



German
OWASP
Day 2024

SSRF: Attacks, Defense and Status Quo

MALTE WESSELS

- PhD Student @ IAS / TU Braunschweig
- Privacy @ Datenanfragen.de e.V.
- CTF @ CyberTaskForce Zero



IAS

INSTITUTE FOR
APPLICATION
SECURITY



Technische
Universität
Braunschweig

Link Previews

M

Malte Wessels

17:19

<https://unsplash.com/photos/kitten-lying-on-red-and-white-quatrefoil-textile-Sa1z1pEzjPI>

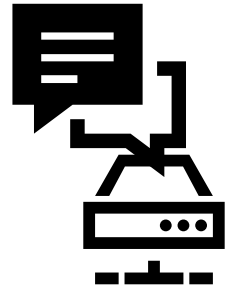


Photo by Jonathan Fink on Unsplash - @unsplash

This is Chip — Chip likes to sleep. We recently got two adorable 6 week old kittens and they absolutely love to wrestle, play and, of course, nap. This photo perfectly captures this young cat's chill personality and encourages us all to take a moment t...

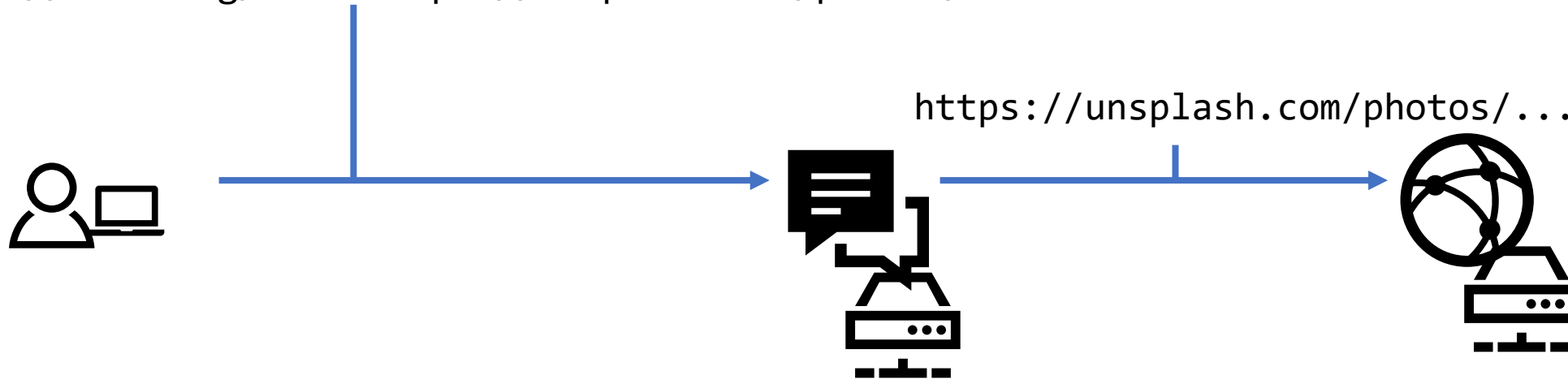
Link Previews

