IoT device discovery con ntopng

Giuseppe Augiero
augiero@ntop.org

Pisa • October 28, 2017

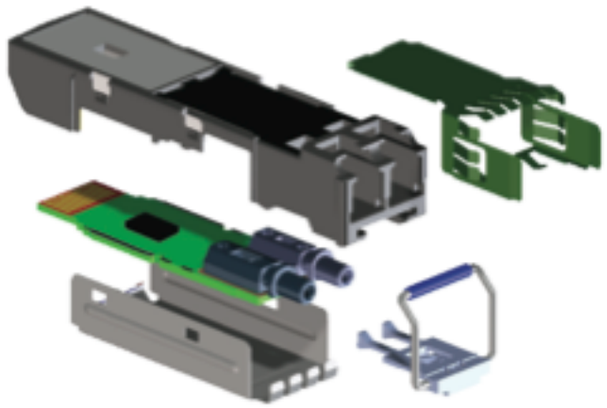
Agenda

- Iot device discovery con ntopng
- Ntopng scripting: estrapolare il traffico delle IoT device
- Deep Packet Inspection con Wireshark

NtopNg

- ntop develops of open source network traffic monitoring applications.
- ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
- Today our products range from traffic monitoring, high-speed packet processing, deep-packet inspection, and IDS/IPS acceleration (snort and suricata).

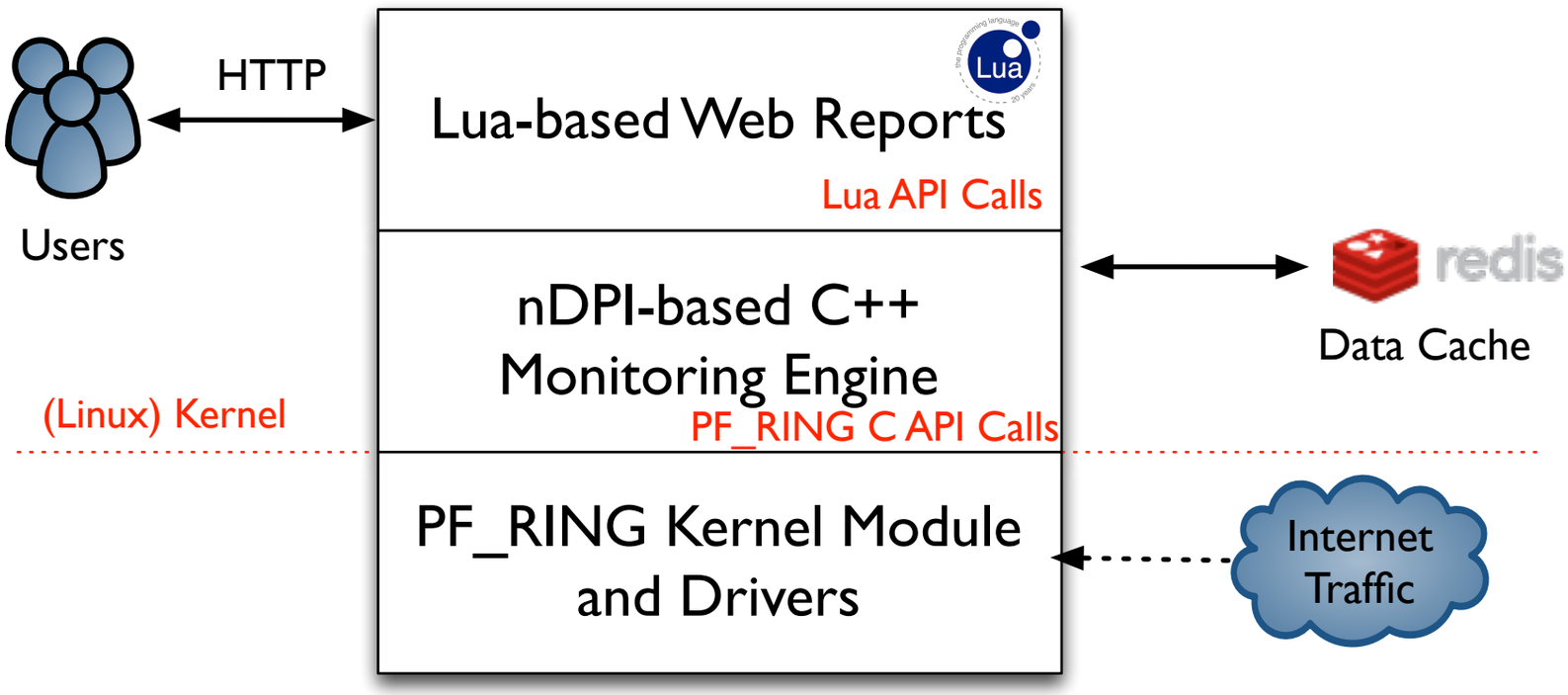
NtopNg (II)



Integrated ASIC with JDSU technology

NtopNg Architetture

- Three different and self-contained components, communicating with clean API calls.



