The Margrave Tool for Firewall Analysis

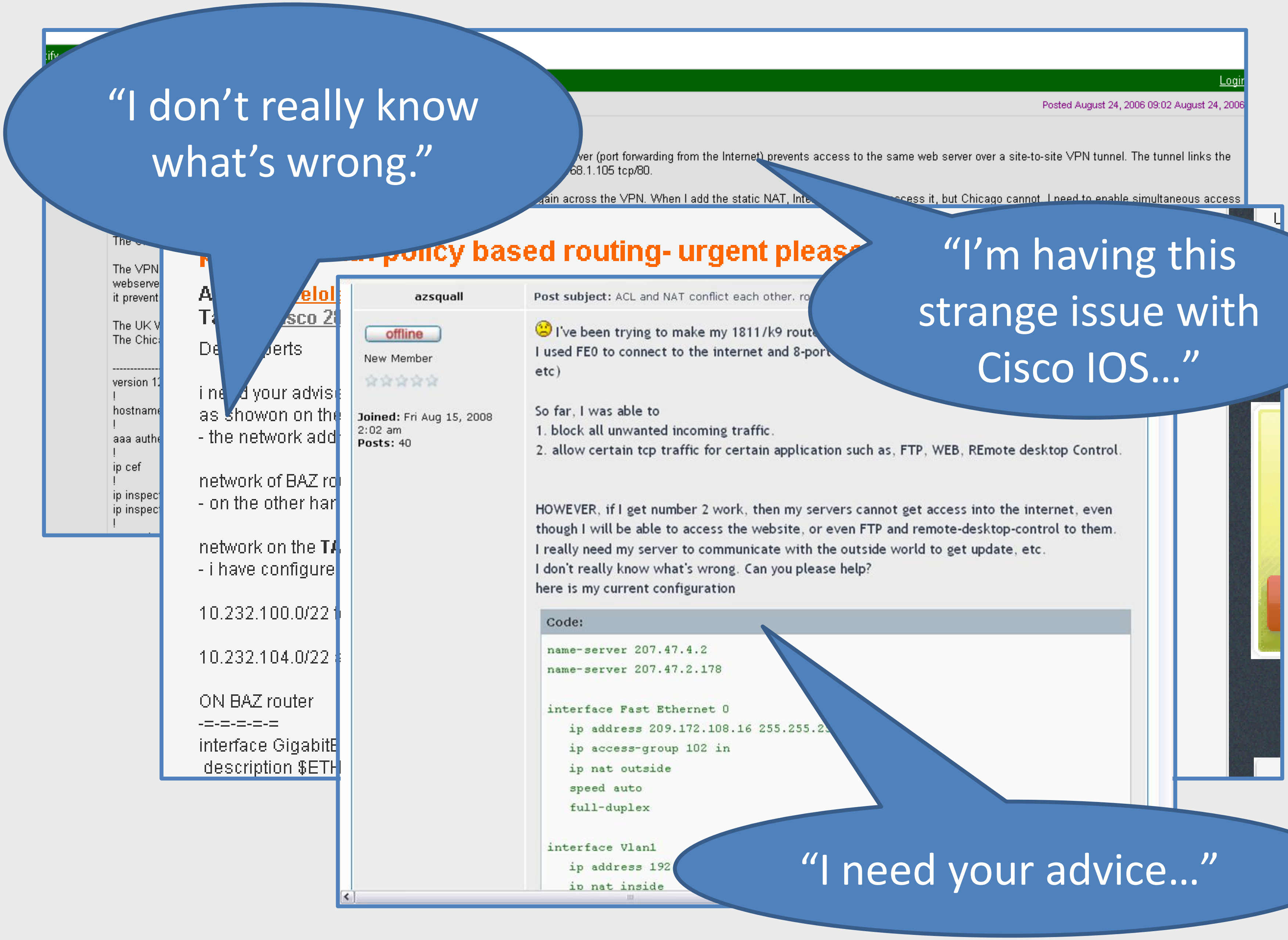
Tim Nelson (WPI), Christopher Barratt (Brown),
Daniel J. Dougherty (WPI), Kathi Fisler (WPI)
and Shriram Krishnamurthi (Brown)

…and other dens of iniquity

"I don't really know what's wrong."

"I'm having this strange issue with Cisco IOS…"

"I need your advice…"



Login

Posted August 24, 2006 09:02 August 24, 2006

ver (port forwarding from the Internet) prevents access to the same web server over a site-to-site VPN tunnel. The tunnel links the
68.1.105 tcp/80.

gain across the VPN. When I add the static NAT, Inte ccess it, but Chicago cannot. I need to enable simultaneous access

The

The VPN
webserve
it prevent

The UK V
The Chic

```
-------------
version 12
!
hostname
!
aaa authe
!
ip cef
!
ip inspec
ip inspec
!
```

