RUB hgi Horst Görtz Institute for IT-Security

On Using Application-Layer Middlebox Protocols for Peeking Behind NAT Gateways

Teemu Rytilahti, Thorsten Holz
Horst Görtz Institute for IT-Security, Ruhr University Bochum, Germany

Network and Distributed System Security Symposium 2020

Motivation

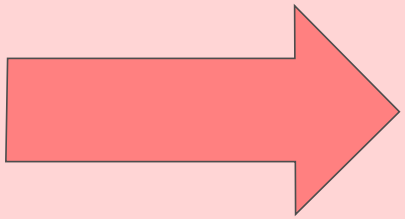
External Network

BOUNDARY

Internal Network

Motivation

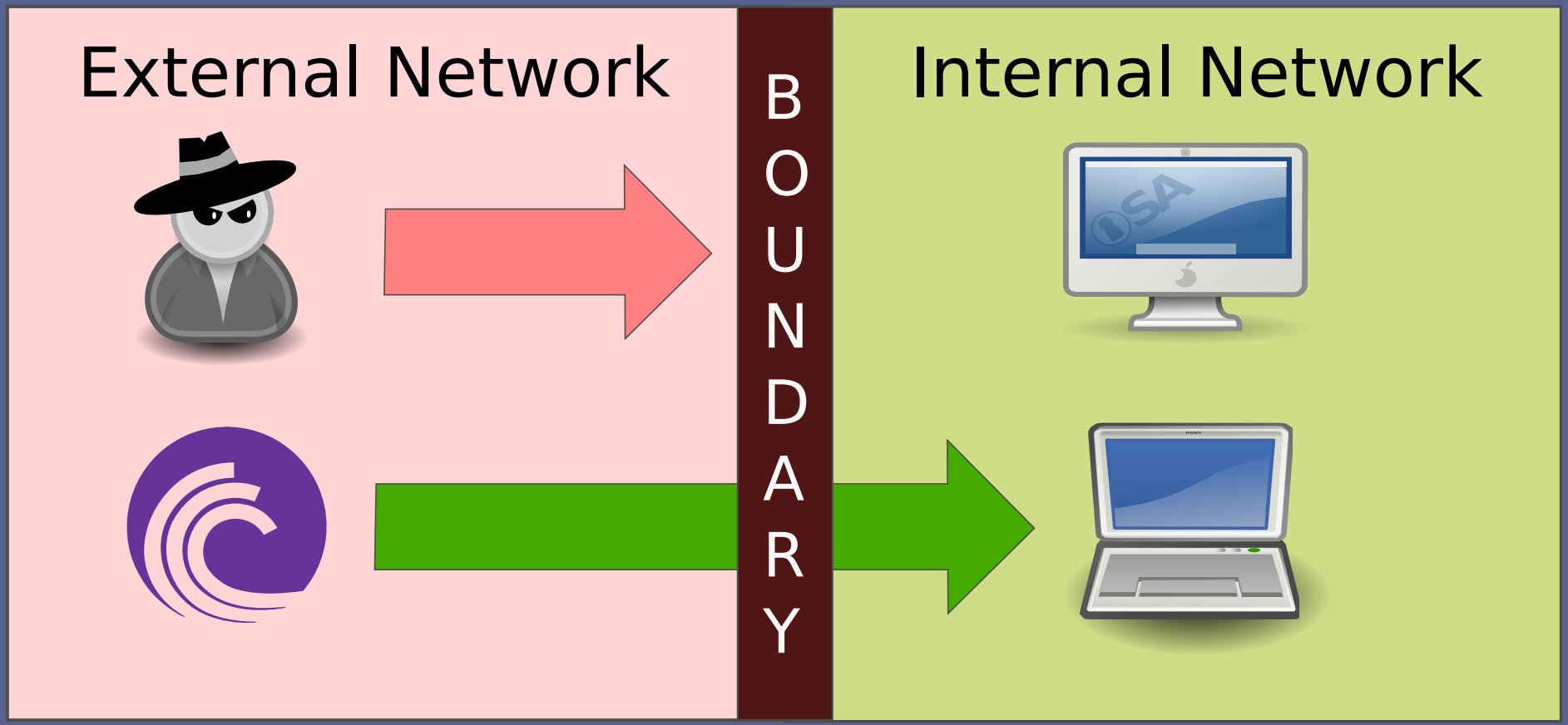
External Network



BOUNDARY

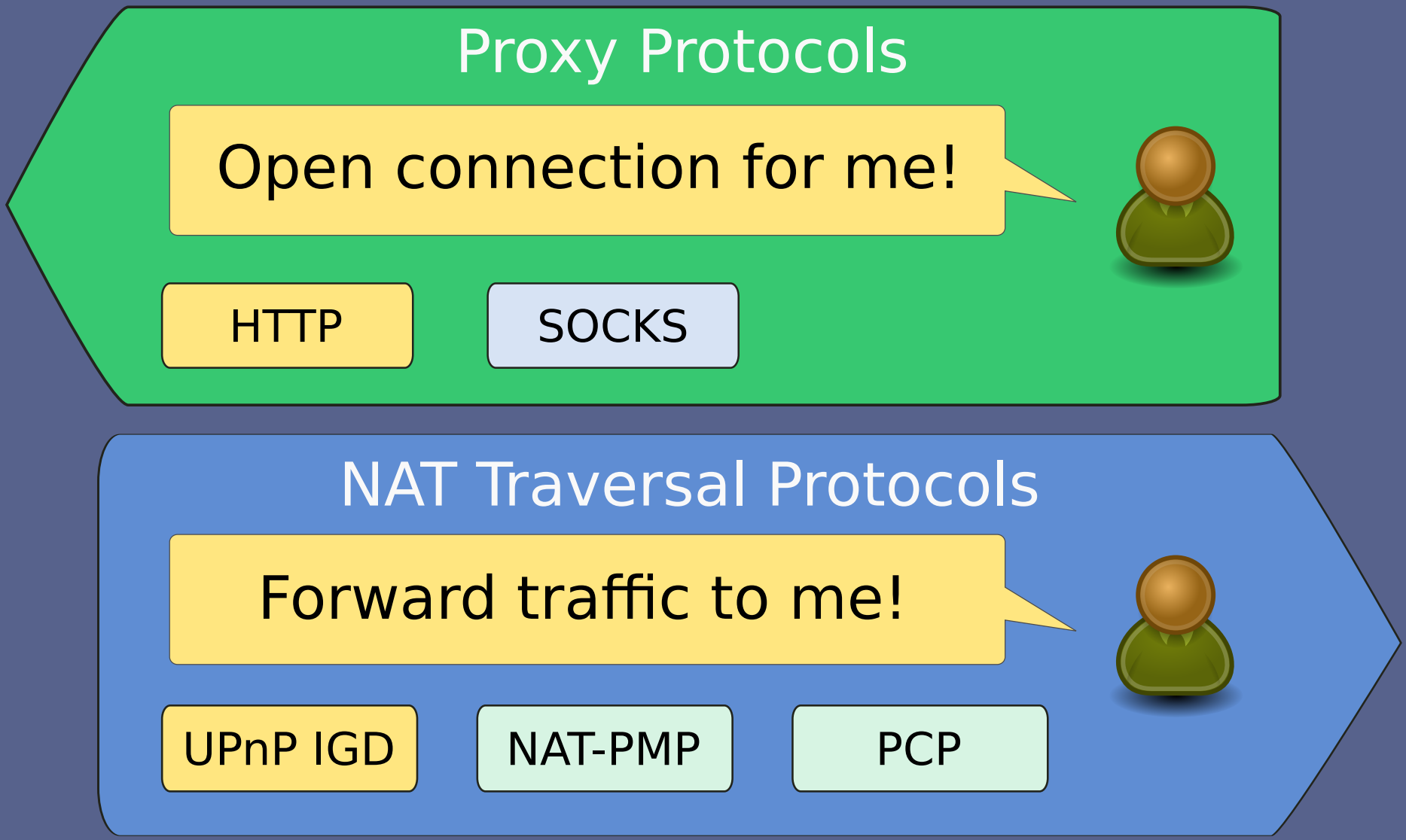
Internal Network

Motivation



Motivation

Motivation


Proxy Protocols
Open connection for me!
HTTP
SOCKS
NAT Traversal Protocols
Forward traffic to me!
UPnP IGD
NAT-PMP
PCP

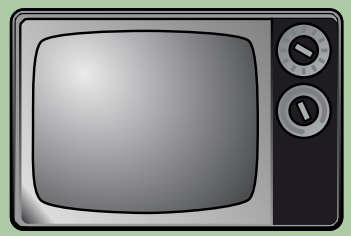
Idea!

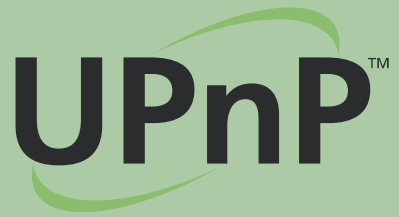
What if we could use these protocols to access networks that are otherwise “hidden”?

Universal Plug'n'Play (UPnP)

UPnP - Discovering Devices

Local Network

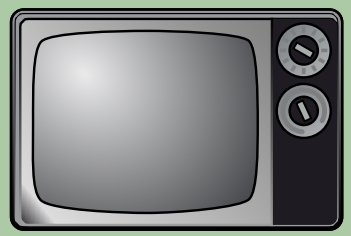




UPnP - Discovering Devices

Local Network

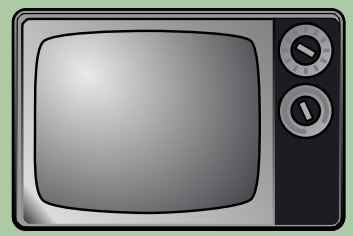
Hey, anyone out there?



