

Proposta di Rete

Theta L.T.D



PAIMEI
EXPLOIT

Indice

Topologia di rete

Configurazioni dispositivi

Protocolli sicurezza

Testing with Python

Introduzione:

L'obiettivo di questo progetto è sviluppare e proporre un'infrastruttura di rete efficiente e sicura, pensata per soddisfare le esigenze operative dell'Azienda Theta. Il lavoro comprende la progettazione logica della rete, l'individuazione dei dispositivi necessari e la stima dei costi associati alla sua realizzazione.

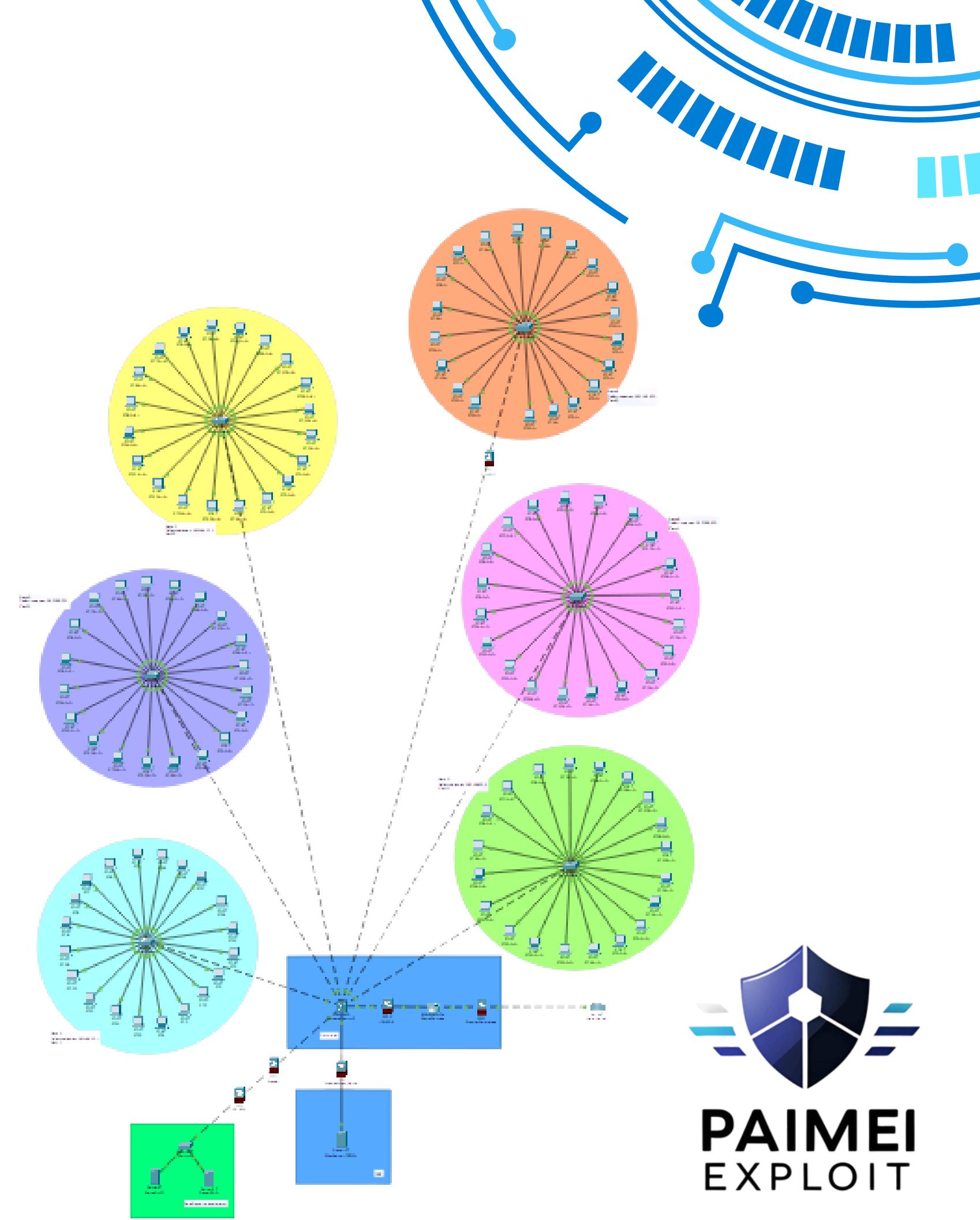
Richiesta

La richiesta iniziale prevedeva lo sviluppo di una rete capace di supportare 120 postazioni distribuite su sei piani, più un seminterrato, oltre all'integrazione di componenti fondamentali come un web server, un firewall perimetrale, un NAS e tre dispositivi IDS/IPS per la sicurezza.

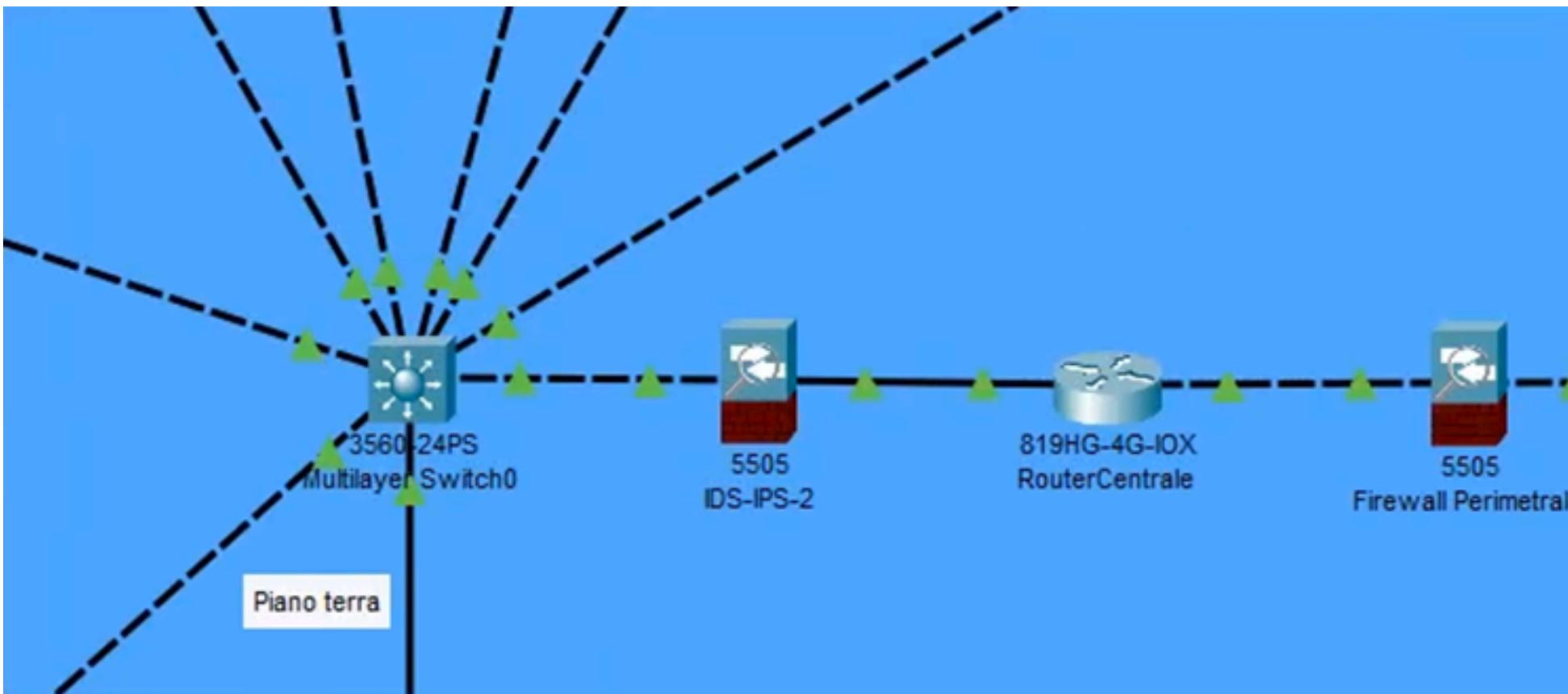
Progettazione e simulazione

Per rappresentare in modo chiaro e realistico la rete che intendiamo realizzare, abbiamo utilizzato il software Cisco Packet Tracer. Il primo passo è stato creare l'ambiente virtuale e inserire al suo interno i dispositivi necessari, seguendo fedelmente le richieste dell'azienda.