`https://chat.org/?url=https://unsplash.com/photos/...`



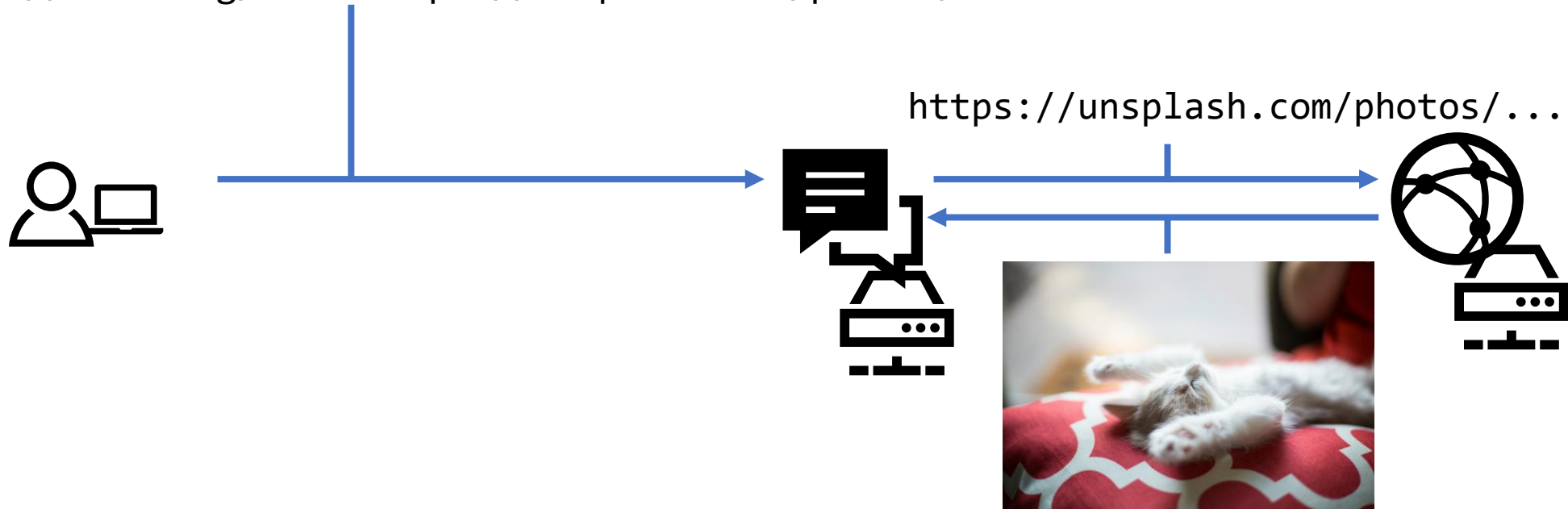
Link Previews

`https://chat.org/?url=https://unsplash.com/photos/...`



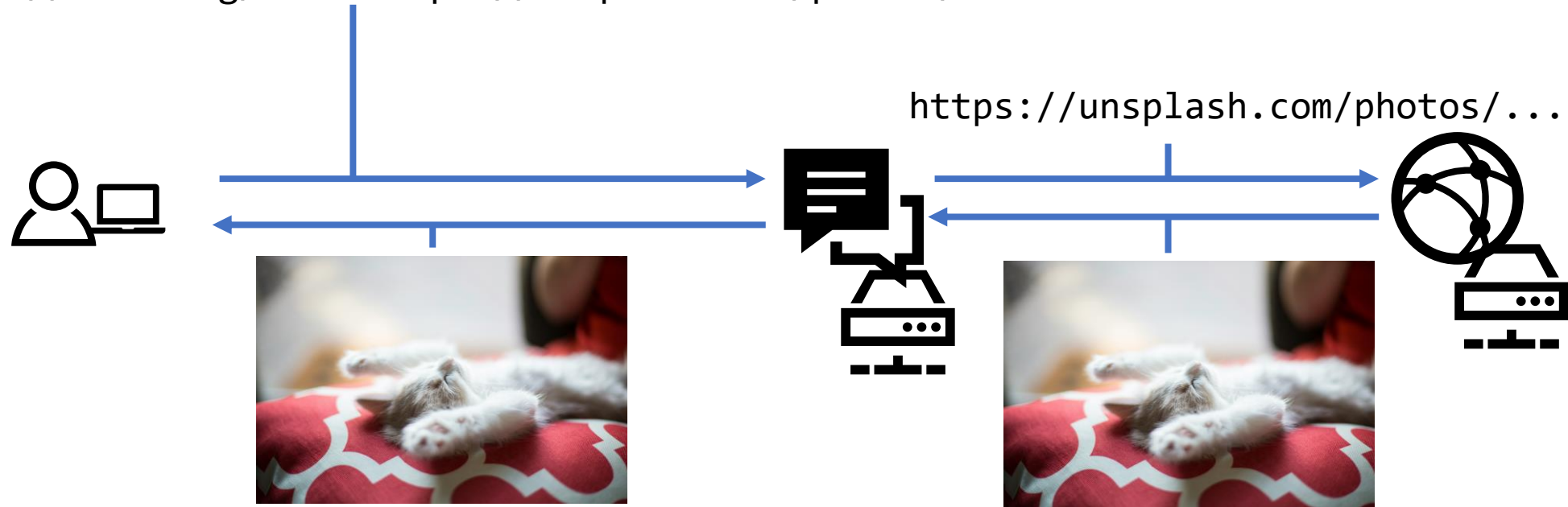
Link Previews

`https://chat.org/?url=https://unsplash.com/photos/...`



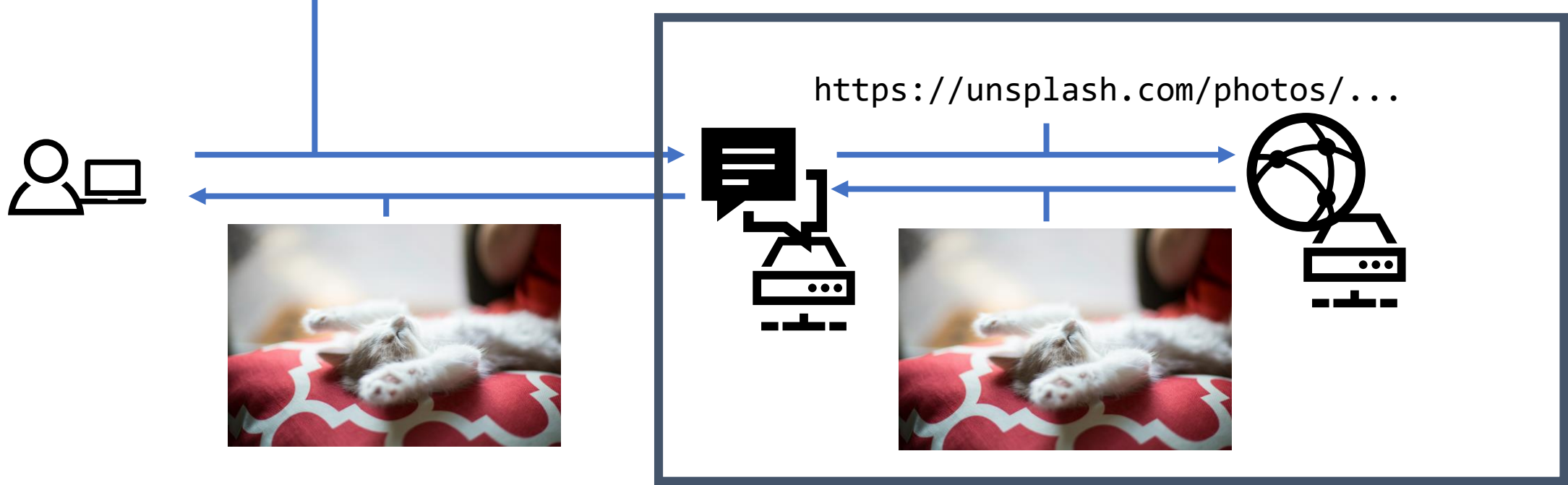
Link Previews

`https://chat.org/?url=https://unsplash.com/photos/...`



Link Previews

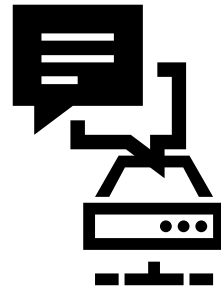
`https://chat.org/?url=https://unsplash.com/photos/...`



Server-Side Request

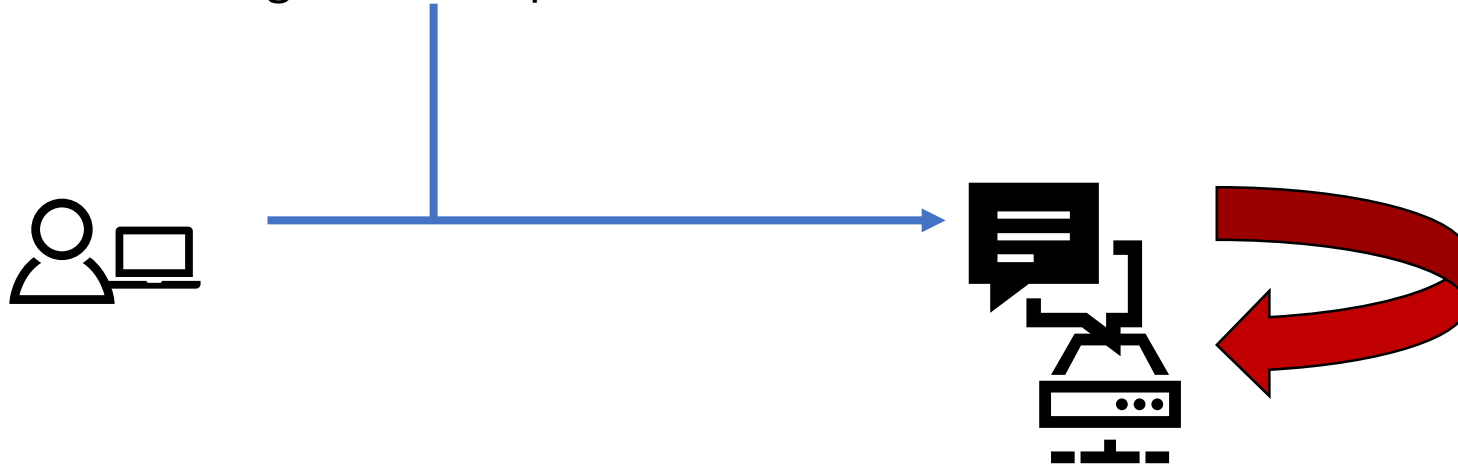
Link Previews

`https://chat.org/?url=http://localhost/...`



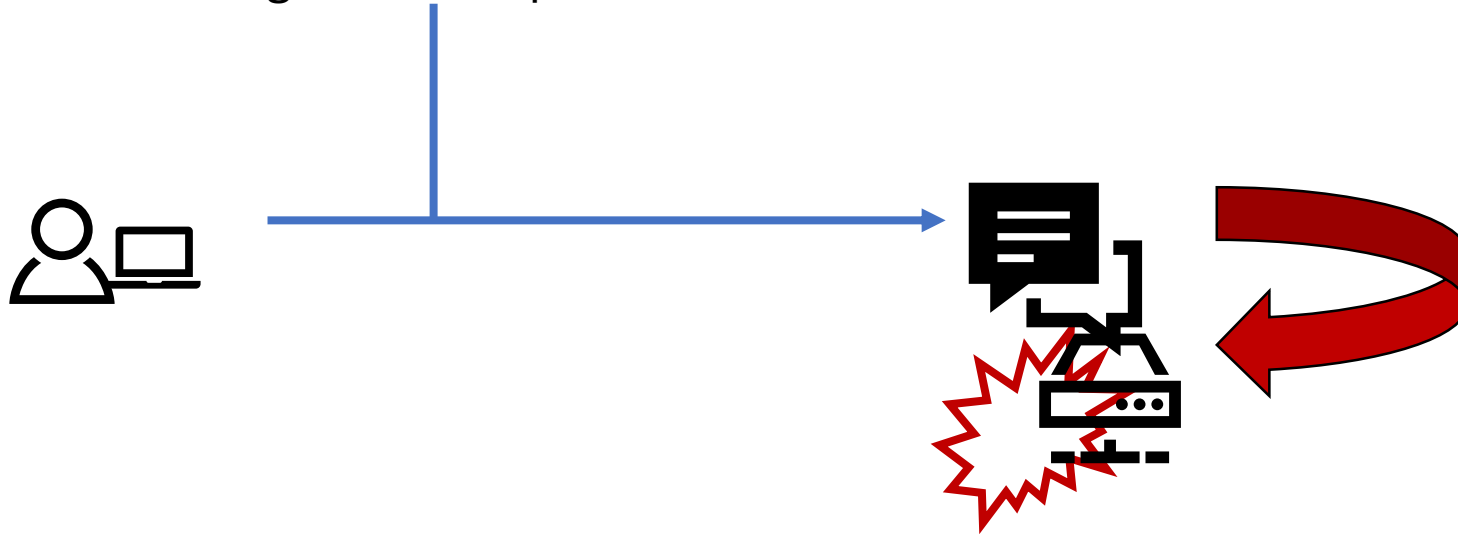
Link Previews

`https://chat.org/?url=http://localhost/...`

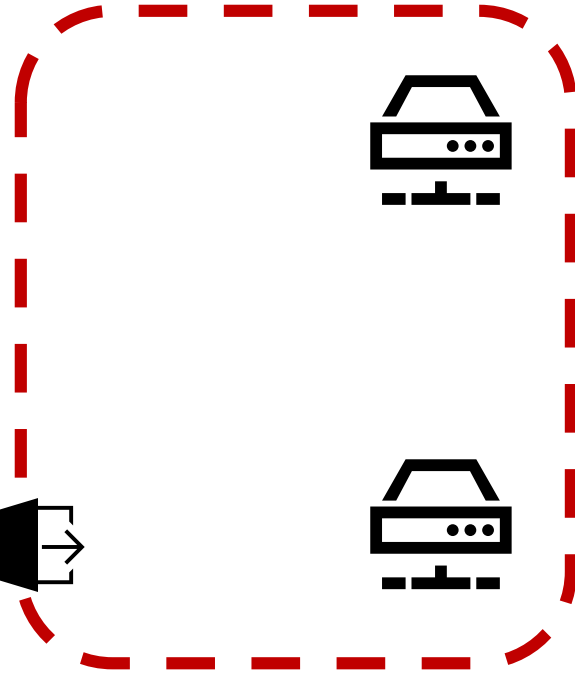
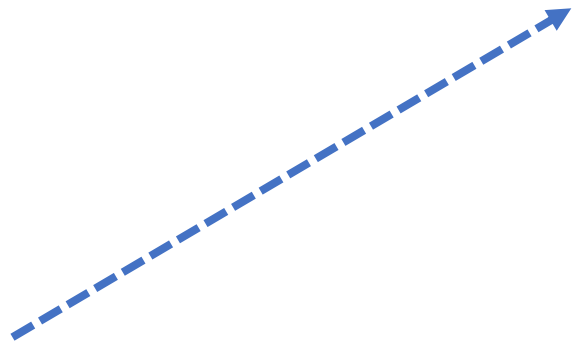


