Monitoraggio di un Hosting Provider: problematiche, strumenti e fattore umano

Francesco Leoncino
Manuele Gioli
Hostingsolutions.it

June, 23-24 · Milan

Agenda

- Problematiche
- Obiettivo
- Esempi/fattore umano
- Monitoraggio infrastruttura

Problematiche

Problematiche

Un HSP offre normalmente una grande varietà di servizi come ad esempio:

- siti Web
- email
- big data
- backup
- VDI
- VPN

Di conseguenza anche il traffico di rete risulta molto vario.

Problematiche

Anche gli attacchi a cui è soggetto un HSP sono estremamente vari, per esempio:

- DDoS contro l’HSP
- DDoS contro un singolo cliente
- Slow DoS
- Scansioni
- Attacchi brute force
- Vulnerabilità applicative (es. Wordpress)
- Spam/Phishing

Problematiche

I **guasti** hardware e software, anche se fanno meno notizia degli attacchi cyber sono ahimé problematiche quotidiane visto il numero di apparecchi in uso e la complessità dell’infrastruttura.

Un ulteriore fattore critico siamo noi esseri umani, che per nostra natura commettiamo errori.

In quest’ultimo fattore rientrano i falsi positivi generati da segnalazione esterne non corrette.

Problematiche

La varietà di clienti e servizi fa sì che traffico considerato indesiderato da alcuni sia invece considerato valido da altri.

Spesso la tipologia di traffico generata da un cliente/servizio ci è ignota a priori, spesso proviene da CDN.

Classificare il traffico quindi non sempre risponde a criteri oggettivi.

Problematiche

I flussi da monitorare non sono solo relativi al traffico di rete e il monitoraggio non può limitarsi al perimetro.

È necessario monitorare i flussi in ingresso e in **uscita** anche a livello **applicativo** operando per singolo servizio differenziando per tipologia e per cliente.

Per esempio lo stesso carico di traffico email può essere sospetto o normale a seconda del servizio che lo genera.

Obiettivo

Obiettivo

Mantenere attivi e fruibili i servizi.

Identificare, mitigare e/o neutralizzare:

- attacchi
- siti problematici
- caselle email compromesse
- apparati guasti o in procinto di guastarsi
- eccessivo uso di risorse
- nuovi problemi

Obiettivo

Mantenere attivi e fruibili i servizi.

L’atteggiamento di HSP è differente da quello di un’azienda “standard”, ovvero non possiamo stabilire policy correlate al business aziendale e alle mansioni degli uffici.

Un HSP non deve comportarsi come censore, deve intervenire esclusivamente se ci sono rischi per la fruibilità dei servizi.

Inoltre non potendo conoscere cosa fanno i clienti siamo costretti a monitorare l’interno al pari dell’esterno

Obiettivo

Mantenere attivi e fruibili i servizi.

Servono strumenti su vari livelli, non ci sono strumenti pensati esplicitamente per gli HSP.

ntopng e **nScrub** operano sul perimetro, **ipt_geofence** ci aiuta sui servizi specifici in cui possiamo permetterci un blocco selettivo per nazione.

Nel tempo abbiamo sviluppato una serie di tool interni che rilevano anomalie e eseguono automaticamente azioni di correzione o ci segnalano anomalie.

Esempi/Fattore umano

Esempi/Fattore umano

Un cliente si lamenta per la ricezione di alcune email.

Cerchiamo nei log e vediamo che si tratta di email inviate da un dispositivo all’interno della sede del cliente, pertanto per noi è tutto regolare.

Il cliente dice che anche se fosse quelle email non le vuole ricevere.

Ci facciamo girare una email, dagli header si capisce che si tratta di una **stampante configurata male,** riusciamo dunque a dare **indicazioni al cliente per individuare la stampante** e riconfigurarla in modo corretto.

