementate dall'Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) sede di Napoli, per quanto riguarda l'utilizzo di una DMZ (Demilitarized Zone) e la configurazione di Snort come sistema di rilevamento delle intrusioni su piattaforma Firewall pfSense. Il documento descrive l'architettura della rete di sicurezza, le configurazioni applicate per isolare i servizi critici, e l'integrazione di Snort come strumento di monitoraggio e analisi del traffico per garantire una protezione proattiva contro potenziali minacce informatiche garantendo la sicurezza e la resilienza dell'infrastruttura.

Keywords: Infrastruttura di Rete, Sicurezza Informatica, Snort, Firewall, Pfsense, Cybersecurity, Intrusion Prevention System

1. Introduzione

Durante il Security Summit del 19 marzo 2024, è stato presentato il Rapporto Clusit 2024, che analizza i dati relativi al 2023. In un contesto in cui i dati indicano una crescita degli attacchi informatici, è fondamentale analizzare la situazione in Italia.

Il rapporto, presentato a Milano, evidenzia un quadro allarmante della sicurezza informatica nel nostro Paese. L'Italia si conferma un obiettivo privilegiato per i cybercriminali, con un aumento del 65% degli attacchi rispetto al 2022, un dato significativamente superiore al +11% registrato a livello globale.

Inoltre, è preoccupante la quota di attacchi che colpiscono l'Italia: l'11% degli attacchi cyber nel mondo è avvenuto nel nostro Paese, rispetto al 3,4% nel 2021 e al 7,6% nel 2022. In altre parole, 11 attacchi su 100 nel mondo si sono verificati in Italia.

Un altro dato molto interessante da tenere in considerazione è il livello di severity di un incidente informatico. Nel 2023 gli attacchi di severità "critica" o "grave" rappresentano l'81% del totale,

contro il 47% del 2019. Anche questo parametro indica che i tipi di attacco crea più problemi rispetto a quelli degli anni precedenti. Nel 2023, l'Italia ha subito 310 attacchi gravi, una nuova impennata (+132) rispetto al 2022, dopo il +118 del 2022 vs 2021 (nel 2021 invece si era registrato "solo" un +22 rispetto all'anno precedente).

I settori più colpiti in Italia sono: il settore Government / Military / Forze dell'Ordine al primo posto, con il 19% sul totale degli attacchi; il Manufacturing si attesta al secondo posto, con il 13%, dato molto al di sopra della media globale (il 25% degli attacchi mondiali è a imprese manifatturiere italiane!); il settore Logistica e Trasporti rappresenta il 12% del totale; all'11% troviamo i Multiple Targets, cioè campagne generalizzate che non hanno per obiettivo uno specifico settore; al quinto posto il settore Finance / Insurance, con il 9% di attacchi; il Retail è in sesta posizione, con il 9%; segue l'ICT, con il 6%; al 4% un trittico formato da Healthcare, Professional / Scientific / Technical e Organizations.

Le minacce più diffuse in Italia nel 2023 riguardano le seguenti tecniche di attacco:

- DDoS, 36% (con un impressionante aumento del 1486% rispetto al 2022);
- Malware 33%;
- Unknown, 17%;
- Phishing / Social Engineering, 9%;
- Vulnerabilities, 2%;
- Web Attack, 2%;
- Altro 1%.

Del Rapporto Clusit colpisce non tanto l'aumento generalizzato, costante negli anni a livello globale, quanto l'evoluzione della realtà italiana che registra dati molto più alti rispetto al resto del mondo. Ciò vuol dire che l'Italia è presa di mira e le imprese italiane e la pubblica amministrazione devono adottare dei sistemi di sicurezza in grado di diminuire il rischio di compromissione dei loro sistemi informatici.

2. Contesto di riferimento

L'ICAR, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) [1], è un Istituto del Consiglio Nazionale delle Ricerche (CNR) [2] che afferisce al Dipartimento di Ingegneria, ICT e Tecnologie per l'Energia e i Trasporti (DIITET) [3]. L'Istituto è presente sul territorio nazionale con tre sedi, Rende, Napoli e Palermo.

L'Istituto sviluppa applicazioni significative nel campo dell'E-health, energia, sicurezza, bioinformatica, beni culturali e città intelligenti. Ad oggi la sua attività di ricerca è concentrata su quattro grandi aree tematiche: Intelligenza Artificiale, IoT & Cyber Physical Systems, Data Science e Tecnologia.

L'ICAR dispone di diverse infrastrutture di calcolo che erogano servizi su rete pubblica (Siti web istituzionali, Siti web di progetto, servizi web di software di progetto, etc.).

Tutti i servizi esposti su rete sono dei potenziali bersagli per i cyber criminali ed è per questo motivo che è stato predisposto dagli autori di questo RT un firewall a protezione dei servizi esposti, con una zona demilitarizzata (DMZ) costituita dai principali server che espongono servizi su rete pubblica. Il firewall è stato dotato di un sistema di Intrusion Prevention System.

Questo RT descrive le attività svolte per l'implementazione di una Demilitarized Zone (DMZ) con l'integrazione di un sistema Firewall e di un Intrusion Prevention System (IPS) a protezione di servizi web. La DMZ è progettata per isolare i server web e altri servizi critici dal resto della rete, creando una zona intermedia che minimizza i rischi derivanti da attacchi esterni. Il Firewall è configurato per monitorare e filtrare il traffico in ingresso e in uscita, mentre l'IPS è implementato per identificare e bloccare attacchi in tempo reale. Il rapporto illustra la progettazione della rete,

la configurazione degli apparati di sicurezza, la gestione delle politiche di accesso e le tecniche di monitoraggio per garantire una protezione efficace contro le minacce informatiche. Vengono inoltre analizzati i benefici derivanti dall'adozione di questa architettura, tra cui una maggiore resilienza, la protezione contro vulnerabilità note e sconosciute, e il miglioramento della gestione del traffico verso i servizi esposti. L'adozione di questa soluzione consente una difesa proattiva contro attacchi DDoS, tentativi di accesso non autorizzati e altre forme di compromissione delle risorse.

3. Demilitarized Zone e Intrusion Prevention System

In questo capitolo è fornita una breve introduzione al concetto di DMZ (Demilitarized Zone) e IPS (Intrusion Prevention System).

3.1 DMZ

La **DMZ**, nel contesto dell'informatica, è una rete perimetrale isolata che funge da zona intermedia tra una rete interna sicura (ad esempio, una rete aziendale) e una rete esterna non affidabile, come Internet. Il suo scopo principale è fornire un ulteriore livello di protezione separando i servizi pubblicamente accessibili (come server web, server di posta, o server FTP) dalla rete interna, minimizzando il rischio che una compromissione dei primi possa estendersi alla seconda.

La DMZ permette alle organizzazioni di esporre alcuni servizi all'esterno in modo controllato. Tipicamente, i server all'interno di una DMZ ospitano risorse che devono essere accessibili al pubblico, come ad esempio:

- Siti web aziendali.
- Portali per l'accesso remoto o VPN.
- Servizi di posta elettronica o DNS.

Grazie alla DMZ, questi server sono raggiungibili dall'esterno, ma sono isolati dalla rete interna, rendendo più difficile per gli aggressori accedere ai sistemi critici.

I vantaggi della DMZ riguardano i seguenti aspetti:

1. **Isolamento della Rete Interna:** Una DMZ separa i server pubblicamente accessibili dalla rete privata interna, limitando l'accesso agli asset sensibili.
2. **Mitigazione del Rischio:** Anche in caso di compromissione di un server nella DMZ, l'attaccante trova ulteriori barriere prima di poter accedere alla rete interna.
3. **Maggiore Controllo:** Grazie a firewall e regole di routing, è possibile controllare quali tipi di traffico possono passare tra la DMZ, la rete interna e l'esterno.
4. **Difesa Stratificata:** La DMZ aggiunge uno strato di sicurezza a una strategia di difesa multilivello, riducendo l'efficacia di attacchi diretti o movimenti laterali all'interno dell'infrastruttura.

In sintesi, la DMZ rappresenta una componente chiave di un'infrastruttura IT sicura, garantendo un equilibrio tra accessibilità dei servizi pubblici e protezione delle risorse interne.

3.2 Sistemi di Intrusion Prevention System

Un Intrusion Prevention System (IPS) è un sistema di sicurezza informatica progettato per monitorare il traffico di rete o i sistemi informatici al fine di identificare, prevenire e rispondere automaticamente a tentativi di intrusione o attacchi.

L'IPS si inserisce nel flusso di traffico di rete o nel sistema che deve proteggere e analizza i dati in tempo reale per rilevare comportamenti sospetti o dannosi. Quando rileva un possibile attacco, l'IPS non solo lo segnala, ma interviene attivamente per fermarlo, bloccare l'accesso o interrompere l'attacco prima che possa causare danni.

Esistono diverse tipologie di IPS, che differiscono in base a come monitorano e proteggono la rete:

1. Host-based IPS (HIPS): Protegge singoli dispositivi (come server o computer) e monitora attività sospette a livello di sistema operativo o applicativo.

2. Network-based IPS (NIPS): Analizza il traffico di rete e monitora il flusso di dati tra i dispositivi per individuare minacce a livello di rete.

Le Funzionalità principali di un IPS sono:

- Rilevamento di anomalie: Identifica modelli di traffico insoliti che potrebbero indicare un attacco, come un flusso di dati anomalo o tentativi di sfruttare vulnerabilità.
- Rilevamento delle firme: Confronta il traffico di rete con una base di dati di "firme" conosciute di attacchi precedenti, per identificare minacce note.
- Bloccare e prevenire gli attacchi: Quando rileva un attacco, l'IPS può bloccare il traffico malevolo, isolare il dispositivo compromesso o terminare la connessione per evitare danni.
- Prevenzione di attacchi noti e sconosciuti: Mentre l'IPS è particolarmente efficace contro gli attacchi noti, alcune varianti avanzate sono in grado di rilevare anche attacchi nuovi o sconosciuti, grazie a tecniche di analisi comportamentale e apprendimento automatico.

