Edge Network Traffic Policing

Luca Deri <deri@ntop.org>
@lucaderi

X

Introduction

- Firewall and IPS (Intrusion Prevention Systems) are security devices designed to analyse traffic inline and implement security policies.
- Firewalls are <u>configurable</u> with policies that are specialised for selected devices (e.g. the mail or the HTTP server) but that are alike for all other devices.
- IPS search configured signatures in traffic (similar to what an antivirus would do) and stop individual communication flows without a global network view.

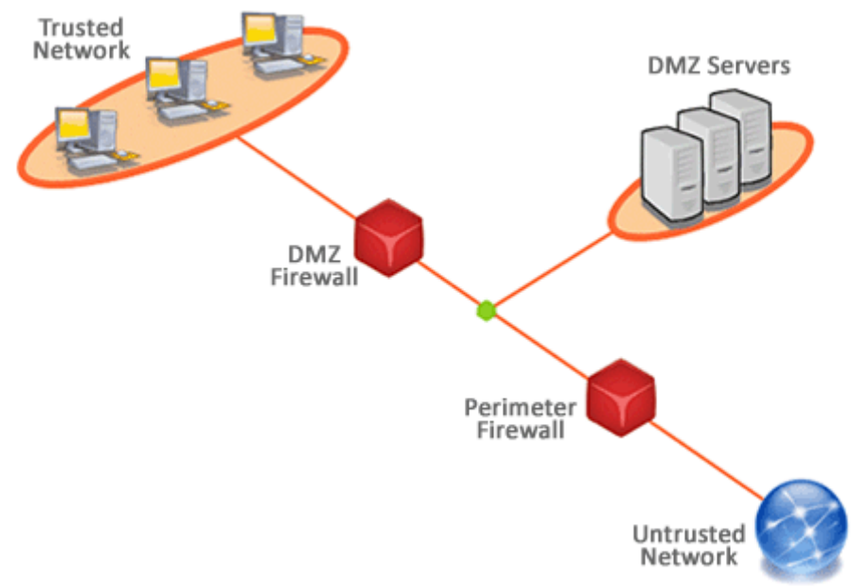
A Middle Age Approach

- For years security was tackled with as a middle age problem:
  - Bad guys are outside of my network
  - Good guys are in
  - If I have an internal service to expose to the Internet I need to place it on a DMZ where the firewall can enforce selected traffic policies
- This approach was good until devices/users where easy to divide in groups but with the advent of BYOD, IoT and cloud computing things got tougher.

A Broken Security Model [1/3]

"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."

Jerome Saltzer



- Procedural Security
- Logical Security
- Physical Security

Denning's Least Privilege Principle

A Broken Security Model [2/3]

- The Low-voltage Environment:
  - Wide-spread use of IoT devices.
  - Increasing interconnection between edge devices and corporate networks: an edge device has important topological privileges.
  - Edge devices lack built-in security features: too simple, yes easy to attack or replace with "trojan" devices.
  - Physical location renders networks vulnerable to external attack – even without Internet connection

A Broken Security Model [3/3]

- Unsecured low-voltage devices:
  - Access control
    - Unauthorised opening of gates/doors, false attendance information.
  - Video surveillance cameras
    - Manipulation of video camera streams, unauthorised viewing or disabling video edge-device elements.
  - Building-management/Fire-alarm systems
    - False readings, disabling or blinding.
  - Perimeter IP-based sensors
    - False readings, disabling or blinding.
  - DDoS (Distributed Denial of Service) attacks, can disrupt network operations and thus break a complex system/factory.

Traditional Metrics Are Becoming Outdated

- Popular metrics such as bytes, packets, need to be complemented with new metrics such as:
  - Layer 7 application protocol (DPI): we need visible insights into protocols as DNS and HTTP are not longer enough to characterise traffic.
  - Device type: not all devices are supposed to behave the same way on the network. A printer should not do a Skype call, a tablet should not accept print jobs.
  - User categories: the widespread use of personal devices such as laptops or smartphones forces to cluster devices according to users and thus set the policy base on this.