Abbiamo quindi progettato una topologia distribuita su più VLAN, organizzando il traffico interno in maniera ordinata e sicura. Ogni piano dispone di una propria VLAN dedicata, fatta eccezione per il piano terra, dove abbiamo previsto due segmentazioni separate: una per gli uffici e una VLAN dedicata alla DMZ, destinata ai servizi esposti all'esterno



Piano terra

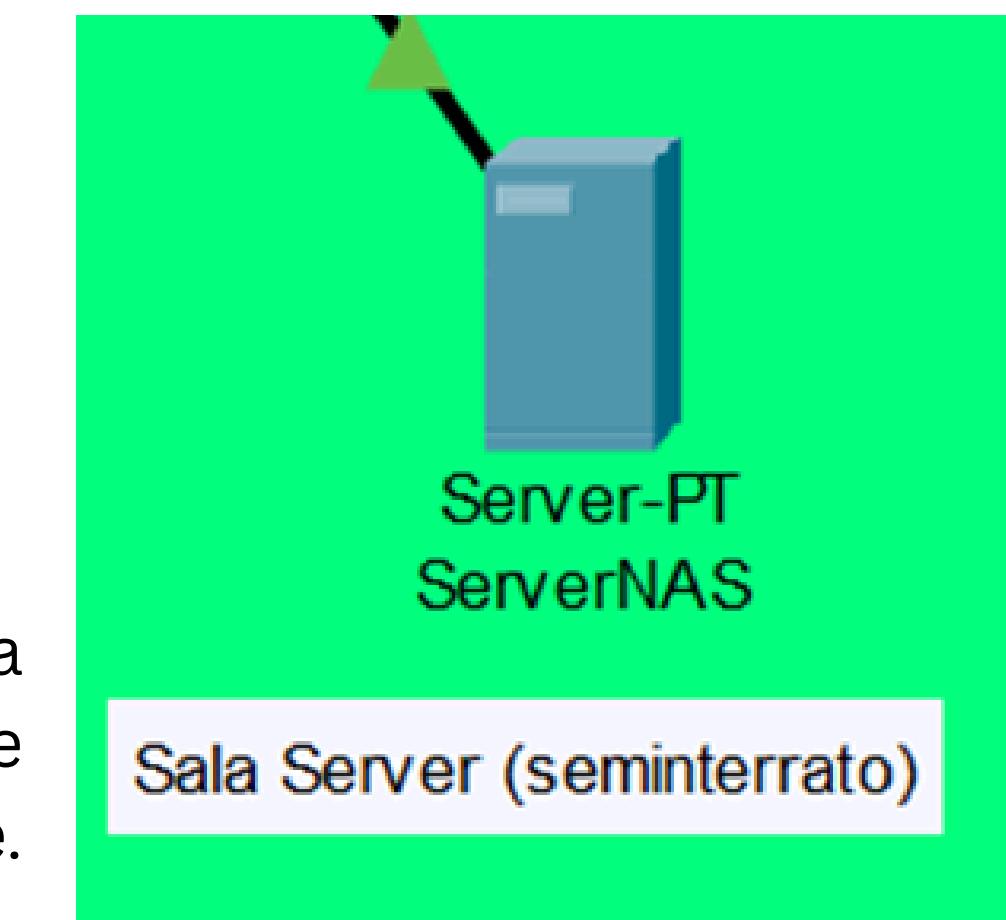


Il cuore del sistema è rappresentato da uno switch Layer 3 installato al piano terra, responsabile della gestione del routing tra le VLAN. Questo dispositivo centralizza il traffico di rete e semplifica la gestione, riducendo i tempi di latenza e migliorando il controllo complessivo dell'infrastruttura.

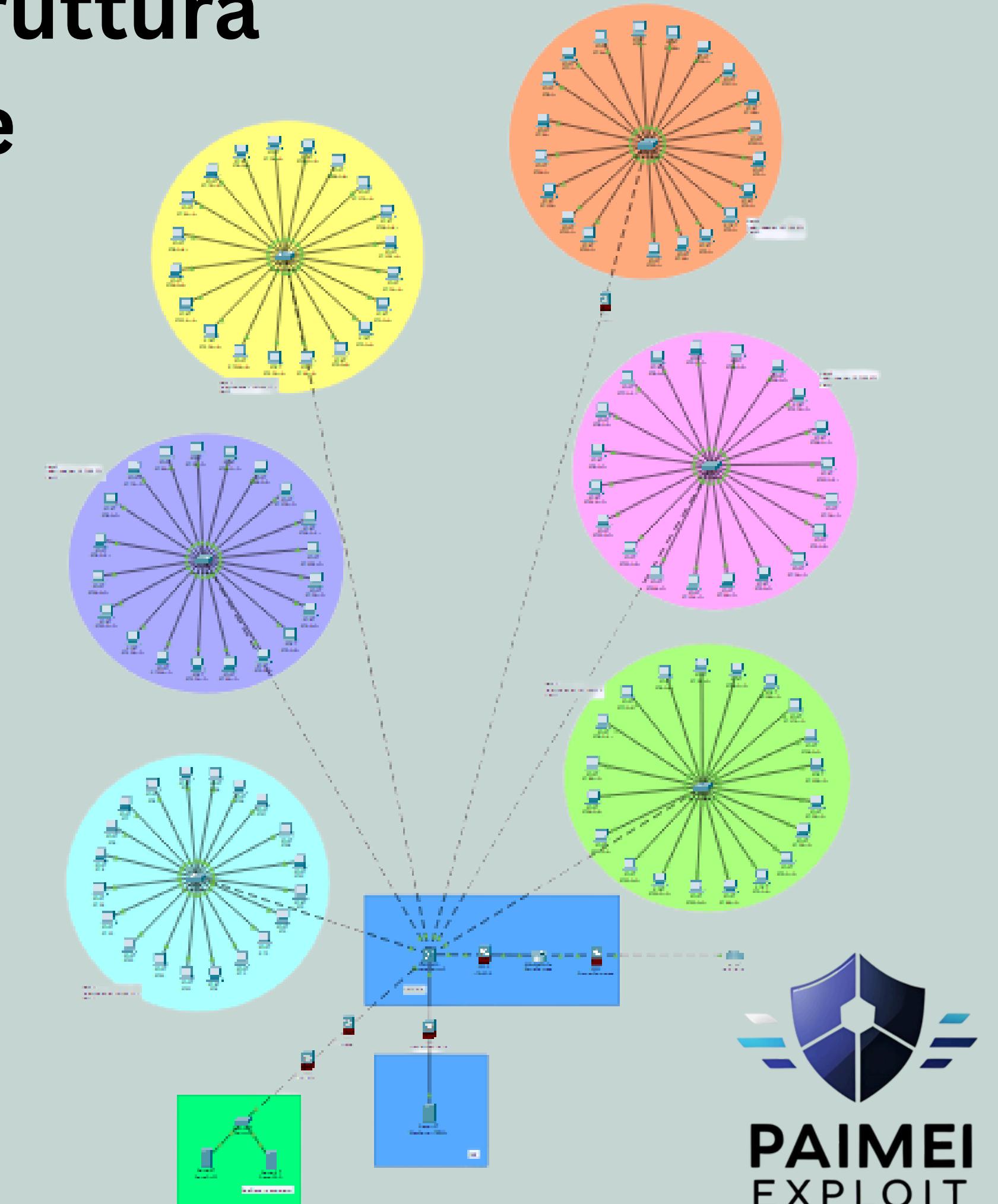
In linea con le richieste, abbiamo inserito un web server all'interno della DMZ (collocata sempre al piano terra), in modo da offrire i servizi aziendali all'esterno in totale sicurezza



Il **NAS** è stato invece collocato nel seminterrato, nella zona server, per offrire uno spazio di archiviazione centralizzato e accessibile solo dalle reti autorizzate.



Prototipo struttura di rete



PAIMEI
EXPLOIT

Configurazione dei Servizi e della Sicurezza

Passiamo ora ad illustrarvi le configurazioni che abbiamo realizzato su vari dispositivi in rete.

Dato il gran numero di dispositivi che prevediamo verranno connessi alla vostra infrastruttura di rete abbiamo ritenuto opportuno proporvi l'installazione di un server DHCP per la gestione dinamica degli indirizzi IP.



PAIMEI
EXPLOIT

Gestione IP e postazioni di lavoro

Considerando l'alto numero di dispositivi connessi, abbiamo ritenuto opportuno introdurre un server DHCP in trunk, incaricato di assegnare dinamicamente gli indirizzi IP all'interno della rete. Questo server è stato configurato con un indirizzo statico (192.168.2.2), così da permettere allo switch Layer 3 di indirizzare correttamente tutte le richieste DHCP provenienti dai client.