I vantaggi principali di un IPS sono:

- Protezione in tempo reale: un IPS monitora costantemente il traffico di rete e può rilevare e bloccare attacchi immediatamente, prima che possano causare danni. Ad esempio, se un attacco DDoS o un tentativo di exploit di vulnerabilità viene rilevato, l'IPS può fermarlo automaticamente.
- Rilevamento e prevenzione automatica degli attacchi: a differenza di un sistema di rilevamento delle intrusioni (IDS), che solo segnala le minacce, un IPS è in grado di reagire direttamente agli attacchi, fermando le minacce prima che possano compromettere la sicurezza del sistema o della rete.
- Migliore protezione contro le vulnerabilità zero-day: Gli IPS sono spesso progettati per rilevare modelli di traffico sospetti e anomalie, consentendo una protezione più efficace contro gli attacchi che sfruttano vulnerabilità sconosciute (zero-day), anche se non è ancora disponibile una patch per tali vulnerabilità.
- Monitoraggio proattivo e prevenzione di minacce interne: L'IPS non solo difende da minacce esterne, ma può anche rilevare comportamenti anomali all'interno della rete aziendale, prevenendo attacchi da parte di utenti malintenzionati o inconsapevoli, come dipendenti o collaboratori.
- Riduzione dei falsi positivi: I sistemi IPS avanzati, tramite tecniche come il rilevamento comportamentale e l'analisi di traffico, possono ridurre il numero di falsi positivi, garantendo che solo gli attacchi reali vengano bloccati e non le operazioni legittime.
- Migliore visibilità sulla rete: Un IPS fornisce un livello di visibilità in tempo reale sul traffico di rete e sugli eventi di sicurezza. Questo permette agli amministratori di rete di identificare tendenze, valutare la sicurezza generale e rispondere rapidamente a minacce emergenti.
- Compliance e adempimento normativo: Molti settori hanno normative di sicurezza rigorose, come PCI-DSS, HIPAA e GDPR, che richiedono misure di protezione avanzate.

Un IPS aiuta le aziende a soddisfare questi requisiti, proteggendo i dati sensibili e riducendo il rischio di sanzioni legali.

- Gestione centralizzata: gli IPS moderni possono essere gestiti centralmente, il che consente ad un team di sicurezza di monitorare più dispositivi in modo centralizzato, semplificando l'amministrazione e migliorando l'efficienza delle operazioni di sicurezza.
- Prevenzione contro attacchi avanzati e persistenti (APT): Gli IPS avanzati sono in grado di rilevare e prevenire attacchi avanzati e persistenti (APT), che sono particolarmente pericolosi in quanto sono progettati per rimanere nascosti e attivi per periodi di tempo prolungati.
- Integrare con altri sistemi di sicurezza: Un IPS può essere integrato con altri sistemi di sicurezza, come i firewall, i sistemi di gestione degli eventi di sicurezza (SIEM) e i sistemi di rilevamento delle intrusioni (IDS), per una protezione più robusta e coordinata.
- Miglioramento della reattività alle minacce: Poiché un IPS può intervenire in tempo reale, consente una risposta rapida agli incidenti, riducendo il tempo di esposizione agli attacchi e minimizzando i danni che potrebbero verificarsi prima di un intervento manuale.

Pertanto, un IPS è una tecnologia fondamentale per la protezione delle reti e dei sistemi informatici, che non solo rileva gli attacchi ma li previene, agendo in tempo reale per fermare minacce prima che causino danni significativi.

In sintesi, un IPS offre una protezione attiva e tempestiva contro una vasta gamma di minacce informatiche, migliorando la sicurezza globale delle reti aziendali, riducendo i rischi e garantendo che le risorse critiche siano al sicuro.

4. Configurazione della rete precedente

Prima di illustrare la soluzione implementata a protezione dei servizi web esposti dalle infrastrutture tecnologiche della sede ICAR di Napoli, in questo paragrafo si illustra la configurazione precedente.

In tale configurazione ad ogni server, che doveva esporre servizi sul web, veniva assegnato un indirizzo IP pubblico. Inoltre, a protezione del singolo server veniva attivato e configurato opportunamente un firewall UFW/iptables. In figura 1 è illustrata la configurazione precedentemente adottata.

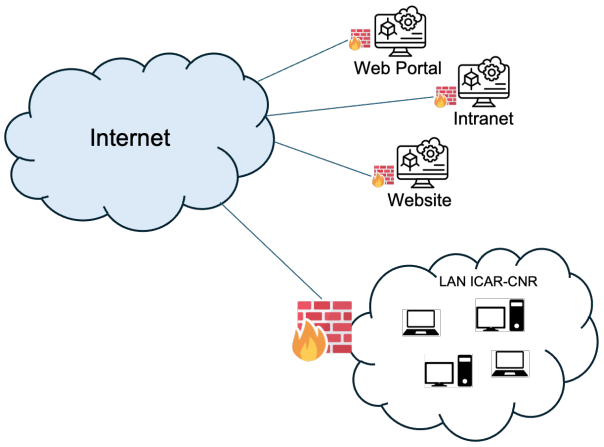

Figura 1 - Precedente configurazione dei firewall e sicurezza di rete

Questo tipo di soluzione prevedeva l'intervento sul singolo server nel caso di aggiornamenti alle regole firewall e controllo sicurezza e integrità. La complessità nella gestione della sicurezza

informatica della rete era proporzionale al numero di VM e servizi espositi su internet. Inoltre, non era presente un sistema di IPS a protezione dei servizi esposti.

5. DMZ, Firewall e IPS nel contesto ICAR sede di Napoli

Come si evince dai paragrafi precedenti, l'importanza di predisporre una DMZ e un Firewall con IPS a protezione dei servizi esposti pubblicamente da ICAR sono di fondamentale importanza per garantire un elevato livello di sicurezza.

5.1 Configurazione DMZ

La configurazione della DMZ ha previsto una pianificazione attenta per garantire la sicurezza della rete interna pur permettendo l'accesso ai servizi pubblici.

L'architettura scelta per la definizione della DMZ è a doppio firewall: due firewall separati (uno esterno e uno interno) proteggono la DMZ.

Per la DMZ è stato scelto uno specifico range di indirizzi IP, distinti dalla rete interna (LAN). La subnet è la seguente: 172.16.2.0/24 con Tag ID della VLAN "ICAR-DMZ" uguale a 51.

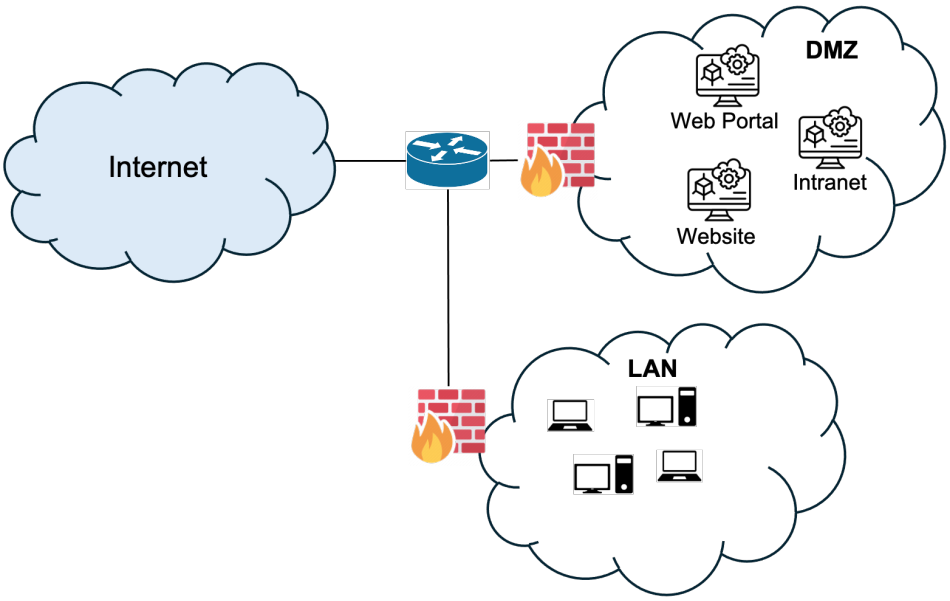

Figura 2 - Attuale configurazione dei firewall e sicurezza di rete

Le macchine server di front-end che prima erano esposte direttamente su internet con indirizzi pubblici sono state spostate nella DMZ, con indirizzi privati appartenenti alla subnet 172.16.2.0/24.

I dispositivi presenti in DMZ sono accessibili su rete DMZ solo mediante VPN, questo consente una separazione netta tra le subnet LAN e DMZ.

5.2 Configurazione Firewall

Il firewall utilizzato e configurato a protezione della DMZ ICAR è PfSense [4], un firewall opensource molto sicuro e affidabile basato su sistema operativo FreeBSD [5].

Al firewall sono state assegnate due interfacce di rete una su WAN e l'altra su DMZ come si evince della figura 3.

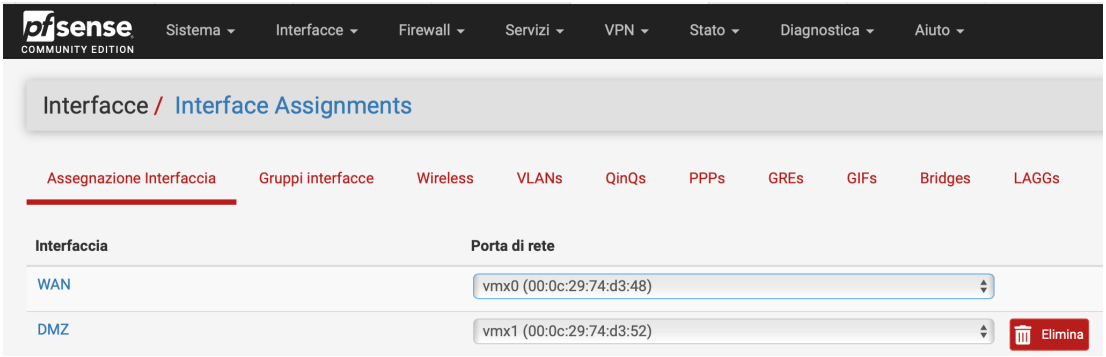

Figura 3 - Interfacce Firewall DMZ

Sono stati assegnati al firewall un insieme di indirizzi IP pubblici virtuali, che corrispondo agli IP precedentemente utilizzati dalle macchine server che esponevano servizi su internet (figura 4).