UPnP™

Local Network

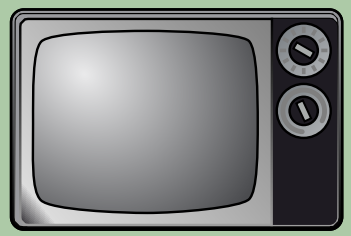
Hi, it's me, your telly!



¡Hola! Did someone ask for cameras?

Hallo, your router here!

Local Network



UPnP - Finding Services

Ah, there you are!

What can you do for me?

UPnP - Finding Services

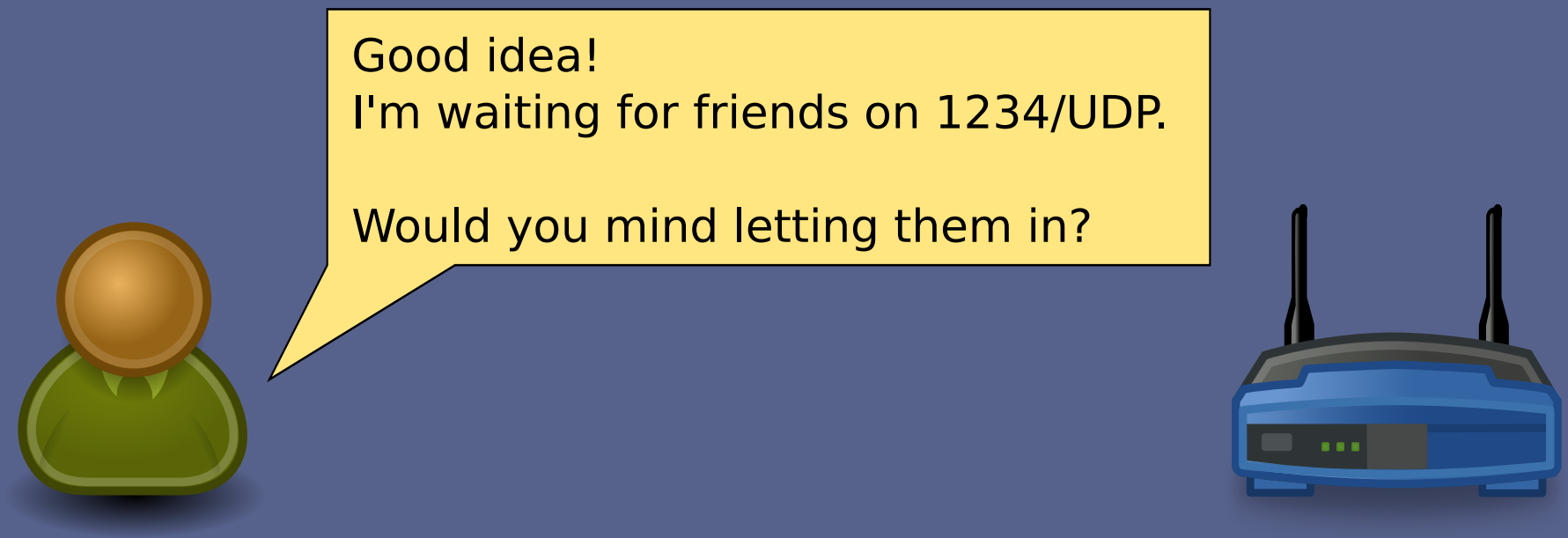
Ah, there you are!

What can you do for me?

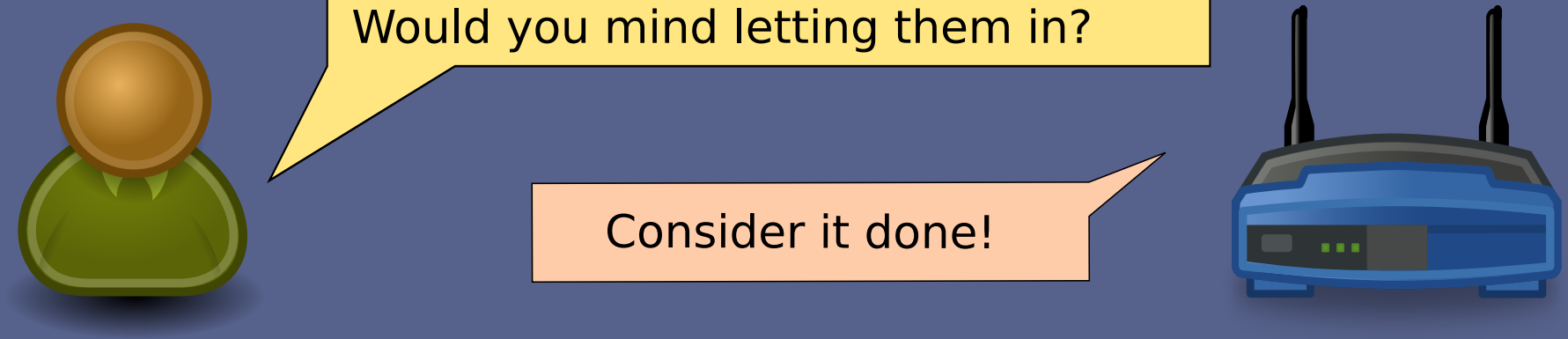
Well, I can do many things!

How about a port forward?

UPnP - Executing Actions



UPnP - Executing Actions



Food for Thought

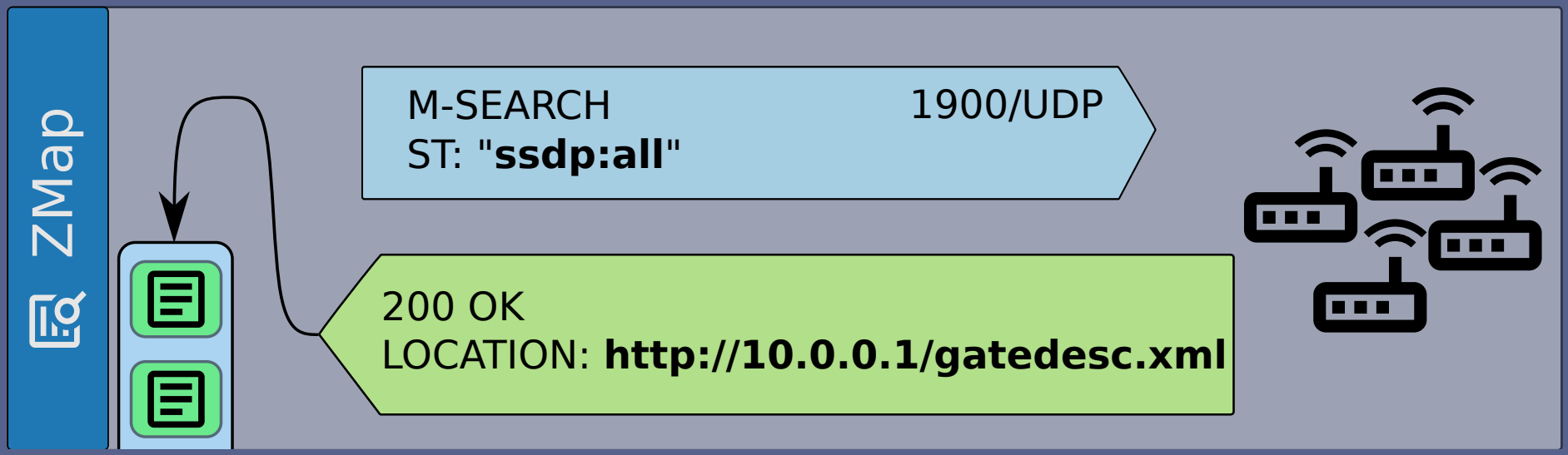
What if I say that there are UPnP devices exposed to the Internet?