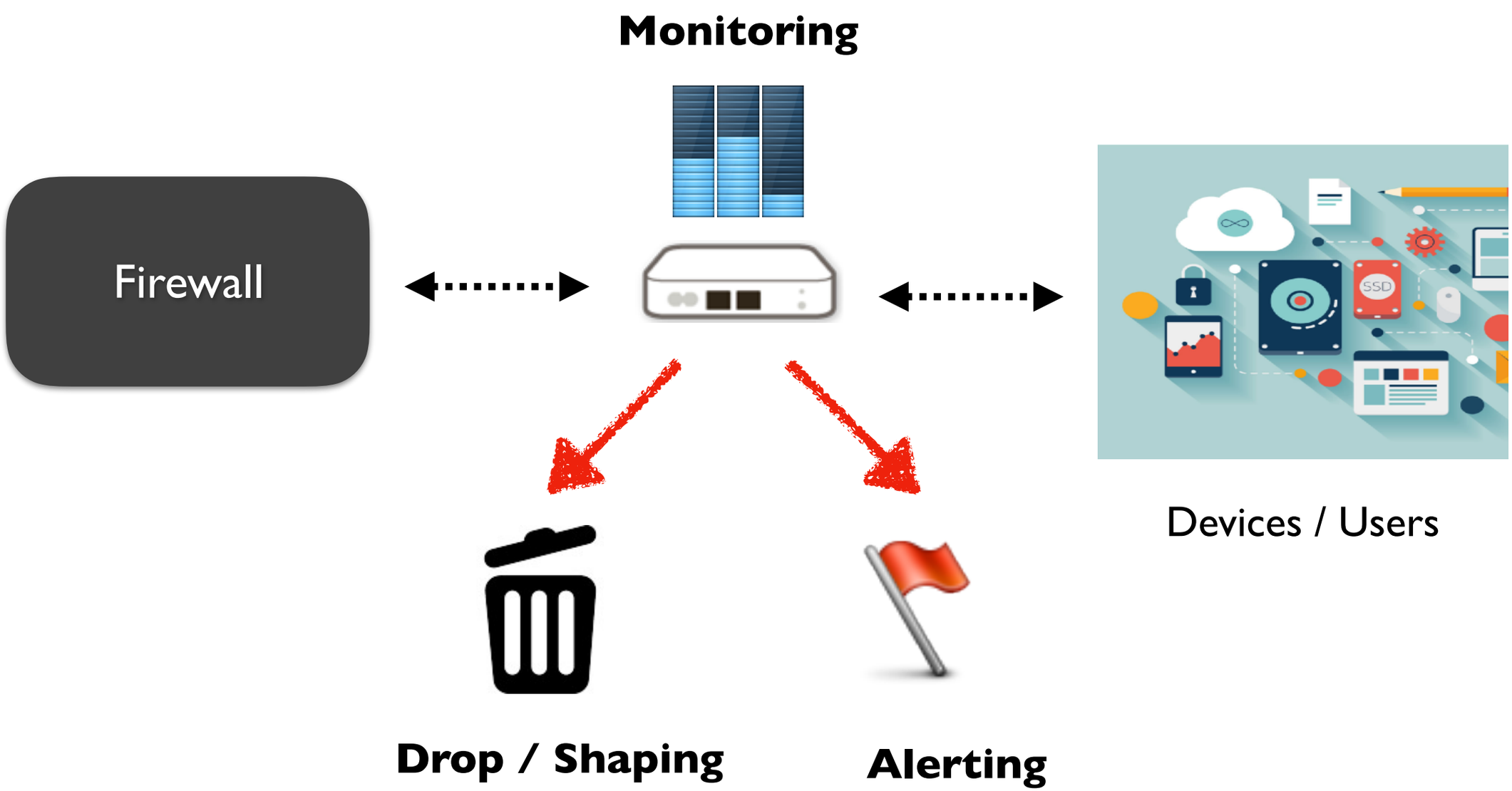
In Essence…

- Track dynamic network topologies and moving components.
- Time of the day and geolocation matters: downloading a file is ok, doing it at 3 AM or from a remote country is not.
- Identify IoT devices and threat them differently from "generic" computers (e.g. laptops or tablets)
- Tag network traffic with application protocol and monitor it continuously overtime looking at specialised metrics (e.g. HTTP return code) in addition to generic ones (e.g. jitter and bandwidth).
- As most devices are not installed in "controlled environments" (e.g. a rack on a datacenter vs on a corridor) physical security needs also to be monitored.