Esempi/Fattore umano

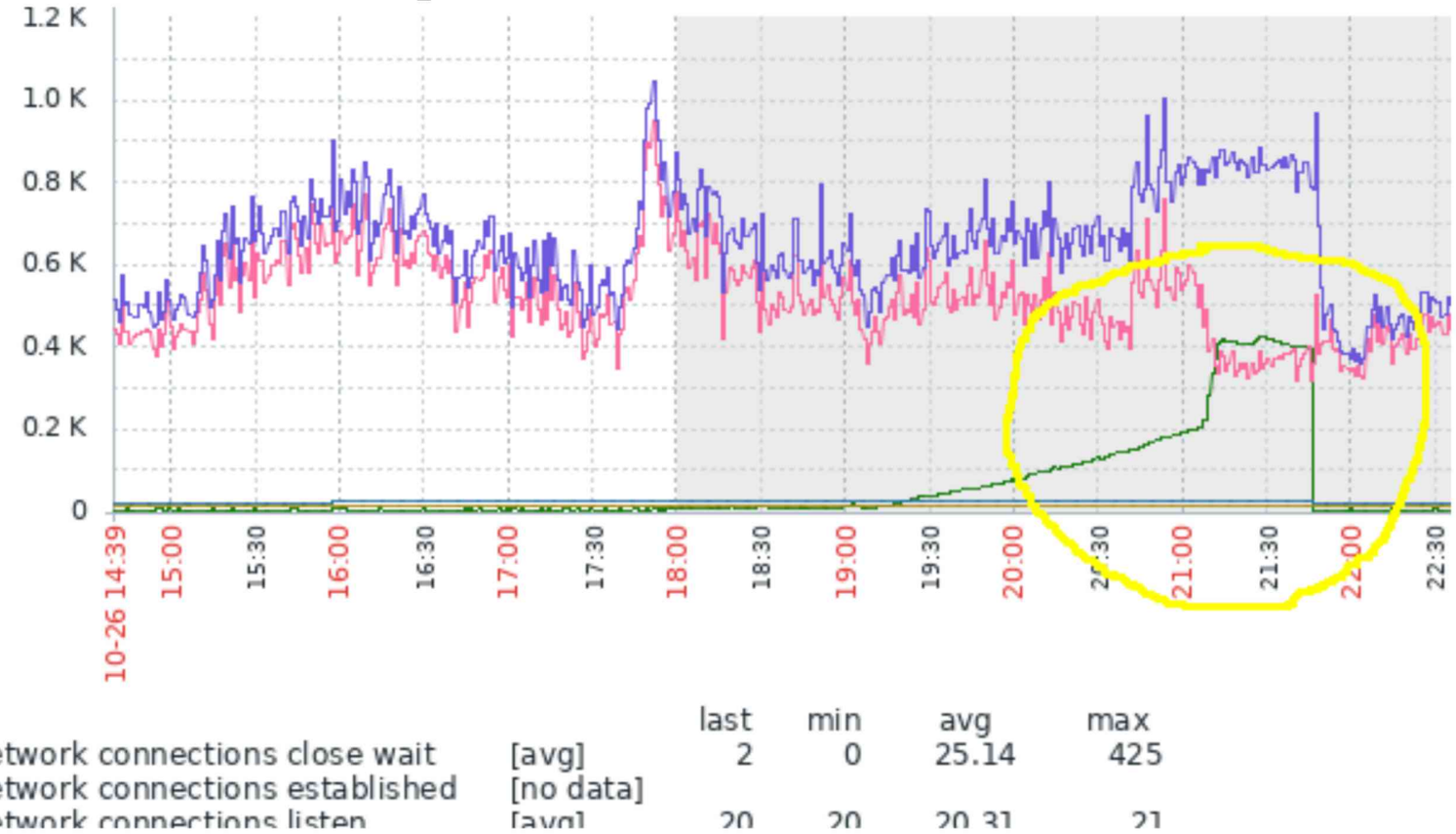
Google bombing (66.249.64.0/19)

I motori di ricerca possono essere veicoli di DoS, se “invitati” a scansionare quantità esorbitanti di pagine.