Link Previews

`https://chat.org/?url=http://localhost/...`



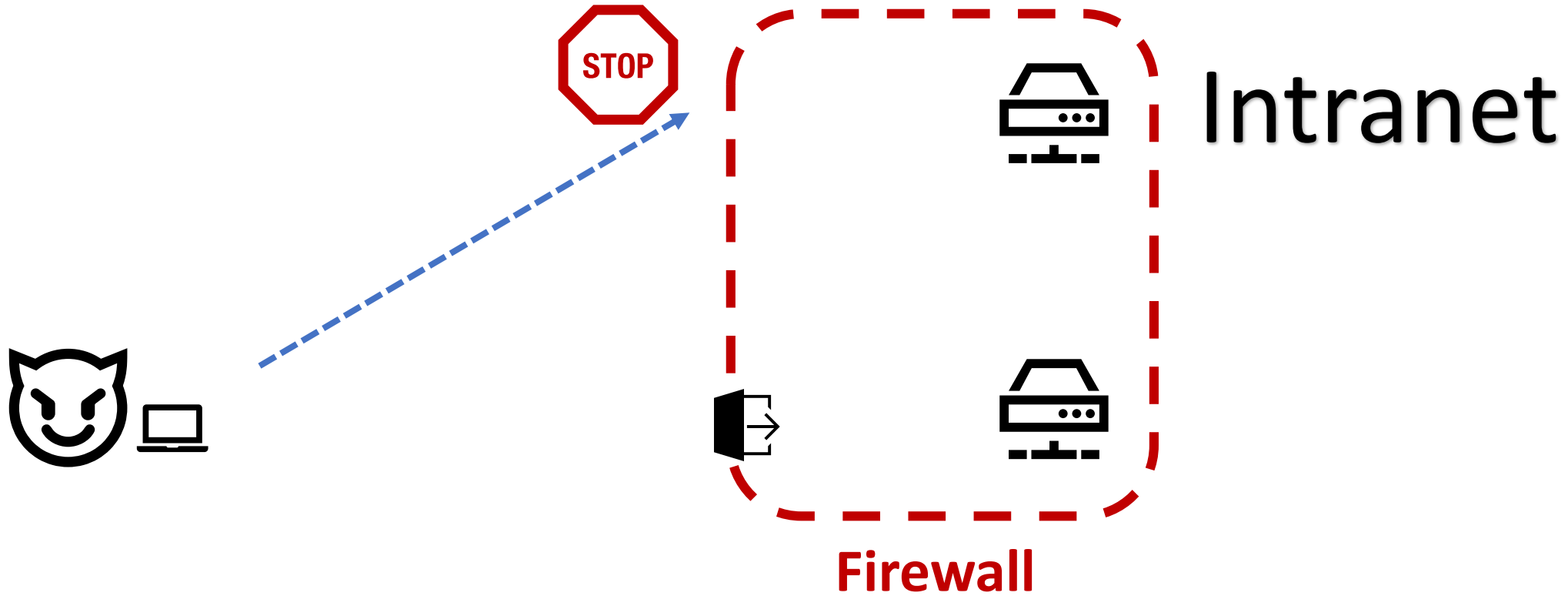
Firewall Bypass



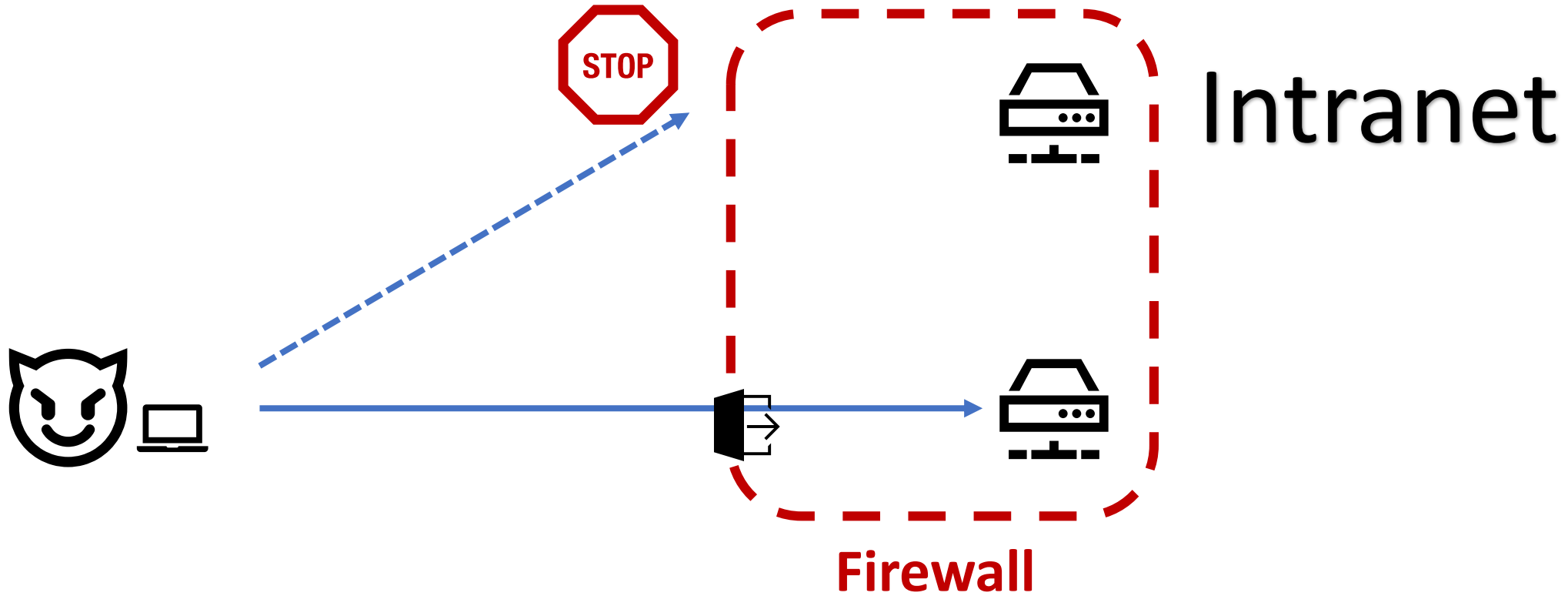
Intranet

Firewall

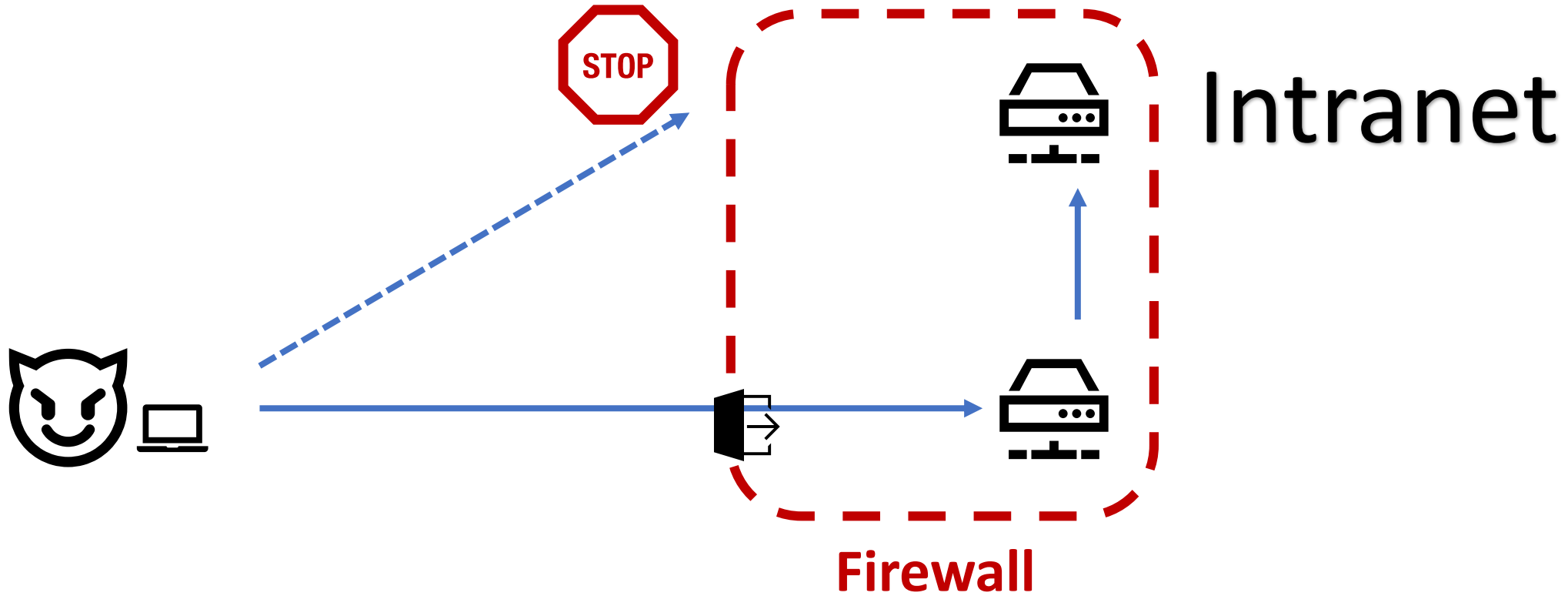
Firewall Bypass



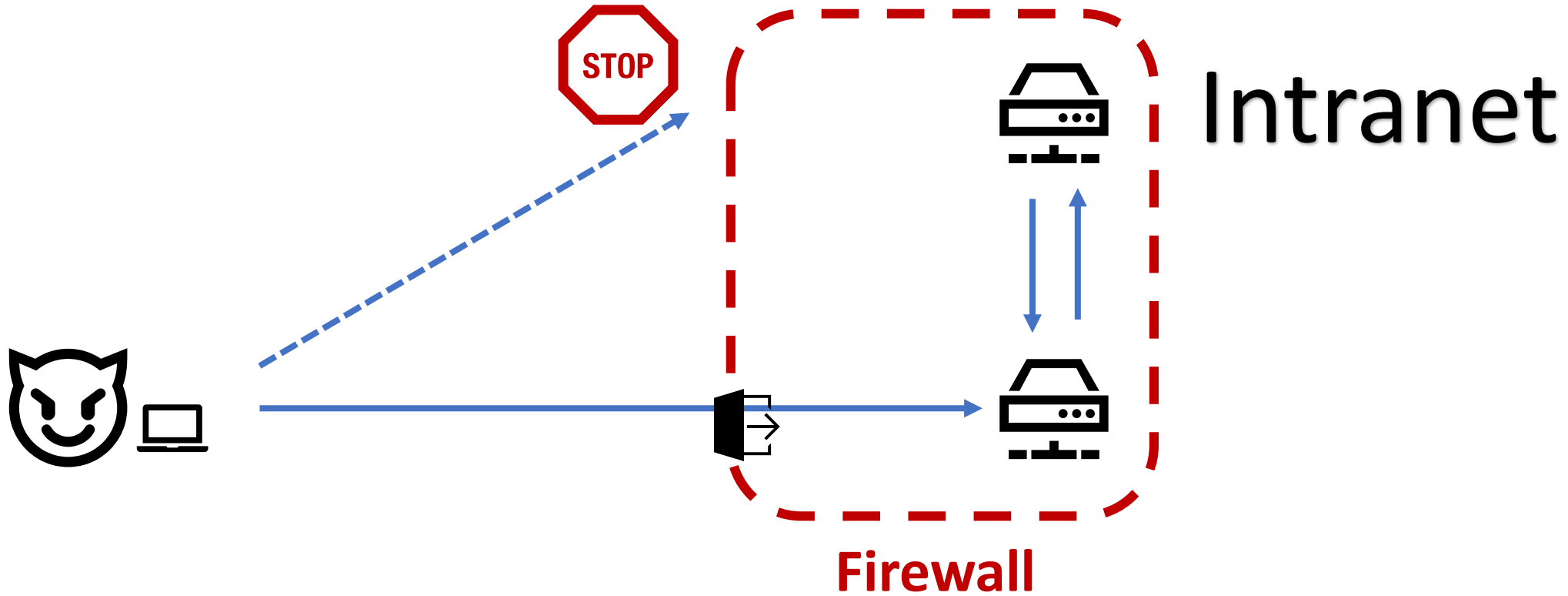
Firewall Bypass



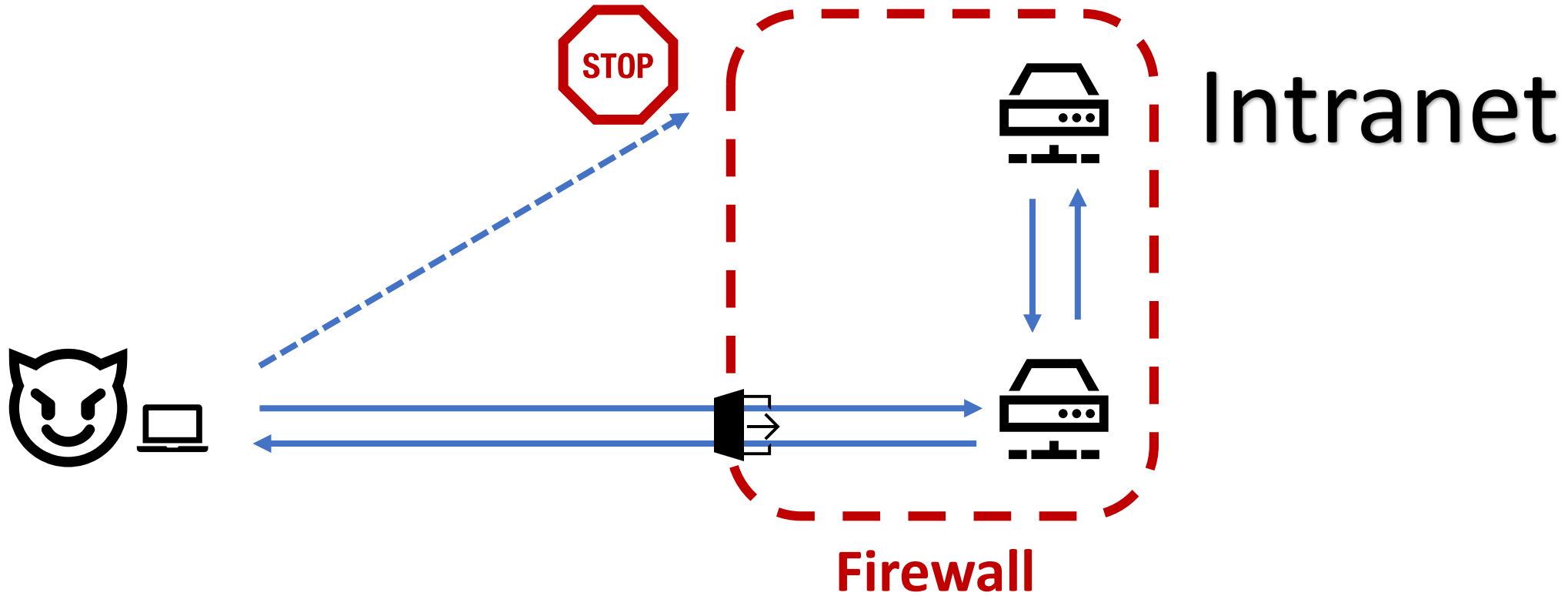
Firewall Bypass



Firewall Bypass



Firewall Bypass



Allowlist Case

- Complete list of trusted hosts

Allowlist Case

- Complete list of trusted hosts
- Use one good URL parser

Allowlist Case

- Complete list of trusted hosts
- Use one good URL parser
- Compare host of URL against list

Allowlist Case

- Complete list of trusted hosts
- Use one good URL parser
- Compare host of URL against list
- Not applicable for many use cases

Allowlist Case

- Complete list of trusted hosts
- Use one good URL parser
- Compare host of URL against list
- Not applicable for many use cases
 - E.g. URL previews, webhooks, etc.
- → Deny listing

String-based Defense?

String-based Defense?

- `str_contains($input, "localhost")`

String-based Defense?

- `str_contains($input, "localhost")`
 - `127.0.0.1`

String-based Defense?

- `str_contains($input, "localhost")`
 - `127.0.0.1`