ServerDHCP

Physical Config Services Desktop Programming

IP Configuration

IP Configuration

DHCP Static 192.168.2.2

IPv4 Address 255.255.255.0

Subnet Mask 192.168.2.1

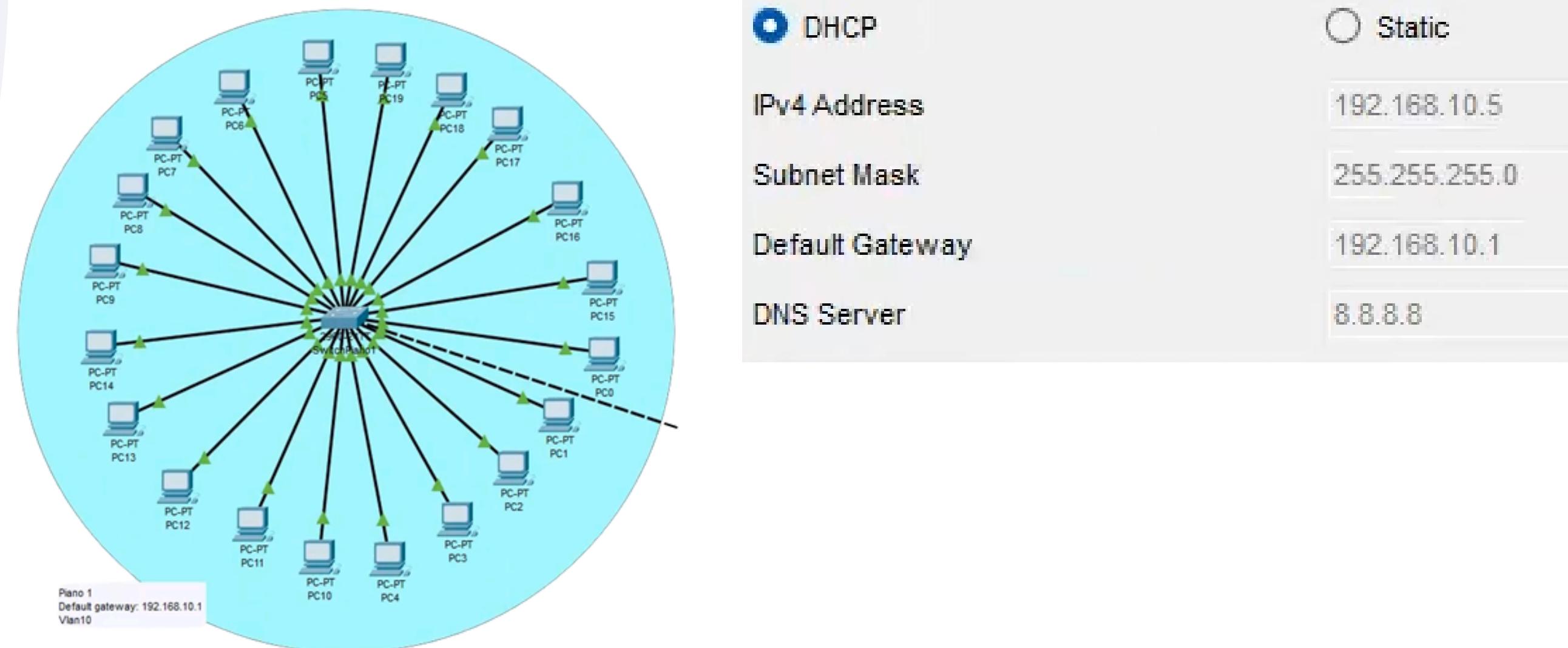
Default Gateway 8.8.8.8

DNS Server

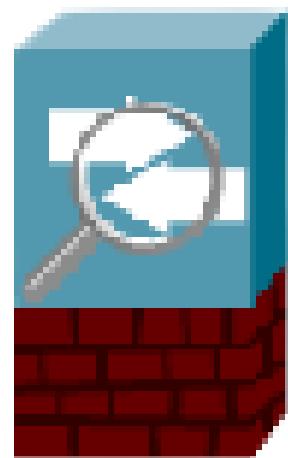
Generazione delle interfacce VLAN gestite dal server:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLI Addr
Vlan60	192.168....	0.0.0.0	192.168....	255.255....	253	0.0.0.0	0.0.0.0
Vlan50	192.168....	0.0.0.0	192.168....	255.255....	253	0.0.0.0	0.0.0.0
Vlan40	192.168....	0.0.0.0	192.168....	255.255....	253	0.0.0.0	0.0.0.0
Vlan30	192.168....	0.0.0.0	192.168....	255.255....	253	0.0.0.0	0.0.0.0
Vlan20	192.168....	0.0.0.0	192.168....	255.255....	253	0.0.0.0	0.0.0.0
Vlan10	192.168....	0.0.0.0	192.168....	255.255....	253	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168....	255.255....	512	0.0.0.0	0.0.0.0

Le postazioni di lavoro, infine, sono state organizzate secondo una topologia a stella, con switch di piano collegati direttamente allo switch centrale che a sua volta è connesso allo switch layer3 del piano terra. Tutti i PC ricevono un indirizzo IP dinamico attraverso il server DHCP, rendendo semplice la gestione e la scalabilità della rete nel tempo.



Per garantire un elevato livello di sicurezza, sono stati configurati tre dispositivi IDS/IPS, ognuno con regole personalizzabili:



5505

IDS_IPS1



5505

IDS-IPS-2



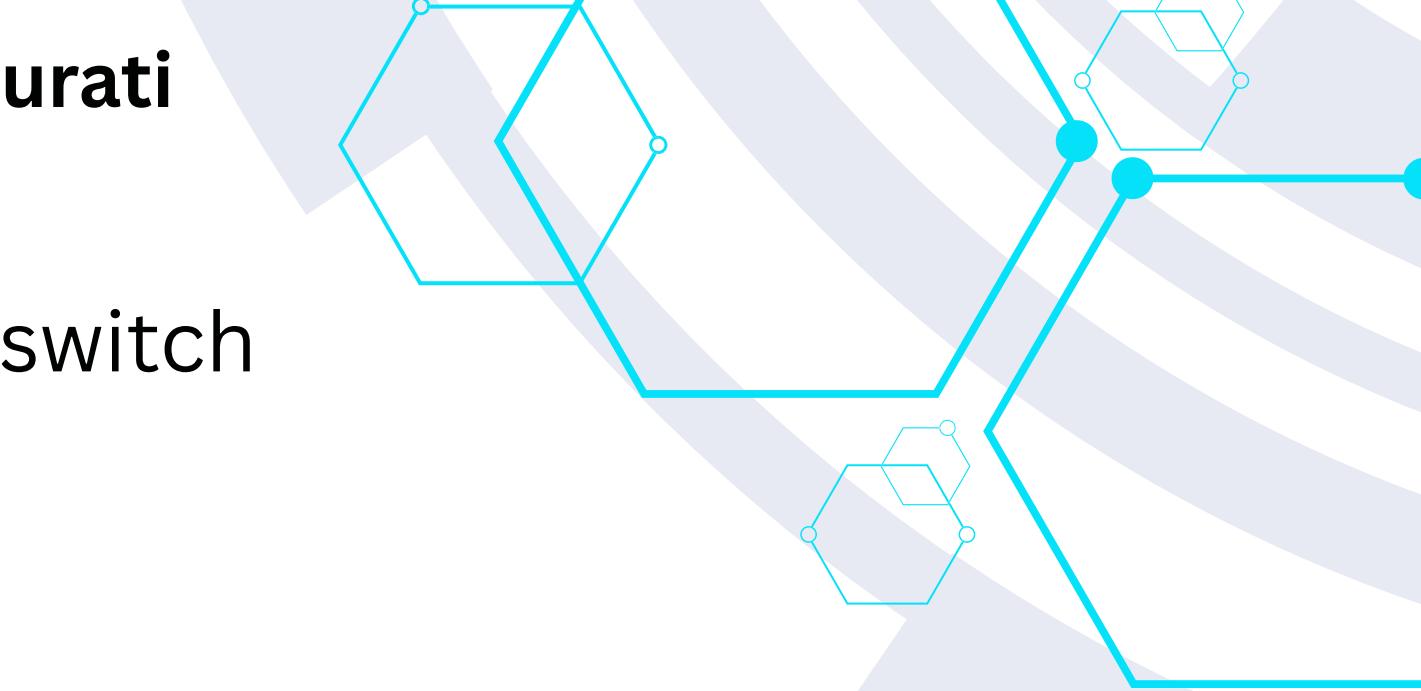
5505

IDS-IPS-3

il primo monitora i flussi tra lo switch Layer 3 e la sala server, così da prevenire accessi anomali ai dati;

il secondo controlla il traffico tra la rete interna e l'esterno, proteggendo l'infrastruttura da eventuali intrusioni via Internet;

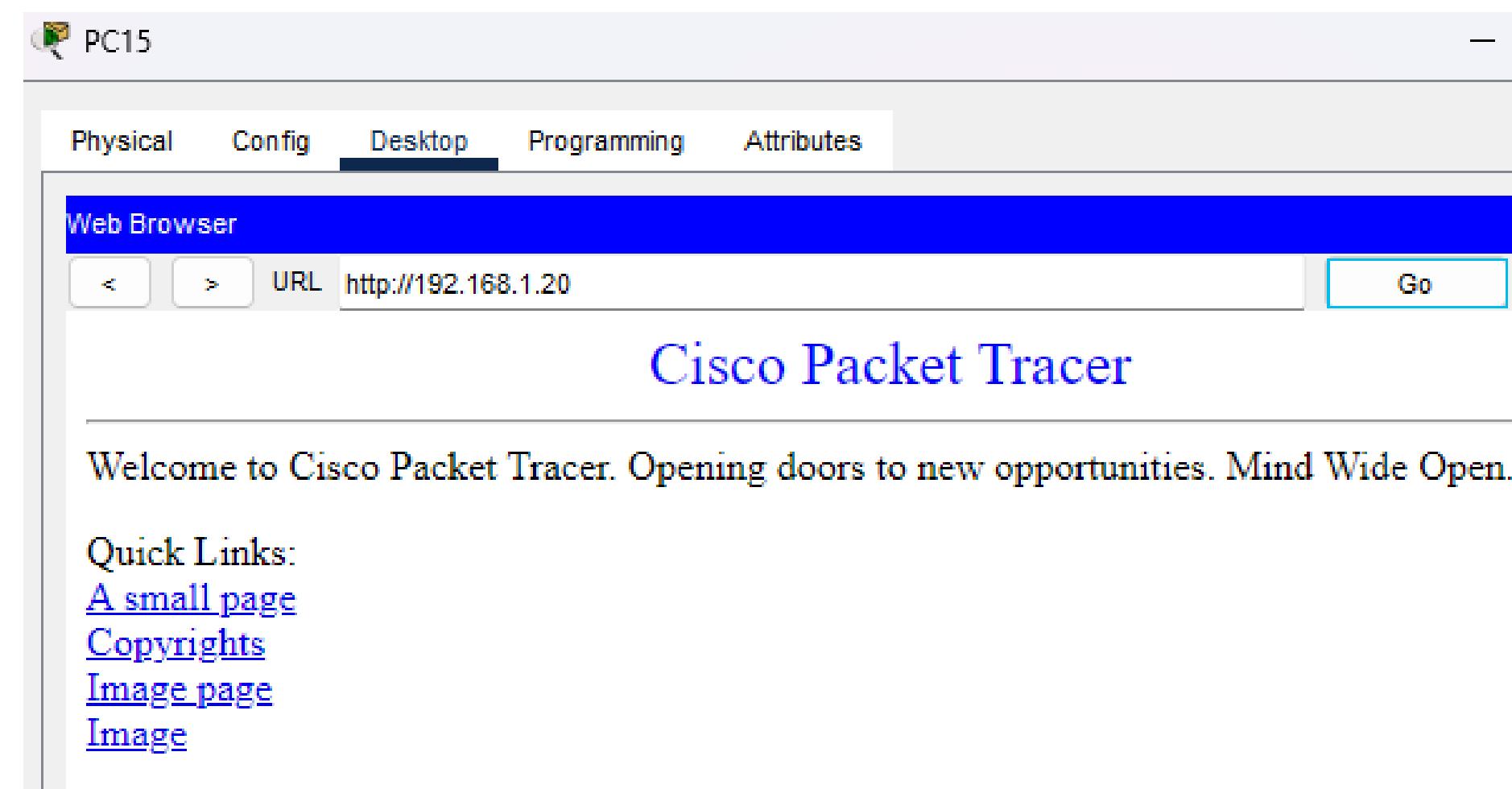
il terzo è stato posizionato a difesa dell'ufficio amministrativo, per tutelare eventuali informazioni sensibili.