Cosa accade?

- Abbiamo il controllo del nostro network?
- Non è possibile immaginare una rete in perfetta salute senza sapere cosa accade, in maniera puntuale, su di essa.
- La conoscenza è il primo passo per poter effettuare valutazioni dal punto di vista della sicurezza informatica.
- La correlazione di eventi ci può fornire

I pacchetti non tradiscono mai

- L'analisi del pacchetti ci fornisce interessanti informazioni che ci permettono di capire se ci siano:
  - problematiche di rete legate alla trasmissione dei dati
  - utilizzo inappropriato delle risorse
  - performance non coerenti
  - rischi dal punto di vista delle sicurezza
  - attacchi in corso
  - data breach

I pacchetti non tradiscono mai

- L'analisi del pacchetti ci fornisce interessanti informazioni che ci permettono di capire se ci siano:
  - problematiche di rete legate alla trasmissione dei dati
  - utilizzo inappropriato delle risorse
  - performance non coerenti
  - rischi dal punto di vista delle sicurezza
  - attacchi in corso
  - data breach

L’esigenza

- L’esigenza è capire se sulla nostra lan ci sono host (iot) di cui non conosciamo l’esistenza.

Sonda

- L'utilizzo di una sonda di analisi generica.

Sonda (II)

- Limiti della sonda.

Sonda (III)

- Scopo dell'analisi.

IOT

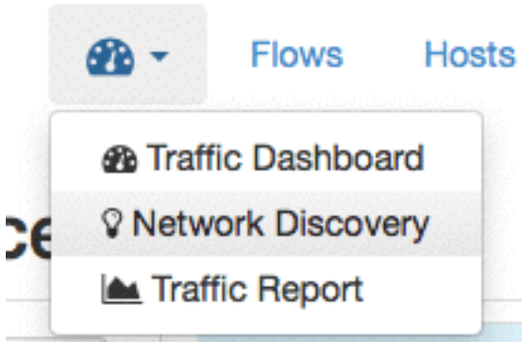
- Device silenti.