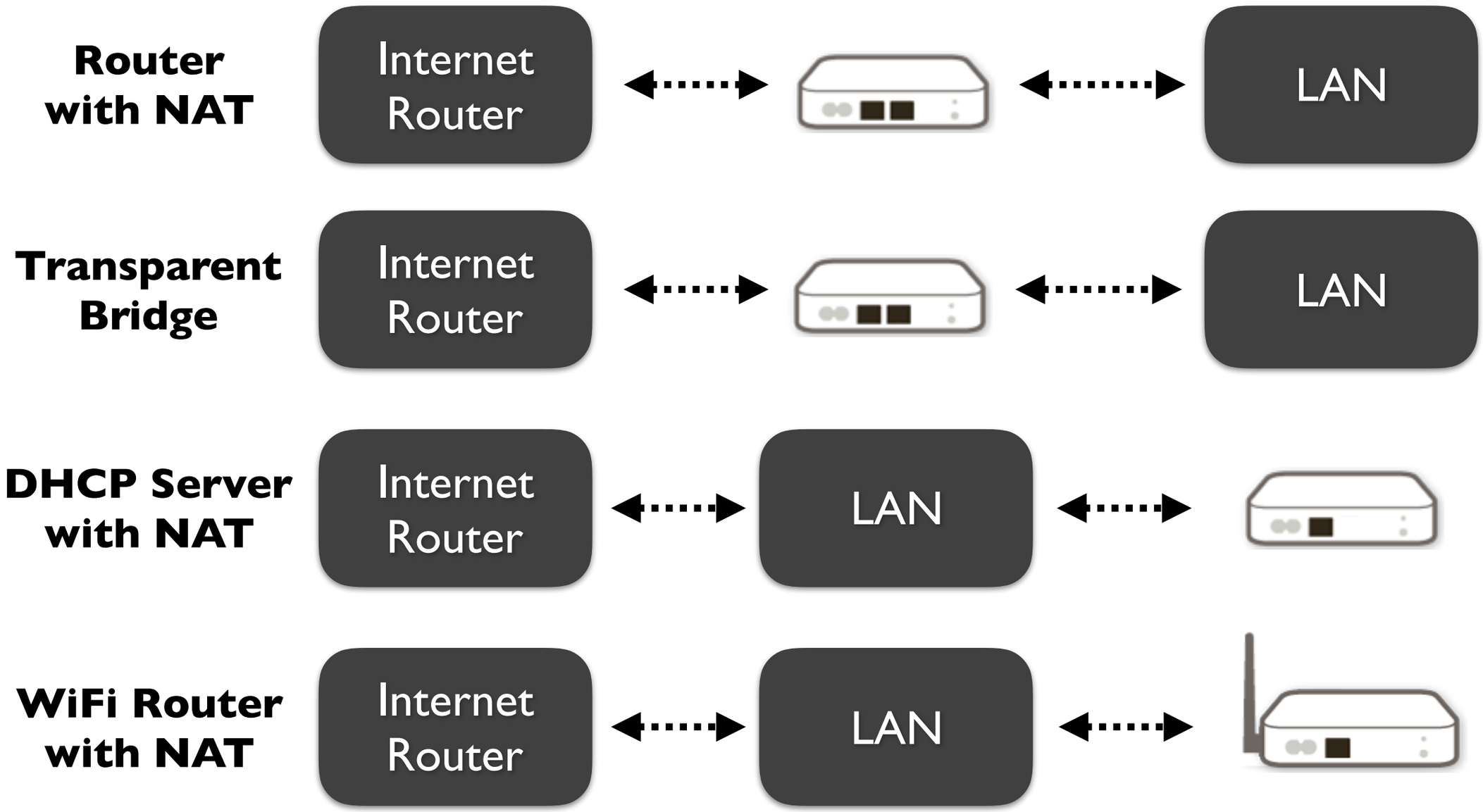
Security in Three Phases

- Learning
  - Identify network elements (discovery), assign them a role (e.g. a printer).
- Profiling
  - Bind a device to a profile (e.g. a printer cannot Skype or share files using BitTorrent) and enforce it via alarms or traffic policy enforcement.
- Continuous Monitoring
  - Physical constraints (e.g. MAC/IP binding and switch port location), traffic constraints (e.g. a new protocol serviced by a device or throughput above/under its historical baseline can be an indication of a problem).