Un sito soggetto a google bombing può risultare irraggiungibile e se ospitato su un server condiviso creare problemi agli altri siti.

In questo caso si fa un blocco selettivo della classe IP di googlebot solo per il sito problematico per non danneggiare il ranking degli altri siti.

Esempi/Fattore umano



Anomalia nel software del cliente che in particolari condizioni lascia in CLOSE_WAIT le connessioni. Siamo intervenuti con uno script che le chiude forzatamente.

Esempi/Fattore umano

cattura89_2.pcap

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

http

No.	Time	Source	Destination	Protocol	Length	Info
5	1.509749	217.160.145.62	[redacted]	HTTP	1749	POST /wp-admin/admin-ajax.php HTTP/1.1
7	2.107813	[redacted]	217.160.145.62	HTTP	479	HTTP/1.1 400 Bad Request (text/html)
18	6.142511	217.160.145.62	[redacted]	HTTP	664	GET /wp-content/uploads/typehub/custom/putzkbzr/.sp3ctra_XO.php?Fox=d3wL7

```
Frame 5: 1749 bytes on wire (13992 bits), 1749 bytes captured (13992 bits)
Ethernet II, Src: Cisco_0f:ad:c2 (40:55:39:0f:ad:c2), Dst: Dell_1b:ad:82 (44:a8:42:1b:ad:82)
Internet Protocol Version 4, Src: 217.160.145.62, Dst: [redacted]
Transmission Control Protocol, Src Port: 49234, Dst Port: 80, Seq: 1, Ack: 1, Len: 1695
Hypertext Transfer Protocol
  POST /wp-admin/admin-ajax.php HTTP/1.1\r\n
  Host: [redacted]\r\n
  Connection: keep-alive\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  User-Agent: Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36\r\n
  Accept-Language: en-US,en;q=0.9,fr;q=0.8\r\n
  Cache-Control: max-age=0\r\n
  referer: www.google.com\r\n
  Cookie: GC=; ON=exec; T=; g=echo Sp3ctra; j=system; xL=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Content-Length: 1029\r\n
  Content-Type: multipart/form-data; boundary=e9cf6380d2a999be7d0e529910e48e83\r\n
  \r\n
  [Full request URI: http://www.paolomelasi.com/wp-admin/admin-ajax.php]
  [HTTP request 1/1]
  [Response in frame: 7]
  File Data: 1029 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "e9cf6380d2a999be7d0e529910e48e83"
```

```
0000  44 a8 42 1b ad 82 40 55  39 0f ad c2 08 00 45 00   D·B···@U 9·····E·
0010  06 c7 ba 09 40 00 76 06  37 82 d9 a0 91 3e 59 1f   ····@·v· 7····>Y·
0020  48 a7 c0 52 00 50 0e 44  87 3c db 95 72 4f 50 18   H··R·P·D ·<··rOP·
0030  04 02 13 5f 00 00 50 4f  53 54 20 2f 77 70 2d 61   ···_··PO ST /wp-a
0040  64 6d 69 6e 2f 61 64 6d  69 6e 2d 61 6a 61 78 2e   dmin/adm in-ajax.
0050  70 68 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   php HTTP /1.1··Ho
0060  73 74 3a 20 77 77 77 2e  70 61 6f 6c 6f 6d 65 6c   st: www. [redacted]
0070  61 73 69 2e 63 6f 6d 0d  0a 43 6f 6e 6e 65 63 74   [redacted] ·Connect
0080  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
0090  0a 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   ·Accept- Encoding
00a0  3a 20 67 7a 69 70 2c 20  64 65 66 6c 61 74 65 0d   : gzip,  deflate·
00b0  0a 41 63 63 65 70 74 3a  20 74 65 78 74 2f 68 74   ·Accept:  text/ht
00c0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
00d0  68 74 6d 6c 2b 78 6d 6c  2c 61 70 70 6c 69 63 61   html+xml ,applica
00e0  74 69 6f 6e 2f 78 6d 6c  3b 71 3d 30 2e 39 2c 69   tion/xml ;q=0.9,i
00f0  6d 61 67 65 2f 77 65 62  70 2c 69 6d 61 67 65 2f   mage/web p,image/
0100  61 70 6e 67 2c 2a 2f 2a  3b 71 3d 30 2e 38 0d 0a   apng,*/* ;q=0.8··
0110  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 6c   User-Age nt: Mozl
0120  69 6c 61 2f 35 2e 30 20  28 4c 69 6e 75 78 3b 20   ila/5.0  (Linux;
0130  41 6e 64 72 6f 69 64 20  37 2e 30 3b 20 53 4d 2d   Android  7.0; SM-
```