Finding UPnP IGD Devices on the Internet

Our Approach

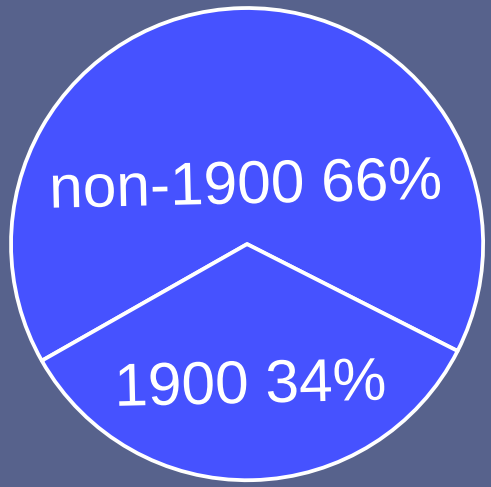
1. Discovering UPnP Devices
2. Finding IGD Services
3. Enumerating Existing Forwards

1. Discovering UPnP Devices



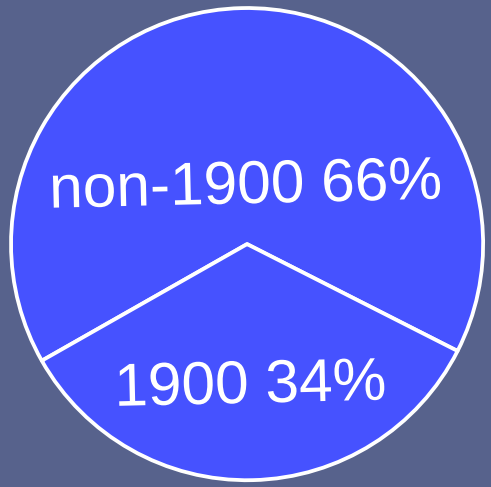
UPnP Devices (2,800,000 hosts)

DoS Amplifiers: 2.8M



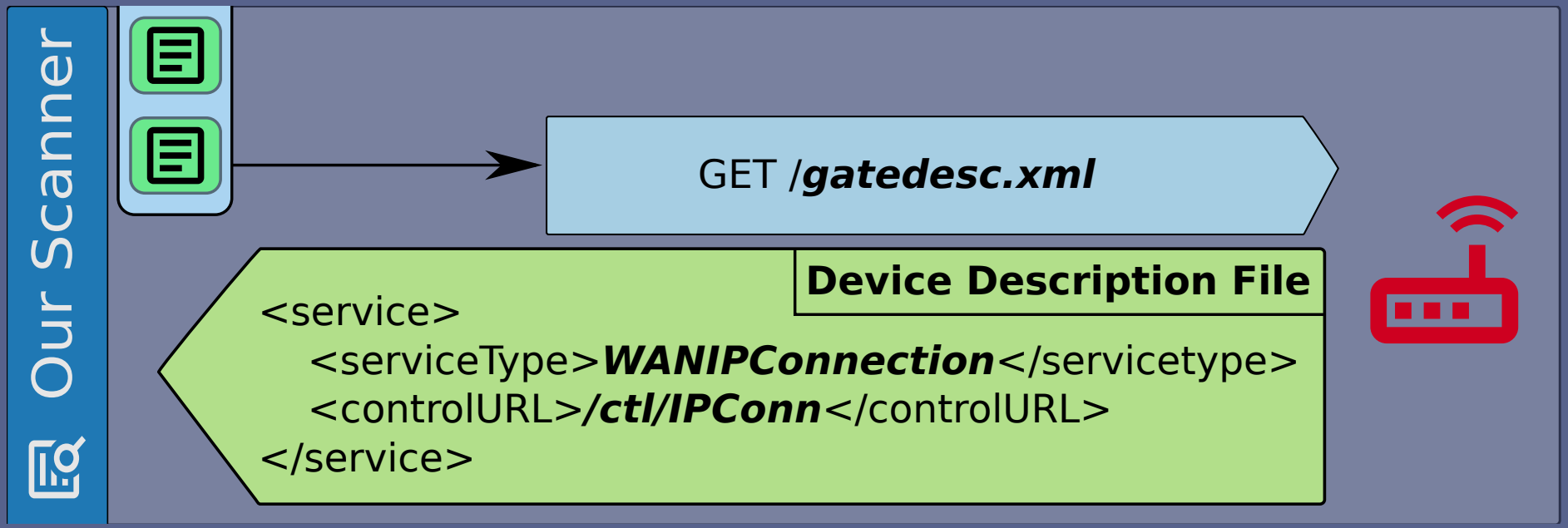
UPnP Devices (2,800,000 hosts)

