|  |
| --- |
| Immagine che contiene testo, grafica, poster, Elementi grafici  Il contenuto generato dall'IA potrebbe non essere corretto.  Relazione  buildweek  Progetto Infrastruttura  Theta |
| FalconLockFalconLock |



Sommario

[1. STRUTTURA DEL PROGETTO 2](#_Toc190879815)

[**2.** **GLOSSARIO** 3](#_Toc190879816)

[**3.** **SUBNETS** 4](#_Toc190879817)

[**4.** **FIREWALL** 4](#_Toc190879818)

[4.1. Configurazione Porte GigabitEthernet 4](#_Toc190879819)

[4.2. Creazione Alias 5](#_Toc190879820)

[4.3. Aggiunta Regole pfSense 5](#_Toc190879821)

[**5.** **ANALISI DVWA** 8](#_Toc190879822)

[5.1. Enumerazione Porte Aperte 8](#_Toc190879823)

[5.2. Analisi Metodi http 9](#_Toc190879824)

## STRUTTURA DEL PROGETTO

L’infrastruttura di rete della società Theta è stata divisa in quattro zone:

* ZONA INTERNA: raggruppa gli uffici dell’azienda Theta che sono disposti su sei piani.

La struttura della zona è a stella estesa per semplicità di implementazione e facilità di una possibile futura espansione.

Ogni piano è composto da:

* + 20 personal computer
  + 1 switch 24p

Messi in collegamento da un centro stella costituito da un router con 8 porte GigabitEthernet.

Come sistema di archiviazione aziendale è stato predisposto un NAS accessibile da tutti i client della rete interna.

All’interno del NAS è in esecuzione un HIDS che invia messaggi di allert nel caso riscontrasse accessi/operazioni sui file non consuete.

* DMZ: zona a cui è permesso l’accesso dall’esterno della rete aziendale. I dispositivi presenti non possono contattare la rete interna.

Composta da:

* + Server Web: DVWA di Metasploitable.
* ZONA ESTERNA: raffigurata per completezza ma non gestita dalla FalconLock. Rete pubblica che permette l’accesso alla WAN.
* ZONA CENTRALE: Assolve i compiti di
  + Collegamento tra le diverse zone che compongono l’infrastruttura
  + Filtraggio del traffico tramite la presenza di un Firewall
  + Monitoraggio del traffico mediante l’implementazione di:
    - IDS all’interno della DMZ per ricevere avvisi in caso di attività malevola o di violazione di policy.
    - IPS posto tra il firewall e la rete interna per intervenire prontamente in caso di una breccia nella rete interna.

1. **GLOSSARIO**

* DMZ – Demilitarized Zone

sottorete fisica o logica che contiene ed espone dei servizi ad una rete esterna non ritenuta sicura, come ad esempio Internet. Lo scopo di una DMZ è di proteggere la rete LAN di un'organizzazione.

* IDS - Intrusion Detection System

dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali.

* IPS - Intrusion Prevention System

componenti software attivi sviluppati per incrementare la sicurezza informatica di un sistema informatico, individuando, registrando le informazioni relative e tentando di segnalare e bloccare le attività dannose.

* WAN – Wide Area Network

rete di telecomunicazioni che si estende su una grande area geografica con lo scopo di mettere in comunicazione altre reti di computer. La più grande rete WAN mai realizzata, a cui si fa riferimento, è Internet.

* DHCP - Dynamic Host Configuration Protocol

è un protocollo di rete che permette ai dispositivi di una rete locale di ricevere automaticamente la configurazione IP.

* NAS - Network Attached Storage

è un dispositivo di archiviazione di rete che permette di salvare, condividere e accedere ai file da più dispositivi connessi.

* DVWA - Damn Vulnerable Web Application

è un'applicazione web intenzionalmente vulnerabile, progettata per testare e migliorare le competenze in cybersecurity e penetration testing.

* FIREWALL

è un componente hardware e/o software di difesa perimetrale di una rete che può anche svolgere funzioni di collegamento tra due o più segmenti di rete.

1. **SUBNETS**

Per dividere logicamente i piani degli uffici sono state create sei subnets.

Vista la presenza di computer fissi e di numero ben definito si è optato di assegnare staticamente ad ogni client un IP. Questa scelta permetterà al reparto IT, in caso di necessità, di connettersi da remoto in modo più agevole sapendo a quale IP corrisponde ogni macchina.