Esempi/Fattore umano

Dump di un attacco contro il plugin Tatsu di Wordpress.

Anche se non c’è Wordpress sul sito viene comunque effettuato l’upload di un file malevolo che viene neutralizzato da un servizio EPP.

Abbiamo realizzato script che rilevano questo attacco e tramite **nScrub** li blocchiamo all’origine.

Esempi/Fattore umano

DDoS verso un sito

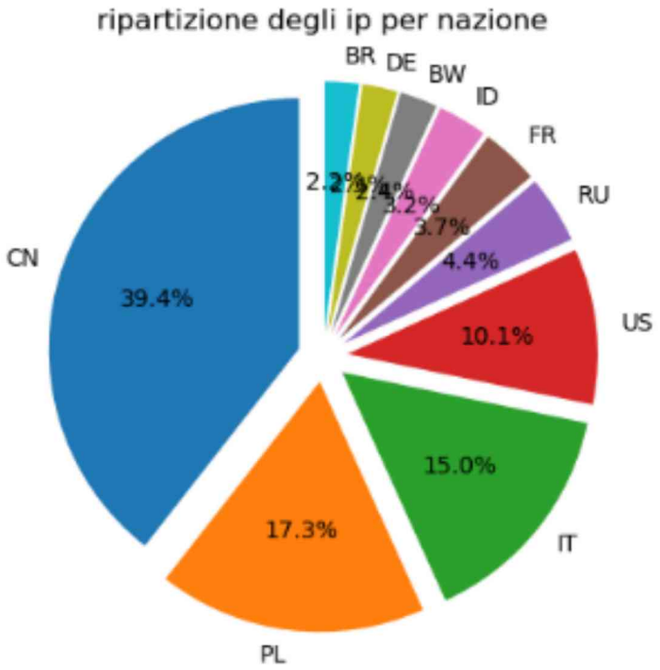
Il sito di un conservatorio italiano è da anni sotto attacco, saltuariamente riceve decine di milioni di richieste in poche ore.

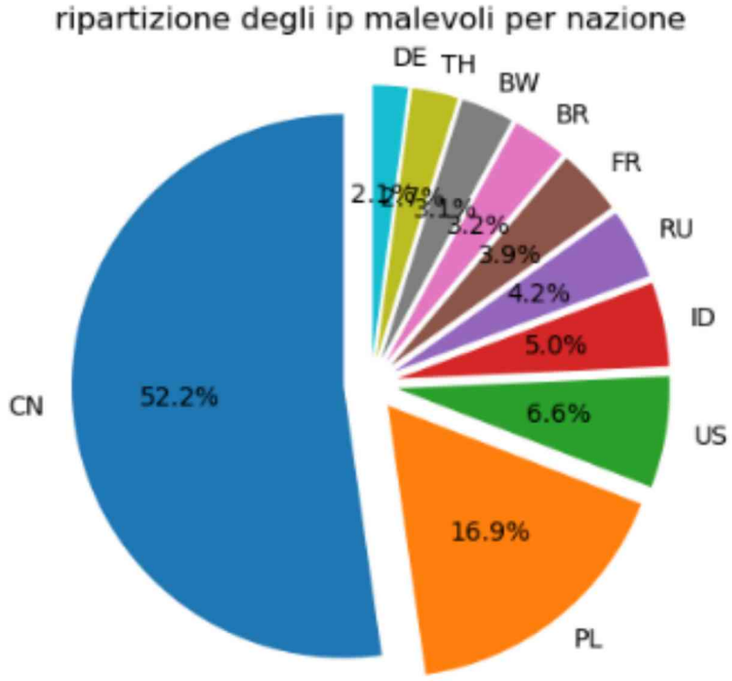
Non possiamo applicare **geofence** perché si tratta di un sito di respiro internazionale.