DoS Amplifiers: 2.8M

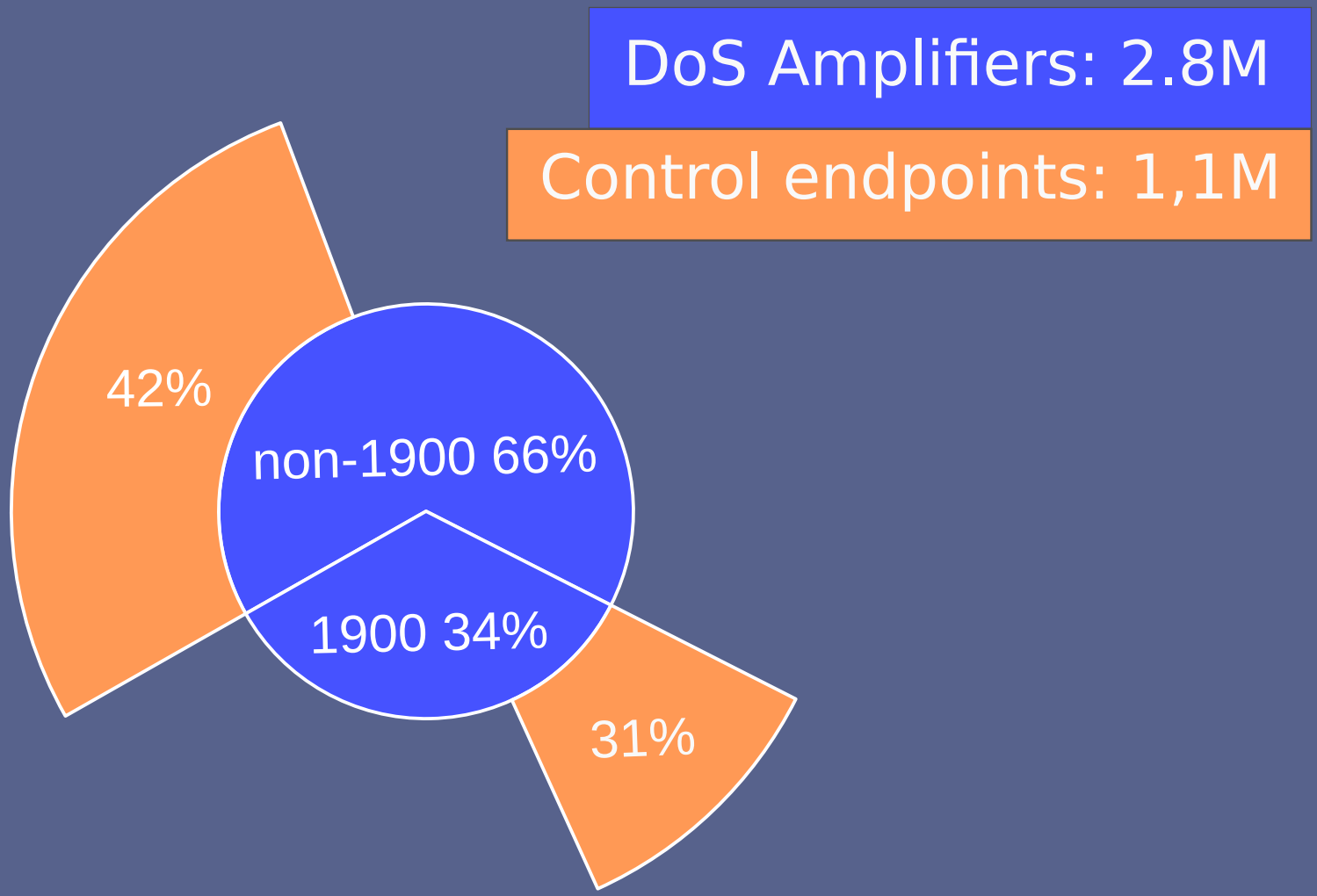


With vanilla ZMap

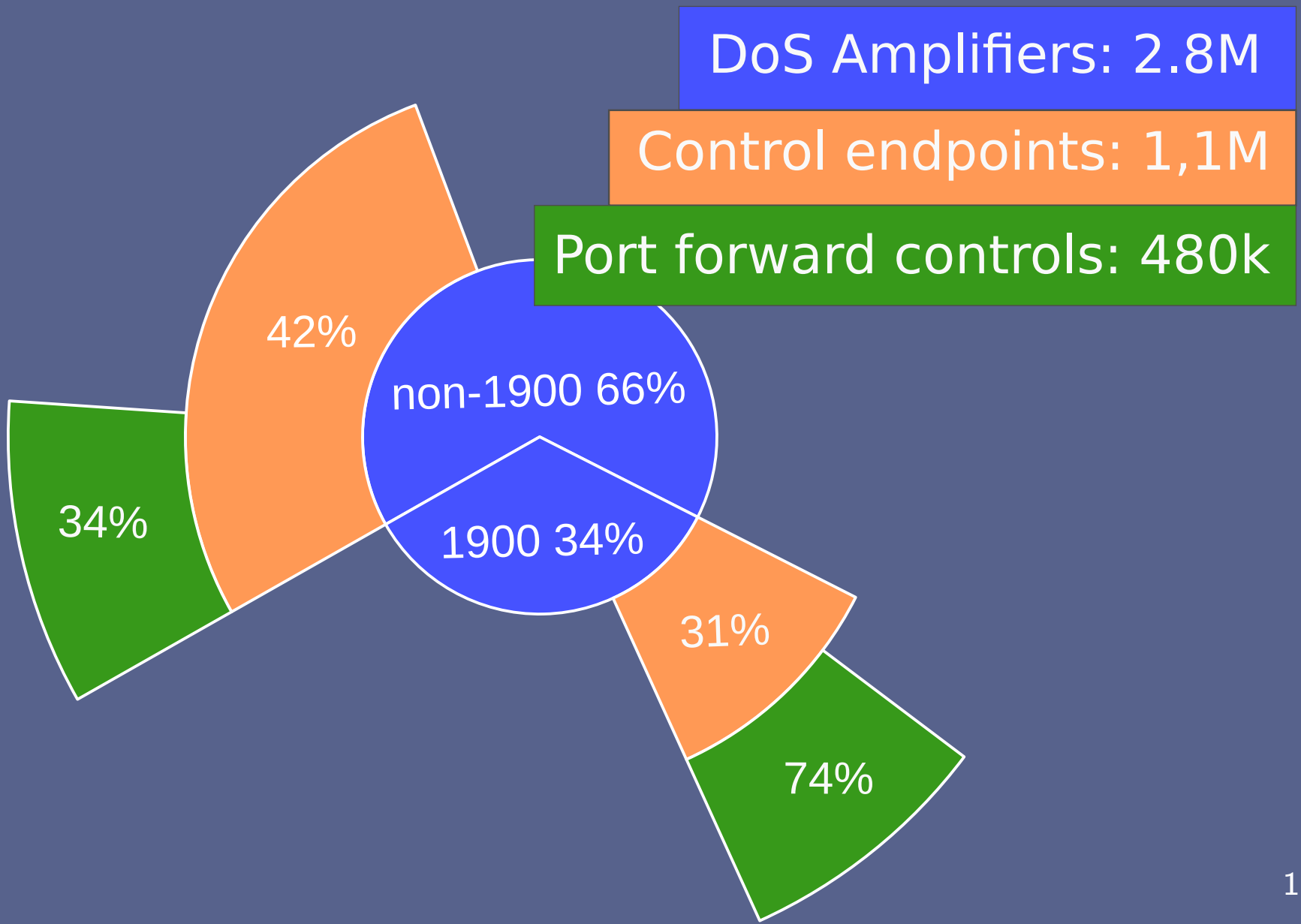
2. Finding WAN*Connection services



Exposed HTTP endpoints (1,100,000 hosts)



Exposed Port Forward Controls (480,000 hosts)

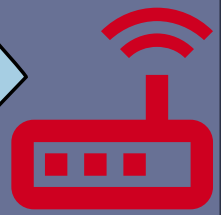


3. Listing Existing Port Forwards

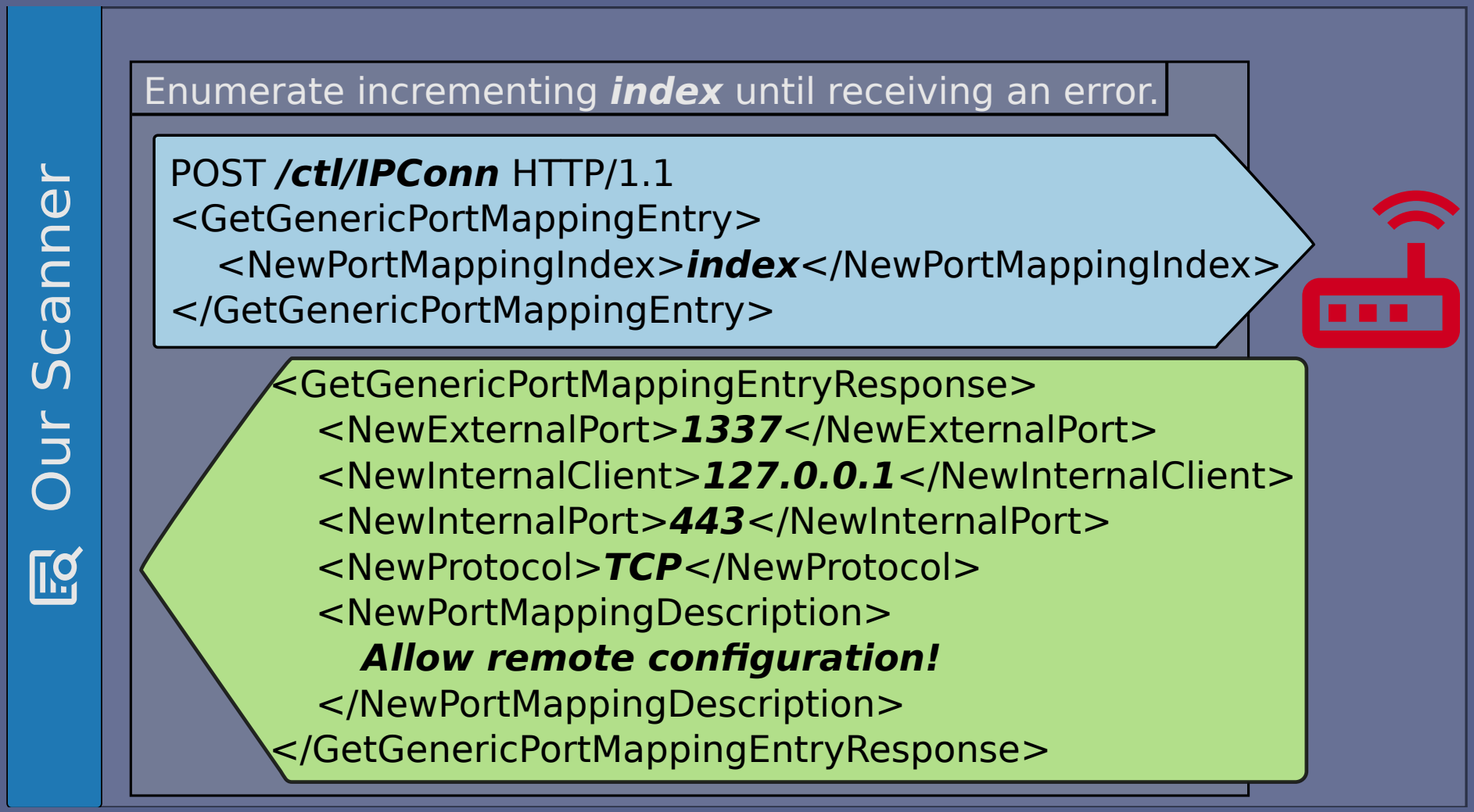
Our Scanner

Enumerate incrementing ***index*** until receiving an error.

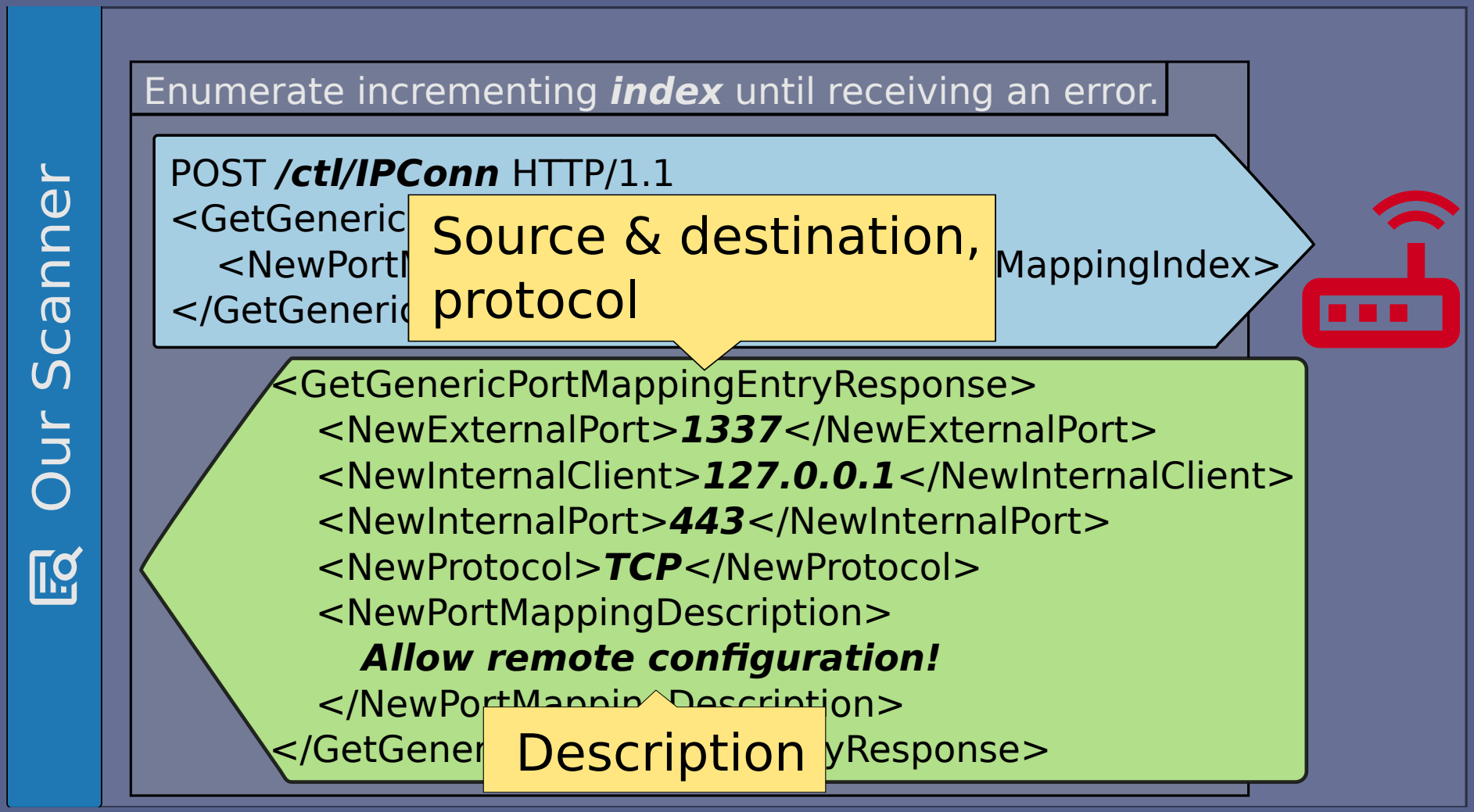
```
POST /ctl/IPConn HTTP/1.1
<GetGenericPortMappingEntry>
   <NewPortMappingIndex>index</NewPortMappingIndex>
</GetGenericPortMappingEntry>
```