Web Server in DMZ

Per rispondere alle esigenze di pubblicazione e accesso esterno ai servizi aziendali, all'interno della DMZ abbiamo predisposto un Web Server con indirizzo IP statico. Su questo server sono stati attivati i servizi HTTP e HTTPS, così da consentire l'accesso al sito o ai servizi web aziendali in modo controllato.

Nella seguente immagine possiamo notare l'interfaccia del Web server una volta reso operativo



```
Verbi_HHTP.py x
home > kali > Desktop > wetransfer_porte-py_2025-07-24_0744 > Verbi_HHTP.py > ...
1
2 #Presento il programma all'utente
3 print("Ciao! Tramite questo programma potrai analizzare quali opzioni sono attive su un determinato server HTTP!")
4 print("Per procedere mi servirà l'indirizzo IPv4 del server da analizzare.")
5
6 #importo libreria requests per le richieste http
7 import requests
8
9 #importo libreria ipaddress per il controllo dell'input dell'IP
10 import ipaddress
11
12 #importo libreria ping per testare connessione con il server
13
14
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
/bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/Verbi_HHTP.py
[kali㉿kali] ~
$ /bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/Verbi_HHTP.py
Ciao! Tramite questo programma potrai analizzare quali opzioni sono attive su un determinato server HTTP!
Per procedere mi servirà l'indirizzo IPv4 del server da analizzare.
Ti va di procedere?(Rispondere solamente si o no) si
Grandioso! Inserisci qui di seguito l'ipv4 del server da analizzare: 192.168.1.20
Il server 192.168.1.20 ha risposto al ping!

Se si vuole, inserire di seguito il path da analizzare (es. /phpMyAdmin) altrimenti lasciare vuoto: /phpMyAdmin
GET option DISPONIBILE per http://192.168.1.20/phpMyAdmin
POST option DISPONIBILE per http://192.168.1.20/phpMyAdmin
PUT option DISPONIBILE per http://192.168.1.20/phpMyAdmin
DELETE option DISPONIBILE per http://192.168.1.20/phpMyAdmin

[kali㉿kali] ~
$ /bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/Verbi_HHTP.py
Ciao! Tramite questo programma potrai analizzare quali opzioni sono attive su un determinato server HTTP!
Per procedere mi servirà l'indirizzo IPv4 del server da analizzare.
Ti va di procedere?(Rispondere solamente si o no) si
Grandioso! Inserisci qui di seguito l'ipv4 del server da analizzare: 192.168.1.20
Il server 192.168.1.20 ha risposto al ping!

Se si vuole, inserire di seguito il path da analizzare (es. /phpMyAdmin) altrimenti lasciare vuoto: /dvwa/login.php
GET option DISPONIBILE per http://192.168.1.20/dvwa/login.php
POST option DISPONIBILE per http://192.168.1.20/dvwa/login.php
PUT option DISPONIBILE per http://192.168.1.20/dvwa/login.php
DELETE option DISPONIBILE per http://192.168.1.20/dvwa/login.php

[kali㉿kali] ~
```

Per verificare che il server rispondesse correttamente alle richieste, abbiamo realizzato un semplice script in Python, che simula il comportamento di un client HTTP. L'utente inserisce l'indirizzo IP del server e un eventuale path, e il programma:

verifica la raggiungibilità del server con un ping, esegue test per i principali metodi HTTP (GET, POST, PUT, DELETE), e infine stampa un report che indica quali operazioni sono effettivamente supportate dal server.

Questo test ci ha permesso di simulare il comportamento reale del Web Server e verificare il corretto funzionamento delle impostazioni previste per l'ambiente operativo dell'azienda.

server NAS

All'interno dell'infrastruttura abbiamo previsto anche un **server NAS**, che potrà essere utilizzato sia per l'archiviazione centralizzata dei dati aziendali, sia per la gestione dei backup. La sua collocazione è stata pensata per il seminterrato, all'interno della sala server, in un'area separata dalla rete pubblica e accessibile solo dalle VLAN autorizzate.

Il NAS sarà configurato per offrire servizi via FTP, SSH e SMB, così da supportare i vari sistemi operativi e garantire un accesso sicuro e tracciabile.