Edge Traffic Policing



Deployment Modes



Routing Modes

When used in routing mode it can:

- Use a single routing policy for all devices (default for most routers and firewalls)
- Specify a routing policy per device/user (e.g. host X uses gateway Y, host A uses gateway B) and eventually device/user/protocol (e.g. user K BitTorrent traffic will use gateway C)

Some Facts: What is About

- Designed to complement (not replace) firewalls and security devices by:
  - Enforcing per user/device traffic policies and assigning devices to users.
  - Layer 7 traffic policy (drop + shaping) based on device type, user, and time of the day.
  - Periodic asset discovery to detect new devices connected to the LAN and enforcing their traffic.
  - Multicast/broadcast monitoring to fingerprint devices and discover network overlays created by users.
  - Prevent access to malware, inappropriate (for minors) and unsafe Internet contents.

Some Facts: What is Not

- This is not a firewall replacement but rather it complements firewall policies.
- Not just a parental control device.
- Not an IPS as traffic control is enforced at layer 7 protocol level and not based on signatures.
- A cloud device: it can operate stand-alone without having to store date on the Internet or need to access Internet-based services to work.

Network Device Discovery

ntop | Dashboard | People | Devices | 243.38 kbit/s | 0 bps

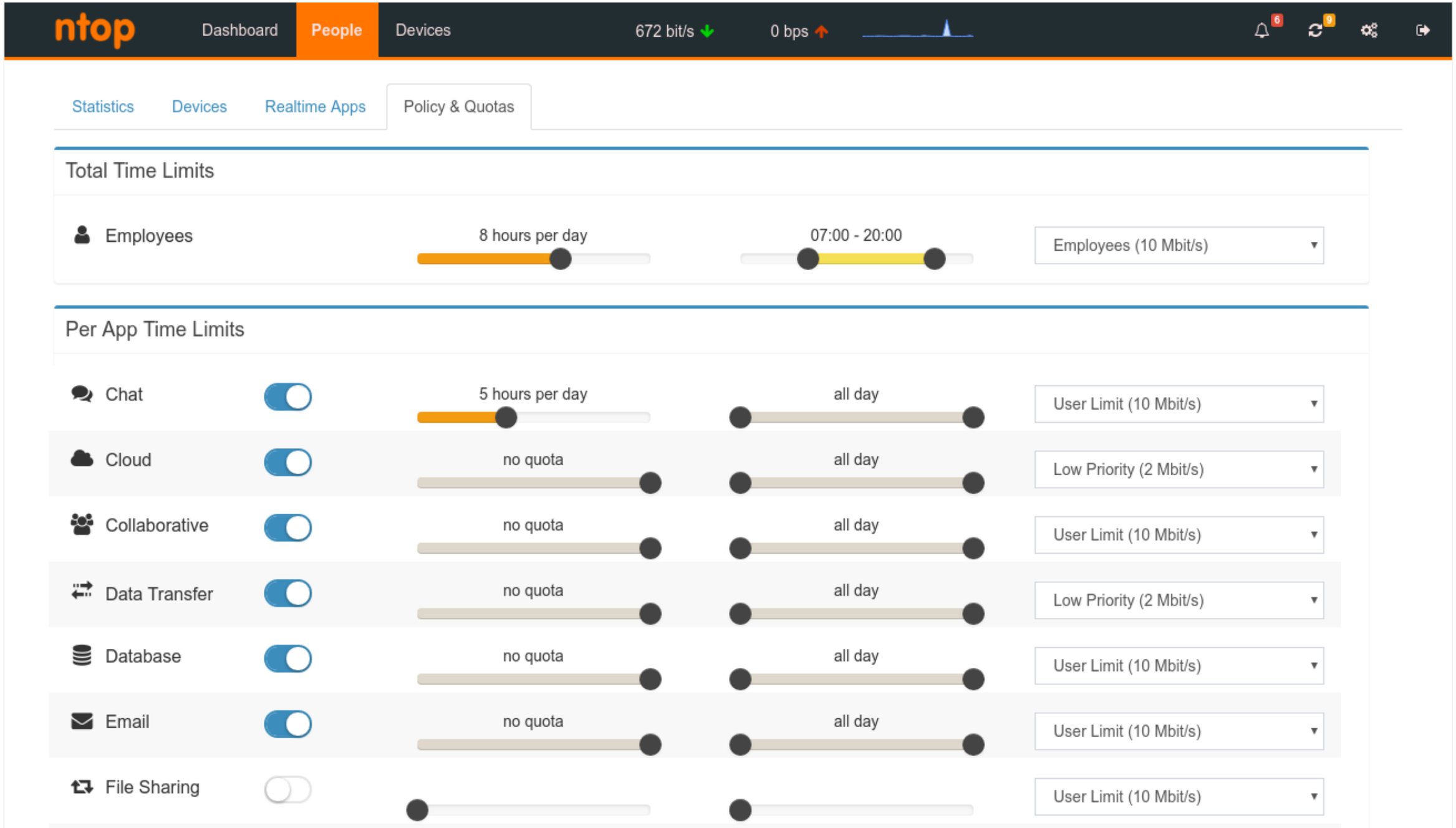
Home

Statistics | Devices | Realtime Apps | Policy & Quotas

Search:

Status	Device	Last Seen	IP Address	Traffic	Actions
Online	mattia-ux305	56 sec ago	192.168.1.8	6.61 KB	
Online	Windows-Phone	1 min ago	fe80::bcfb:609e:6bbd:6794	128 Bytes	
Online	iPhonediChiara	52 sec ago	192.168.1.15	216 Bytes	