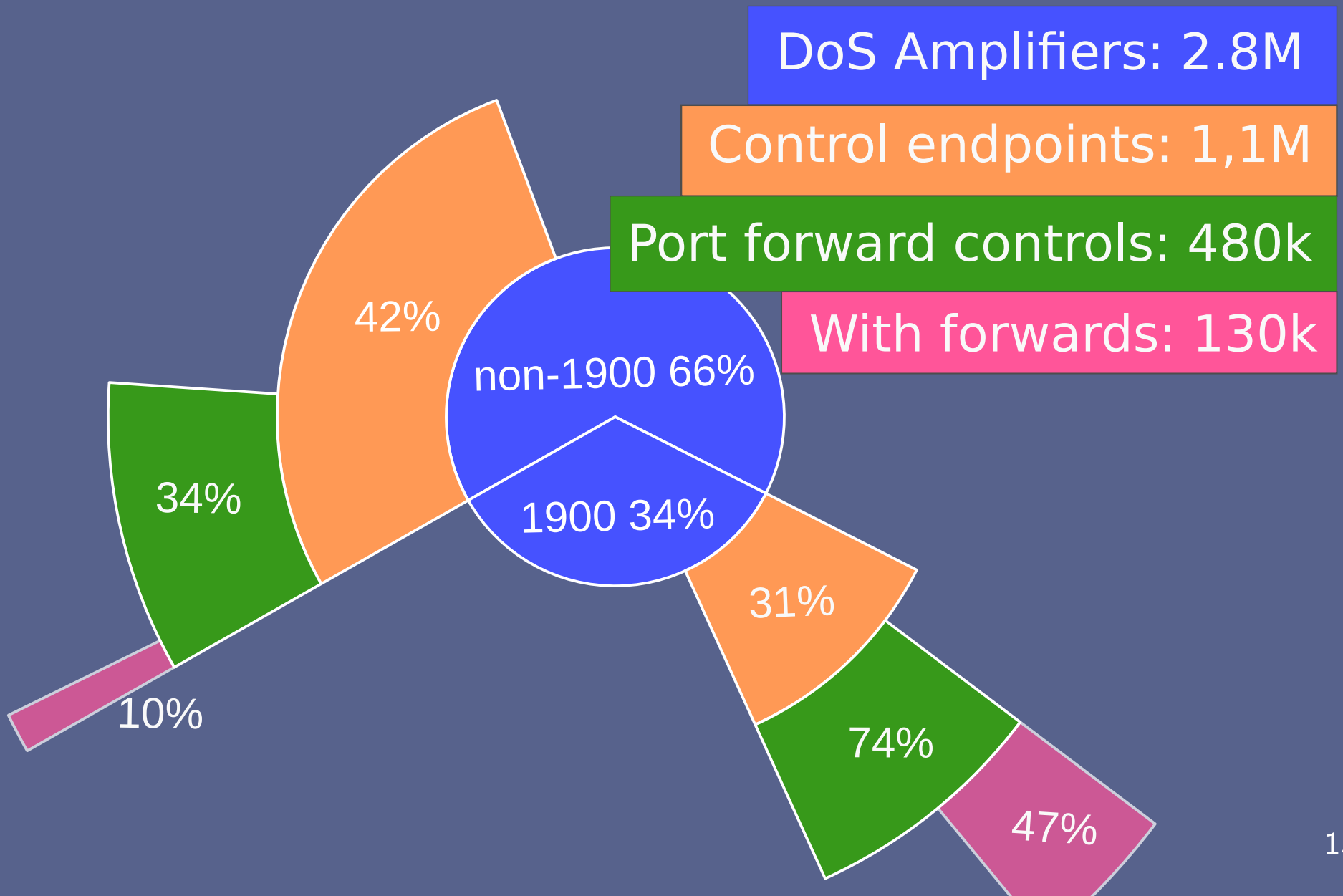
3. Listing Existing Port Forwards



3. Listing Existing Port Forwards



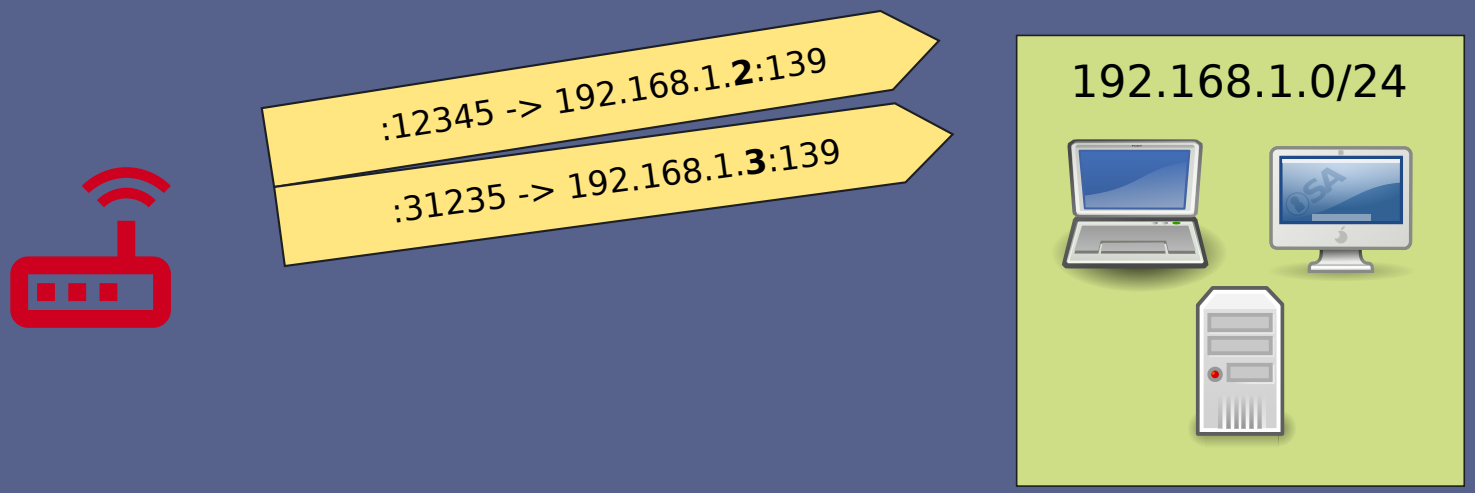
Hosts with Forwards (130,000 hosts)



Categorizing Forwards

1. Forwards with “galleta silenciosa” (42,000 hosts)
2. Forwards to external target IP addresses (18,000 hosts)
3. Rest of the forwards we consider benign (110,000 hosts)

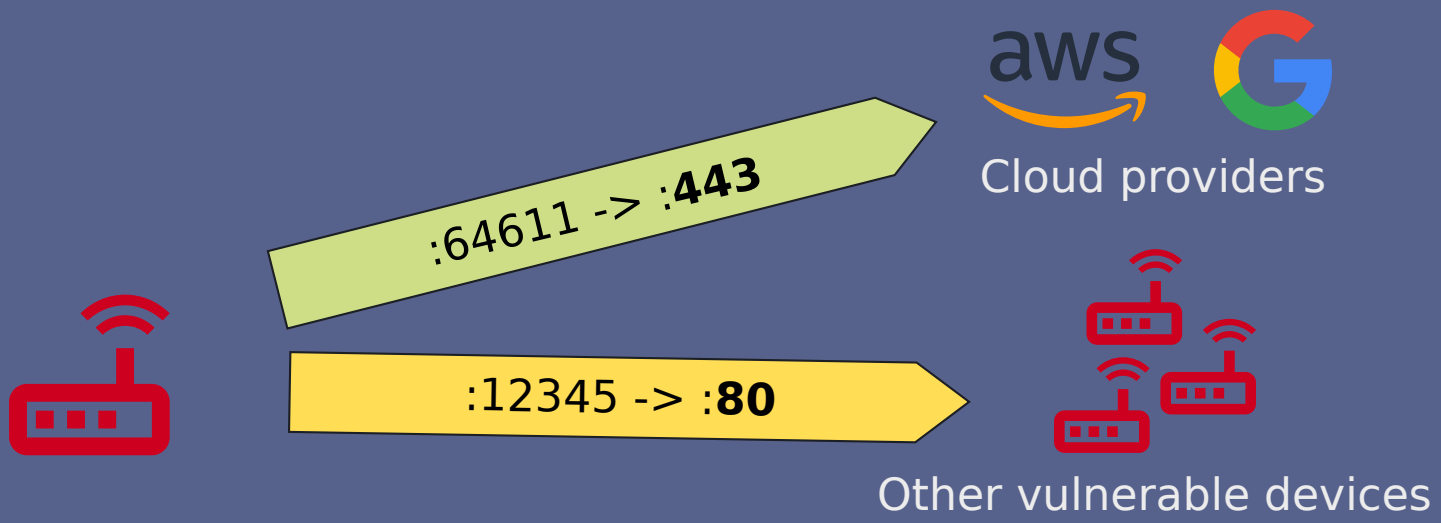
Galleta silenciosa – Silent cookie (On 42,000 hosts)