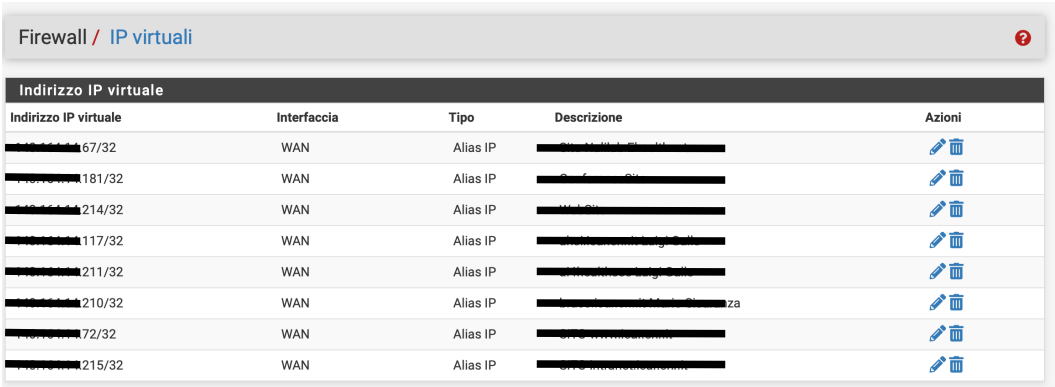

Figura 4 – Insieme di indirizzi IP virtuali

Successivamente sono state definite delle regole di NAT 1:1 tra gli indirizzi pubblici della WAN e quelli privati della DMZ (figura 5).

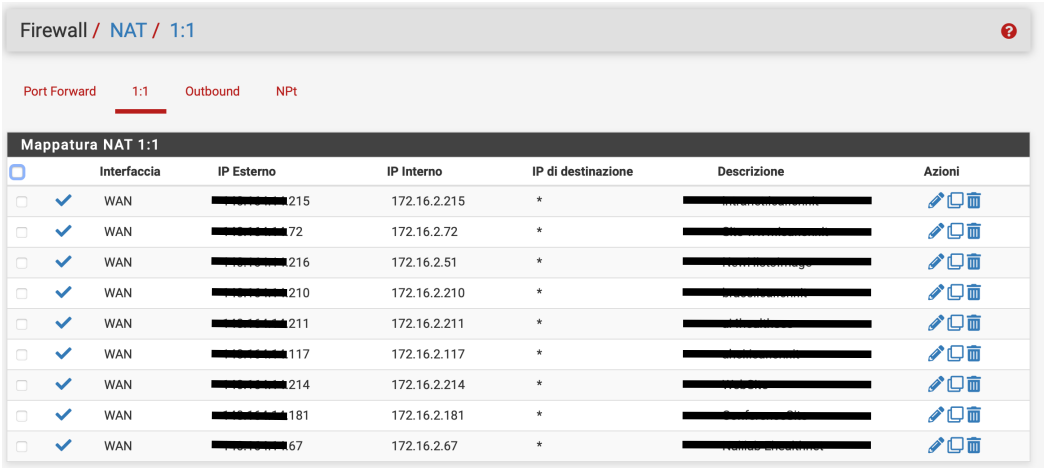

Figura 5 – Insieme di regole NAT 1:1

Sono state definite delle regole sul firewall per controllare il traffico di rete che passa attraverso di esso, sia in ingresso (inbound) che in uscita (outbound). In figura 6, a titolo esemplificativo, sono riportate alcune delle regole definite.

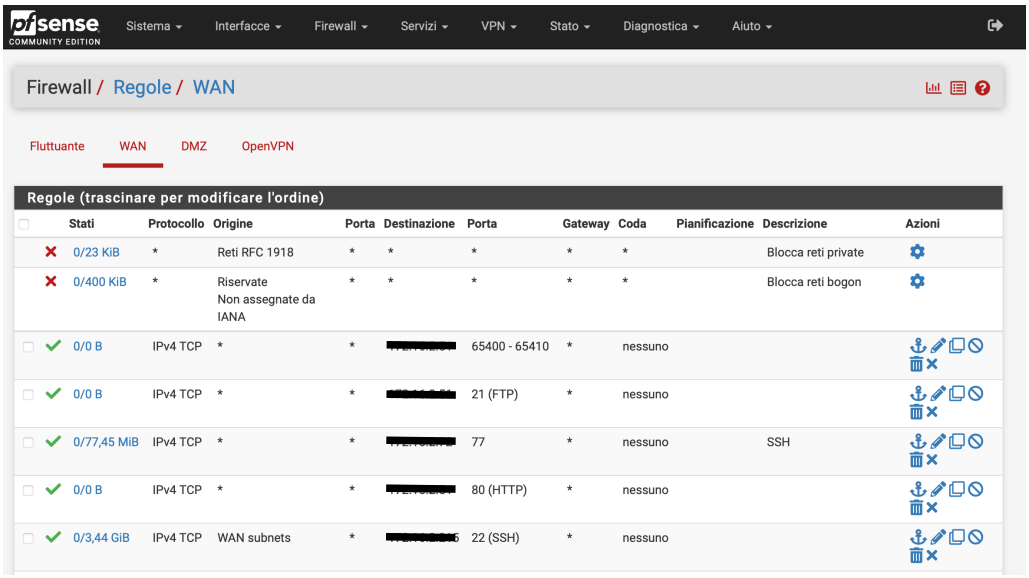

Figura 6 - Regole per il controllo del traffico di rete

5.3 Configurazione IPS

5.3.1 Snort

Snort [6] è un **Intrusion Prevention System** open source sviluppato da Sourcefire, ora parte di Cisco [7]. Utilizzato per monitorare il traffico di rete in tempo reale, Snort analizza i pacchetti di dati per identificare attività sospette o malevole, come attacchi informatici, tentativi di intrusione o altre minacce alla sicurezza della rete. Basato su una combinazione di regole di rilevamento delle firme, analisi del comportamento e pre-processori, Snort è in grado di rilevare una vasta gamma di attacchi, inclusi quelli basati su buffer overflow, scansioni di porta, attacchi DoS e molto altro.

Il funzionamento di Snort si basa su tre modalità principali: sniffer, logger e rilevatore di intrusioni. In modalità sniffer, Snort legge i pacchetti di rete e li visualizza in tempo reale. In modalità logger, registra i pacchetti su disco per un'analisi successiva. Come rilevatore di intrusioni, Snort utilizza un database di regole per confrontare il traffico di rete con schemi noti di attività malevola, generando allarmi quando rileva anomalie. La flessibilità e la configurabilità di Snort lo rendono uno strumento prezioso per gli amministratori di rete e i professionisti della sicurezza informatica, permettendo di mantenere un elevato livello di protezione contro le minacce emergenti.

Nei paragrafi seguenti sono descritte le configurazioni principali adottate per Snort a protezione della DMZ di ICAR sede di Napoli.

5.3.2 Snort interface

In questa sezione sono evidenziate le interfacce di rete su cui Snort effettuerà la sorveglianza del traffico. Questa sezione permette di specificare su quali segmenti di rete si vuole applicare il monitoraggio e le regole di sicurezza di Snort.

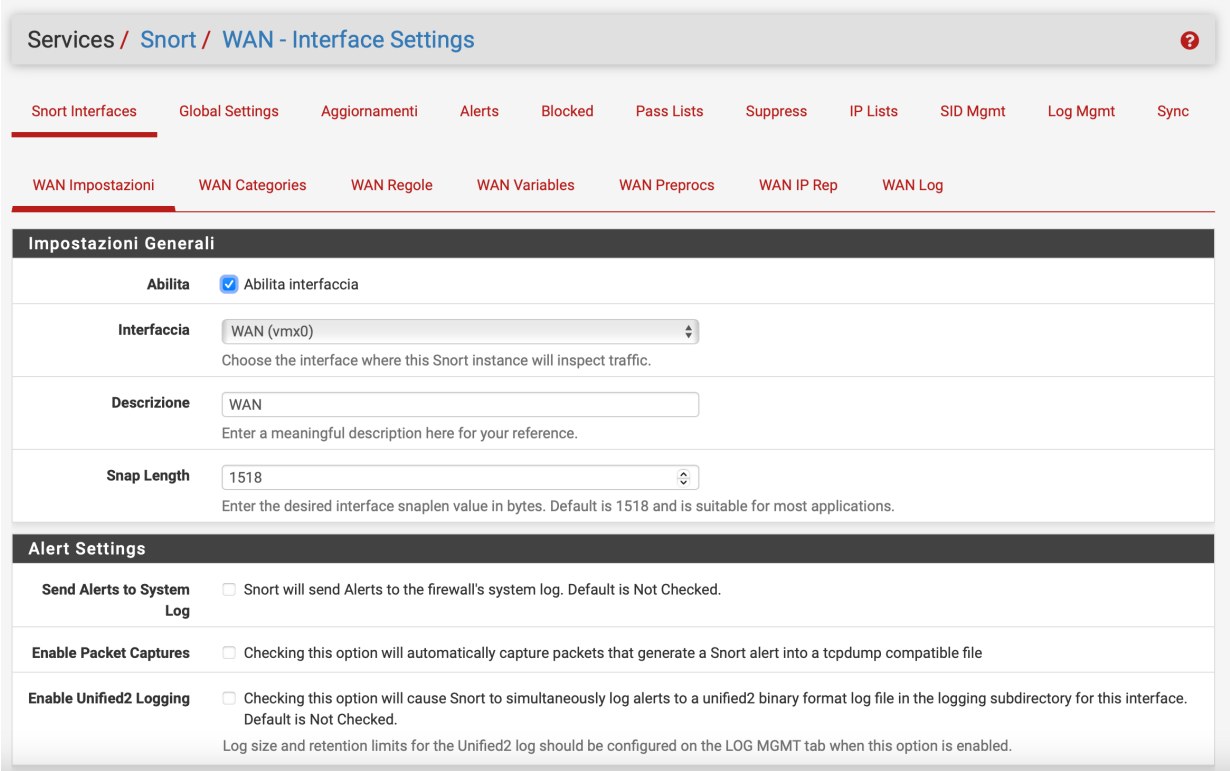

Figura 7 - Sezione WAN Interfaces Settings di Snort

Block Settings in questa sezione è stato configurare il modo in cui Snort blocca il traffico sospetto rilevato su una specifica interfaccia. In figura 8 è riportata la configurazione adottata.