Online	DESKTOP-ulx35	5 sec ago	192.168.1.10	97.11 KB	
Online	iPhonediMarco	3 min ago	192.168.1.12	672 Bytes	
Online	android-c814e63b0114ec25	43 sec ago	192.168.1.5	12.76 KB	
Online	HP-Inkjet 3830	3 sec ago	192.168.1.107	46.85 KB	
Offline	Azurewav_02:F1:41	1 day, 3 min ago	-	193.13 KB	
Offline	D-Link	5 h, 9 min ago	-	184.69 KB	
Offline	Raspberry	15 min ago	-	138 Bytes	

Policies and Quotas



Child/Malware-Safe DNS

ntop Dashboard People Devices 0 bps 0 bps

Settings

- Authentication
- Network
- Wifi
- **DNS Security**
- Speed Limits
- Quick Setup

DNS Security

Global DNS

The global DNS specifies the DNS server to use for the nDevice and your clients.

Server Preset: Custom

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

Children DNS

The children DNS specifies and override for the DNS server to use for your children.
You need to tick the *Child* checkbox on the person details to enable this.

Server Preset: Norton ConnectSafe: Sec

- Comodo Secure DNS
- Dyn Internet Guide
- FoolDNS
- GreenTeam Internet
- OpenDNS
- OpenDNS - FamilyShield
- Norton ConnectSafe: Security
- Norton ConnectSafe: Security + Pornography
- Norton ConnectSafe: Security + Other
- Custom

Primary DNS Server

Secondary DNS Server: 199.85.127.20

Apply

Final Remarks

- Modern devices create new monitoring challenges and require an *integrated monitoring* approach: element + periodic active scans + permanent passive traffic monitoring.
- Monitoring hundred/thousand devices require *scalability* and *intelligence* in the monitoring platform (analytics and big data is not enough, platform must be reactive, distributed, multi-tenant).
- Bytes+Packet-based monitoring must be *complemented* with specialised metrics, DPI, realtime monitoring, flexible (on-the-go) alerting.