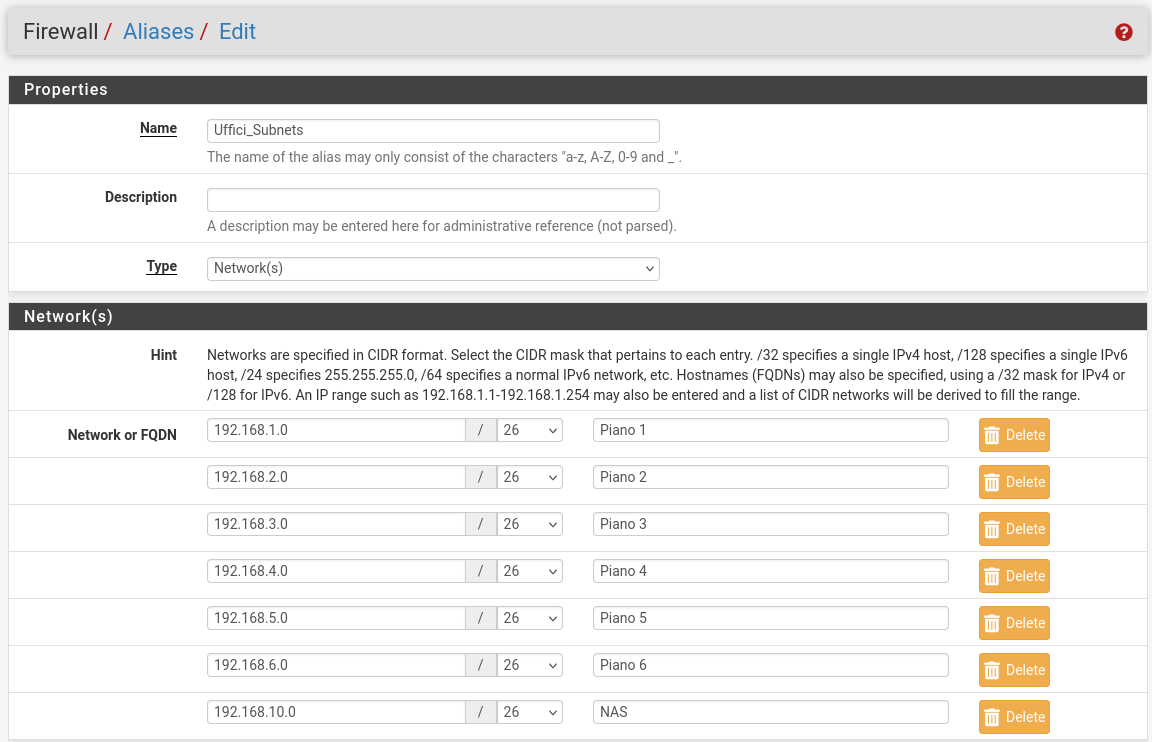
Le subnets sono le seguenti:

* + Piano 1:
    - IP Network: 192.168.1.0
    - Subnetmask: 255.255.255.192
    - IP Gateway: 192.168.1.1
    - IP Broadcast: 192.168.1.63
  + Piano 2:
    - IP Network: 192.168.2.0
    - Subnetmask: 255.255.255.192
    - IP Gateway: 192.168.2.1
    - IP Broadcast: 192.168.2.63
  + Piano 3:
    - IP Network: 192.168.3.0
    - Subnetmask: 255.255.255.192
    - IP Gateway: 192.168.3.1
    - IP Broadcast: 192.168.3.63
  + Piano 4:
    - IP Network: 192.168.4.0
    - Subnetmask: 255.255.255.192
    - IP Gateway: 192.168.4.1
    - IP Broadcast: 192.168.4.63
  + Piano 5:
    - IP Network: 192.168.5.0
    - Subnetmask: 255.255.255.192
    - IP Gateway: 192.168.5.1
    - IP Broadcast: 192.168.5.63
  + Piano 6:
    - IP Network: 192.168.6.0
    - Subnetmask: 255.255.255.192
    - IP Gateway: 192.168.6.1
    - IP Broadcast: 192.168.6.63