ServerNAS

Physical Config Services Desktop Programm

IP Configuration

IP Configuration

DHCP Static

IPv4 Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

ServerNAS

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

FTP

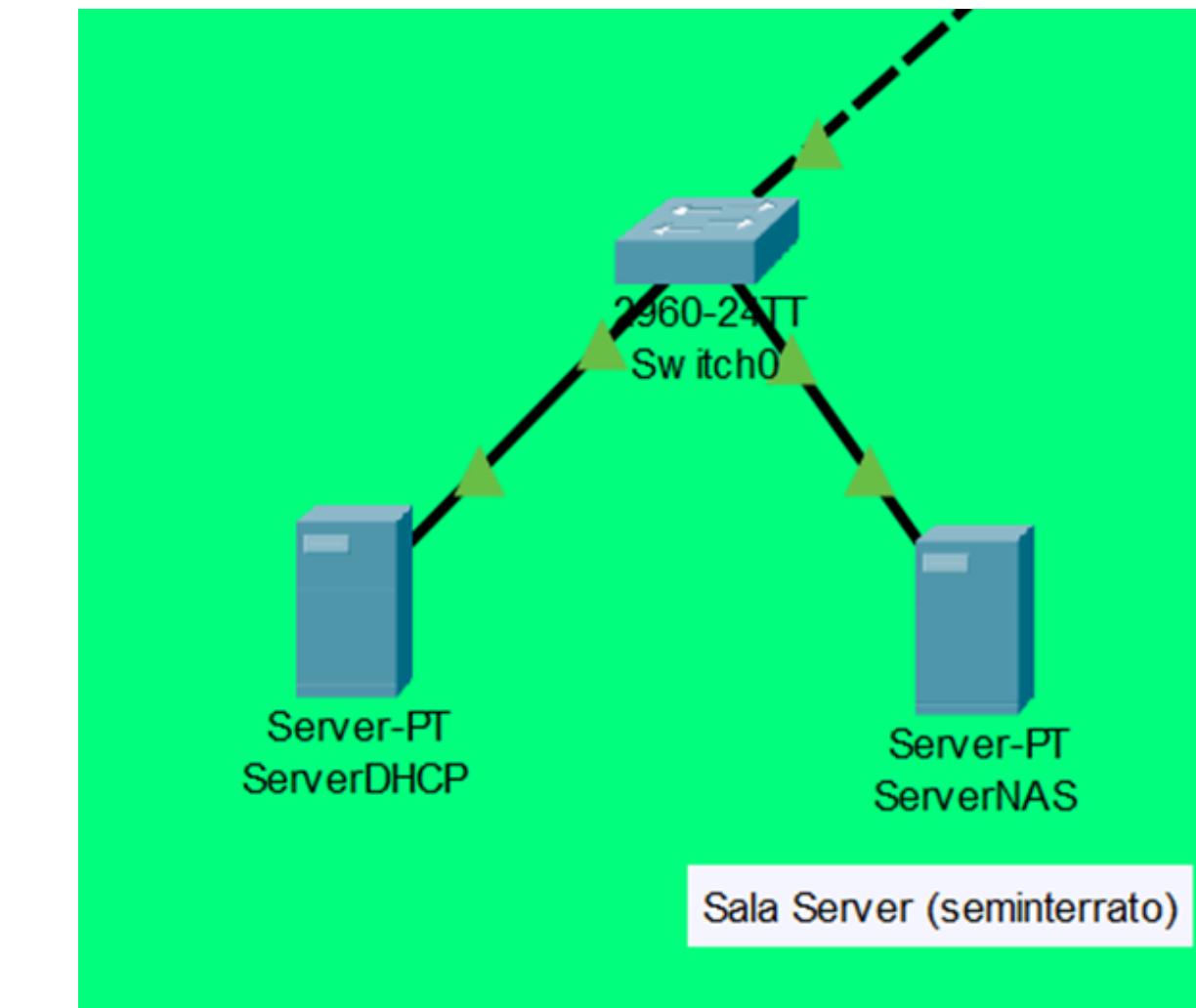
Service: On

User Setup

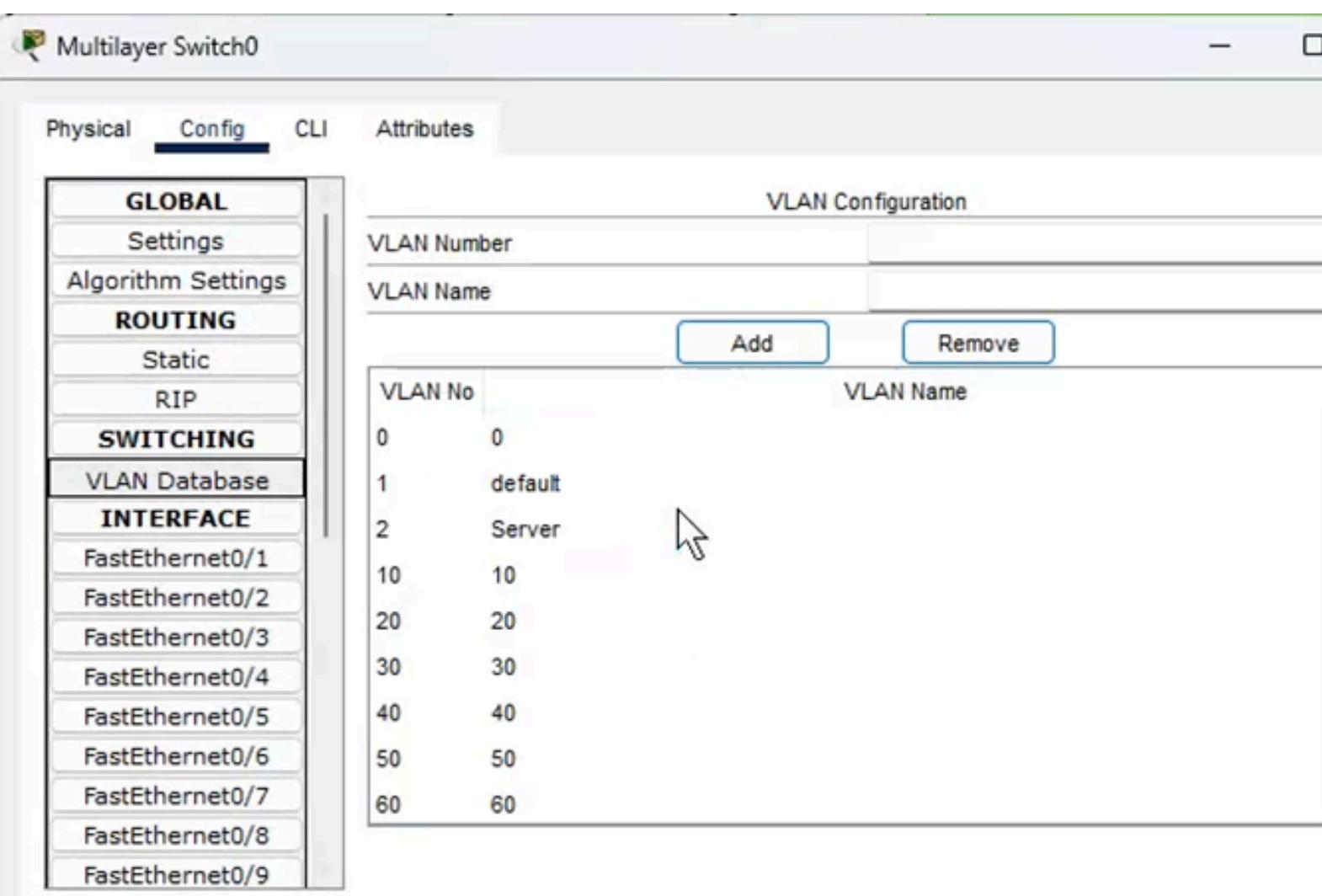
Username	Password	Perms
amministratori	password1	RWDNL
cisco	cisco	RWDNL
dipendenti	password2	RW
tecnicci	password3	RNL

Collegamenti tra gli apparati di rete

Nella sala server abbiamo predisposto uno **switch** dedicato, che gestisce le connessioni tra i server locali e lo switch Layer 3 centrale. Le porte collegate ai server sono state configurate in modalità **Access**, mentre la porta che collega lo switch della sala server a quello principale è impostata in modalità **Trunk**, così da consentire il passaggio del traffico proveniente da più **VLAN**.



Collegamenti tra gli apparati di rete



Anche lo switch Layer 3 è stato configurato nel dettaglio: abbiamo creato tutte le VLAN previste dal progetto, impostato gli indirizzi IP per ogni interfaccia e infine attivato il routing IP, così da permettere la comunicazione tra i vari segmenti di rete.

Firewall e regole di accesso

Per garantire la sicurezza della rete, è stato installato un firewall perimetrale, dotato di tre interfacce:

- una dedicata alla connessione **WAN** (rete esterna),
- una per la **LAN** interna,
- una per la gestione, che abbiamo chiamato **META**.

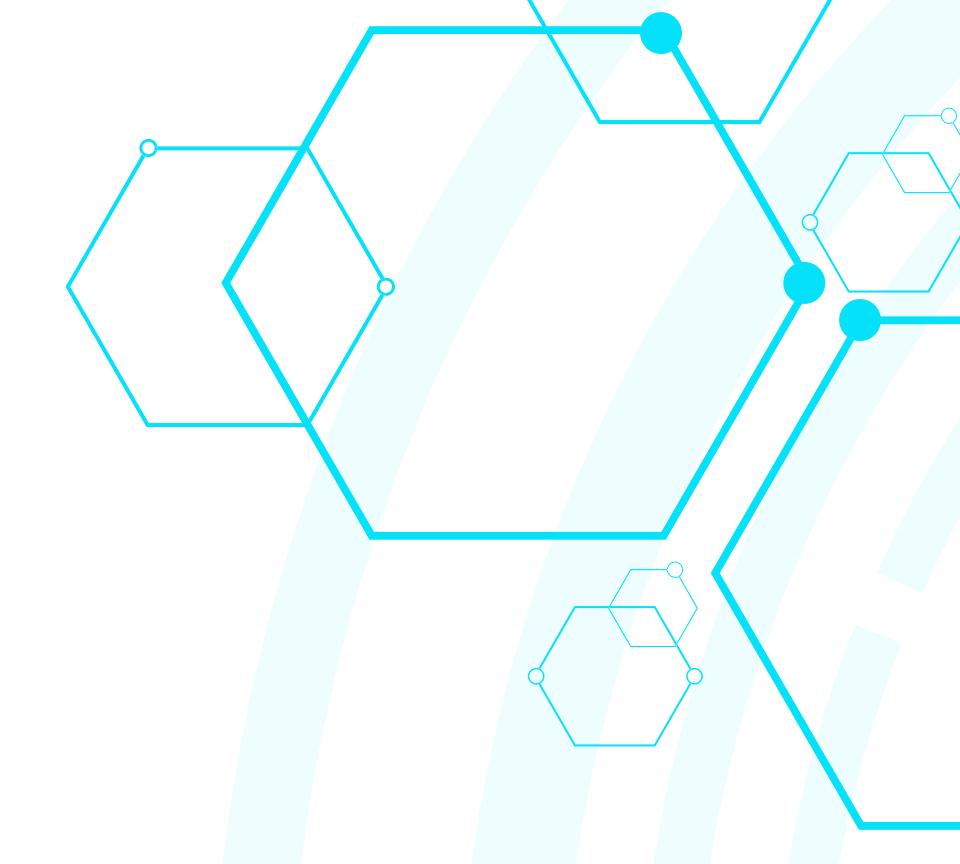
Interfaces / Interface Assignments	
Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:54:85:90)
Meta	em0 (08:00:27:e8:f8:e3)



PAIMEI
EXPLOIT

Creazione e impostazione regole su WAN e LAN e Meta

Sulla porta **WAN**, abbiamo applicato una politica di blocco totale in ingresso, eccezion fatta per una regola specifica che consente il traffico verso il Web Server tramite le porte 80 e 443. Questo approccio permette di minimizzare la superficie esposta a possibili attacchi dall'esterno.



The screenshot shows the Pfsense Firewall Rules configuration interface. The title bar includes the Pfsense logo, navigation links (System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help), and a warning message about the default admin password. The main area displays the 'Firewall / Rules / WAN' section. A tab bar at the top allows switching between Floating, WAN, LAN, and META rules. The 'WAN' tab is selected, showing a list of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
X 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	WAN subnets	*	192.168.1.20	80 - 443	*	none	Permesso di accesso alla DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	WAN address	*	*	none	Blocca traffico sospetto in ingresso dalla rete internet	

At the bottom are buttons for Add, Delete, Toggle, Copy, Save, and Separator.



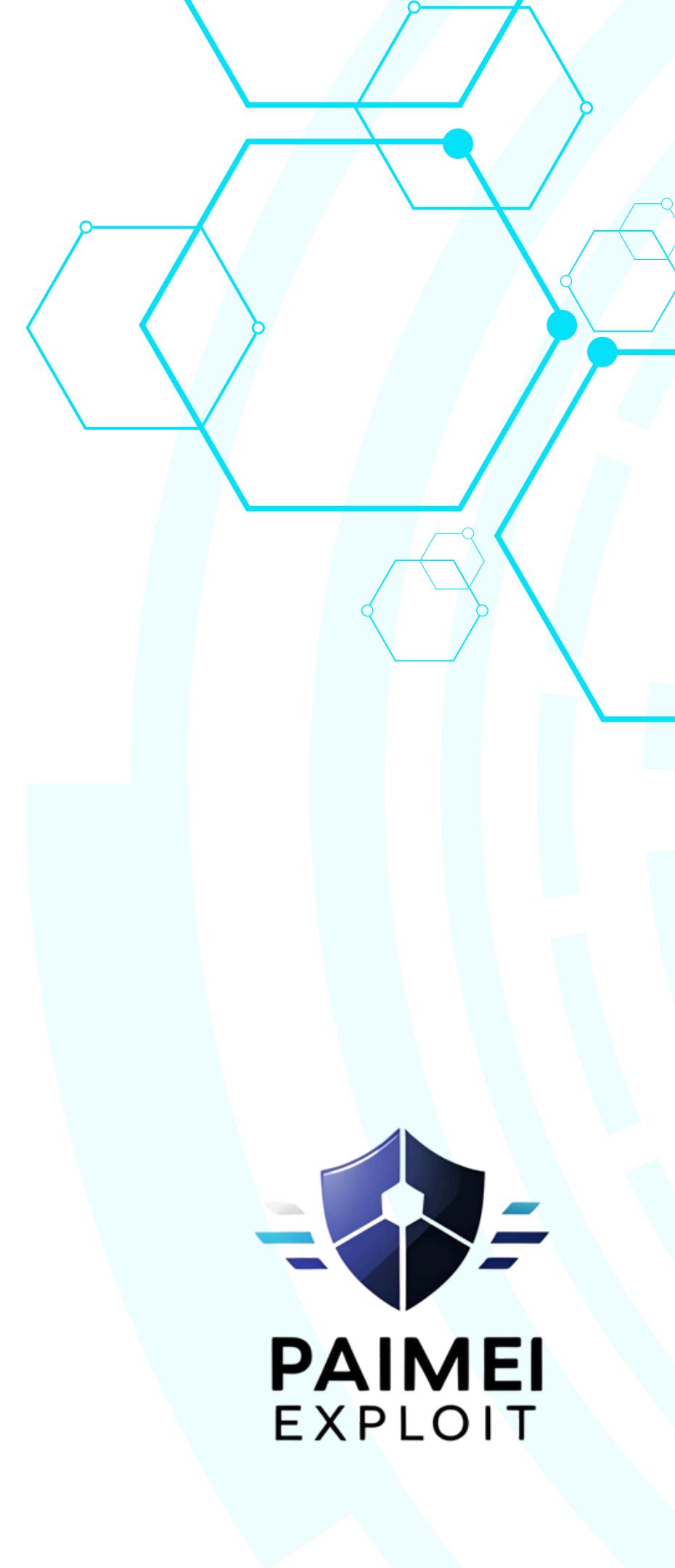
Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/1.62 MiB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	LAN subnets	*	8.8.8.8	53 (DNS)	*	none	*	Permesso DNS solo su Server specifici	
<input checked="" type="checkbox"/>	✗ 0/734 B	IPv4 TCP/UDP	LAN subnets	*	*	53 (DNS)	*	none	*	Blocco delle altre richieste DNS	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 UDP	LAN subnets	*	192.168.2.2	67 - 68	*	none	*	Raggiungimento Server DHCP da parte dei client	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.2.3	21 - 22	*	none	*	Accesso sicuro alla Shell del NAS + trasferimento dei file	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.2.3	445 (MS DS)	*	none	*	Permesso di accesso file da Windows/macOS/Linux	
<input checked="" type="checkbox"/>	✗ 0/0 B	IPv4 UDP	LAN subnets	*	192.168.2.3	*	*	none	*	Blocca tutte le altre porte	
<input checked="" type="checkbox"/>	✓ 0/5.10 MiB	IPv4 *	LAN subnets	*	*	*	*	none	*	Permette comunicazione tra LAN e rete internet	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	*	Default allow LAN IPv6 to any rule	