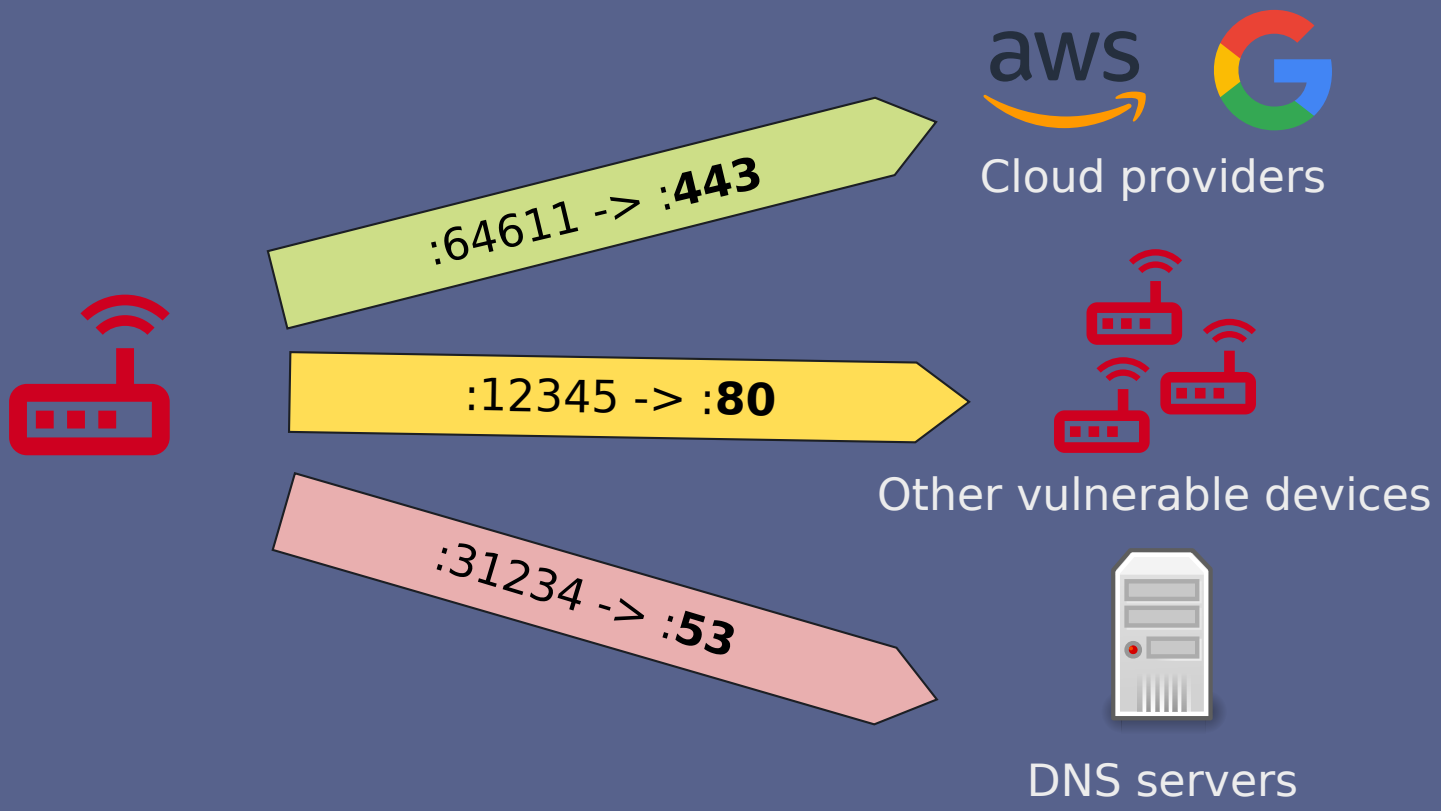
Galleta silenciosa – Silent cookie (On 42,000 hosts)

External Forwards (on 18,000 hosts)

External Forwards (on 18,000 hosts)



External Forwards (on 18,000 hosts)



Benign Forwards (on 110,000 hosts)

- Torrent clients (uTorrent, libtorrent, ..)
- Chat software (Whatsapp, Wechat, ..)

Conclusion

UPnP

- Ubiquous in home networks (tester in our github repo!)
- Unfortunately **still** exposed to the Internet

UPnP IGD

- Allows configuring port forwards
- Actively misused by malicious actors

Remediation

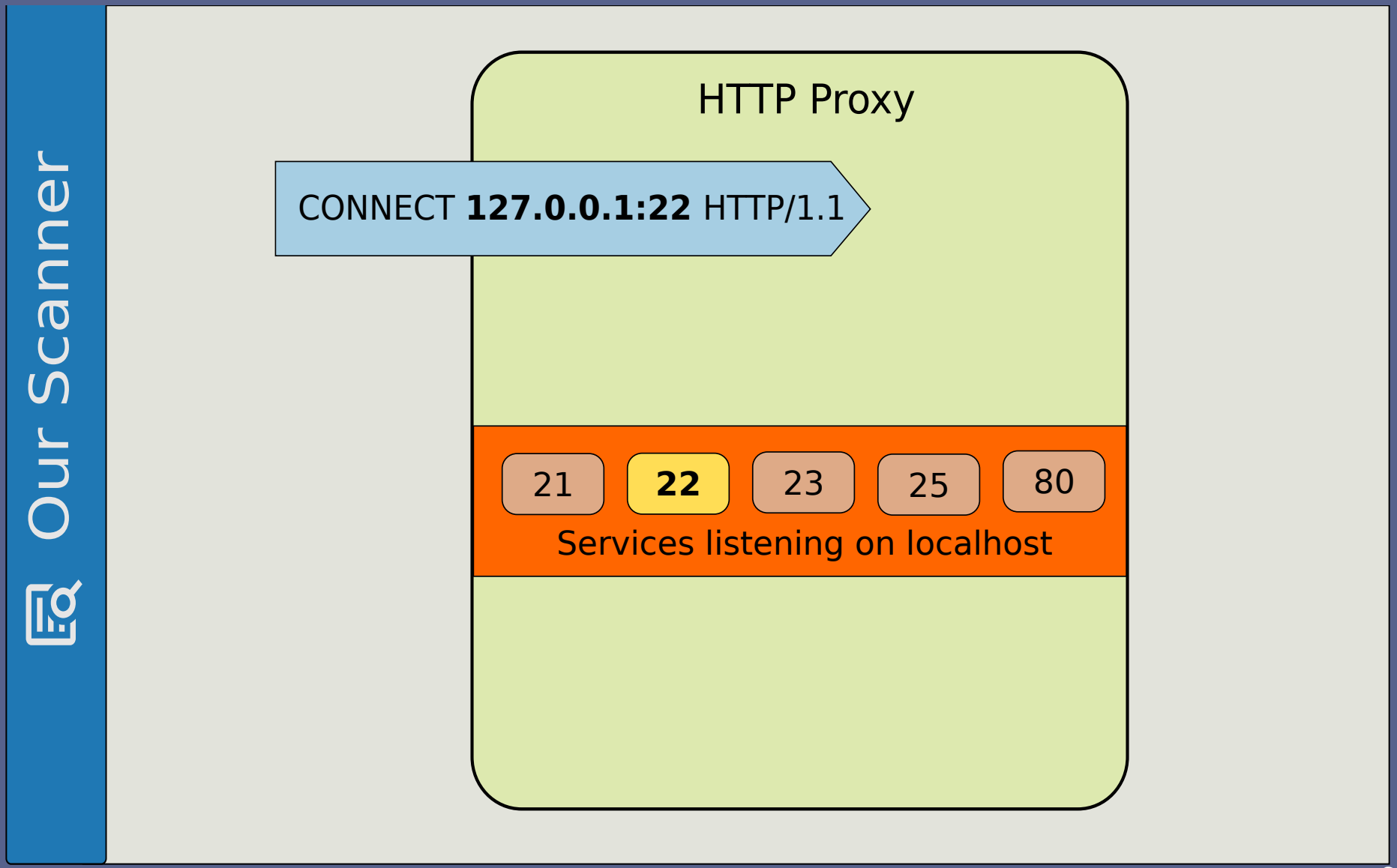
- Filter ingress 1900/UDP (common industry practice)