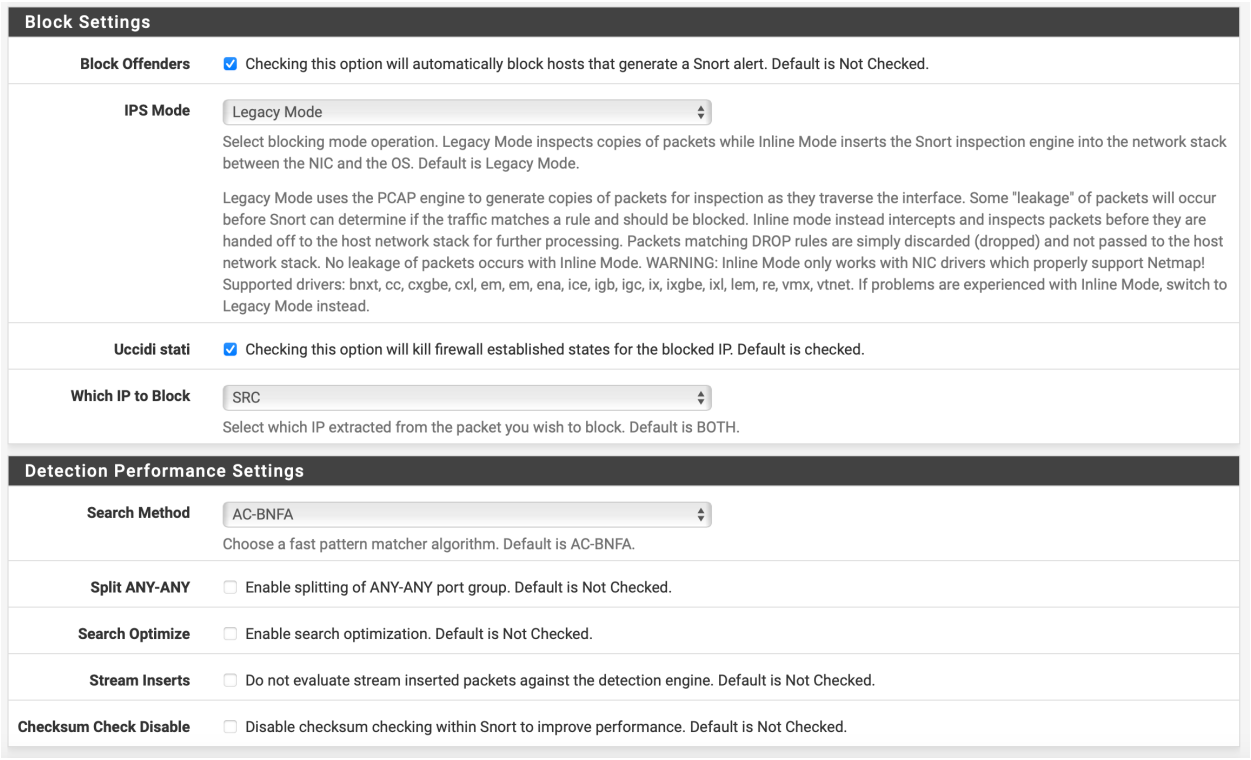

Figura 8 - Configurazione del blocco traffico sospetto

In figura 9 è riportata la configurazione della scheda **Choose the Networks Snort Should Inspect and Whitelist** tale sezione consente di configurare quali reti Snort deve monitorare per rilevare attività sospette e quali IP o subnet sono invece da considerare in whitelist per escluderli dal monitoraggio o dal blocco**.**

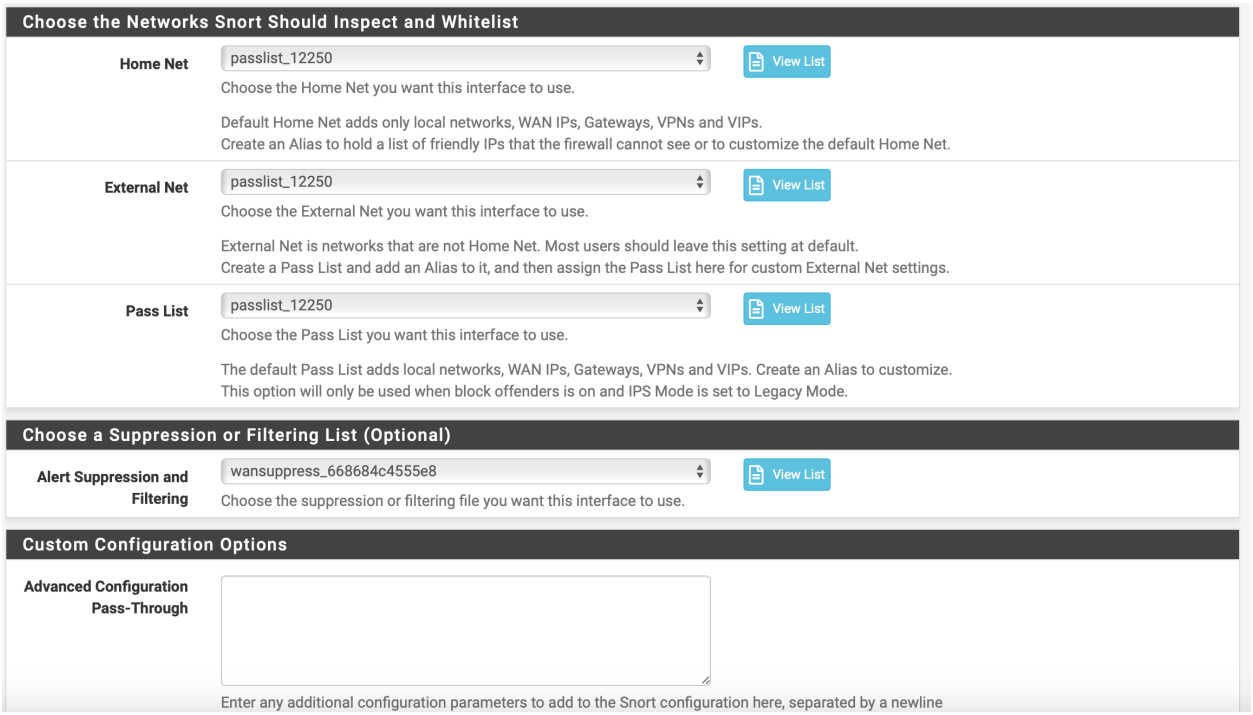

Figura 9 - Configurazione del monitoraggio con selezione delle reti sospette e whitelist

WAN Categories (Figura 10) sono state configurate le categorie di regole di Snort per l'interfaccia WAN. Questa sezione consente di selezionare e personalizzare le categorie di regole che Snort utilizzerà per monitorare il traffico in entrata sulla WAN, adattandolo ai requisiti di sicurezza della rete. In questa sezione troviamo:

- **Automatic Flowbit Resolution** permette di gestire automaticamente le dipendenze delle regole basate su flowbits. I flowbits sono variabili utilizzate nelle regole di Snort, per mantenere uno stato del flusso di traffico, permettendo a determinate regole di attivarsi solo quando vengono soddisfatte specifiche condizioni precedenti.
- **Snort Subscriber IPS Policy Selection** permette di selezionare una politica di rilevamento delle minacce preconfigurata, sviluppata da Snort, per personalizzare il livello di protezione offerto dall'Intrusion Prevention System (IPS) su una determinata interfaccia.
- **Select the rulesets (Categories) Snort will load at startup** in questa sezione ci sono tutta una serie di regole e/o categorie di regole che possono essere selezionate/deselezionate all'avvio di Snort.

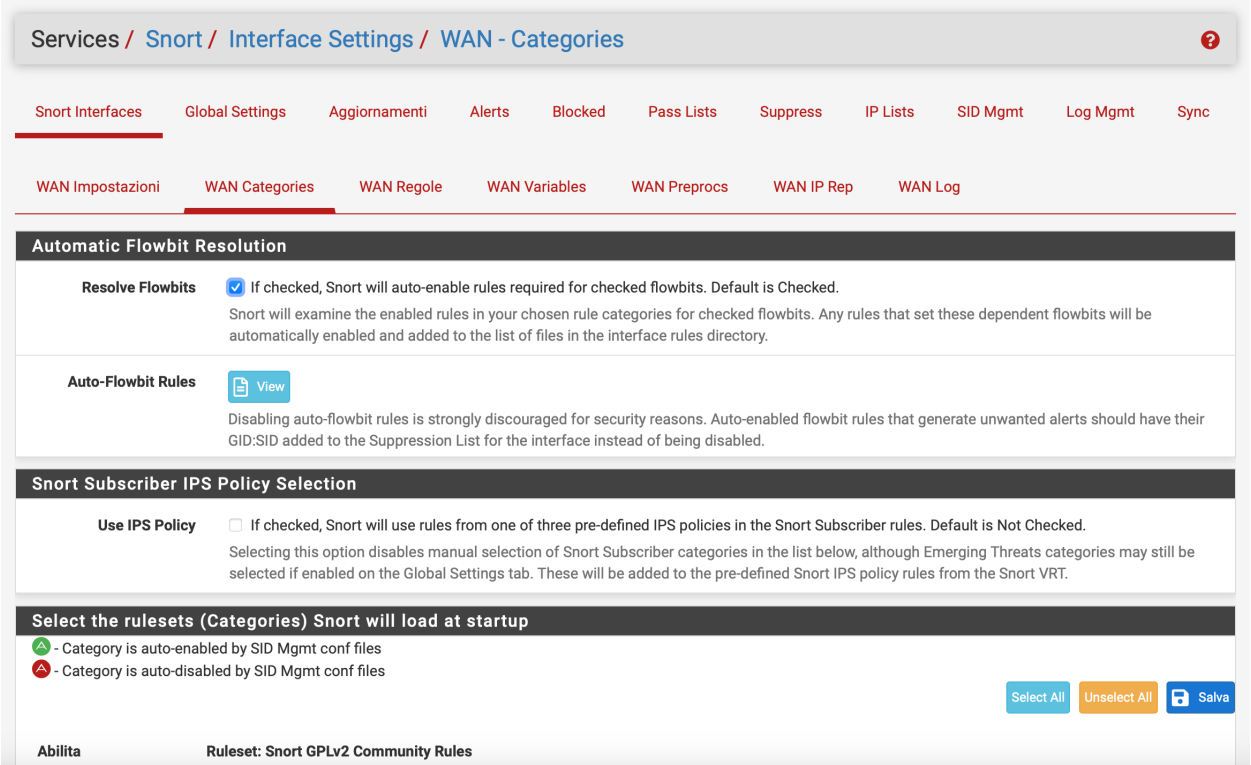

Figura 10 – Configurazione delle categorie di regole di Snort per l'interfaccia WAN

WAN Rules (Figura 11) sono state configurate le regole di rilevamento delle minacce che Snort applica al traffico in entrata attraverso l'interfaccia WAN. La sezione permette di personalizzare il comportamento di Snort selezionando, gestendo e affinando le regole di sicurezza specifiche per il rilevamento delle minacce, al fine di adattarsi alle esigenze particolari della tua rete.