Per la **rete interna (LAN)**, sono state definite alcune regole base:

- abbiamo autorizzato il traffico **DNS** soltanto verso l'indirizzo 8.8.8.8 (Google DNS),
- consentito il traffico **DHCP** per permettere l'assegnazione dinamica degli indirizzi IP,
- permesso l'accesso al **NAS** tramite le porte 22 (SSH) e 21 (FTP),
- abilitato la condivisione file tramite la porta 445, necessaria per l'accesso **SMB/CIFS** dai vari sistemi operativi.
- a conclusione delle regole **LAN**, è stata inserita una regola di blocco generale, che intercetta ogni altra comunicazione non esplicitamente autorizzata.



PAIMEI
EXPLOIT



Firewall / Rules / META

Floating WAN LAN META

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
<input checked="" type="checkbox"/>	0/23 KiB	IPv4 *	META subnets	*	*	*	*	none

Infine, sulla rete **META**, è stata configurata una regola più permissiva, che consente la comunicazione verso qualunque destinazione. Questo ci permette di utilizzare questa rete per eventuali interventi di amministrazione e gestione remota dei dispositivi.

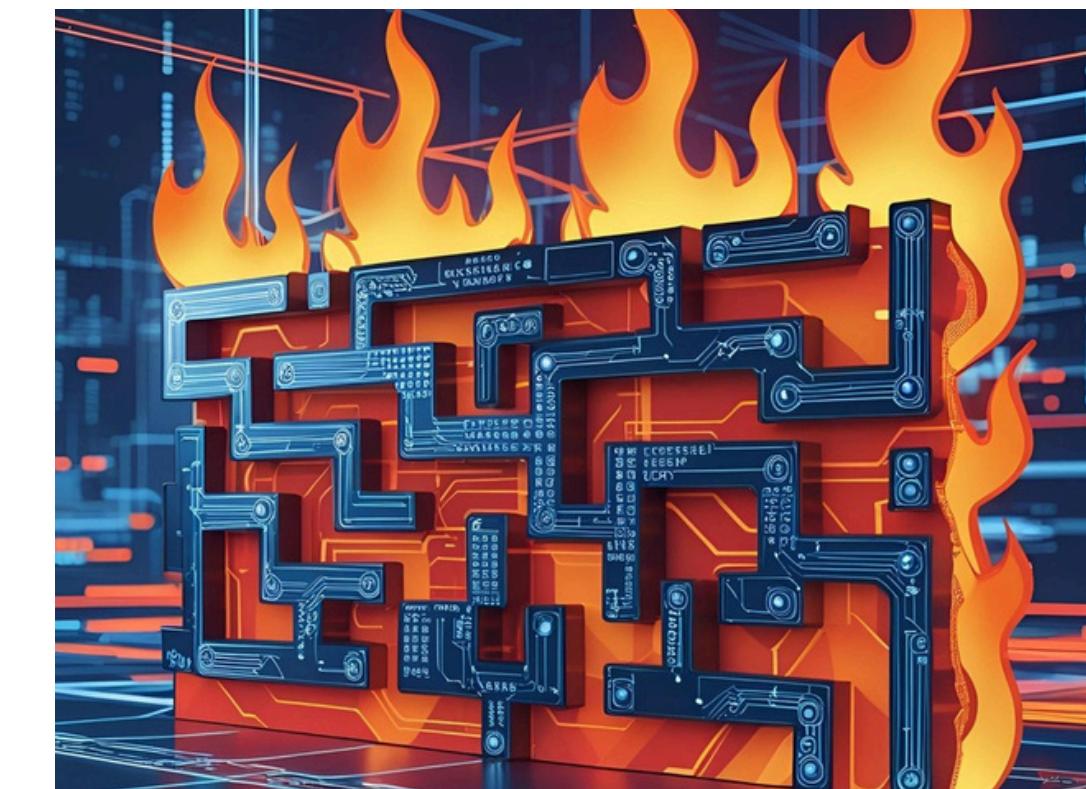
Firewall aggiuntivi per segmentazione e protezione interna

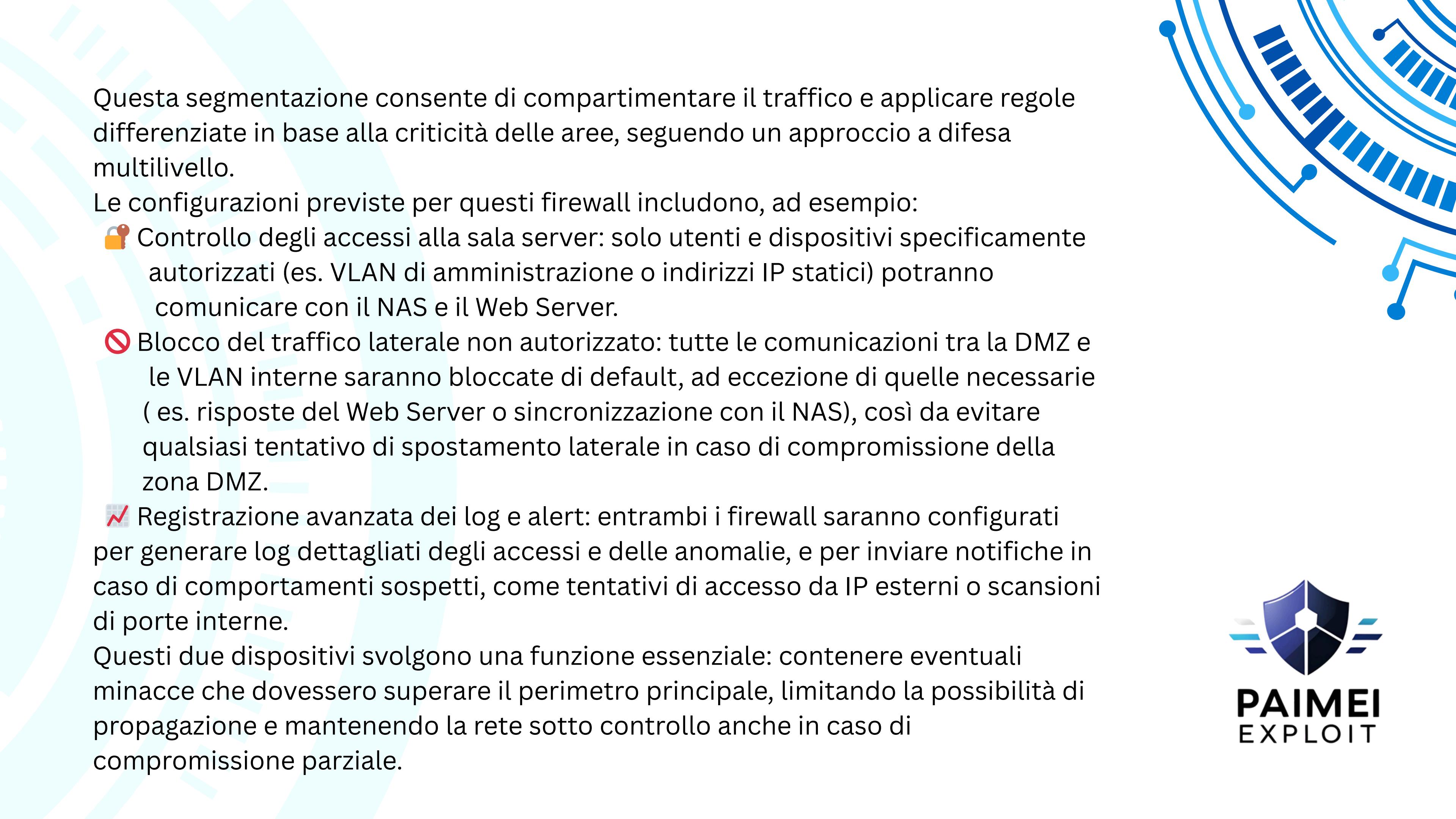
Per rafforzare ulteriormente la sicurezza dell'infrastruttura, sono stati previsti due firewall aggiuntivi, entrambi posizionati al piano terra, in prossimità dei nodi più critici della rete:

Il primo è stato collocato a protezione della sala server, per isolare i sistemi centrali dal resto della rete e garantire un controllo rigoroso sugli accessi.