policy based routing- urgent pleas

A elol
T sco 2

De perts

i ne d your advise
as showon on the
- the network add

network of BAZ ro
- on the other han

network on the TA
- i have configure

10.232.100.0/22

10.232.104.0/22

ON BAZ router
-=-=-=-=-=
interface GigabitE
description $ETH

azsquall

offline

New Member

☆☆☆☆☆

Joined: Fri Aug 15, 2008 2:02 am
Posts: 40

Post subject: ACL and NAT conflict each other. ro

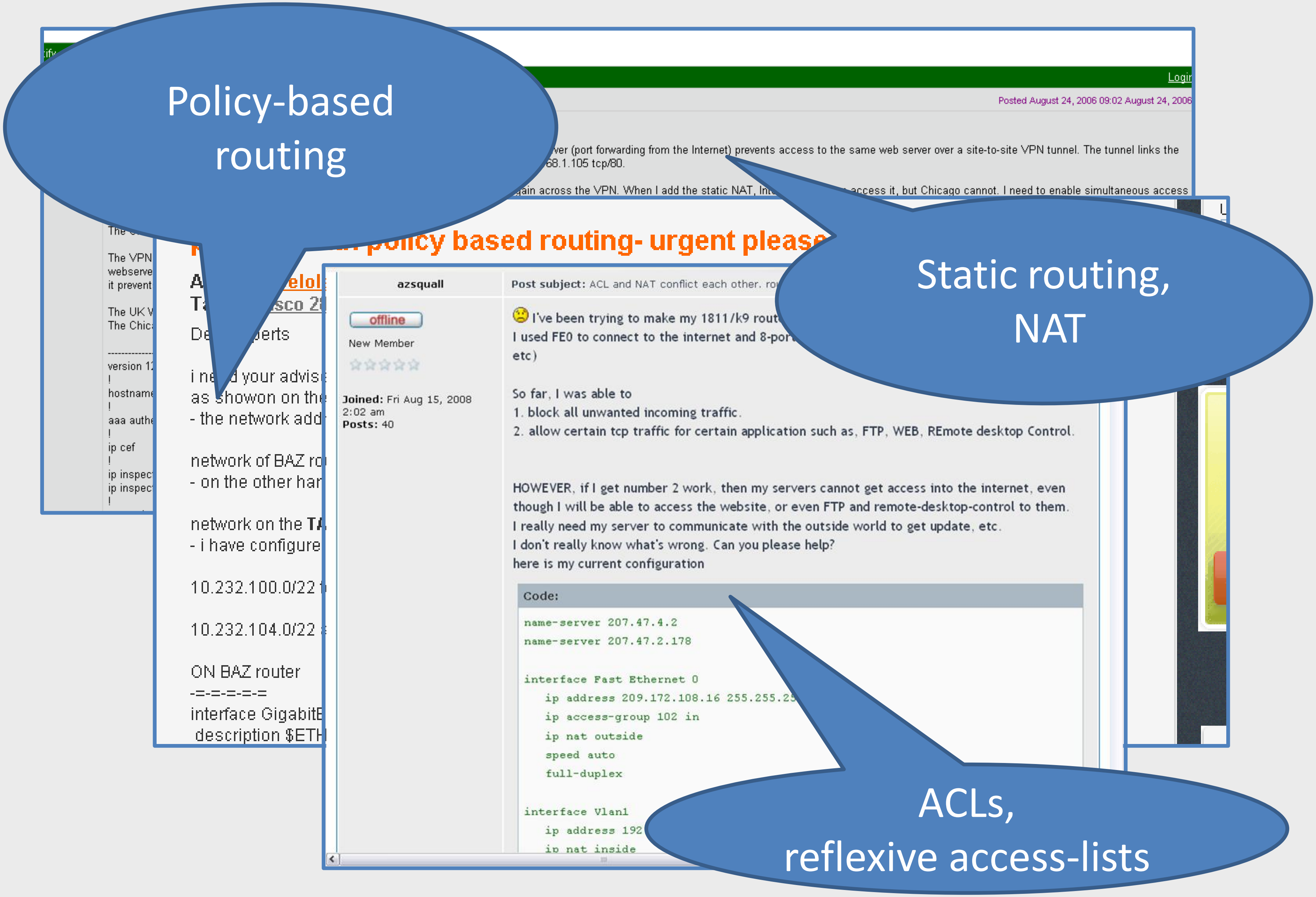
I've been trying to make my 1811/k9 route
I used FE0 to connect to the internet and 8-port
etc)

So far, I was able to
1. block all unwanted incoming traffic.
2. allow certain tcp traffic for certain application such as, FTP, WEB, REmote desktop Control.

HOWEVER, if I get number 2 work, then my servers cannot get access into the internet, even though I will be able to access the website, or even FTP and remote-desktop-control to them.
I really need my server to communicate with the outside world to get update, etc.
I don't really know what's wrong. Can you please help?
here is my current configuration

Code:

```
name-server 207.47.4.2
name-server 207.47.2.178

interface Fast Ethernet 0
   ip address 209.172.108.16 255.255.2
   ip access-group 102 in
   ip nat outside
   speed auto
   full-duplex

interface Vlan1
   ip address 192
   ip nat inside
```



Policy-based routing

Static routing, NAT

ACLs,
reflexive access-lists

Login

Posted August 24, 2006 09:02 August 24, 2006

ver (port forwarding from the Internet) prevents access to the same web server over a site-to-site VPN tunnel. The tunnel links the
68.1.105 tcp/80.

gain across the VPN. When I add the static NAT, Int access it, but Chicago cannot. I need to enable simultaneous access

The

The VPN
webserve
it prevent

The UK V
The Chic

```
-------------
version 12
!
hostname
!
aaa authe
!
ip cef
!
ip inspect
ip inspect
!
```

policy based routing- urgent please

A elol
T sco 2

De perts

i ne d your advise
as showon on the
- the network add

network of BAZ ro
- on the other har

network on the TA
- i have configure

10.232.100.0/22 t

10.232.104.0/22

ON BAZ router
-=-=-=-=-=
interface GigabitE
 description $ETH

azsquall

offline

New Member

☆☆☆☆☆

Joined: Fri Aug 15, 2008 2:02 am
Posts: 40

Post subject: ACL and NAT conflict each other. ro

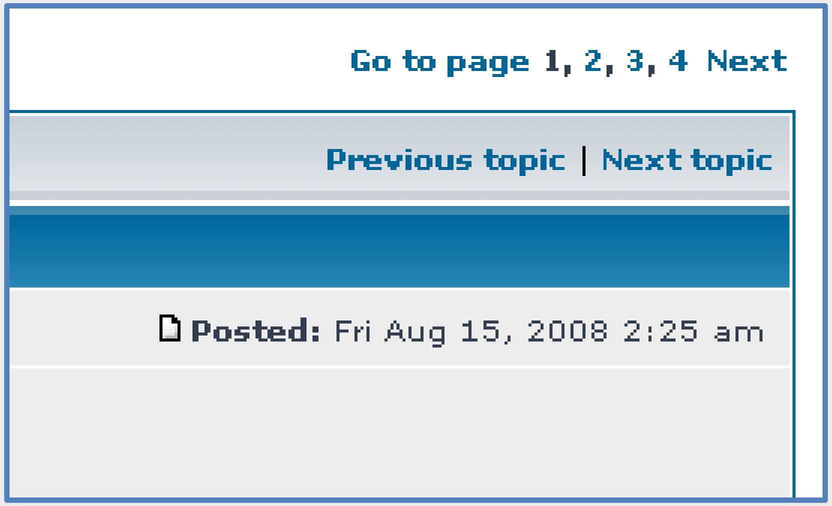
I've been trying to make my 1811/k9 rout
I used FE0 to connect to the internet and 8-por
etc)

So far, I was able to
1. block all unwanted incoming traffic.
2. allow certain tcp traffic for certain application such as, FTP, WEB, REmote desktop Control.

HOWEVER, if I get number 2 work, then my servers cannot get access into the internet, even though I will be able to access the website, or even FTP and remote-desktop-control to them.
I really need my server to communicate with the outside world to get update, etc.
I don't really know what's wrong. Can you please help?
here is my current configuration

Code:

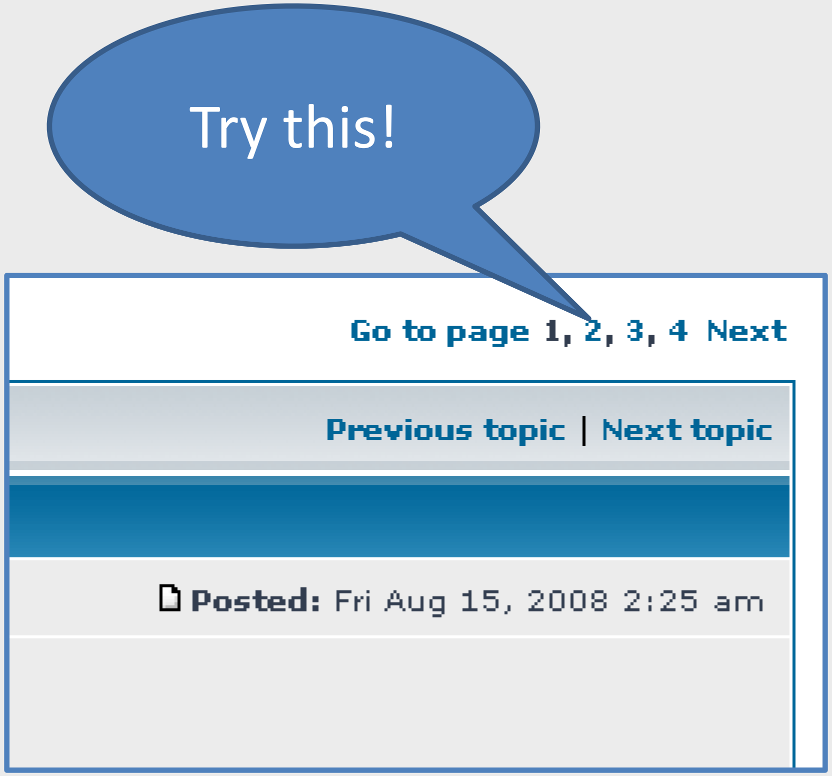
```
name-server 207.47.4.2
name-server 207.47.2.178

interface Fast Ethernet 0
   ip address 209.172.108.16 255.255.25
   ip access-group 102 in
   ip nat outside
   speed auto
   full-duplex

interface Vlan1
   ip address 192
   ip nat inside
```



Go to page 1, 2, 3, 4 Next

Previous topic | Next topic

Posted: Fri Aug 15, 2008 2:25 am

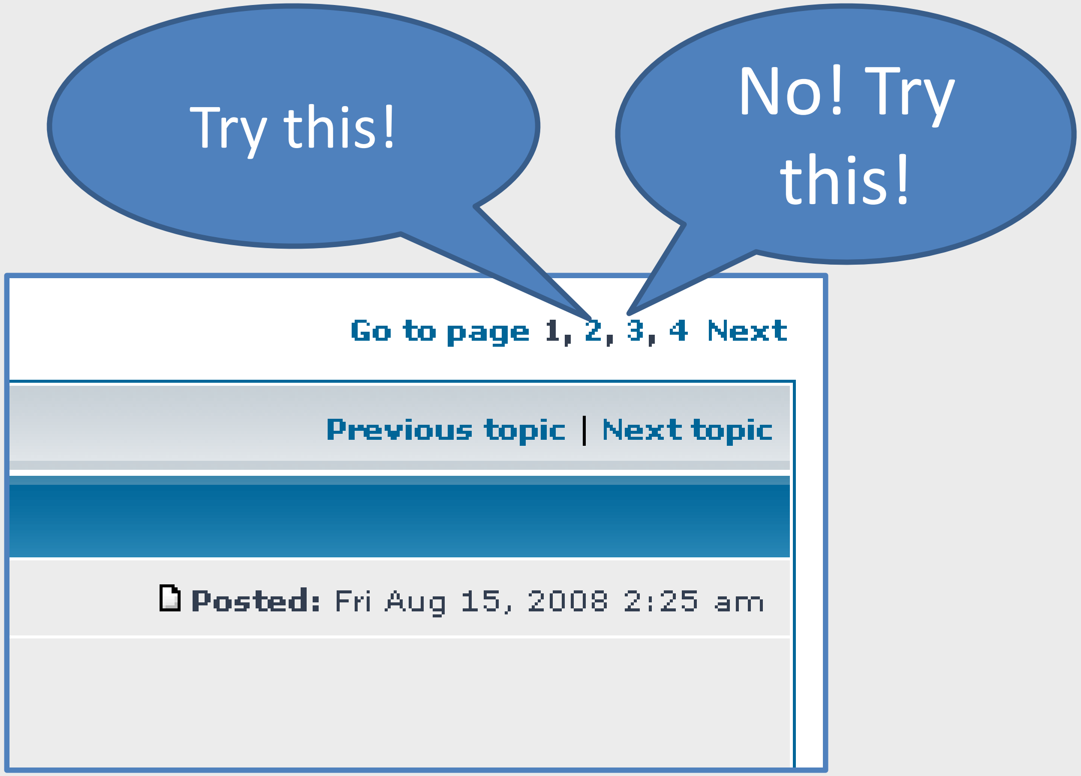


Try this!