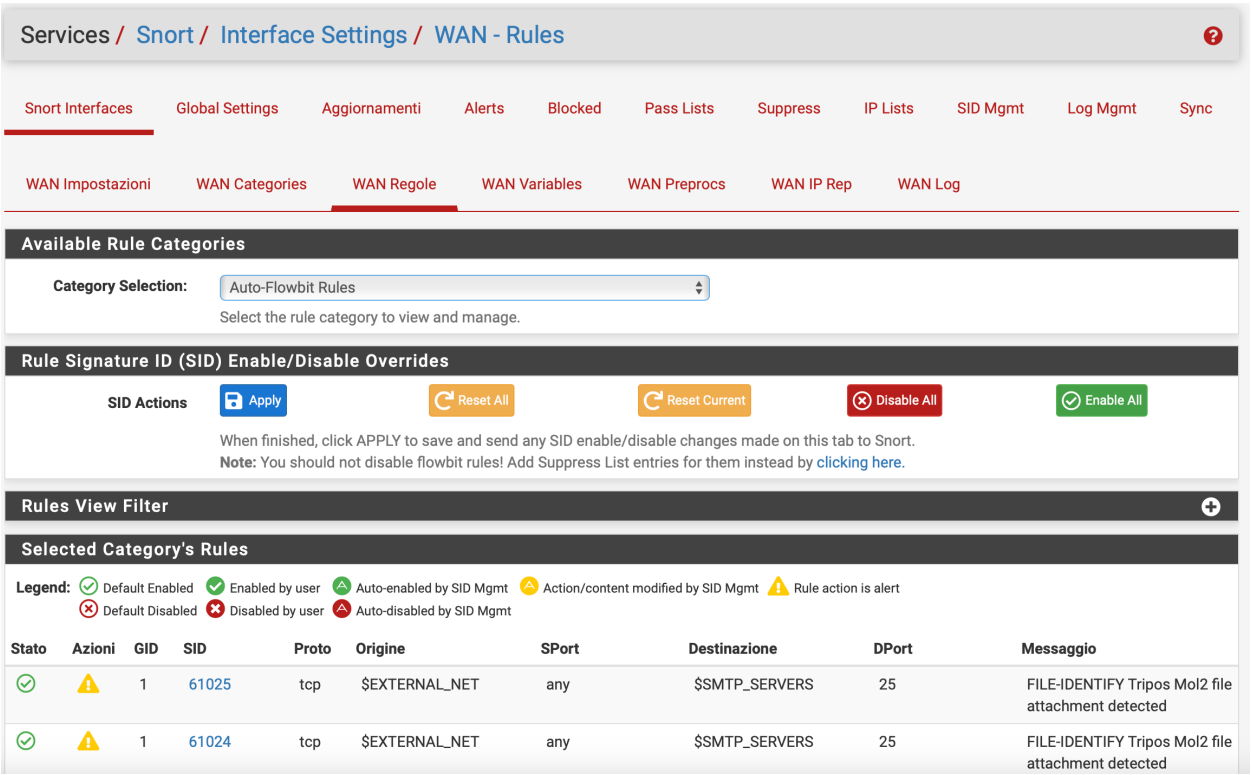

Figura 11 - Configurazione delle regole di rilevamento delle minacce in entrata sull'interfaccia WAN

WAN - Preprocessors and Flow (Figura 12) consente di gestire le configurazioni dei preprocessori e delle impostazioni di flusso per l'interfaccia WAN. I preprocessori sono moduli di Snort che analizzano e modificano il traffico prima dell'applicazione delle regole, migliorando la rilevazione delle minacce e l'efficacia del sistema.

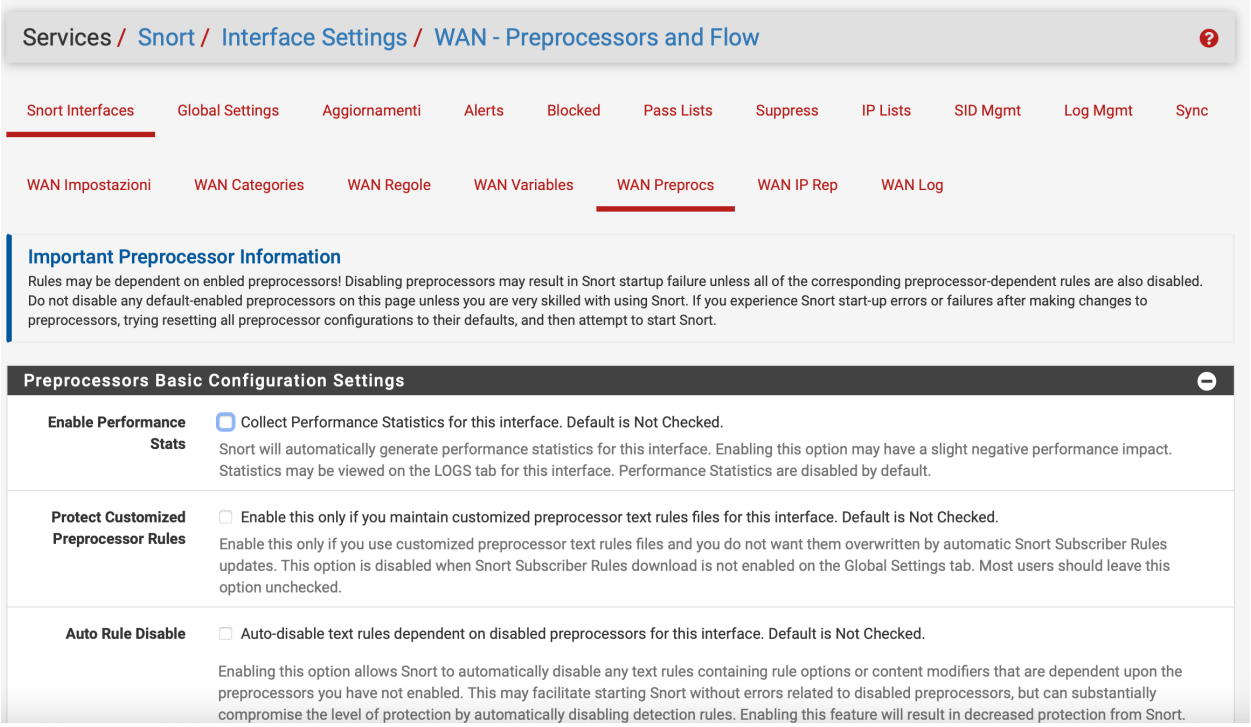

Figura 12 - configurazione dei preprocessori e impostazioni di flusso per interfaccia WAN

5.3.3 Global settings

Le **Snort Subscriber Rules** sono un insieme di regole di rilevamento delle intrusioni mantenute e aggiornate da Cisco per l'uso con Snort. Queste regole sono progettate per identificare specifiche minacce e vulnerabilità basate su firme note di attacchi. Le Snort Subscriber Rules coprono una vasta gamma di attacchi e sono aggiornate regolarmente per includere le nuove minacce man mano che emergono.

L'uso delle Snort Subscriber Rules consente di mantenere un elevato livello di sicurezza, assicurandosi che il loro sistema di rilevamento delle intrusioni sia sempre aggiornato con le più recenti difese contro le minacce emergenti. Le regole sono create e aggiornate da esperti di sicurezza e sono ottimizzate per fornire un rilevamento efficace e minimizzare i falsi positivi. In Figura 13 a titolo esemplificativo è riportato un estratto della configurazione adottata. Nei paragrafi successivi sono specificate nel dettaglio le varie configurazioni di regole abilitate a protezione dei server della DMZ di ICAR.

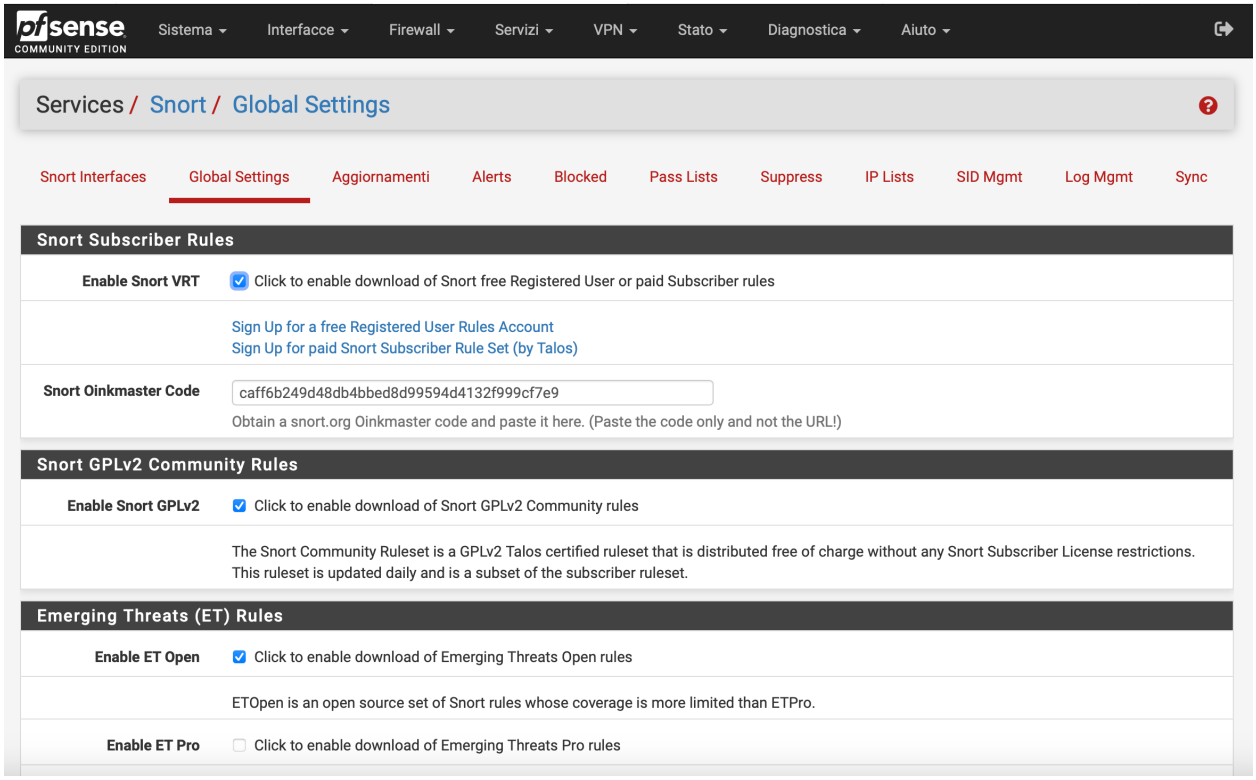

Figura 13 - Sezione Global Settings di Snort

5.3.3.1 Snort GPLv2 Community Rules

Le **Snort GPLv2 Community Rules** sono un insieme di regole di rilevamento delle intrusioni che sono sviluppate e mantenute dalla comunità open source di Snort. Queste regole sono rilasciate sotto la licenza GPLv2 (GNU General Public License version 2). Le Snort GPLv2 Community Rules vengono sviluppate collaborativamente dalla comunità di utenti e sviluppatori di Snort, includendo contributi di esperti di sicurezza, ricercatori e altre persone interessate alla sicurezza delle reti. Queste regole sono progettate per identificare una vasta gamma di minacce e vulnerabilità, simili a quelle coperte dalle Snort Subscriber Rules, ma senza i vincoli di una sottoscrizione a pagamento.