Il secondo firewall è stato inserito tra la DMZ e la rete interna, così da filtrare qualsiasi traffico che potrebbe attraversare questa zona esposta e raggiungere sistemi sensibili interni.

Questa segmentazione consente di compartimentare il traffico e applicare regole differenziate in base alla criticità delle aree, seguendo un approccio a difesa multilivello.





Questa segmentazione consente di compartimentare il traffico e applicare regole differenziate in base alla criticità delle aree, seguendo un approccio a difesa multilivello.

Le configurazioni previste per questi firewall includono, ad esempio:

- 🔒 Controllo degli accessi alla sala server: solo utenti e dispositivi specificamente autorizzati (es. VLAN di amministrazione o indirizzi IP statici) potranno comunicare con il NAS e il Web Server.
- 🚫 Blocco del traffico laterale non autorizzato: tutte le comunicazioni tra la DMZ e le VLAN interne saranno bloccate di default, ad eccezione di quelle necessarie (es. risposte del Web Server o sincronizzazione con il NAS), così da evitare qualsiasi tentativo di spostamento laterale in caso di compromissione della zona DMZ.
- 📈 Registrazione avanzata dei log e alert: entrambi i firewall saranno configurati per generare log dettagliati degli accessi e delle anomalie, e per inviare notifiche in caso di comportamenti sospetti, come tentativi di accesso da IP esterni o scansioni di porte interne.

Questi due dispositivi svolgono una funzione essenziale: contenere eventuali minacce che dovessero superare il perimetro principale, limitando la possibilità di propagazione e mantenendo la rete sotto controllo anche in caso di compromissione parziale.



PAIMEI
EXPLOIT

Monitoraggio e Prevenzione

Implementazione di Snort

Per potenziare ulteriormente il livello di sicurezza dell'infrastruttura, abbiamo scelto di adottare Snort come sistema IDS/IPS (Intrusion Detection e Prevention System). Questo strumento, ampiamente utilizzato in contesti professionali, ci permette di monitorare il traffico di rete in tempo reale, identificare comportamenti anomali e, se necessario, bloccare le comunicazioni sospette.

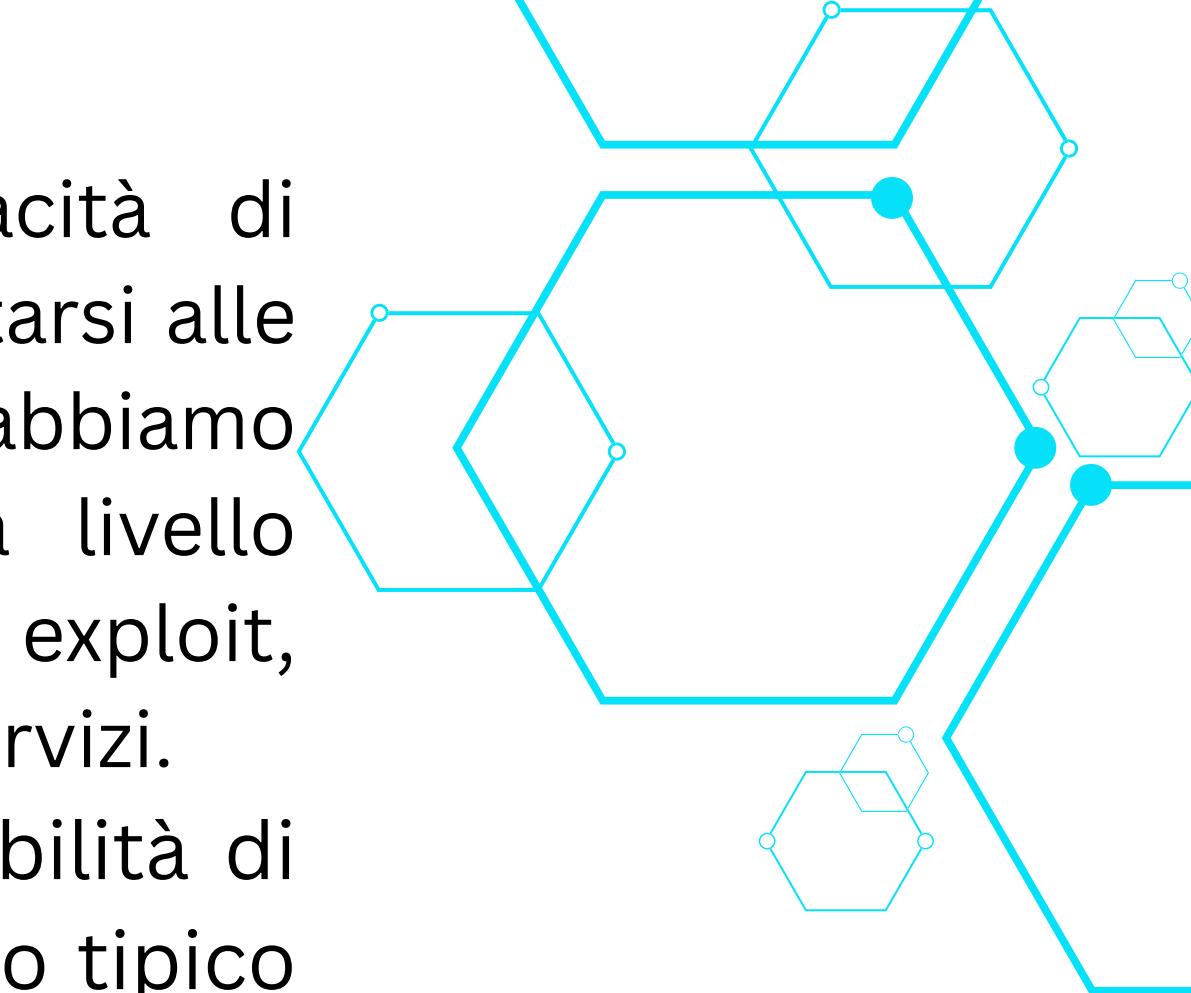


PAIMEI
EXPLOIT

La scelta di **Snort** si basa sulla sua flessibilità e capacità di personalizzazione, caratteristiche che lo rendono ideale per adattarsi alle esigenze specifiche dell'Azienda Theta. Dopo l'installazione, abbiamo scaricato un insieme di regole open source riconosciute a livello internazionale, in grado di proteggere da un'ampia varietà di exploit, scansioni di rete, attacchi DoS e tentativi di compromissione dei servizi.

Tuttavia, uno degli aspetti più interessanti di Snort è la possibilità di scrivere regole su misura, basate sull'analisi del comportamento tipico degli utenti e dei flussi di rete interni all'azienda. Questo approccio ci consente di creare un sistema di difesa dinamico, capace di adattarsi nel tempo.

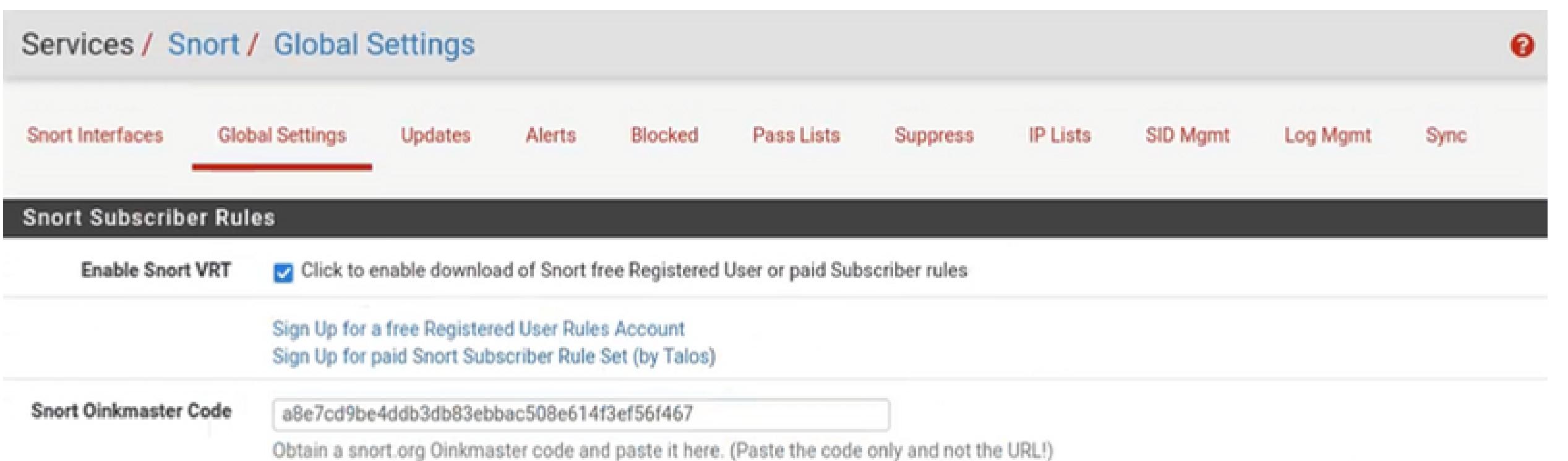
Tra le regole personalizzabili che potranno essere adottate all'interno della rete Theta, proponiamo le seguenti:



1. Blocco delle connessioni SSH fuori dall'orario lavorativo

Per ridurre i rischi legati ad accessi non autorizzati in orari non presidiati, è possibile configurare una regola che blocchi o allerti su connessioni SSH provenienti da IP interni o esterni al di fuori della fascia oraria 8:00–19:00, dal lunedì al venerdì.