Internet Proxies

Proxies on the Internet

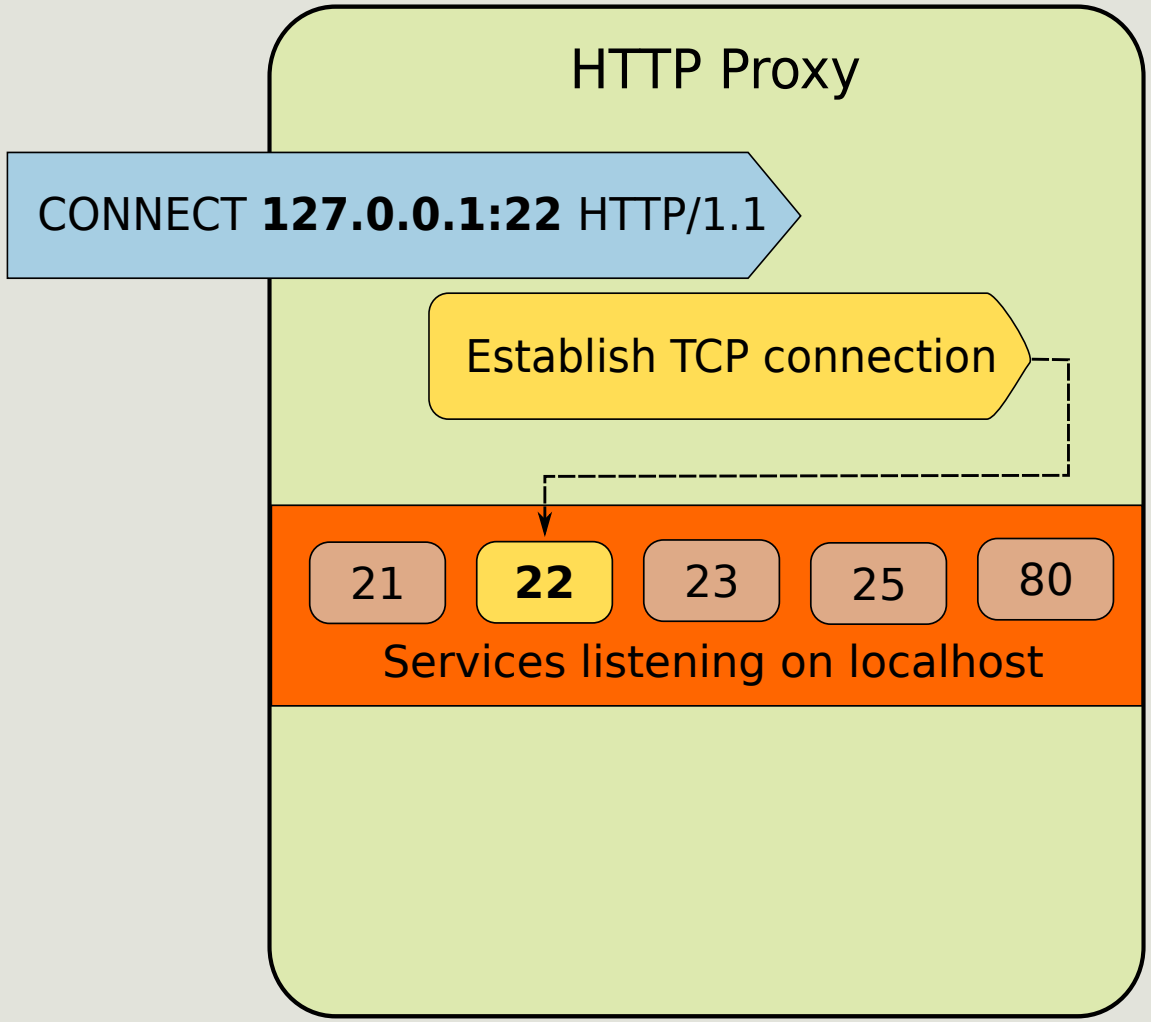
- Non-persistent, temporary relays
- We did an extensive analysis of the proxy ecosystem
- Found 690,000 proxies, **3% (20,000)** were open proxies!

Checking for Internal Access (on open proxies)



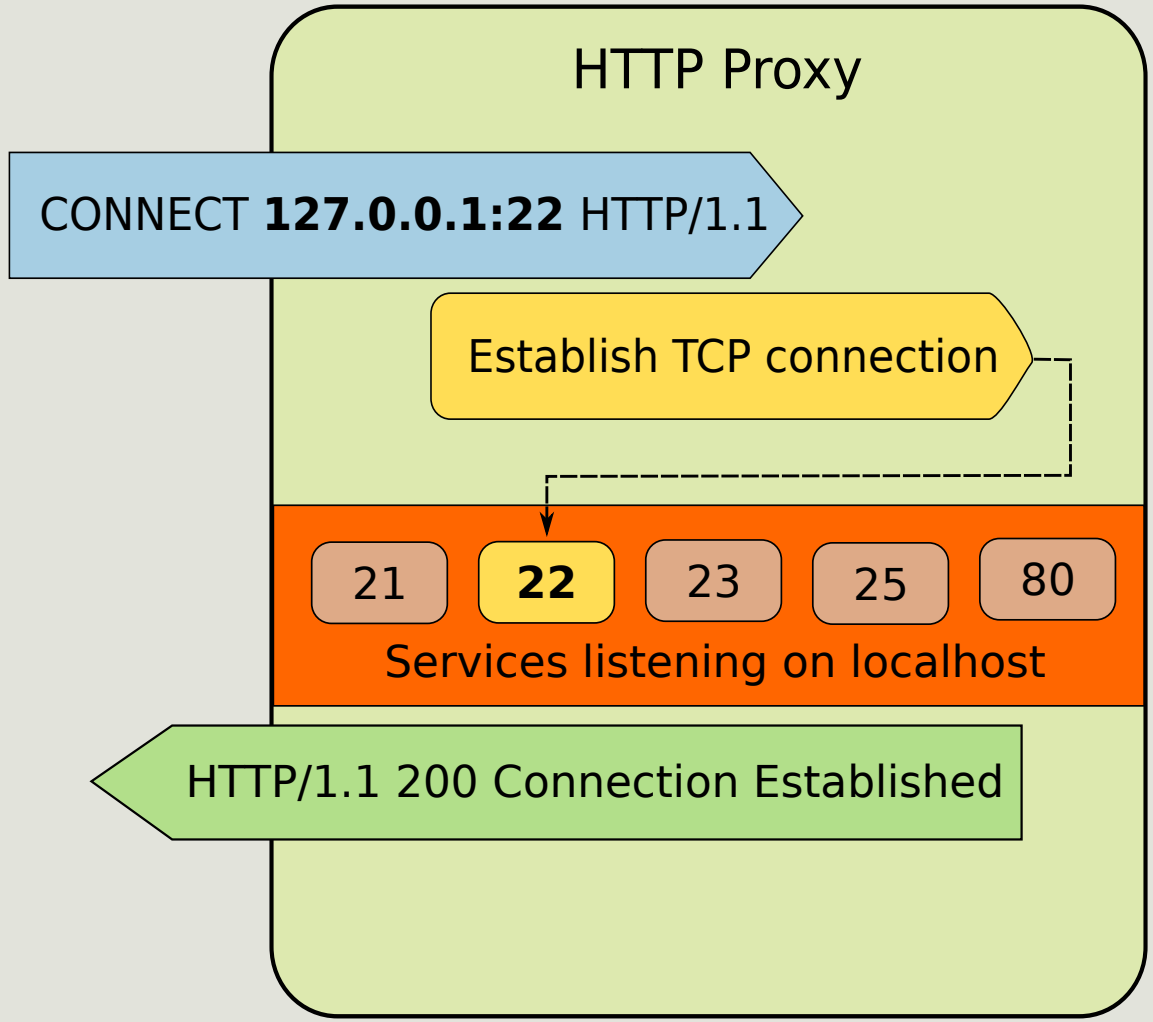
Checking for Internal Access (on open proxies)

Our Scanner



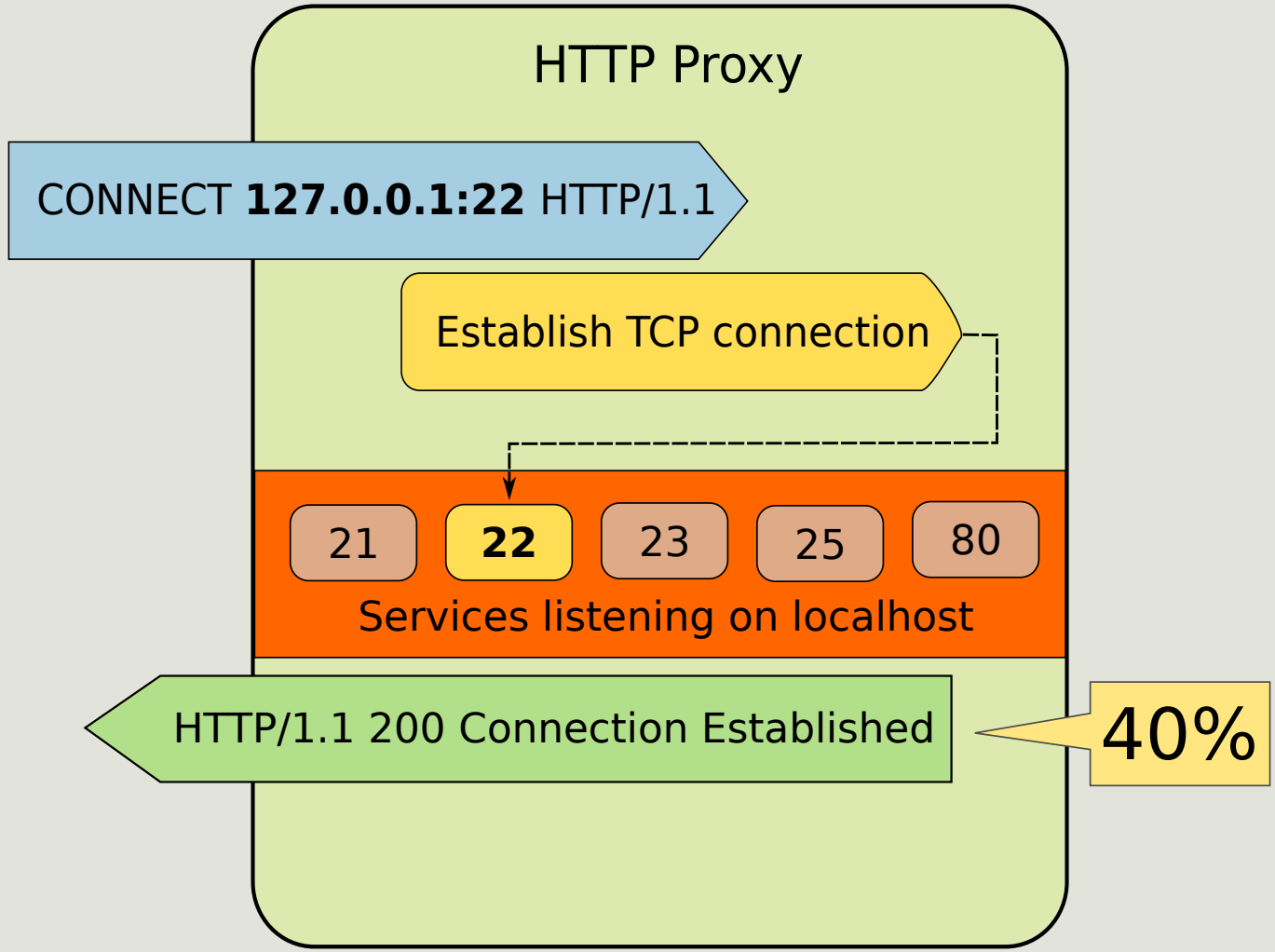
Checking for Internal Access (on open proxies)