Go to page 1, 2, 3, 4 Next

Previous topic | Next topic

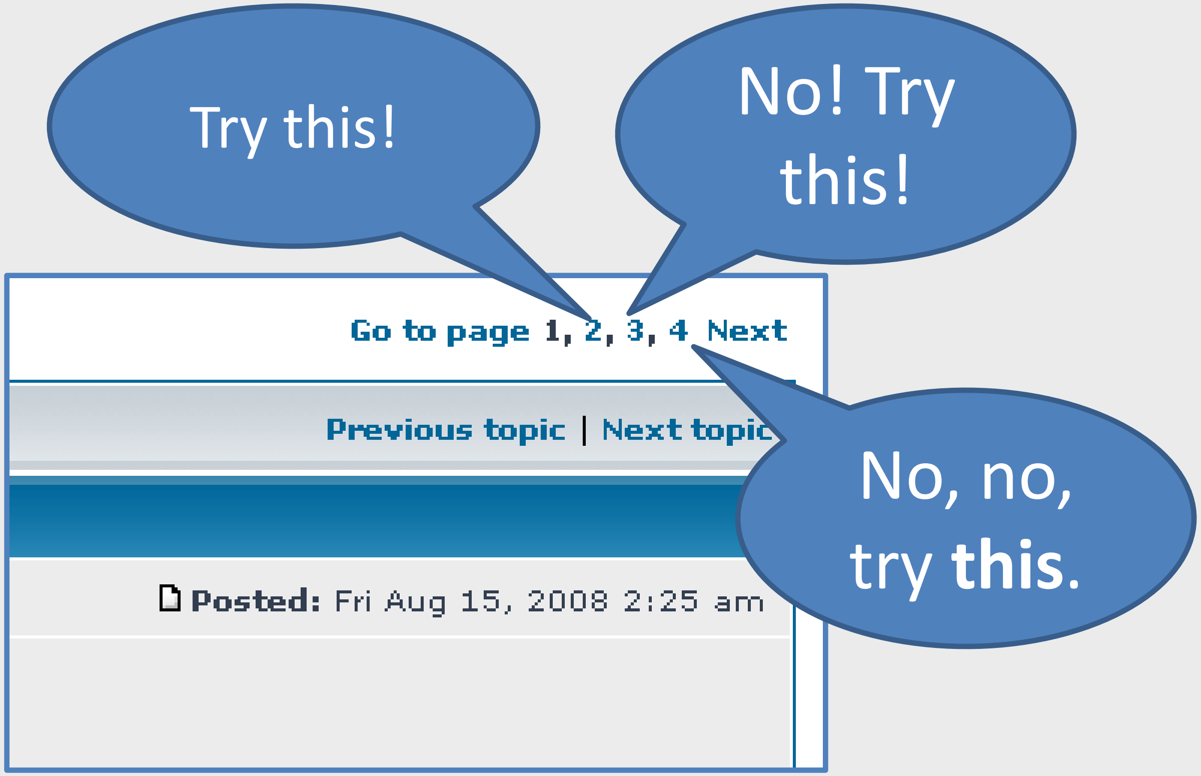
Posted: Fri Aug 15, 2008 2:25 am



Go to page 1, 2, 3, 4 Next

Previous topic | Next topic

Posted: Fri Aug 15, 2008 2:25 am



Go to page 1, 2, 3, 4 Next

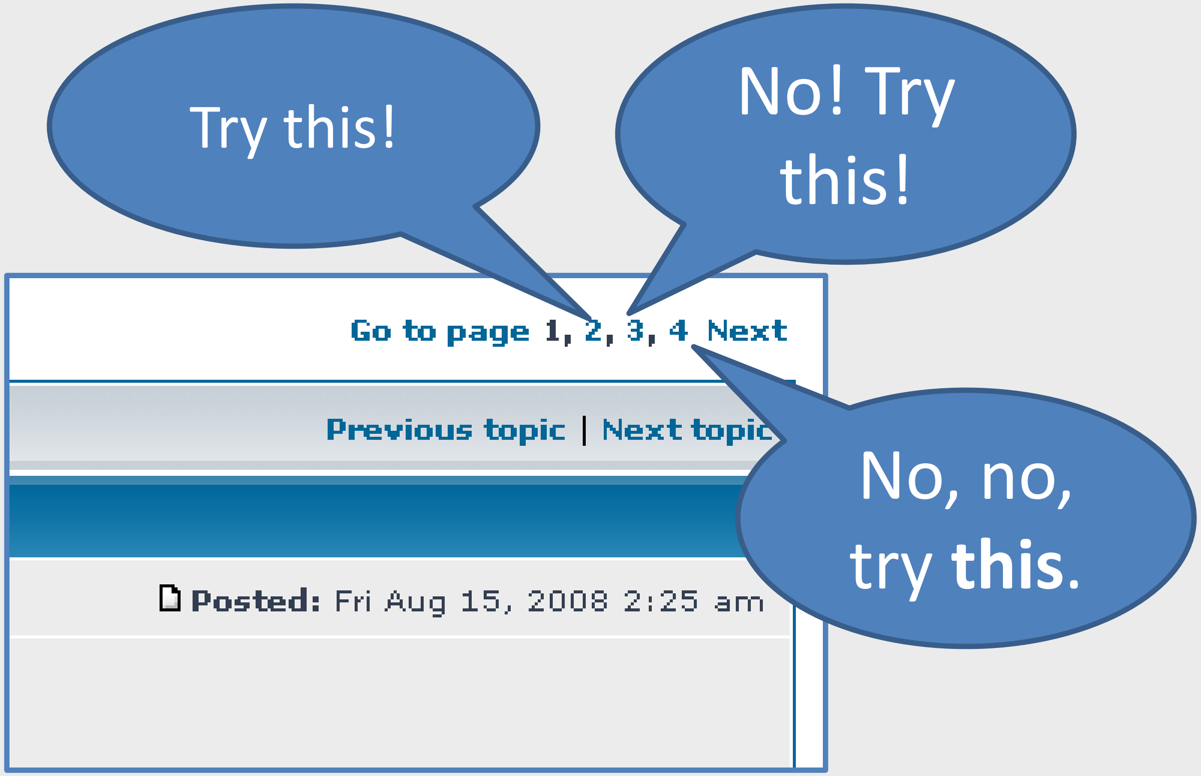
Previous topic | Next topic

Posted: Fri Aug 15, 2008 2:25 am

Try this!

No! Try this!

No, no, try **this**.



Go to page 1, 2, 3, 4 Next

Previous topic | Next topic

Posted: Fri Aug 15, 2008 2:25 am

Suggestions do not always agree.

Debugging Questions:

Debugging Questions:

Q: Which hop will SMTP packets take next?

Debugging Questions:

Q: Which hop will SMTP packets take next?

A: 192.168.100.4

192.168.200.5

…

Debugging Questions:

Q: Which hop will SMTP packets take next?

A:

192.168.100.4

192.168.200.5

…

Q: Which configuration rules caused the incorrect routing?

Debugging Questions:

Q: Which hop will SMTP packets take next?

A:

192.168.100.4

192.168.200.5

…

Q: Which configuration rules caused the incorrect routing?

A:

Line 14 applied to…

Line 15 applied to…

…

Debugging Questions:

Q: Which hop will SMTP packets take next?

A: 192.168.100.4

192.168.200.5

…

Q: What packets will pass the firewall?

Q: Which configuration rules caused the incorrect routing?

A: Line 14 applied to…

Line 15 applied to…

…

Debugging Questions:

Q: Which hop will SMTP packets take next?

A: 192.168.100.4

192.168.200.5

…

Q: What packets will pass the firewall?

A: TCP From **X** to **Y**

…

Q: Which configuration rules caused the incorrect routing?

A: Line 14 applied to…

Line 15 applied to…

…

Debugging Questions:

Q: Which hop will SMTP packets take next?

A: 192.168.100.4

192.168.200.5

…

Q: What packets will pass the firewall?

A: TCP From **X** to **Y**

…

Q: Which configuration rules caused the incorrect routing?

A: Line 14 applied to…

Line 15 applied to…

…

Q: How do a pair of configurations behave differently?

Debugging Questions:

Q: Which hop will SMTP packets take next?

A: 192.168.100.4

192.168.200.5

…

Q: What packets will pass the firewall?

A: TCP From **X** to **Y**

…

Q: Which configuration rules caused the incorrect routing?

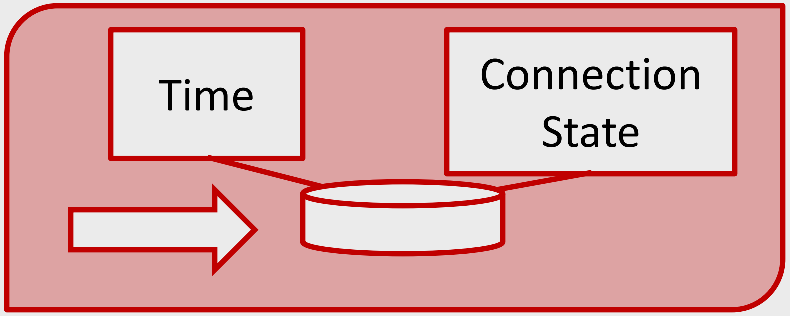
A: Line 14 applied to…

Line 15 applied to…

…

Q: How do a pair of configurations behave differently?