- `str_contains($input, "127.0.0.1")`

String-based Defense?

- `str_contains($input, "localhost")`
 - `127.0.0.1`
- `str_contains($input, "127.0.0.1")`
 - `http://0x7F000001`, etc.

String-based Defense?

- `str_contains($input, "localhost")`
 - `127.0.0.1`
- `str_contains($input, "127.0.0.1")`
 - `http://0x7F000001`, etc.
- Unicode

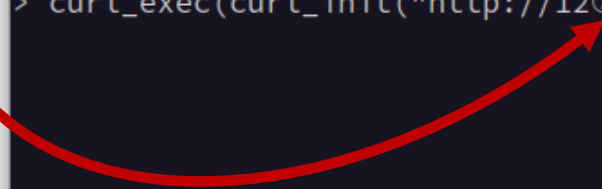
String-based Defense?

- `str_contains($input, "localhost")`
 - `127.0.0.1`
- `str_contains($input, "127.0.0.1")`
 - `http://0x7F000001`, etc.
- Unicode

String-based Defense?

```
malte@malte-xps159520: tmux
malte@malte-xps159520 ~ % ncat -k -l 0.0.0.0 -p 9000

malte@malte-xps159520 ~ % psysh
Psy Shell v0.12.0 (PHP 8.3.2 - cli) by Justin Hileman
> curl_exec(curl_init("http://127.0.0.1:9000"));
```



[0] 0:php*

"malte-xps159520" 14:22 19-Feb-24

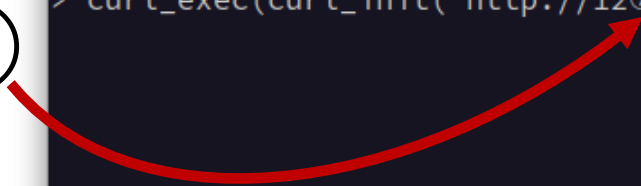
String-based Defense?

```
malte@malte-xps159520: tmux
malte@malte-xps159520 ~ % ncat -k -l 0.0.0.0 -p 9000
GET / HTTP/1.1
Host: 127.0.0.1:9000
Accept: */*

malte@malte-xps159520 ~ % psysh
Psy Shell v0.12.0 (PHP 8.3.2 - cli) by Justin Hileman
> curl_exec(curl_init("http://127.0.0.1:9000"));

[0] 0:php* "malte-xps159520" 14:22 19-Feb-24
```