Abbiamo impostato dei controlli che identificano gli IP delle richieste e li bloccano, in breve tempo abbiamo collezionato una blacklist di più di 150.000 IP, riportando il sito alla piena utilizzabilità.

Esempi/Fattore umano

DDoS verso un sito



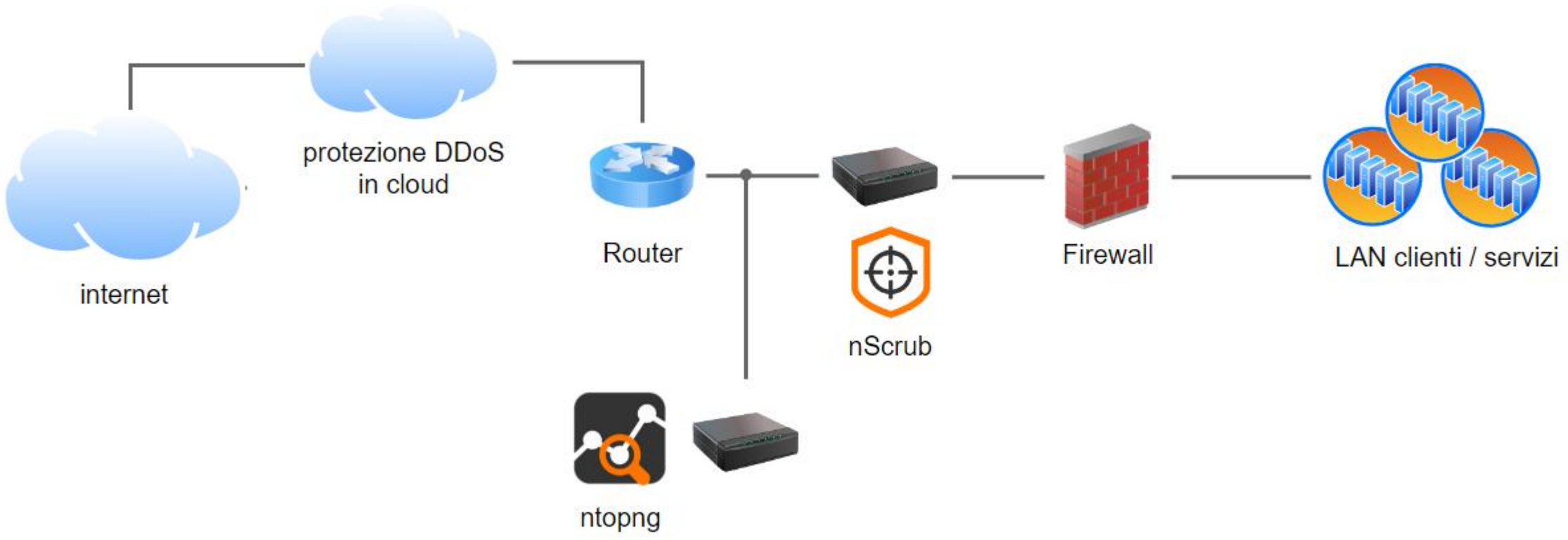