A:



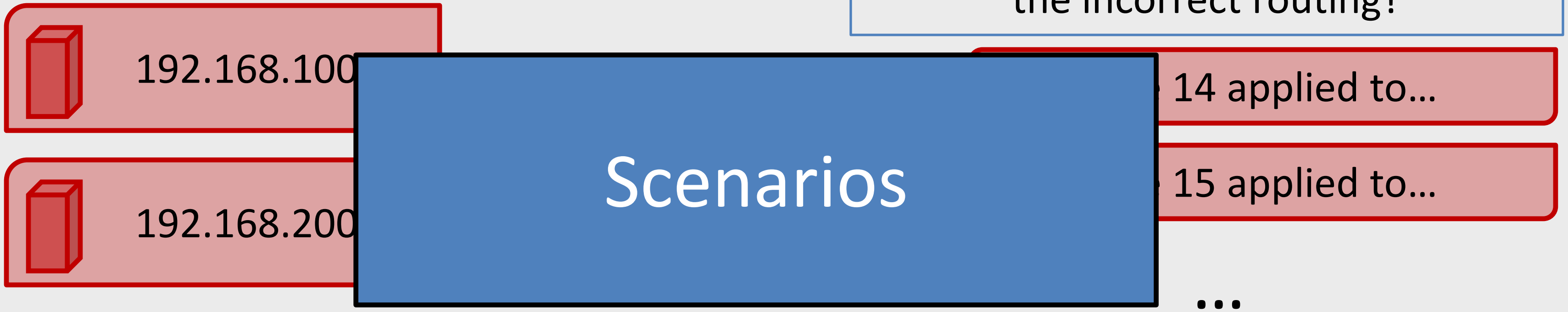
…

Debugging Questions:

Q: Which hop will SMTP packets take next?

Q: Which configuration rules caused the incorrect routing?

A:



192.168.100

192.168.200

Scenarios

14 applied to…

15 applied to…

…

…

Q: What packets will pass the firewall?

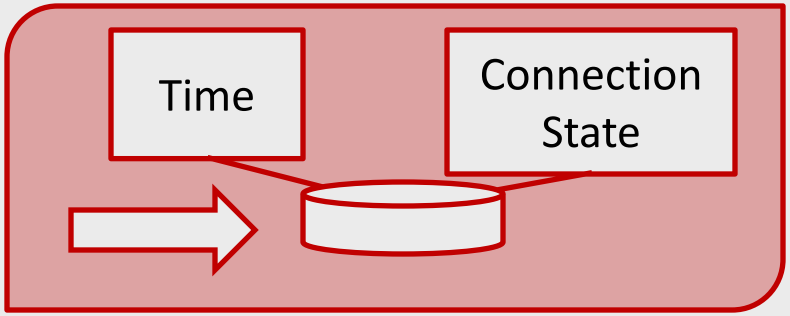
A:

TCP From **X** to **Y**

…

Q: How do a pair of configurations behave differently?

A:

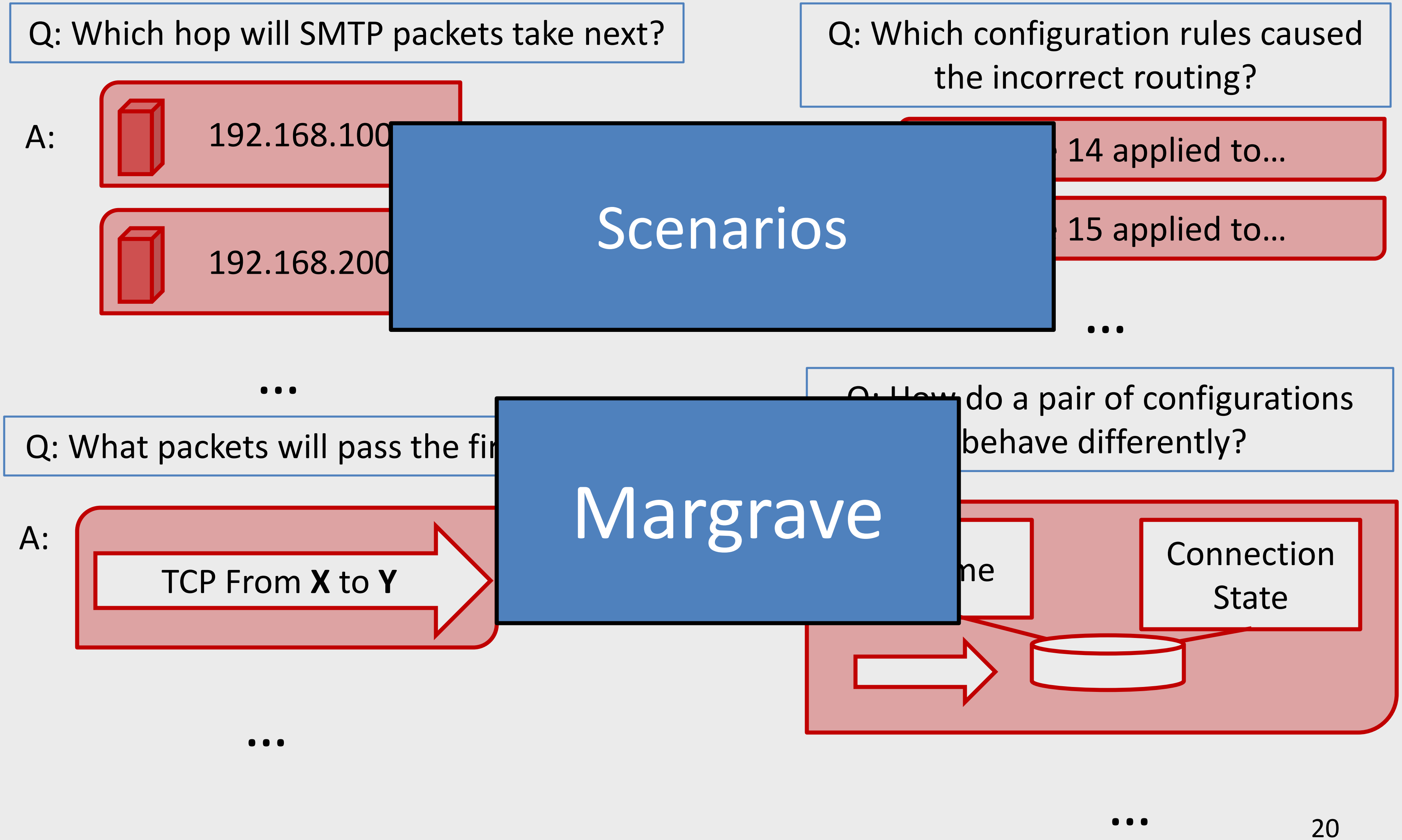


Time

Connection State

…

Debugging Questions:



Q: Which hop will SMTP packets take next?