L'utilizzo delle Snort GPLv2 Community Rules, in combinazione con le Snort Subscriber Rules, può fornire una copertura di sicurezza completa e aggiornata, permettendo agli amministratori di rete di proteggere le loro infrastrutture contro una vasta gamma di minacce e attacchi.

5.3.3.2 Emerging Threats (ET) Rules - ET Open Rules

Le **Emerging Threats (ET) Rules** sono un set di regole di rilevamento delle intrusioni sviluppate e mantenute da Proofpoint, ma originariamente create come un progetto di comunità open source. Queste regole sono utilizzate per identificare una vasta gamma di minacce di sicurezza di rete e vulnerabilità. Le ET Rules sono note per la loro capacità di rilevare minacce emergenti e zero-day, che spesso non sono ancora coperte da altri set di regole.

Le Emerging Threats Rules utilizzate su IPS-ICAR-DMZ sono:

1. **ET Open Rules**: Queste regole sono liberamente disponibili per la comunità e sono rilasciate sotto una licenza open source. ET Open è simile alle Snort GPLv2 Community Rules in quanto è accessibile a chiunque voglia utilizzarle e beneficiare del contributo collettivo della comunità di

sicurezza informatica. Le regole ET Open coprono un'ampia gamma di minacce e sono aggiornate regolarmente per affrontare nuove vulnerabilità e attacchi emergenti.

L'uso delle Emerging Threats Rules offre numerosi vantaggi:

1. **Rapidità di aggiornamento**: Sia le regole open source che quelle a pagamento sono aggiornate frequentemente per rispondere rapidamente alle nuove minacce, garantendo una protezione continua contro le vulnerabilità più recenti.
2. **Ampia copertura delle minacce**: Le ET Rules sono progettate per rilevare una vasta gamma di attacchi, inclusi malware, attacchi di rete, exploit di vulnerabilità e molto altro.
3. **Contributo della comunità e supporto professionale**: Mentre le ET Open Rules beneficiano del contributo collettivo della comunità di sicurezza, le ET Pro Rules offrono supporto e aggiornamenti professionali, combinando il meglio di entrambi i mondi.

Utilizzare le **Emerging Threats Rules**, insieme ad altri set di regole come le **Snort Subscriber Rules** e le **Snort GPLv2 Community Rules**, consente agli amministratori di rete di implementare una strategia di sicurezza multilivello, migliorando la capacità di rilevamento e risposta alle minacce.

5.3.3.3 Sourcefire OpenAppID Detectors

I **Sourcefire OpenAppID Detectors** sono una componente chiave della piattaforma Snort, progettata per migliorare la capacità di rilevamento delle applicazioni all'interno del traffico di rete. OpenAppID è un'iniziativa open source di Cisco che consente agli utenti di identificare, classificare e controllare le applicazioni in base al loro comportamento e al traffico generato. Questo strumento è particolarmente utile per la gestione della sicurezza delle applicazioni e il monitoraggio delle attività su reti complesse.

Caratteristiche Principali di Sourcefire OpenAppID Detectors:

1. **Identificazione delle Applicazioni**: OpenAppID utilizza una serie di "detectors" per identificare specifiche applicazioni basandosi su caratteristiche uniche del loro traffico. Questo include protocolli, firme comportamentali e pattern specifici che consentono di distinguere un'applicazione da un'altra. È in grado di rilevare migliaia di applicazioni, dalle più comuni alle più specifiche per settori particolari.
2. **Classificazione e Controllo**: Una volta identificate, le applicazioni possono essere classificate e soggette a politiche di controllo della rete. Gli amministratori possono decidere di consentire, limitare o bloccare il traffico di determinate applicazioni in base alle politiche aziendali e ai requisiti di sicurezza.
3. **Flessibilità e Personalizzazione**: OpenAppID consente agli utenti di creare i propri detectors personalizzati per applicazioni specifiche non coperte dai detectors predefiniti. Questa flessibilità è particolarmente utile per le aziende che utilizzano applicazioni interne o meno comuni che necessitano di un monitoraggio personalizzato.
4. **Integrazione con Snort**: Integrandosi perfettamente con Snort, OpenAppID consente di arricchire le capacità di rilevamento delle intrusioni con una visibilità dettagliata delle applicazioni. Questa integrazione consente agli amministratori di correlare eventi di sicurezza con l'utilizzo delle applicazioni, migliorando la capacità di risposta agli incidenti.

Benefici dell'Utilizzo di OpenAppID:

- **Maggiore Visibilità**: Fornendo una visibilità dettagliata sulle applicazioni che attraversano la rete, OpenAppID aiuta gli amministratori a comprendere meglio quali applicazioni vengono utilizzate e come.
- **Miglioramento della Sicurezza**: La capacità di identificare e controllare il traffico delle applicazioni permette di implementare politiche di sicurezza più granulari, riducendo il rischio di utilizzo non autorizzato delle risorse di rete.
- **Ottimizzazione delle Risorse di Rete**: Classificando e controllando il traffico delle applicazioni, è possibile ottimizzare l'utilizzo della larghezza di banda e delle risorse di rete, garantendo che le applicazioni critiche ricevano priorità.

I Sourcefire OpenAppID Detectors rappresentano un potente strumento per il rilevamento e la gestione delle applicazioni in rete. La loro capacità di identificare, classificare e controllare il traffico delle applicazioni migliora notevolmente la visibilità della rete e la sicurezza, consentendo agli amministratori di implementare politiche di rete più efficaci e rispondere rapidamente alle minacce emergenti. Integrando OpenAppID con Snort, le organizzazioni possono beneficiare di una soluzione di sicurezza completa e flessibile, adatta alle esigenze delle reti moderne.

5.3.3.4 FEODO Tracker Botnet C2 IP Rules

Le **FEODO Tracker Botnet C2 IP Rules** sono un insieme di regole di sicurezza informatica utilizzate per rilevare e mitigare le attività delle botnet, in particolare la botnet Feodo (anche nota come Cridex o Bugat). Queste regole sono sviluppate e mantenute da progetti di sicurezza collaborativi, come Abuse.ch, che si dedicano al monitoraggio e alla segnalazione delle attività di botnet.

Caratteristiche delle FEODO Tracker Botnet C2 IP Rules:

1. **Monitoraggio delle Botnet**: Le regole sono progettate per identificare i server di comando e controllo (C2) utilizzati dalla botnet Feodo. Questi server sono punti di contatto cruciali attraverso i quali i criminali informatici controllano i dispositivi infetti.
2. **Database Aggiornato di IP Malevoli**: Le regole si basano su un database di indirizzi IP aggiornato in tempo reale, fornito da servizi come Feodo Tracker di Abuse.ch. Questo database elenca gli indirizzi IP noti per essere associati alle attività della botnet Feodo.
3. **Blocco e Mitigazione**: Quando un dispositivo di rete, come un firewall o un sistema di rilevamento delle intrusioni (IDS) come Snort, utilizza queste regole, può bloccare automaticamente il traffico verso e dagli indirizzi IP sospetti, prevenendo la comunicazione con i server C2 e riducendo la propagazione della botnet.
4. **Integrazione con Sistemi di Sicurezza**: Le FEODO Tracker Botnet C2 IP Rules possono essere integrate con vari strumenti di sicurezza, tra cui Snort, Suricata e altri IDS/IPS. Questa integrazione permette di migliorare la capacità di rilevamento e risposta alle minacce in tempo reale.

Benefici dell'Utilizzo delle FEODO Tracker Botnet C2 IP Rules:

- **Protezione Proattiva**: L'uso di queste regole consente alle organizzazioni di adottare un approccio proattivo nella difesa contro le botnet, bloccando le comunicazioni dannose prima che possano causare danni significativi.
- **Aggiornamenti Continui**: Grazie all'aggiornamento continuo del database di indirizzi IP, le regole offrono una protezione aggiornata contro le ultime varianti e tattiche utilizzate dalla botnet Feodo.

- **Riduzione del Rischio**: Bloccando l'accesso ai server di comando e controllo, si riduce il rischio che i dispositivi infetti possano eseguire ulteriori azioni dannose, come il furto di dati, l'invio di spam o l'esecuzione di attacchi DDoS.

Le FEODO Tracker Botnet C2 IP Rules rappresentano uno strumento essenziale per la sicurezza delle reti, fornendo una difesa robusta contro le botnet. Integrando queste regole con i sistemi di rilevamento e prevenzione delle intrusioni, le organizzazioni possono migliorare significativamente la loro capacità di rilevare e bloccare le comunicazioni malevole associate alla botnet Feodo, proteggendo così le loro reti e dati sensibili da potenziali attacchi.

5.3.3.5 Rules Update Settings

Le **Rules Update Settings** sono una componente critica della gestione di un sistema di rilevamento delle intrusioni efficace. Queste impostazioni, combinate con pratiche di verifica e monitoraggio, contribuiscono a mantenere una robusta struttura di sicurezza informatica.