Our Scanner

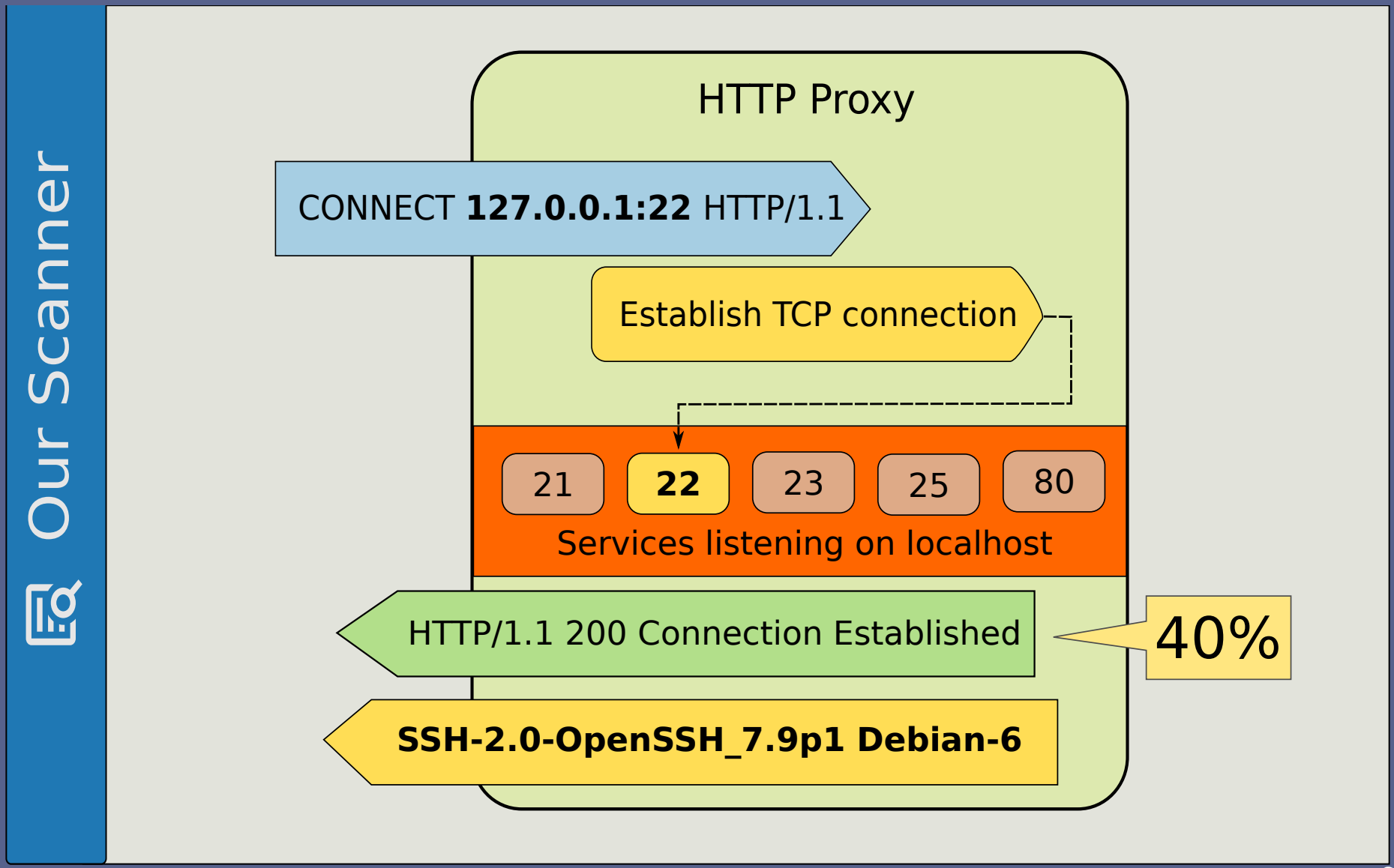


Checking for Internal Access (on open proxies)

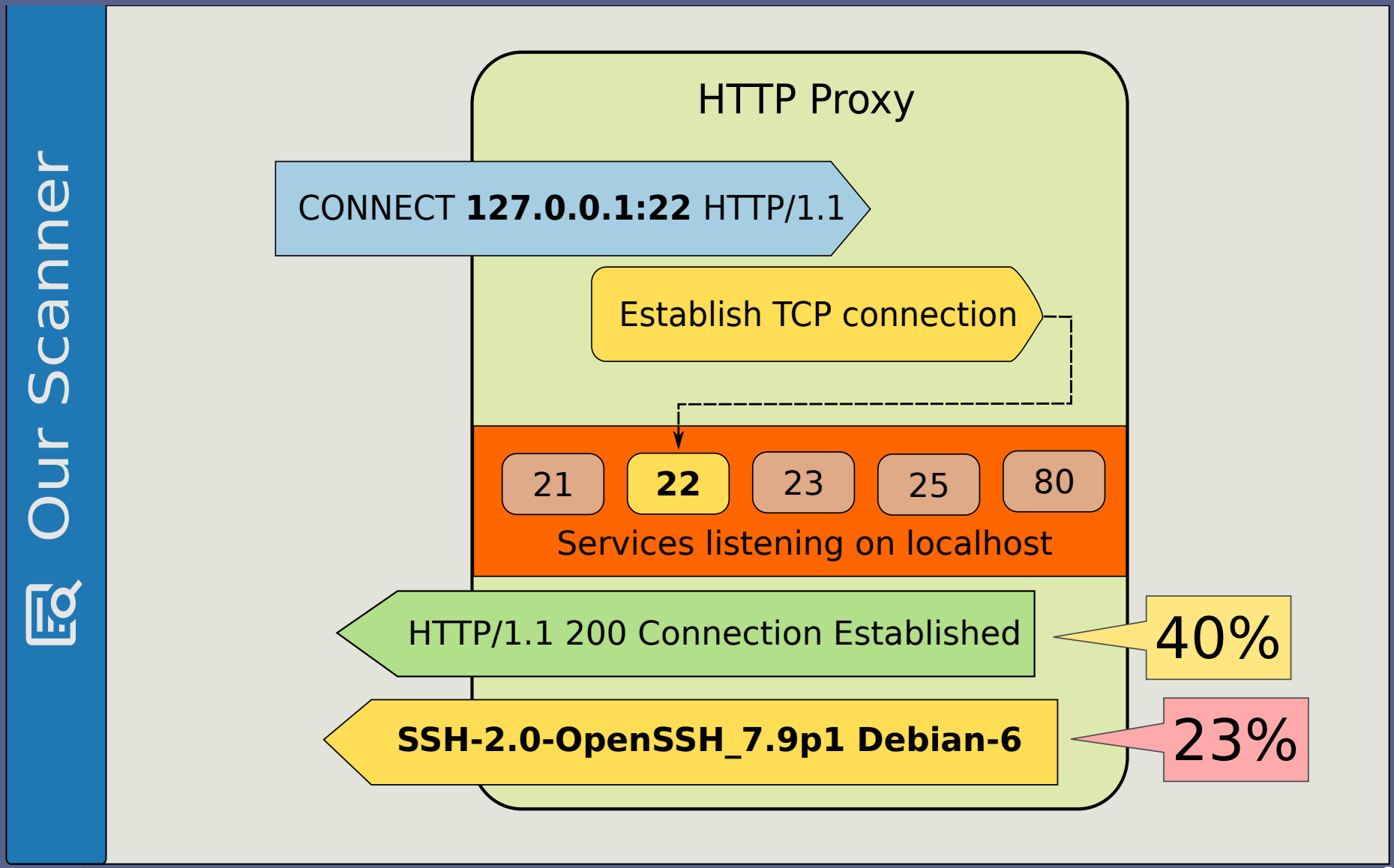
Our Scanner



Checking for Internal Access (on open proxies)



Checking for Internal Access (on open proxies)



Takeaways

- Two examples of protocols for crossing network boundaries
- Enabling **unwanted** access to internal networks
- At least one type is being actively exploited!

Thanks for your attention!

Takeaways

- Two examples of protocols for crossing network boundaries
- Enabling **unwanted** access to internal networks
- At least one type is being actively exploited!

Thanks for your attention!

https://github.com/RUB-SysSec/MiddleboxProtocolStudy/