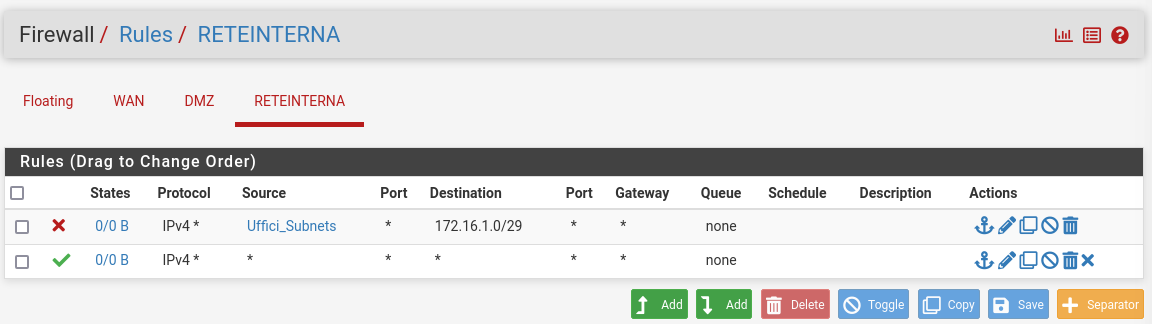
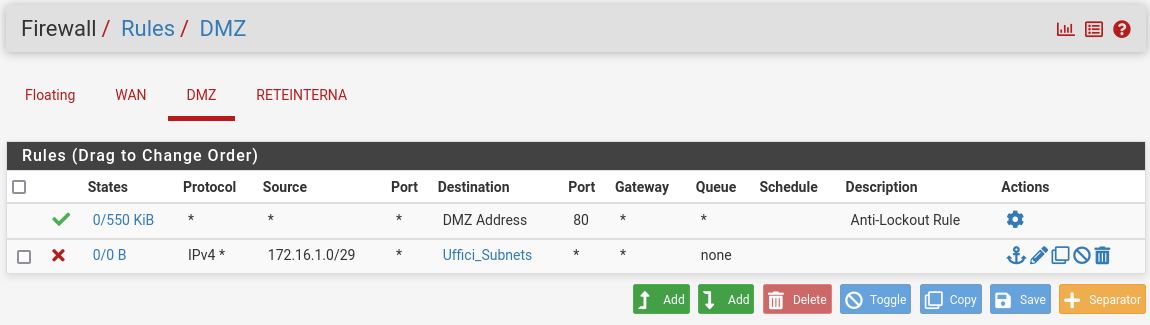
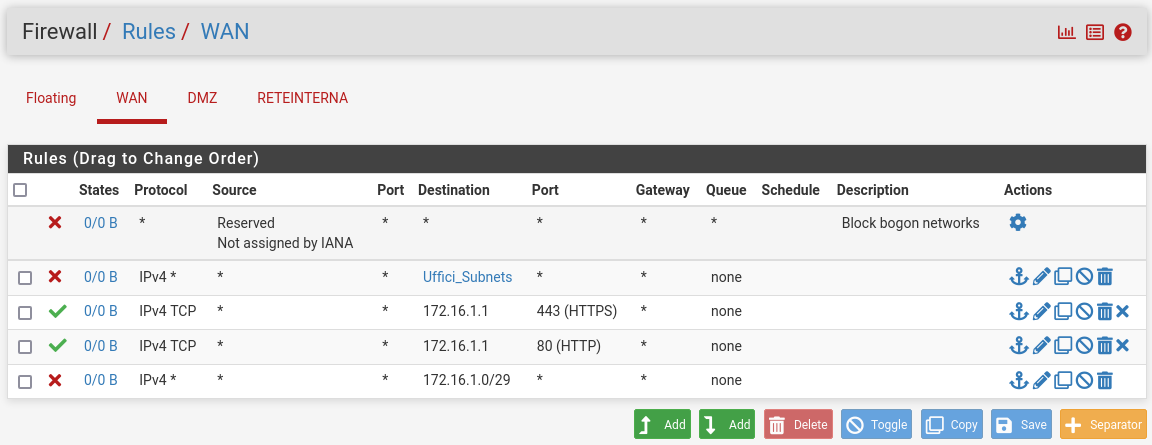
All’interno del Router0 sono state caricate, mediante file di configurazione, le ACL per bloccare il traffico tra i piani dello stabile consentendo, allo stesso tempo, a tutti di collegarsi al NAS.

1. **FIREWALL**

A protezione dell’intera infrastruttura è stato predisposto un firewall NETGATE 1537 MAX pfSense+. Il software firewall in esecuzione al suo interno è la versione a pagamento di pfSense.

* 1. Configurazione Porte GigabitEthernet
     + WAN: la configurazione della porta rispecchia i parametri forniti dall’ISP
     + DMZ
       - IP: 172.16.1.1
       - Subnet Mask: 255.255.255.248 (CIDR /29)
     + RETEINTERNA
       - IP: 172.16.1.9
       - Subnet Mask: 255.255.255.248 (CIDR/29)
  2. Creazione Alias

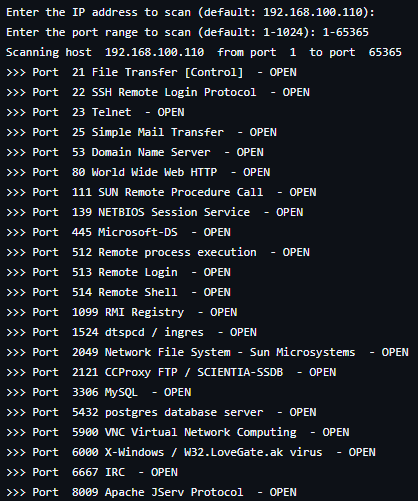
Per una gestione migliore delle regole si definisce un nome per indicare un gruppo di reti.