Nella configurazione sono state importate la seguente configurazione:

Update Interval settato su 12 ore

Update Start Time settato per le 00:15

Hide Deprecated Rules Categories attivato in modo da nascondere le regole deprecate, e mantenere un ambiente di sicurezza più ordinato, efficiente e reattivo, ottimizzando le risorse di sistema e migliorando la protezione complessiva della rete.

Disable SSL Peer Verification disattivato in quanto disabilitare la verifica del peer SSL è una configurazione che può essere necessaria in specifiche circostanze, come lo sviluppo o la risoluzione di emergenze. Tuttavia, comporta rischi significativi per la sicurezza che devono essere attentamente considerati.

5.3.3.6 Impostazioni Generali

Remove Blocked Hosts Interval settato su 6 ore - La funzionalità **"Remove Blocked Hosts Interval"** è una configurazione presente in sistemi di rilevamento delle intrusioni (IDS) o sistemi di prevenzione delle intrusioni (IPS), e serve a determinare l'intervallo di tempo dopo il quale gli host bloccati vengono rimossi dalla lista dei blocchi.

Remove Blocked Hosts After Deinstall attivo - La funzionalità "**Remove Blocked Hosts After Deinstall**" in Snort si riferisce a una configurazione che gestisce la rimozione degli indirizzi IP bloccati quando Snort viene disinstallato o riavviato.

Keep Snort Settings After Deinstall attivo - La funzionalità **"Keep Snort Settings After Deinstall"** in Snort è progettata per mantenere le configurazioni e le impostazioni del sistema di rilevamento delle intrusioni (IDS) anche dopo che il software è stato disinstallato. Questa impostazione è utile per vari motivi e offre numerosi benefici, soprattutto in ambienti dove le configurazioni di sicurezza sono complesse e richiedono un ripristino rapido in caso di reinstallazione.

Startup/Shutdown Logging attivo - La funzionalità di **Startup/Shutdown Logging** in Snort è progettata per registrare eventi critici relativi all'avvio e allo spegnimento del sistema di rilevamento delle intrusioni (IDS). Questo tipo di logging è essenziale per il monitoraggio e la gestione efficiente del sistema, fornendo agli amministratori informazioni cruciali sulle operazioni del sistema.

5.3.4 Aggiornamenti

Il tab **Aggiornamenti** in Snort è una sezione dell'interfaccia di gestione che permette agli amministratori di gestire e monitorare gli aggiornamenti delle regole di rilevamento delle intrusioni e, talvolta, degli aggiornamenti del software stesso. Questa funzionalità è fondamentale per mantenere il sistema aggiornato con le ultime regole di sicurezza, che sono essenziali per rilevare le nuove minacce e vulnerabilità emergenti.

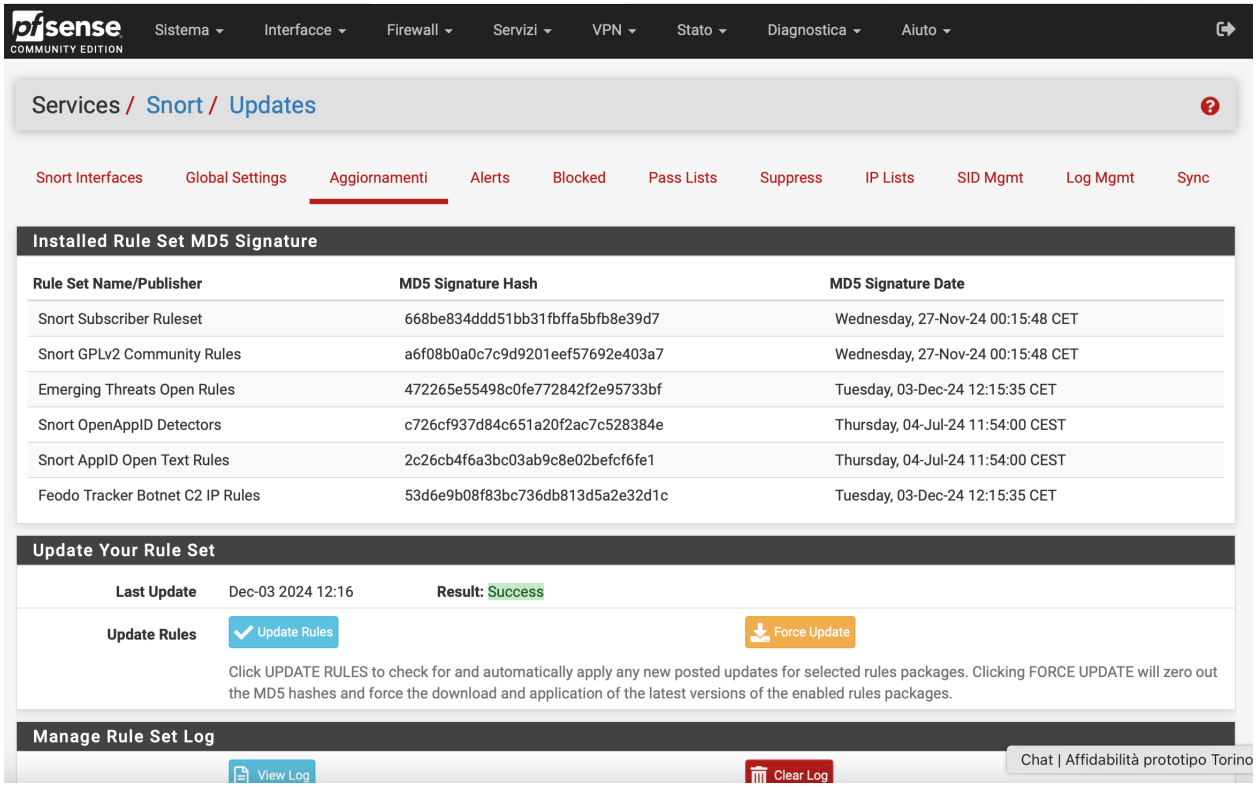

Figura 14 - Sezione Aggiornamenti di Snort

5.3.5 Alerts

Il tab **Alerts** (Figura 15) di Snort su pfSense è una sezione che consente di monitorare e analizzare le attività sospette rilevate dal sistema IDS/IPS. Questa sezione contiene informazioni dettagliate sugli avvisi generati da Snort quando rileva potenziali minacce o comportamenti anomali nella rete. Ecco una descrizione dettagliata di cosa contiene e come utilizzare questa sezione:

- **Alert Log View Settings** – sono presenti varie informazioni relative al modo in cui si vogliono visualizzare i dati degli alerts e in particolare:
- **Alert Log Actions** - si possono scaricare o cancellare il file di log.
- **Alert Log View Filter** - è possibile creare uno o più filtri per la visualizzazione degli Alerts.

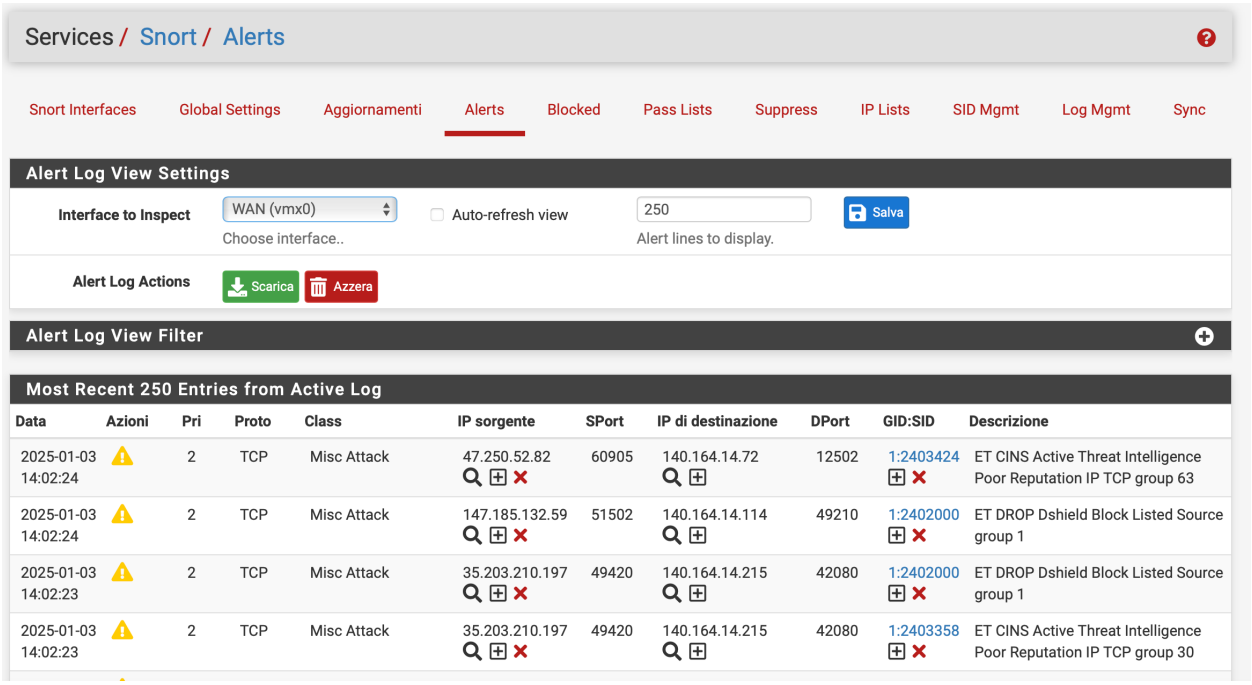

Figura 15 - Sezione Alerts

Most Recent 250 Entries from Active Log - in questa sezione si trovano i record secondo le impostazioni viste precedentemente, le colonne sono così impostate:

- **Data** - la data del record
- **Azioni** - il tipo di evento (Alert, Pass, Dynamic, Log, e/o Activate)
- **Pri** - la priorità dell'evento
- **Proto** - il protocollo interessato (TCP, UDP, etc.)
- **Class** - la tipologia di evento riscontrato
- **IP Sorgente** - l'IP da cui è partita l'attività
- **SPort - Source Port** la porta da cui è partita l'attività
- **IP Destinazione** - l'IP interno e/o esterno monitorato dal firewall dove era diretta l'attività
- **DPort - Destination Port** la porta a cui era destinata l'attività
- **GID:SID** - il Generator ID e il Signature ID della regola impostata sul firewall che è stata violata
- **Descrizione** - descrizione dell'attività rilevata

Le azioni che si possono operare sui records sono descritte di seguito:

- **Lente di Ingrandimento -** se si clicca viene mostrato dove quell'indirizzo IP viene risolto
- **Segno di Addizione** - Aggiungi l'IP alla Suppress List, La **Suppress List** è una lista di regole che istruiscono Snort a ignorare determinati avvisi. Quando un avviso viene aggiunto a questa lista, Snort non genererà più notifiche per quell'avviso specifico, permettendo di mantenere il log degli avvisi pulito e concentrato su potenziali minacce reali.
- **Croce Rossa** - Rimuove l'host dalla Blocked Table, permette di rimuovere un indirizzo IP dalla tabella degli host bloccati. Questa funzione è utile quando un indirizzo IP è stato erroneamente bloccato o quando non rappresenta più una minaccia.