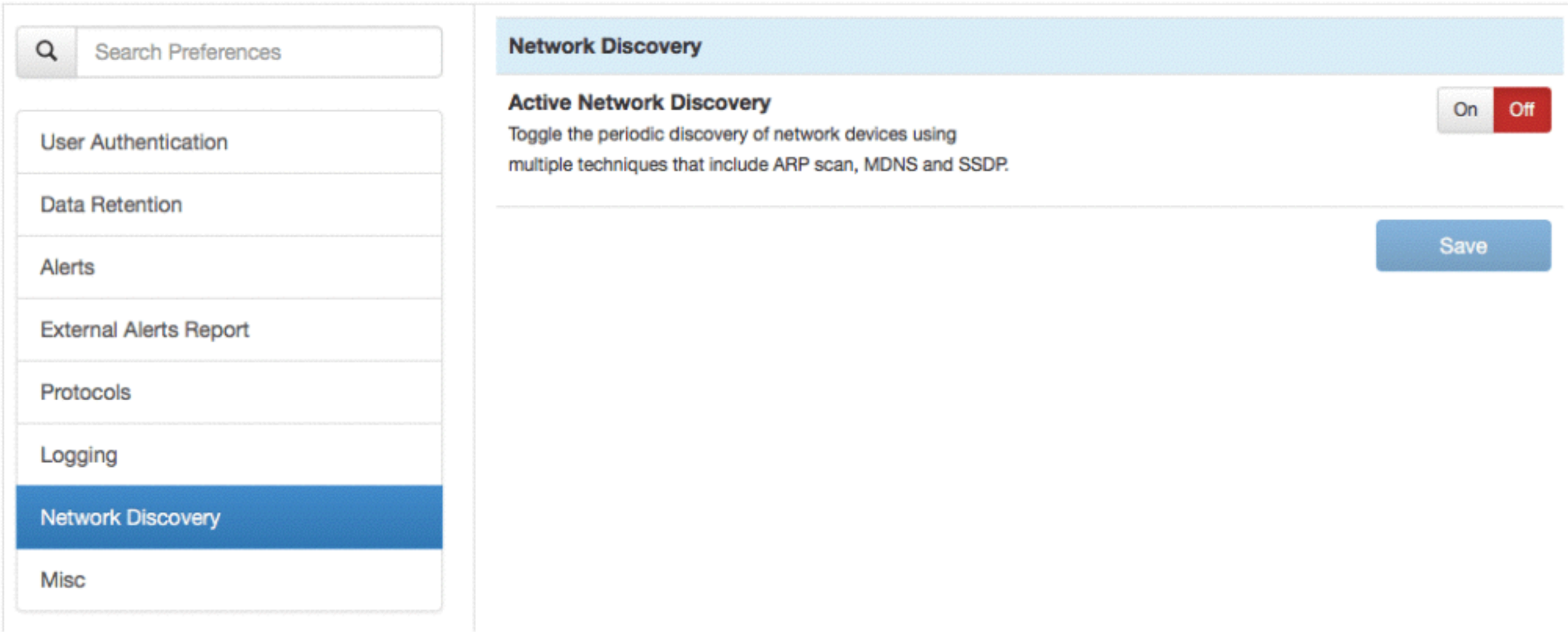
Network Device Discovery

- Con le ultime versioni di ntopng è stato implementato il discovery della rete.
- Ricerca dei dispositivi silenti.
- Indicazione dei servizi offerti.

Network Device Discovery (active)

Attivazione del servizio





Risultato

Il risultato della scoperta di rete viene memorizzato in redis e mantenuto per uso futuro. Il discovery consente di determinare il tipo di dispositivo (è una stampante, un router o una tavoletta?) e le loro funzioni OS / servizi offerti.

Network Discovery

Last Network Discovery	27/10/2017 09:02:01					
IP Address	**Name**	**Manufacturer**	**MAC Address**	**OS**	**Info**	**Device**
192.168.2.1	fritz.box	AVM Berlin [FRITZ!Box 3272]	5C:49:79:75:4E:6A		urn:any-com:serviceId:l2tpv31 urn:any-com:serviceId:fritzbox urn:upnp-org:serviceId:ContentDirectory urn:upnp-org:serviceId:ConnectionManager urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar urn:avm.de:serviceId:AVM_ServerStatus urn:any-com:serviceId:any1 urn:any-com:serviceId:any1 FRITZ!Box 3272 FRITZ!Box 3272 AVM FRITZ!Mediaserver InternetGatewayDeviceV2 - FRITZ!Box 3272 FRITZ!Box 3272	
192.168.2.20	Lucas-iMac	Apple, Inc.	C4:2C:03:06:49:FE		_smb._tcp.local _afpovertcp._tcp.local _ssh._tcp.local _sftp-ssh._tcp.local _nfs._tcp.local	iMac "Core i7" 2.93 27-Inch (Mid-2010)

Discovery (I)

- In prima battuta ntopng effetta a **arp ping** a tutta la sottorete che sta monitorando.
- Ntopng riconosce la subnet dall'interfaccia di rete.
- Viene usato un arp ping (L2) e non un semplice ping (L3) in quanto i pacchetti icmp potrebbero essere bloccati o filtrati.
- Al termine di questo processo ntopng ha la lista degli host attivi.
- Un dispositivo presente nella lista del discovery attivo e non in quella dei dispositivi L2 viene marcato come fantasma.

Discovery (II)

- Viene effettuato un SSDP Discovery in modo che i dispositivi possano indicare i servizi offerti.
- Viene inviata la richiesta a un indirizzo multicast e viene attesa la risposta.
- E' possibile ricevere risposta da dispositivi non presenti sulla nostra subnet.

Discovery (III)

- Nel frattempo, mentre vengono ricevute le risposte SSDP, per tutti gli host attivi scoperti tramite ARP, ntopng invia una richiesta **SNMP** per avere ulteriori informazioni sul dispositivo.
- Poiché viene utilizzata la comunità "public" possiamo scoprire solo una parte dei dispositivi.
- SNMP aiuta a rilevare le funzionalità di dispositivi quali stampanti o punti di accesso / router.

Discovery (IV)

- Poiché le piccole reti non hanno un DNS, utilizziamo **MDNS** per risolvere i nomi degli host locali quando DNS non è disponibile.
- Via MDNS è anche possibile conoscere (in particolare per i dispositivi / telefoni Apple) i servizi pubblicizzati e il modello / tipo di dispositivo.
- Le versioni recenti di OSX sono molto più verbose delle versioni precedenti.

Discovery (V)

- Alla fine uniamo le informazioni finora raccolte e generiamo le informazioni di discovery.
- Le informazioni sulla scoperta vengono mantenute su redis in modo da sopravvivere a riavvii di ntopng.

NAT

- Se hai installato nella tua rete un router NAT che nasconde i tuoi dispositivi privati, ntopng lo scoprirà.
- Ad esempio guardando User-Agent nelle intestazioni HTTP che riportano l'OS e altre informazioni del browser.

Security

- SSDP / MDNS sono protocolli molto chiacchieroni e pubblicizzano molte più informazioni di quelle che potreste immaginare
- Considerate questo fattore quando progetterete la sicurezza della rete.

Thank You!

Giuseppe Augiero
augiero@ntop.org