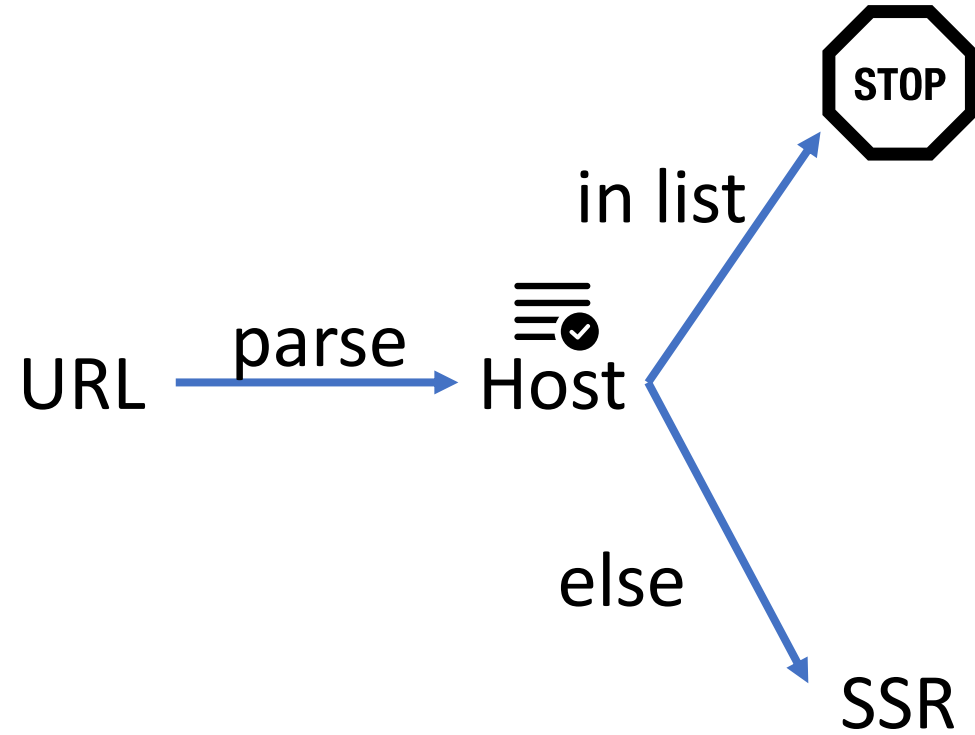
7



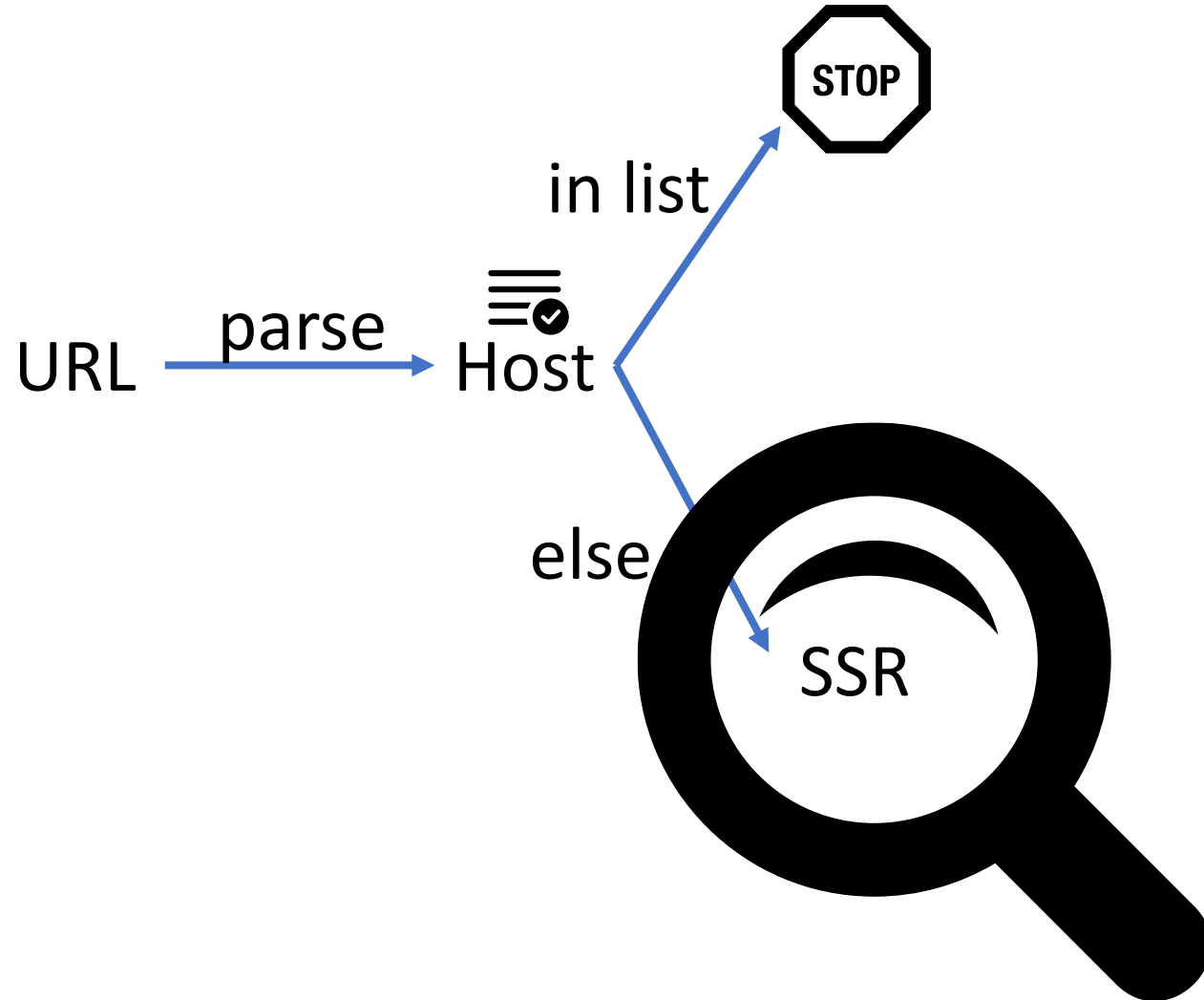
Host Denylist



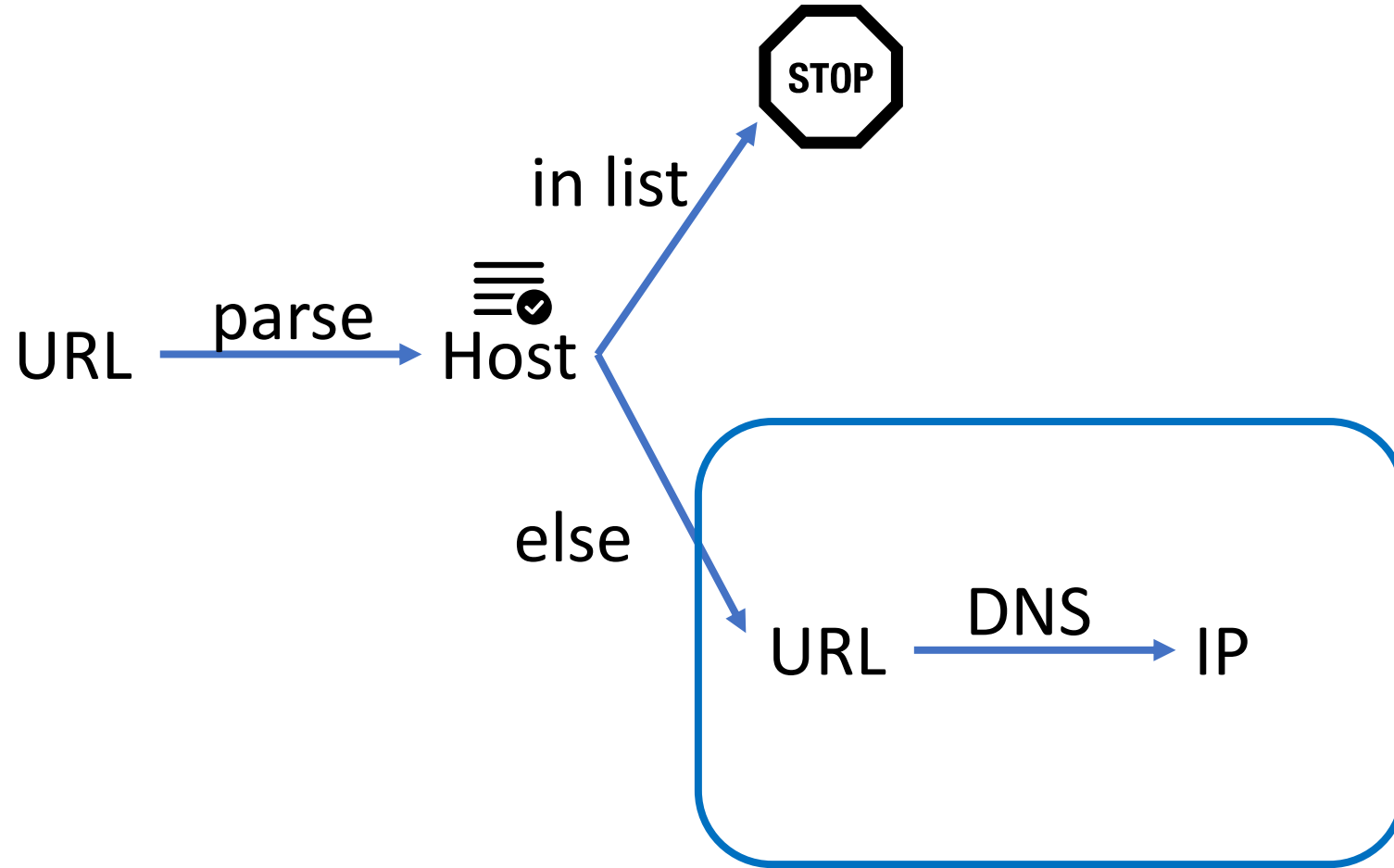
Host Denylist



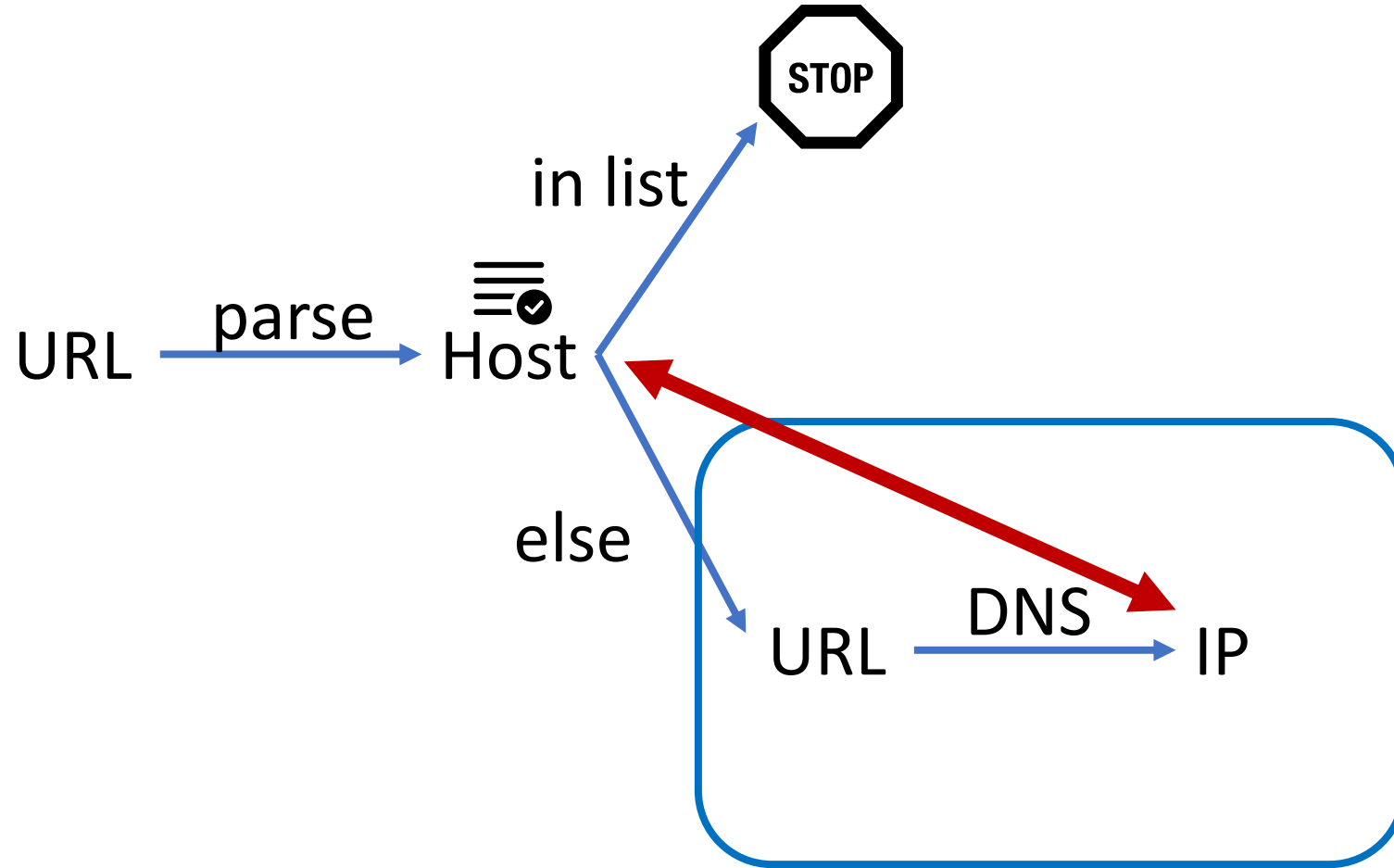
Host Denylist



Host Denylist



Host Denylist



Host Denylists Don't Work

```
sh-5.2$ ping fbi.com
PING fbi.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.034 ms