Queste operazioni possono essere effettuate su:

- **IP Sorgente**: Risolve - Aggiunge a Suppress List - Rimuove da Blocked Table
- **IP Destinazione**: Risolve - Aggiunge a Suppress List
- **GID:SID**: Aggiunge a Suppress List - Disabilita la regola e la rimuove dal set di regole

5.3.5 Blocked

La sezione **Blocked** (Figura 16) di Snort su pfSense è dedicata alla gestione degli indirizzi IP che sono stati bloccati a causa di attività sospette o malevole rilevate dal sistema IDS/IPS di Snort. Questa consente di vedere quali IP sono stati bloccati, comprendere il motivo del blocco e gestire gli IP bloccati. Ecco cosa contiene e come utilizzare questa sezione:

Blocked Hosts and Log View Settings

- **Blocked Hosts - i**n questa sezione è possibile scaricare, tramite il bottone **Scarica,** la lista di tutti gli host che sono stati bloccati per attività sospetta; invece, cliccando sul bottone **Azzera** tutti gli host attualmente bloccati vengono sbloccati.

- **Refresh and Log View** - In questa sezione è possibile modificare i parametri legati alla generazione automatica dei files di log; cliccando sul bottone **Salva** nella sezione **Save auto-refresh and view settings** è possibile salvare le impostazioni di aggiornamento automatico e di visualizzazione nella sezione degli avvisi e delle altre informazioni, in particolare, se si selezione il checkbox **Aggiorna** la lista verrà aggiornata automaticamente, mentre nella sezione **Number of blocked entries to view. Default is 500** si può definire il numero di record da visualizzare (di default sono 500)

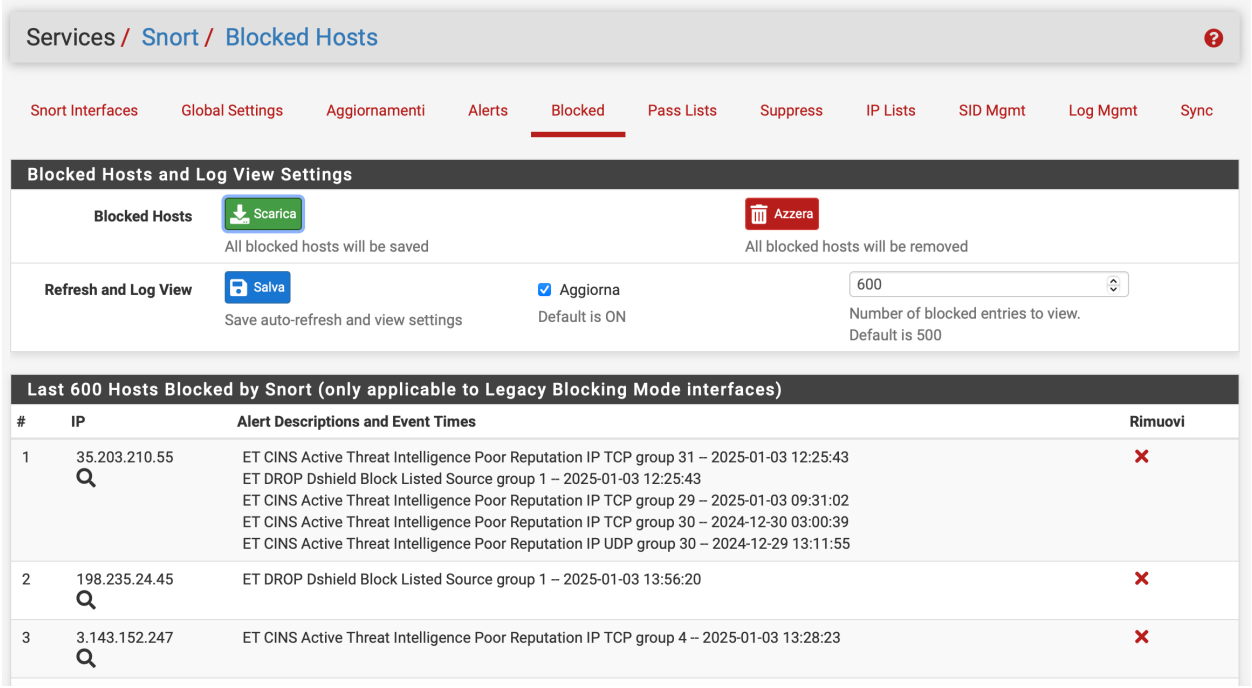

Figura 16 – Sezione Blocked

Last 600 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

Questa sezione fornisce un elenco degli ultimi indirizzi IP che sono stati bloccati da Snort quando è configurato in modalità di blocco legacy. Questa modalità è specifica per le interfacce configurate per utilizzare il blocco legacy piuttosto che il blocco inline o altre modalità di blocco più moderne.

Nella sezione si possono vedere le seguenti colonne:

- **IP** - l'indirizzo IP bloccato
- **Alert Description and Event Times** - il timestamp dell'evento e la sua descrizione
- **Rimuovi** - La possibilità di rimuovere l'IP dalla lista di IP bloccati

6. Risultati

Il sistema Firewall e IPS con DMZ è attivo da circa quattro mesi e rileva in media ogni ora 833 potenziali minacce (Figura 15) e blocca 410 indirizzi IP (Figura 16). Nell'arco di questi quattro mesi il sistema ha rilevato circa 2.598.960 di potenziali minacce, bloccando 1.279.200 di indirizzi IP (Figura 17).

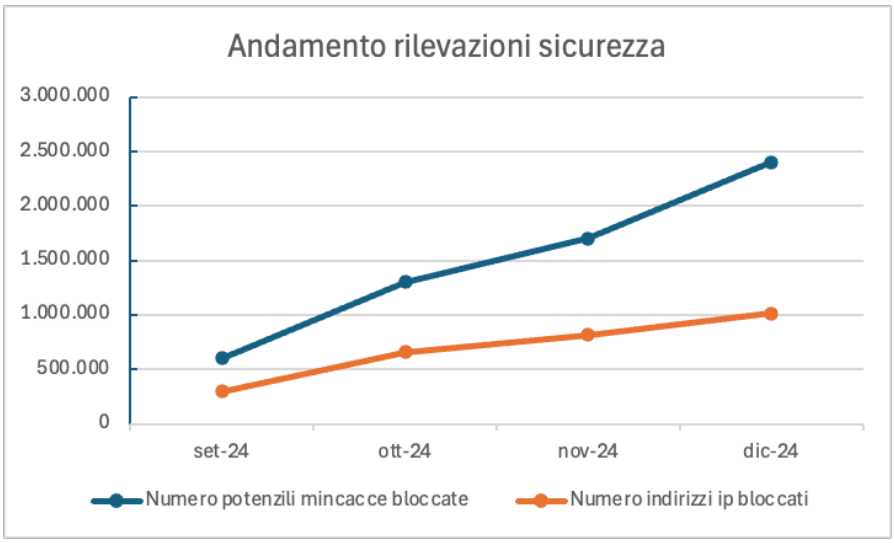

Figura 17 – Andamento rilevazioni di sicurezza

7. Conclusioni

L'implementazione della DMZ e della soluzione proposta basata su pfSense e Snort ha rappresentato un significativo miglioramento nella gestione della sicurezza informatica della sede di Napoli dell'ICAR. La configurazione della DMZ, associata a un firewall robusto e a un sistema di Intrusion Prevention System (IPS), ha permesso di garantire un isolamento efficace tra i servizi pubblicamente accessibili e la rete interna dell'Istituto. Questo approccio ha minimizzato il rischio di compromissione dei sistemi critici, fornendo al contempo un accesso controllato ai servizi esposti su Internet.

La separazione netta tra le subnet LAN e DMZ ha ridotto significativamente il rischio di movimenti laterali degli attacchi, mentre l'utilizzo di VPN per l'accesso alla DMZ ha ulteriormente rafforzato i controlli di sicurezza.

La combinazione delle tecnologie adottate, tra cui le regole granulari del firewall, il NAT 1:1 e l'uso di Snort per il rilevamento e la prevenzione delle intrusioni, ha fornito una protezione stratificata. Ciò ha reso possibile non solo il blocco proattivo delle minacce note ma anche il rilevamento tempestivo di attività anomale o comportamenti malevoli, garantendo così una maggiore resilienza dell'infrastruttura.

Un altro beneficio significativo della soluzione proposta è stato il miglioramento nella gestione centralizzata delle regole e della configurazione di sicurezza. A differenza della configurazione precedente, in cui ogni server richiedeva interventi individuali per l'aggiornamento delle regole firewall, il nuovo approccio ha semplificato l'amministrazione e ridotto la complessità operativa. Questo ha portato a una maggiore efficienza e a una riduzione dei tempi di intervento in caso di incidenti.

In sintesi, la DMZ, il firewall pfSense e Snort hanno rappresentato un passo avanti fondamentale nella strategia di sicurezza dell'ICAR sede di Napoli. La soluzione ha non solo migliorato il livello di protezione contro le minacce informatiche, ma ha anche fornito un'infrastruttura scalabile e sostenibile, in grado di adattarsi alle future esigenze di sicurezza e crescita tecnologica. Questo approccio, oltre a rispondere alle attuali sfide della cybersecurity, costituisce un modello replicabile per altre organizzazioni con esigenze simili.

7. Riferimenti

[1] https://www.icar.cnr.it/
[2] https://www.cnr.it/
[3] https://www.diitet.cnr.it/
[4] https://www.pfsense.org/
[5] https://www.freebsd.org/
[6] https://www.snort.org/
[7] https://www.cisco.com/c/en/us/services/acquisitions/sourcefire.html