100% ~= 92.000.000 righe di log

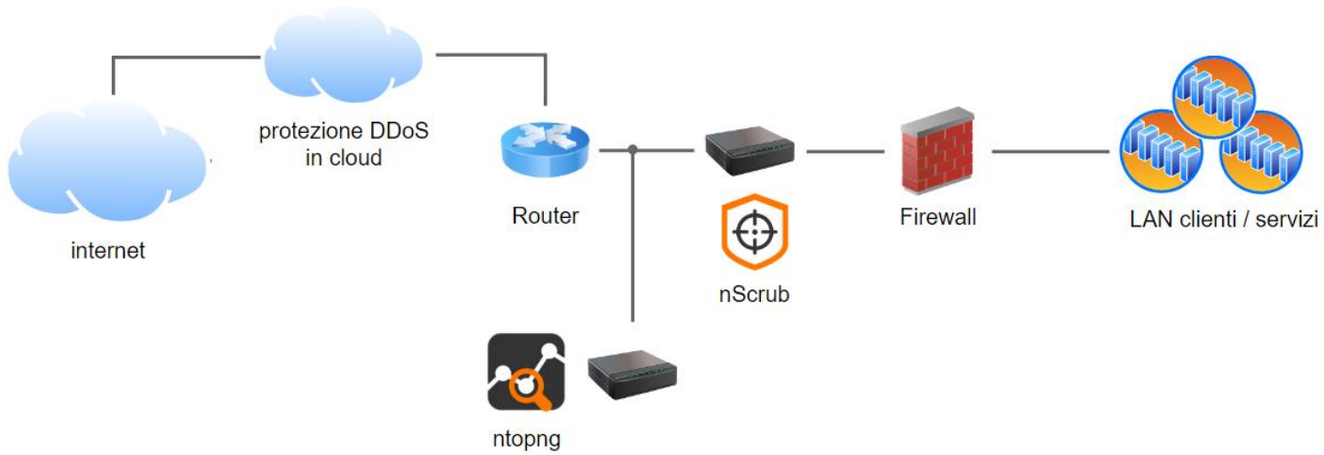
Agenda

- struttura di un hosting provider: panoramica
- cosa conosciamo
- cosa non conosciamo
- monitoraggio efficace con ntopng
- proteggere la rete con nScrub
- esperienza e best practice