* + - Rete\_Interna
      * 192.168.1.0/26 – Piano 1
      * 192.168.2.0/26 – Piano 2
      * 192.168.3.0/26 – Piano 3
      * 192.168.4.0/26 – Piano 4
      * 192.168.5.0/26 – Piano 5
      * 192.168.6.0/26 – Piano 6
      * 192.168.10.0/26 - NAS
  1. Aggiunta Regole pfSense
     + Rete Interna:
       - Regola1:Impedisce qualsiasi richiesta avanzata dalla zona interna verso la DMZ
         * Action: Block
         * Address Family: IPv4
         * Protocol: Any
         * Source Address or Alias: Uffici\_Subnets
         * Source Port: Any
         * Destination: 172.16.1.0/29
         * Destination Port: Any
       - Regola2: permette ai client della rete interna per raggiungere internet
         * Action: Pass
         * Address Family: IPv4
         * Protocol: Any
         * Source: Any
         * Source Port: Any
         * Destination: Any
         * Destination Port: Any
     + DMZ:
       - Regola1:impedisce qualsiasi richiesta avanzata dalla DMZ verso la zona interna
         * Action: Block
         * Address Family: IPv4
         * Protocol: Any
         * Source: 172.16.1.0/29
         * Source Port: Any
         * Destination Address or Alias: Uffici\_Subnets
         * Destination Port: Any
     + WAN:
       - Regola 1:impedisce qualsiasi richiesta proveniente da internet destinata alla rete interna
         * Action: Pass
         * Address Family: IPv4
         * Protocol: Any
         * Source: Any
         * Source Port: Any
         * Destination Address or Alias: Uffici\_Subnets
         * Destination Port: Any
       - Regola 2 + Regola 3 + Regola 4: permette di raggiungere il server web nella DMZ solo sulla porta 80 o 443
         * Action: Pass
         * Address Family: IPv4
         * Protocol: TCP
         * Source: Any
         * Source Port: Any
         * Destination Address or Alias: 172.16.1.1
         * Destination Port: 80
         * Action: Pass
         * Address Family: IPv4
         * Protocol: TCP
         * Source: Any
         * Source Port: Any
         * Destination Address or Alias: 172.16.1.1
         * Destination Port: 443
         * Action: Block
         * Address Family: IPv4
         * Protocol: TCP
         * Source: Any
         * Source Port: Any
         * Destination: 172.16.1.0/29
         * Destination Port: Any

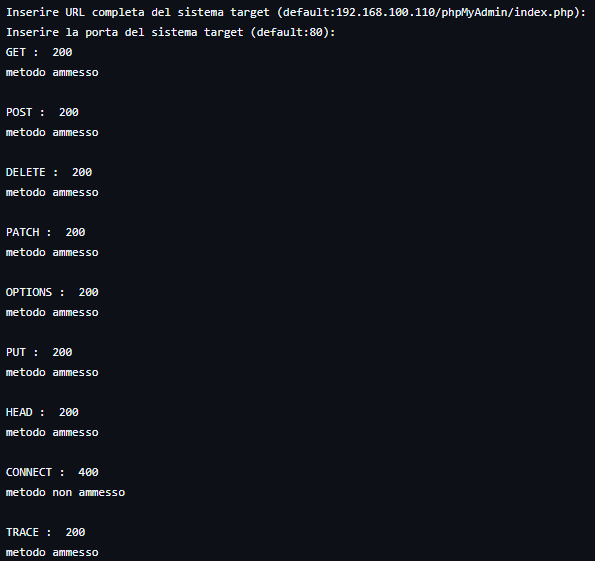
1. **ANALISI DVWA**

Nella DMZ è presente il web server su cui si è andati a svolgere un’attenta analisi in quanto raggiungibile dall’esterno della rete.

* 1. Enumerazione Porte Aperte

Il tool sviluppato ha effettuato una scansione dandoci immediato riscontro delle porte aperte e del servizio ad esse collegata.

* 1. Analisi Metodi http

La seconda parte dell’analisi si è concentrata sull’analisi dei metodi accettati dal Web Server e sui codici di stato restituiti.