```


Host Denylists Don't Work

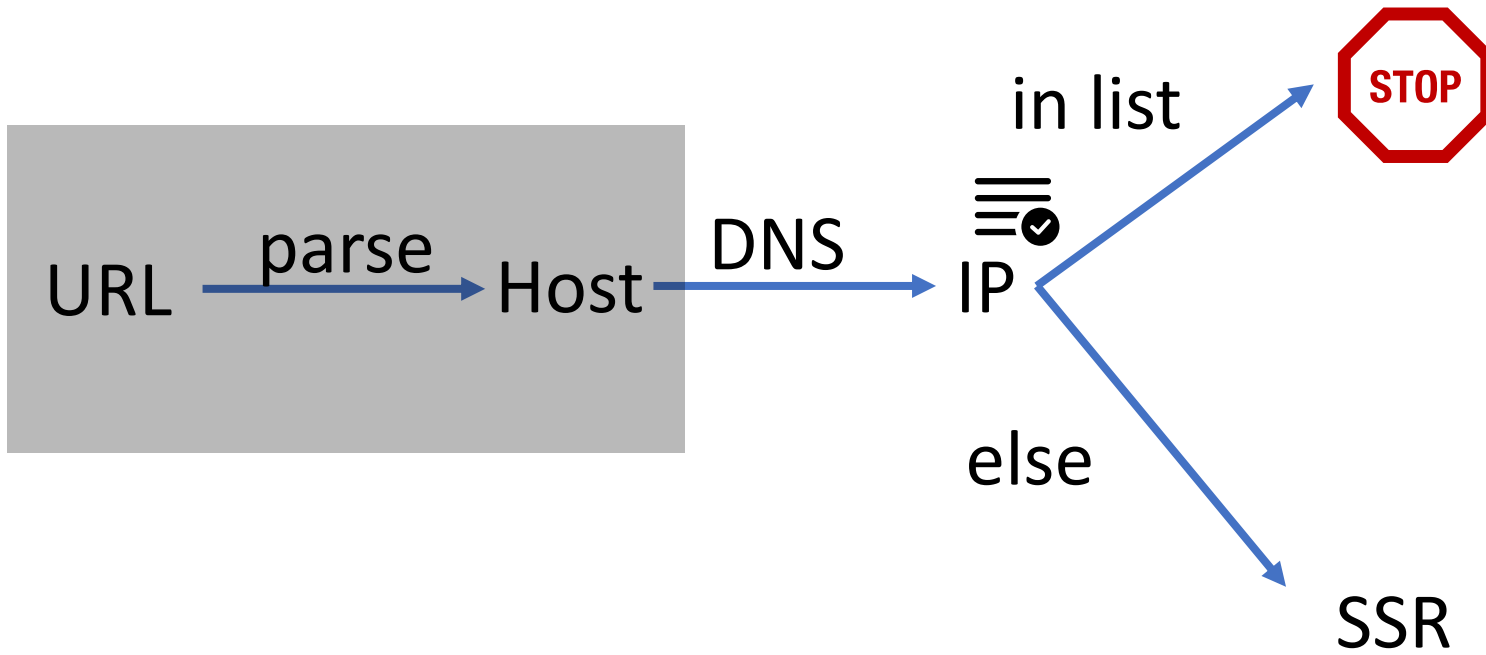
```
sh-5.2$ ping fbi.com
```

```
PING fbi.com (127.0.0.1) 56(84) bytes of data.
```

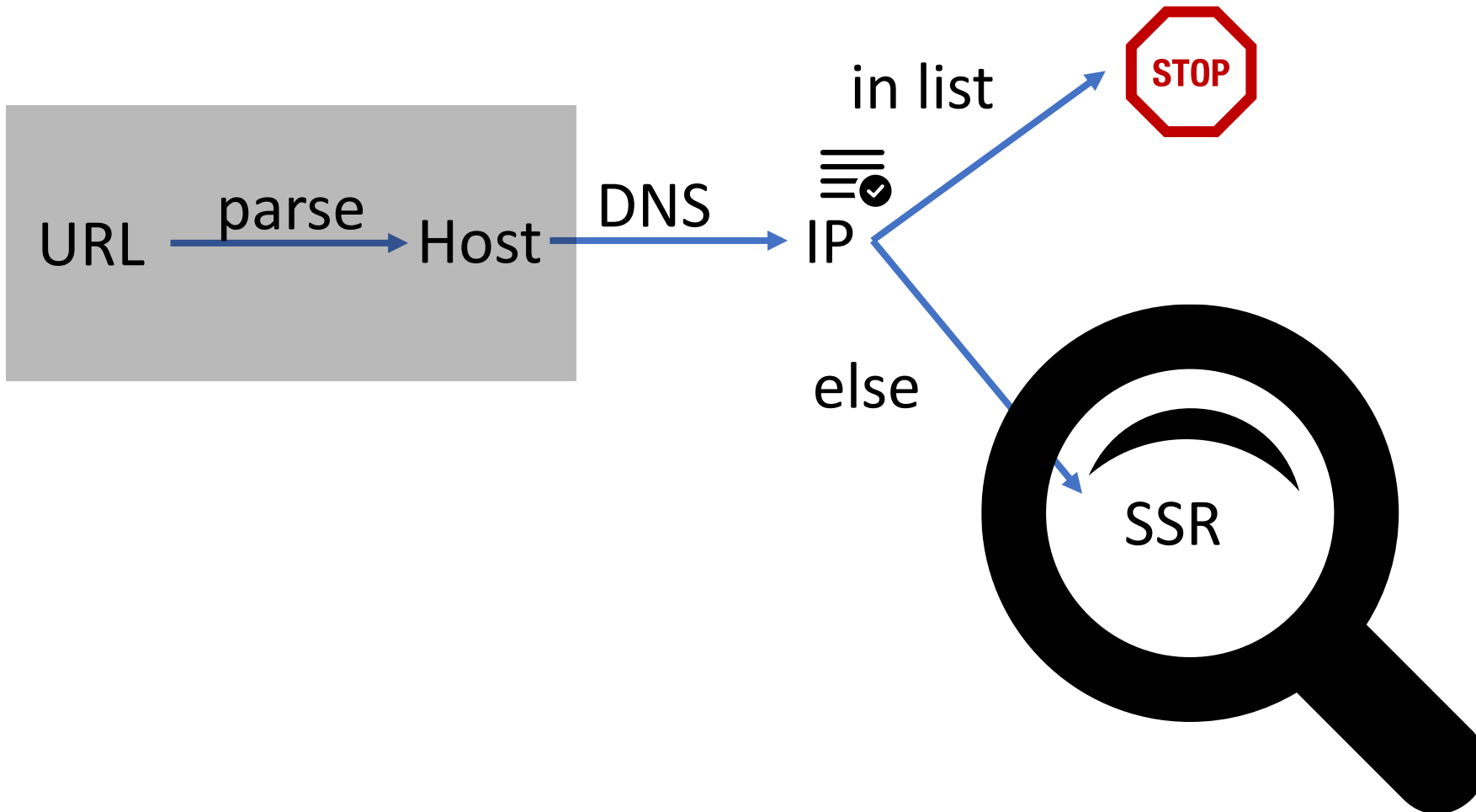
```
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.039 ms
```

```
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.034 ms
```