A:

192.168.100

192.168.200

…

Q: Which configuration rules caused the incorrect routing?

14 applied to…

15 applied to…

…

Scenarios

Q: What packets will pass the fir

A:

TCP From **X** to **Y**

…

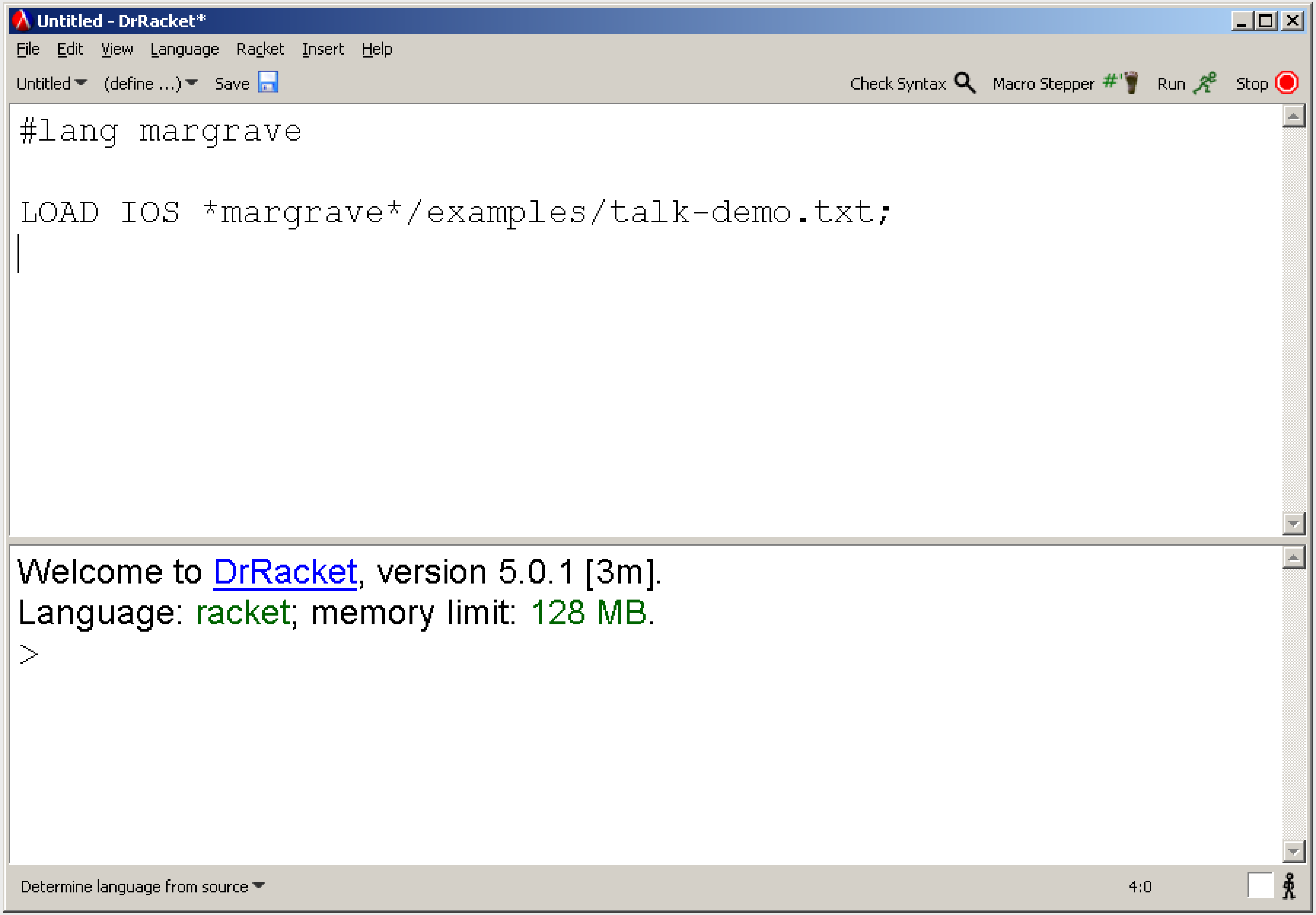
Q: How do a pair of configurations
behave differently?