Struttura di un hosting provider: panoramica

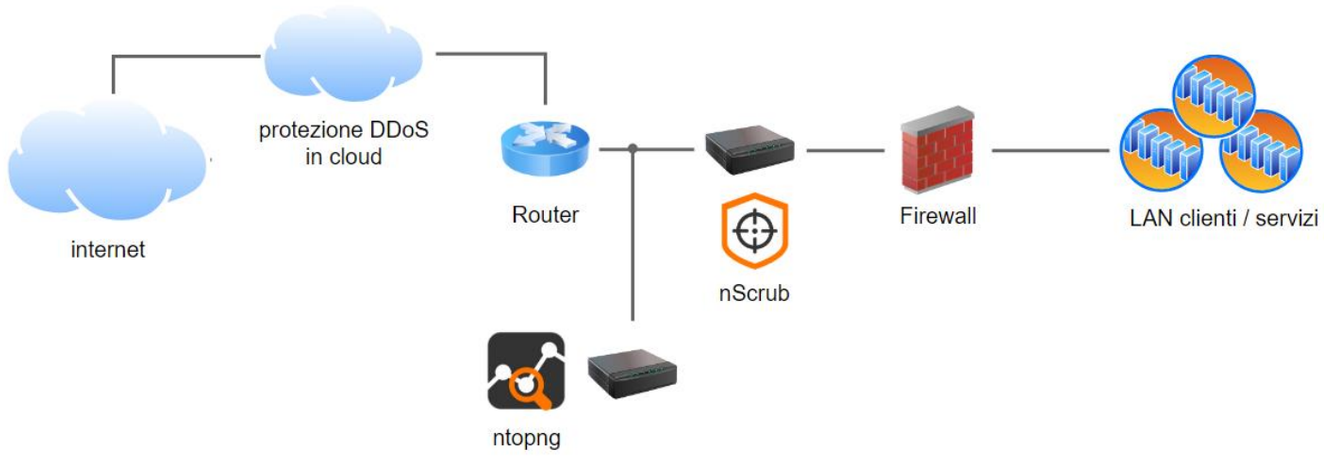


Cosa conosciamo



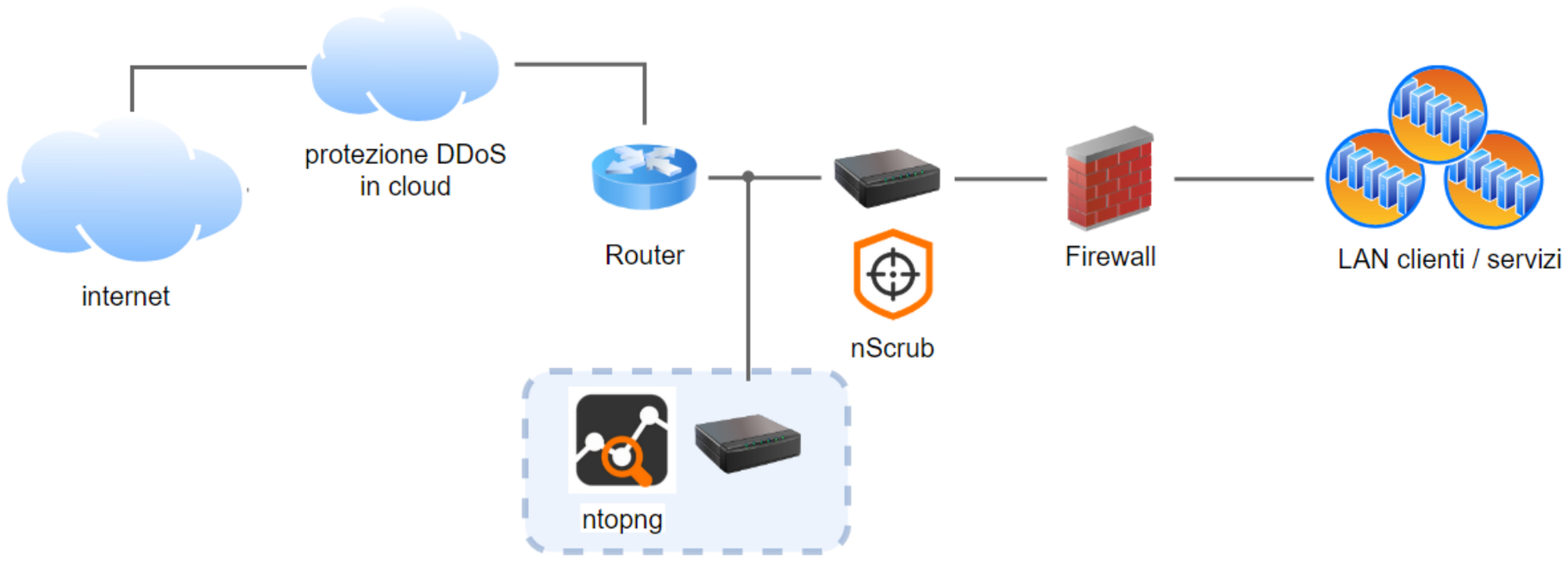
- statistiche da apparati di rete in comune: router, switch, firewall
- server e servizi erogati da HostingSolutions.it
- server/servizi/apparati dedicati al singolo cliente (gestiti)
- traffico a livello di firewall
- traffico da/verso internet