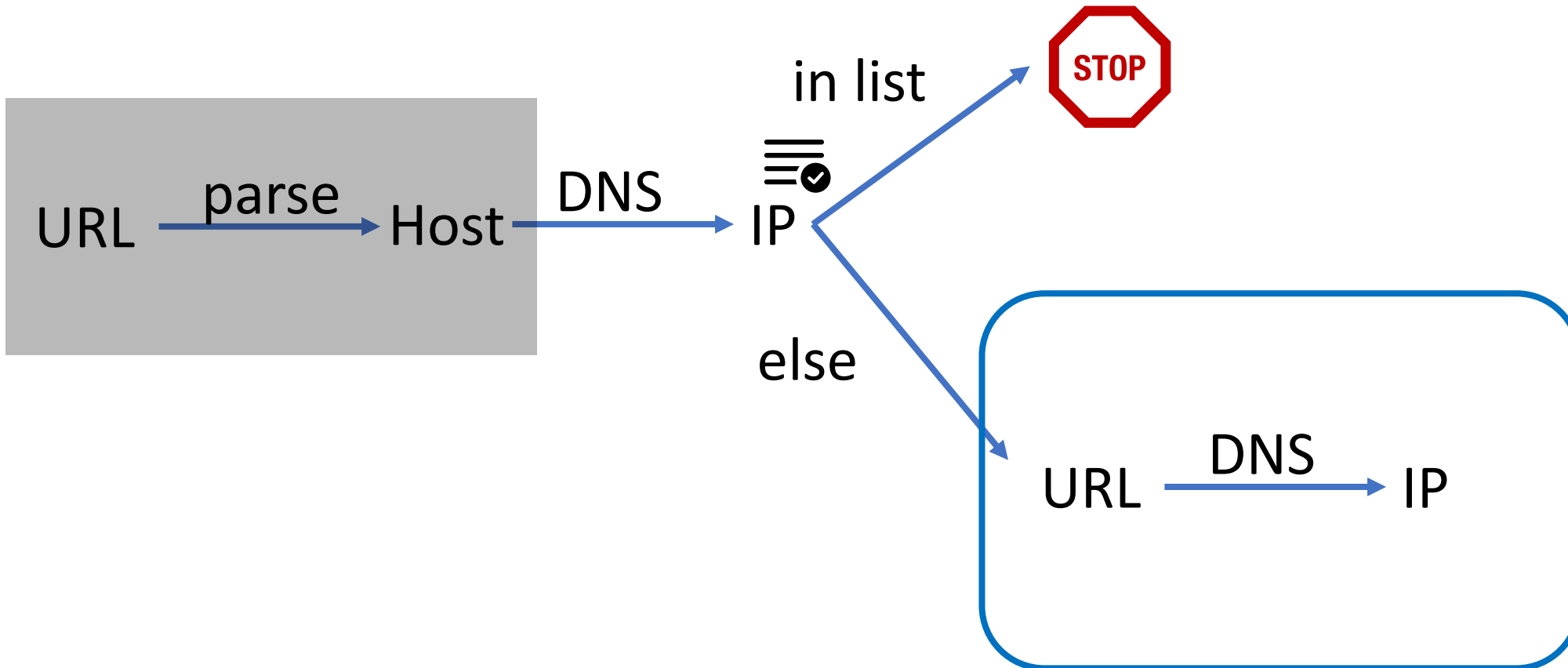
Fix: DNS



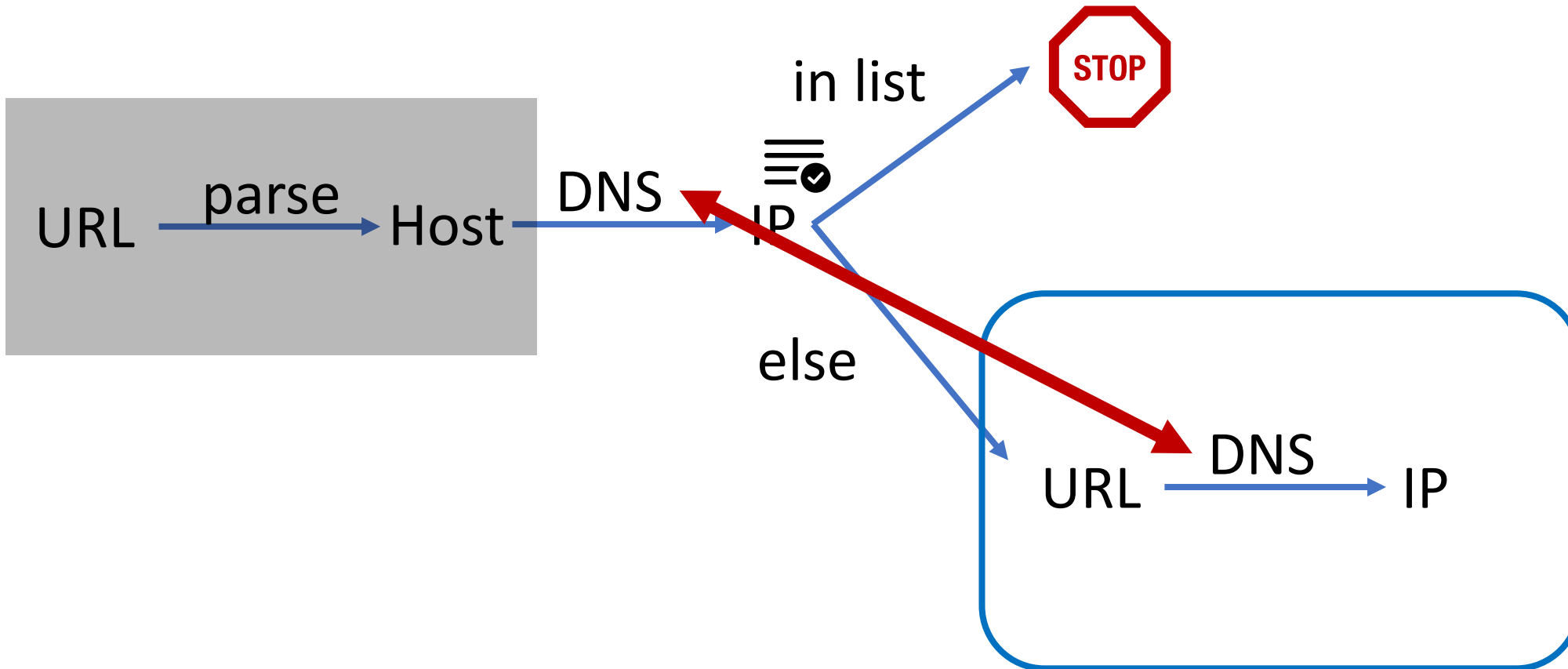
Fix: DNS



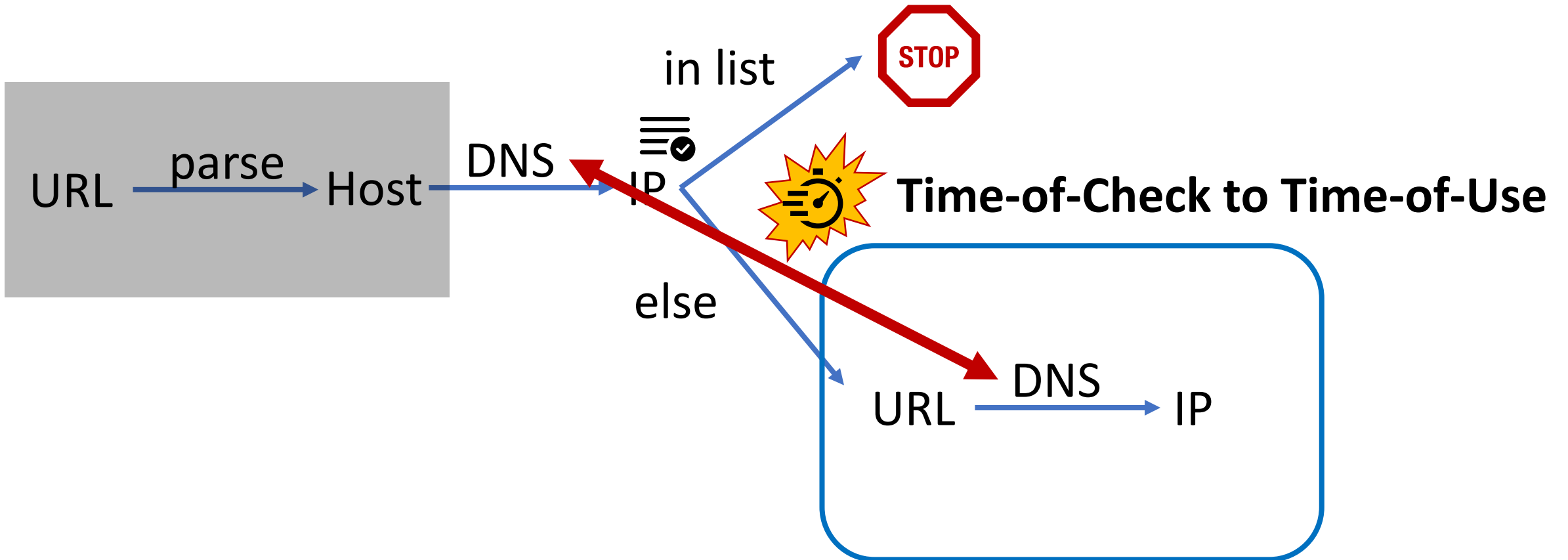
Fix: DNS?