me

Connection State

…

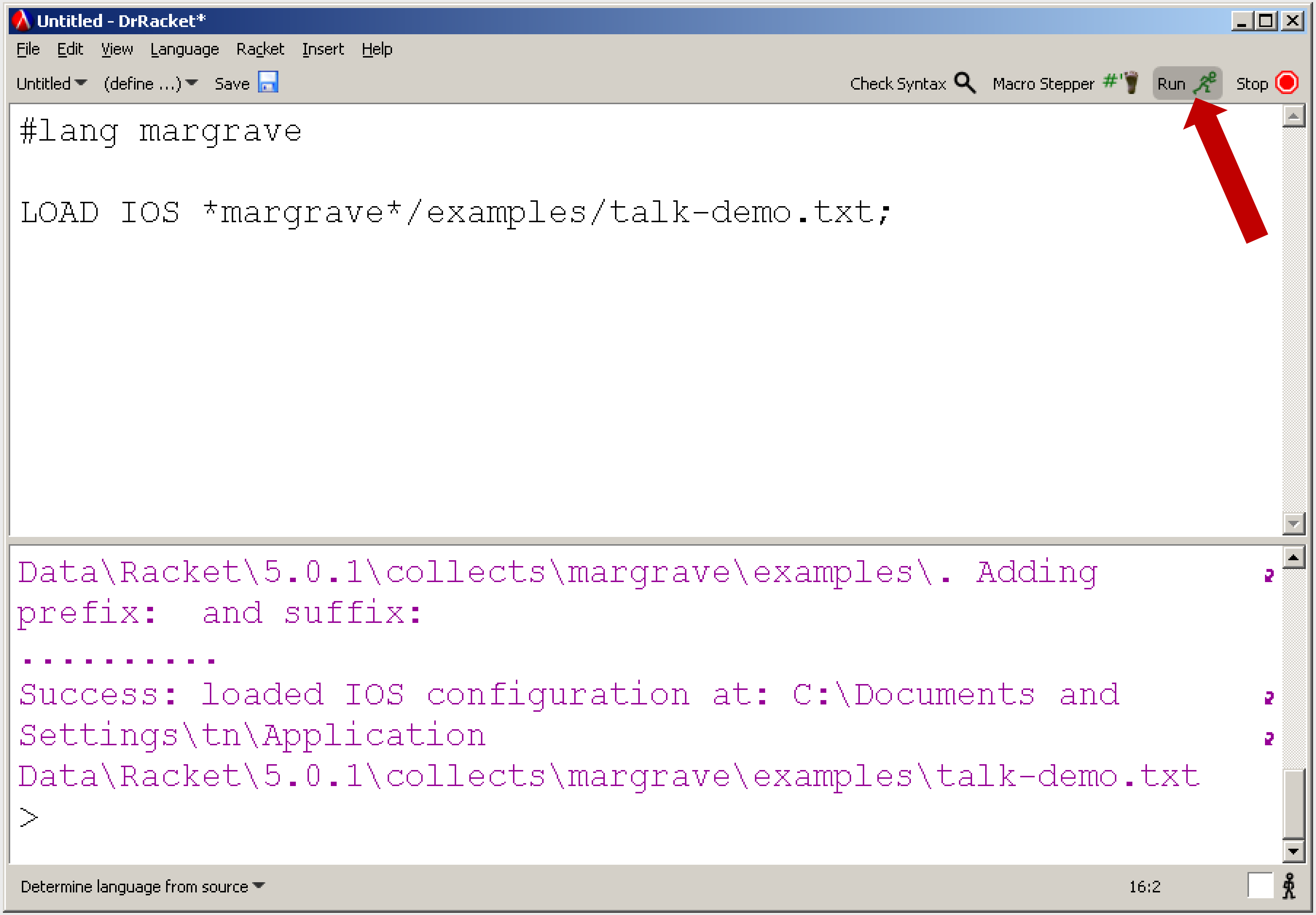
Margrave


Untitled - DrRacket*
File Edit View Language Racket Insert Help
Untitled (define ...) Save
Check Syntax Macro Stepper Run Stop

```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

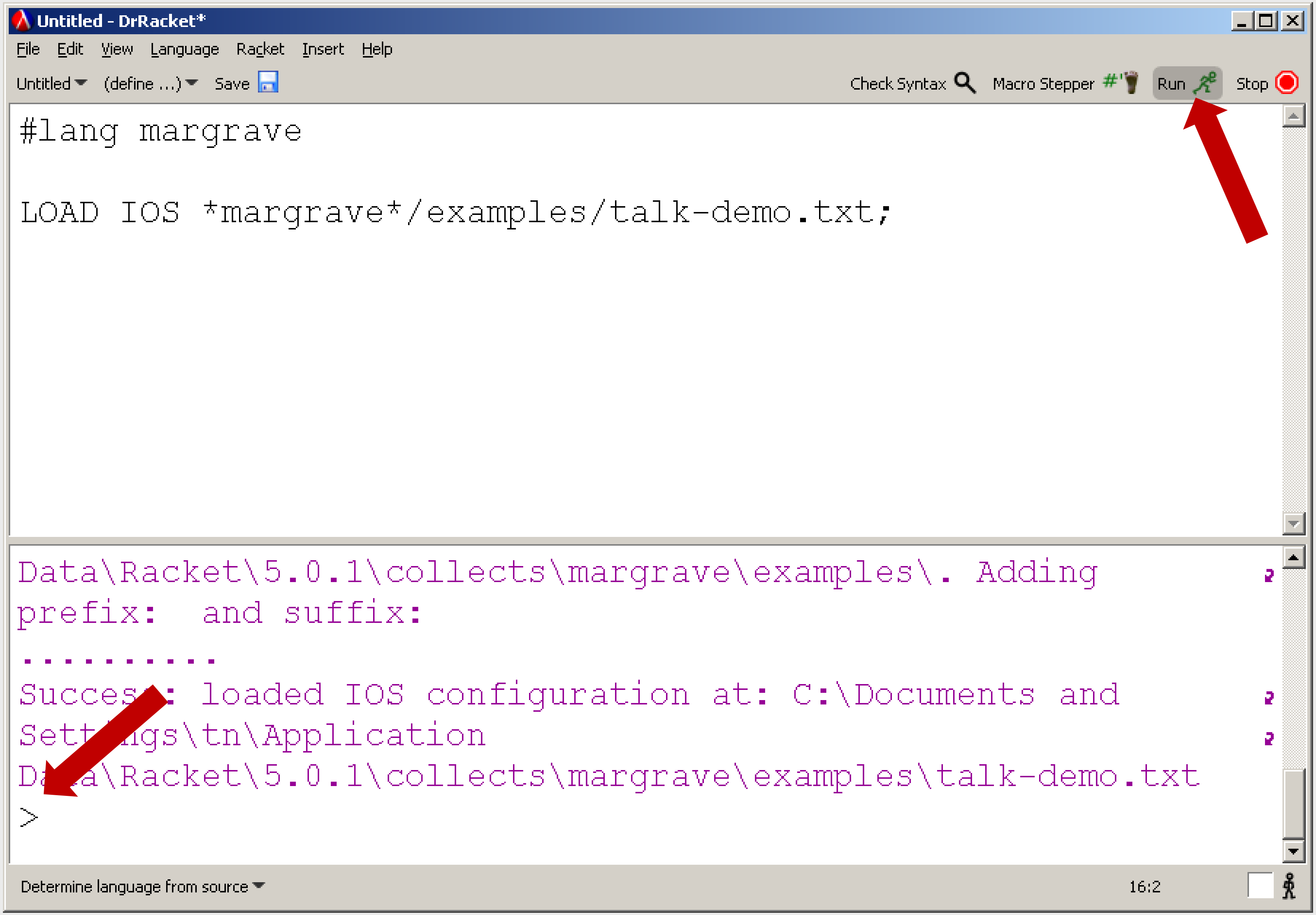
```
Welcome to DrRacket, version 5.0.1 [3m].
Language: racket; memory limit: 128 MB.
>
```

Determine language from source
4:0



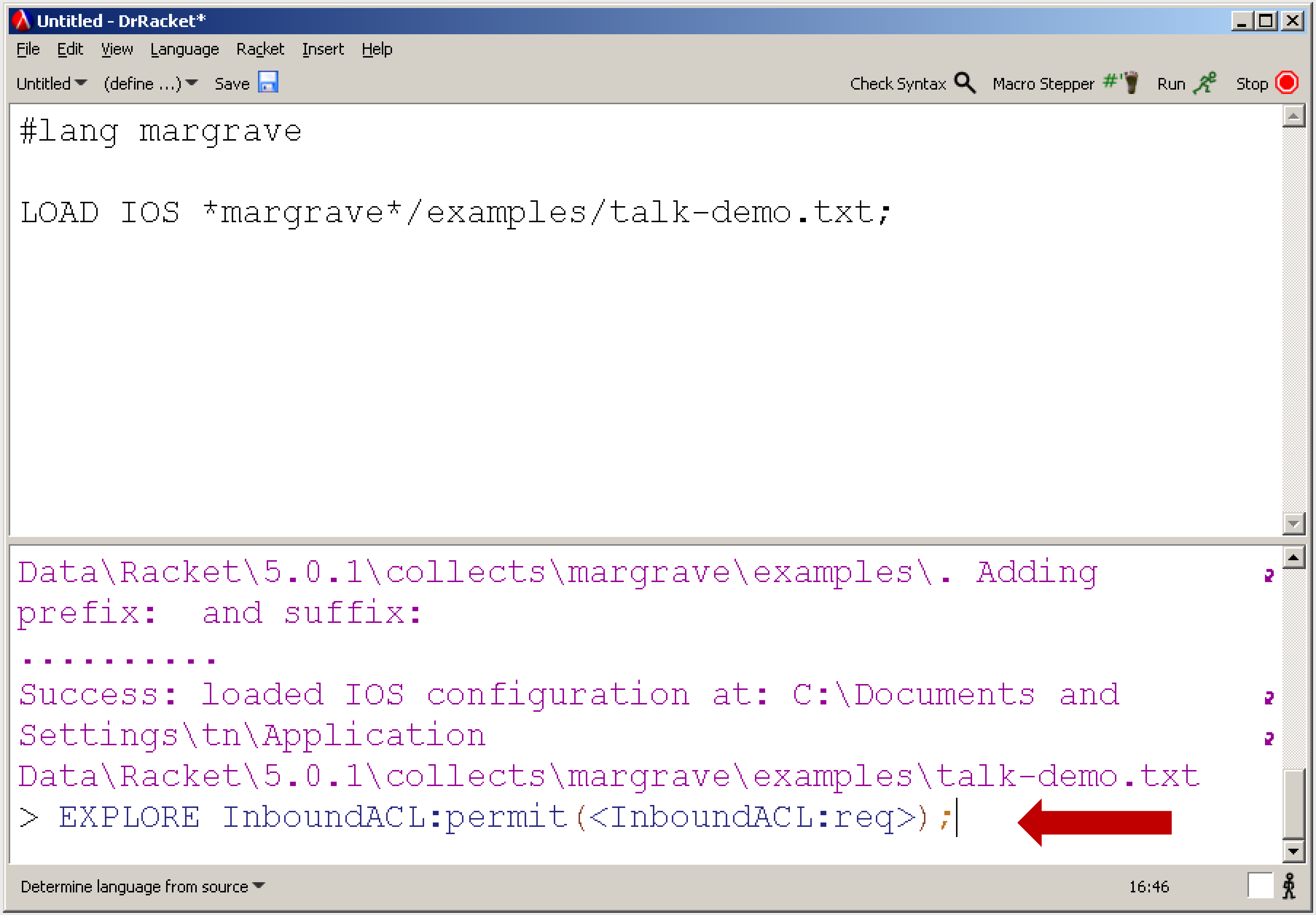
```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
Data\Racket\5.0.1\collects\margrave\examples\. Adding
prefix:  and suffix:
...........
Success: loaded IOS configuration at: C:\Documents and
Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
>
```