Cosa non conosciamo



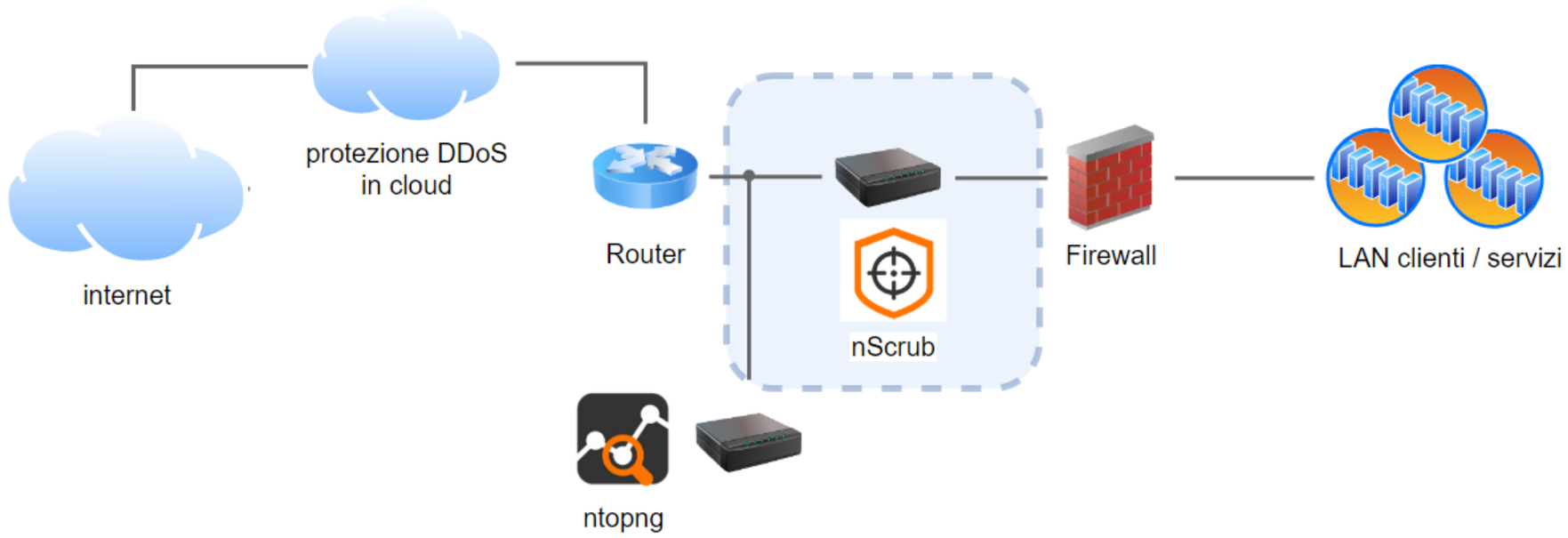
- server e servizi del singolo cliente, es. protetti da NAT
- traffico interno/privato tra server, es: vlan private
- statistiche degli apparati non gestiti

Monitoraggio efficace con ntopng



- posizione: mirror del traffico router lato LAN
- analisi dei flussi e rilevamento problematiche in tempo reale
- monitoraggio specifico su istanze dedicate:
  - qualità dei singoli tratti: active monitoring (icmp/banda)
  - statistiche per interfacce degli apparati di rete (snmp)

Proteggere la rete con nScrub



- posizione: tra router e firewall
- blacklist globale fornita da ntop
- blacklist dinamica generata dai nostri sistemi di rilevazione attività malevole sui server
- mitigazione attacchi media-bassa entità

Esperienza e best practice

- mantenere sistemi di monitoraggio **multipli**, diversificati per tipologia e posizione
- anche l'**infrastruttura** data center necessita del corretto monitoraggio
- garantire **multicanalità**
- combinare monitoraggi **interni** ed **esterni**
- cogliere sempre l'occasione per **migliorare** controlli esistenti ed aggiungerne di nuovi

Grazie

Francesco Leoncino
Manuele Gioli

hostingsolutions.it