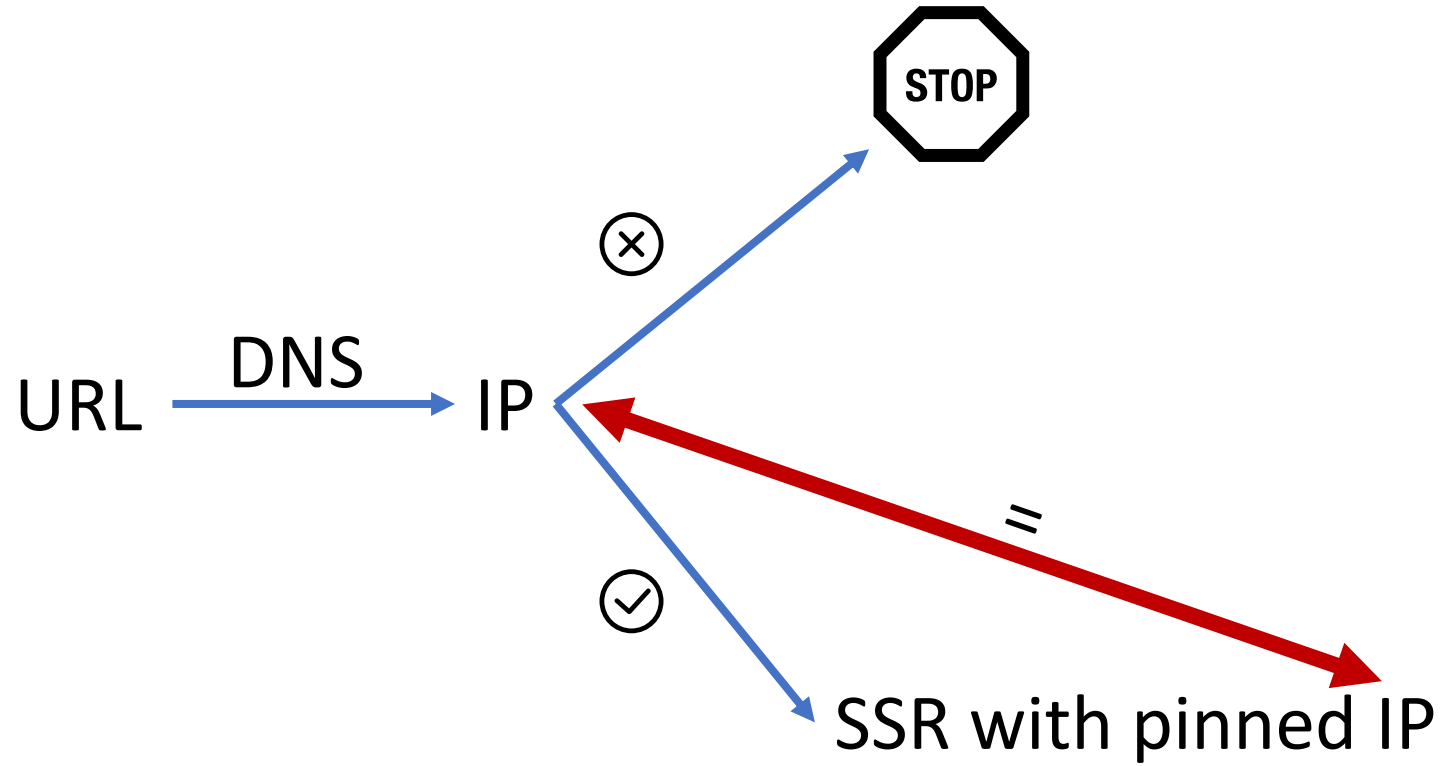
Fix: DNS?



Fix: DNS?



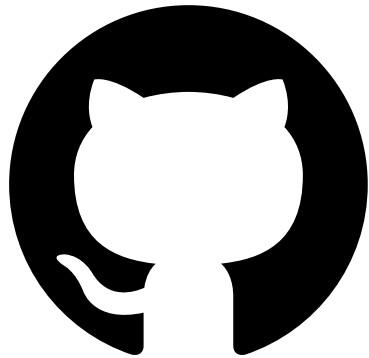
DNS Pinning!



Status Quo of Defenses in the Wild



76 % of websites use PHP



30k repositories with PHP

Frameworks

Framework	SSRF-Defense available?
WordPress	Yes, broken
Laravel	No
Symfony	Yes
CakePHP	No
FuelPHP	No
Windwalker	No
Zend	No
Laminas	No
CodeIgnite	No
PHPixie	No

HTTP-Clients

HTTP-Client	Defense available?
PHP std lib	No
PHP curl extension	No
Guzzle	No
PECL HTTP	No
ReactPHP Sockets	No
WordPress Requests	No
Buzz	No
Httpful	No
SafeCurl, SafeURL	Yes
HTTPLug	As Plugin

Prevalence Study

(30k repositories with PHP)

Prevalence Study

4

(30k repositories with PHP)

Static Dataflow Analysis

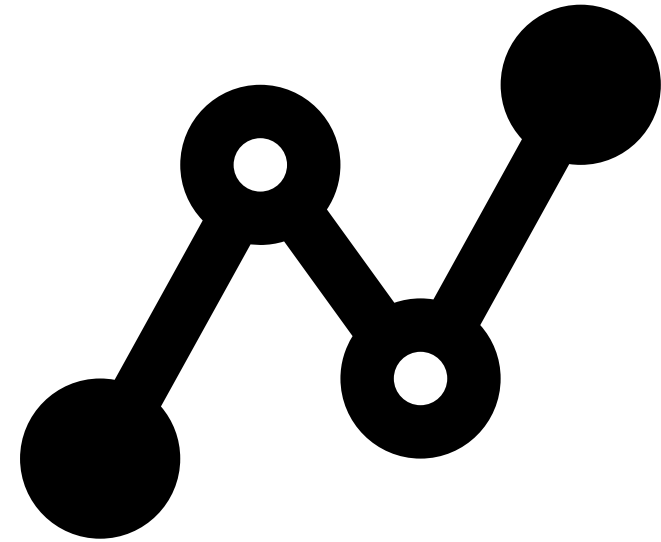
Static Dataflow Analysis

```
<?php  
if(isset($x)) {  
    file_get_contents($x);  
}  
echo "ack";
```



Static Dataflow Analysis

```
<?php  
if(isset($x)) {  
    file_get_contents($x);  
}  
echo "ack";
```



Results

Results

2

Conclusion

We, as a security community, are aware of the risks and solutions.

Conclusion

We, as a security community, are aware of the risks and solutions.

But devs get it wrong.

Practical Take-Aways

- Compile a solid [allow|deny] list

Practical Take-Aways

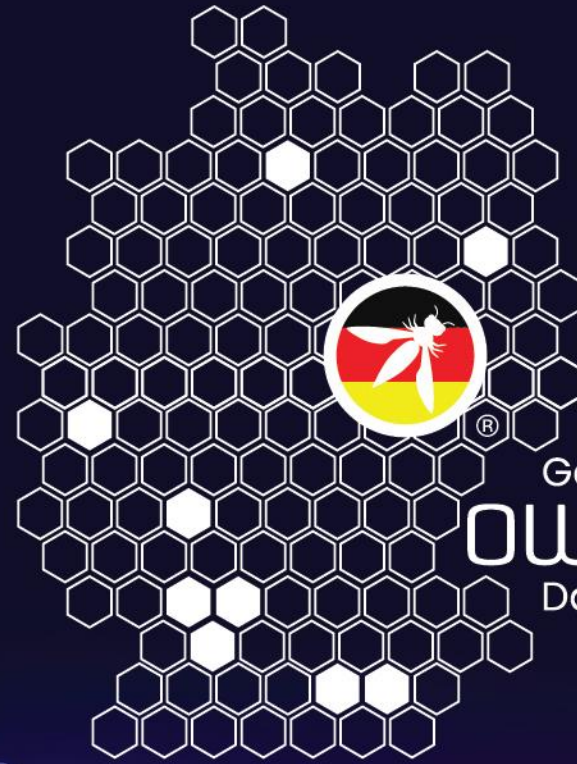
- Compile a solid [allow|deny] list
- Case A: Allow list → Pretty secure

Practical Take-Aways

- Compile a solid [allow|deny] list
- Case A: Allow list → Pretty secure
- Case B: Deny list → Use DNS pinning!

Practical Take-Aways

- Compile a solid [allow|deny] list
- Case A: Allow list → Pretty secure
- Case B: Deny list → Use DNS pinning!
- What we did not talk about:
 - Configure your clients! (HTTPS only, no redirects, ...)
 - Non-application level
 - Network segmentation, etc.
 - ...



German
OWASP
Day 2024

THANK
YOU!



@maltee:chaos.social



malte.wessels@tu-braunschweig.de



/in/malte-wessels