Obiettivo: prevenire accessi sospetti in orari anomali (es. attività notturne automatizzate o compromissioni silenziose).



The screenshot shows the Snort Global Settings interface. The top navigation bar includes 'Services / Snort / Global Settings' and a help icon. Below the bar are tabs: 'Snort Interfaces' (selected), 'Global Settings' (highlighted with a red underline), 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. A dark grey header bar below the tabs contains the text 'Snort Subscriber Rules'. Under this header, there is a checkbox labeled 'Enable Snort VRT' with the sub-instruction 'Click to enable download of Snort free Registered User or paid Subscriber rules'. Below this are two blue links: 'Sign Up for a free Registered User Rules Account' and 'Sign Up for paid Snort Subscriber Rule Set (by Talos)'. At the bottom of the section is a text input field labeled 'Snort Oinkmaster Code' containing the value 'a8e7cd9be4ddb3db83ebbac508e614f3ef56f467', with the instruction 'Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)'



2. Rilevamento di upload non autorizzati tramite HTTP/FTP

Una seconda regola utile potrebbe rilevare grandi quantità di dati in uscita verso server esterni attraverso protocolli come HTTP POST o FTP PUT. Questo tipo di comportamento può indicare un possibile data exfiltration o l'utilizzo improprio della rete aziendale.

Obiettivo: proteggere dati aziendali da trasferimenti non autorizzati verso l'esterno.

3. Avviso su accessi ripetuti a siti web non aziendali

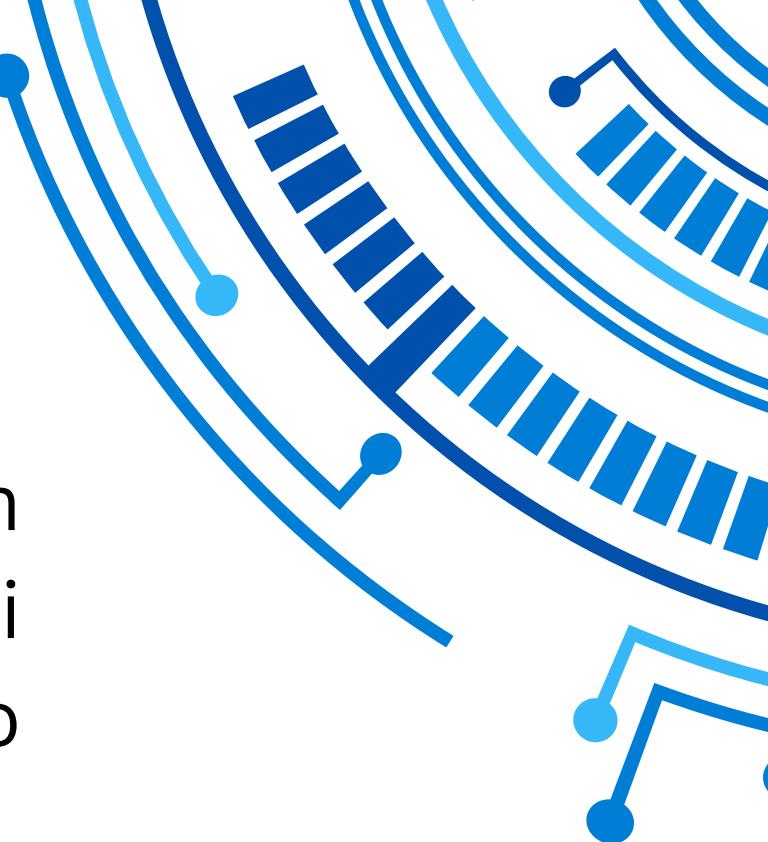
Attraverso il controllo delle richieste DNS e HTTP, è possibile generare avvisi quando un host interno tenta ripetutamente di accedere a determinati domini non lavorativi (es. piattaforme di streaming, download peer-to-peer, social network in orario di lavoro).

Obiettivo: migliorare il controllo sulla produttività e sull'uso corretto della rete.



PAIMEI
EXPLOIT

Analisi di Sicurezza – Scansione delle Porte



Per rafforzare l'analisi della sicurezza all'interno della rete, abbiamo sviluppato un programma in Python dedicato alla scansione delle porte TCP sui dispositivi di rete. Questo strumento consente di verificare rapidamente quali servizi risultano esposti all'esterno e valutare eventuali rischi di sicurezza associati.

Il funzionamento è strutturato per essere semplice ma efficace:

L'utente inserisce l'indirizzo IP del dispositivo da analizzare.

Il programma verifica la raggiungibilità tramite ping.

In caso di risposta positiva, chiede all'utente di specificare un intervallo di porte. Viene quindi avviata la scansione, e per ogni porta rilevata come "aperta" viene fornito un commento sulla sicurezza, con eventuali suggerimenti su come mitigare vulnerabilità comuni.

Al termine viene chiesto anche se visualizzare o meno le porte risultate chiuse.



PAIMEI
EXPLOIT

Questa scansione può essere utilizzata in fase di:
collaudo pre-produzione
verifica post-installazione,
oppure come parte di un processo ciclico di security hardening.



```
1 import os
2 import socket
3 import ipaddress
4
5 print("Questo programma scansionerà le porte aperte di un determinato dispositivo")
6 while True:
7     volontà = input("Mi servirà un l'indirizzo IPv4 che vuoi scansionare. Vuoi procedere? (si o no)")
8     if volontà.lower() == "si" or volontà.lower() == "sì":
9         target = input("Inserisci un indirizzo IP: ")
10        #response = os.system("ping -c 4 " + target)
11        try:
12            ipaddress.IPv4Address(target)
13            response = os.system("ping -c 1 " + target)
14            if response == 0:
15                print("Connesso")
16            else:
17                print("Non raggiungibile")
18                continue
19        break
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
/bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/Porte.py
[(kali㉿kali)-~]
$ ./bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/Porte.py
questo programma scansionerà le porte aperte di un determinato dispositivo
Mi servirà un l'indirizzo IPv4 che vuoi scansionare. Vuoi procedere? (si o no)si
Inserisci un indirizzo IP: 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=0.324 ms

--- 192.168.1.20 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.324/0.324/0.324/0.000 ms
Connesso
Inserisci un range di porte (es.1-1024): 1-1024
Scan di 192.168.1.20 dalla porta 1 alla porta 1024
*** Port 21 - OPEN ***
Porta 21 non sicura, usare le porte 989 e 990 per connessioni sicure
*** Port 22 - OPEN ***
*** Port 23 - OPEN ***
Attenzione porta 23 vulnerabile, preferire ssh porta 22
*** Port 25 - OPEN ***
Porta 25 soggetta a spam e attacchi, si consiglia di utilizzare la 465
```

è possibile osservare un esempio del report generato,
che evidenzia le porte aperte e fornisce
raccomandazioni pratiche per ciascuna di esse.

e anche le porte chiuse? Y/N Y
4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747]



Monitoraggio delle Connessioni – Socket di Rete

Per approfondire la comprensione delle comunicazioni all'interno dell'infrastruttura, abbiamo realizzato un ulteriore script in Python in grado di catturare e gestire un socket di rete lato server.

Lo scopo di questo strumento è simulare il comportamento di un host in ascolto su una porta specifica, utile sia per attività di test che per verificare la raggiungibilità di determinati servizi da altri nodi della rete.
o semplice:

All'avvio, il programma chiede all'utente su quale porta TCP il socket deve restare in ascolto.

Una volta impostata la porta, il programma avvia il listener e si pone in attesa indefinita di connessioni in entrata.

Quando una connessione viene stabilita, il programma ne conferma l'esito positivo sul terminale.



Questo tipo di test può essere molto utile per:
verificare la funzionalità delle regole firewall (es. se una porta è
effettivamente raggiungibile da un altro host),
testare strumenti di port scanning,
o semplicemente simulare la presenza di un servizio in ascolto all'interno
della rete.

Nell'immagine seguente (da inserire) viene mostrata l'esecuzione del programma, con la conferma della connessione ricevuta da un client remoto sulla porta specificata.

The screenshot shows a terminal window titled "File Actions Edit View Help". The window displays network interface information for a Kali Linux system, including interfaces loopback, eth0, and eth0:1. Below this, a netcat listener is running on port 22. A separate terminal window at the bottom shows a client connecting to the server on port 22.

```
40
41     print(f"● Server in ascolto su {HOST}:{port}...")
42
43     conn, addr = server.accept()
44     print(f"Connessione stabilita con {addr[0]}:{addr[1]}")
45
46     while True:
47         data = conn.recv(1024)
48         if not data:
49             break
50         print(f"Ricevuto: {data.decode().strip()}")
51         conn.sendall(b"Messaggio ricevuto\n")
52
53     conn.close()
54     print("Connessione chiusa.")
55     break
56
57 except Exception as e:
58     print(f"Errore durante la creazione del server: {e}")
59     continue
60
61 elif volontà.lower().strip() == "n":
62     print("D'accordo, alla prossima! Buon proseguimento!")
63     exit()
64
65 else:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
/bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/socket_rete.py
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-~]
$ /bin/python /home/kali/Desktop/wetransfer_porte-py_2025-07-24_0744/socket_rete.py
Ciao! Questo software resta in ascolto su una porta, in attesa di una connessione tcp
Se ti va puoi fornirmi la relativa porta su cui restare in ascolto
Ti va di proseguire? (y/n)
Fantastico! Procedi dunque a fornirmi la porta su cui mettermi in ascolto: 22
● Server in ascolto su 0.0.0.0:22...
Connessione stabilita con 10.0.2.15:44766
```



Vi ringraziamo per
l'attenzione!

- Enrico Favaro - Leader
- Paolo Costanzo
- Francesco Ferrera
- Maikol Nosenzo
- Stefano Zagaria
- Bryan Tchakountio
- Mirka Febbo



Contact Information

Per qualunque lamentela
rivolgersi al PROF Rampino