```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
Data\Racket\5.0.1\collects\margrave\examples\. Adding
prefix:  and suffix:
...........
Success: loaded IOS configuration at: C:\Documents and
Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
>
```

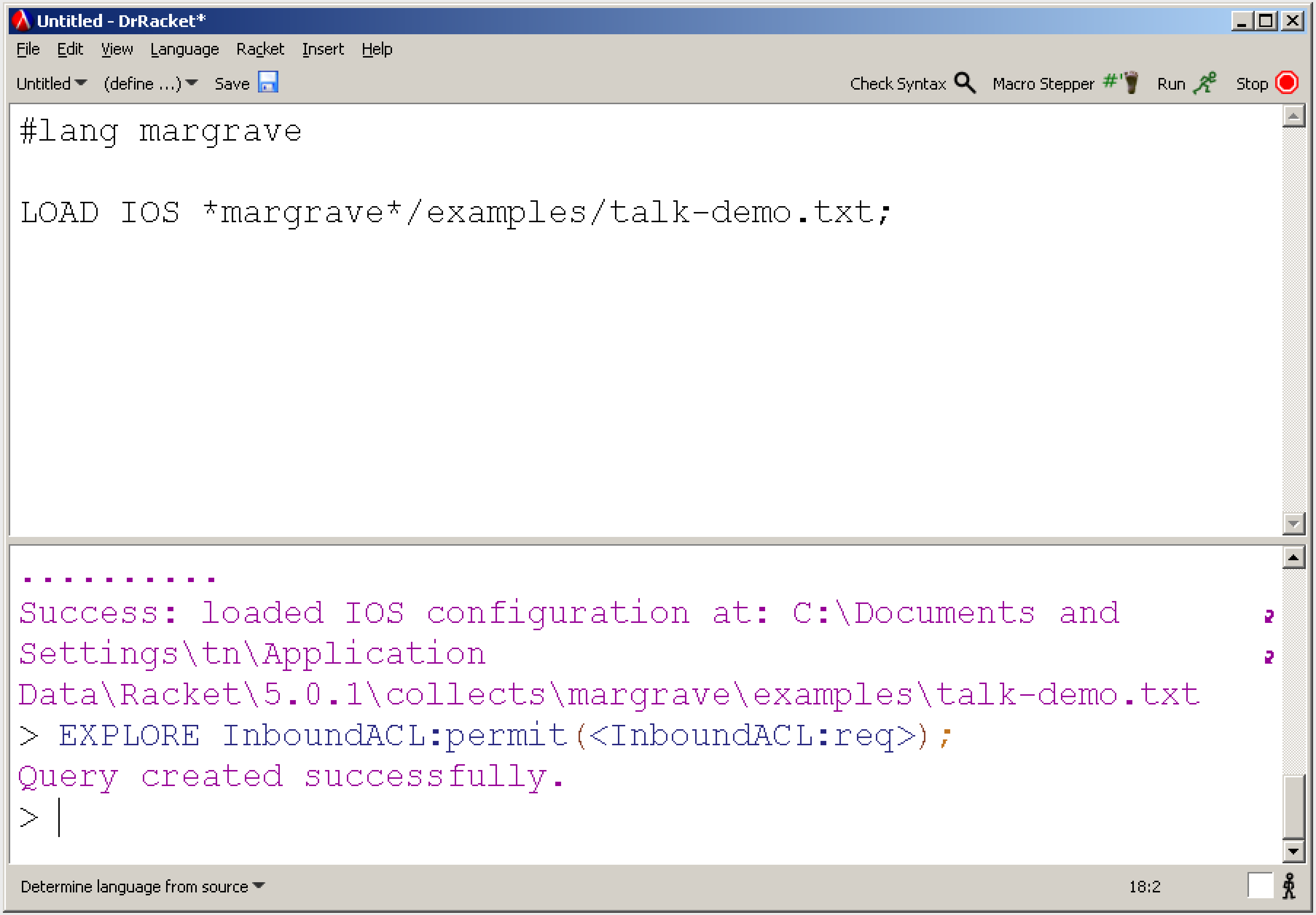


Untitled - DrRacket*
File Edit View Language Racket Insert Help
Untitled (define ...) Save
Check Syntax Macro Stepper Run Stop

```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
Data\Racket\5.0.1\collects\margrave\examples\. Adding
prefix:  and suffix:
...........
Success: loaded IOS configuration at: C:\Documents and
Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
> EXPLORE InboundACL:permit(<InboundACL:req>);
```

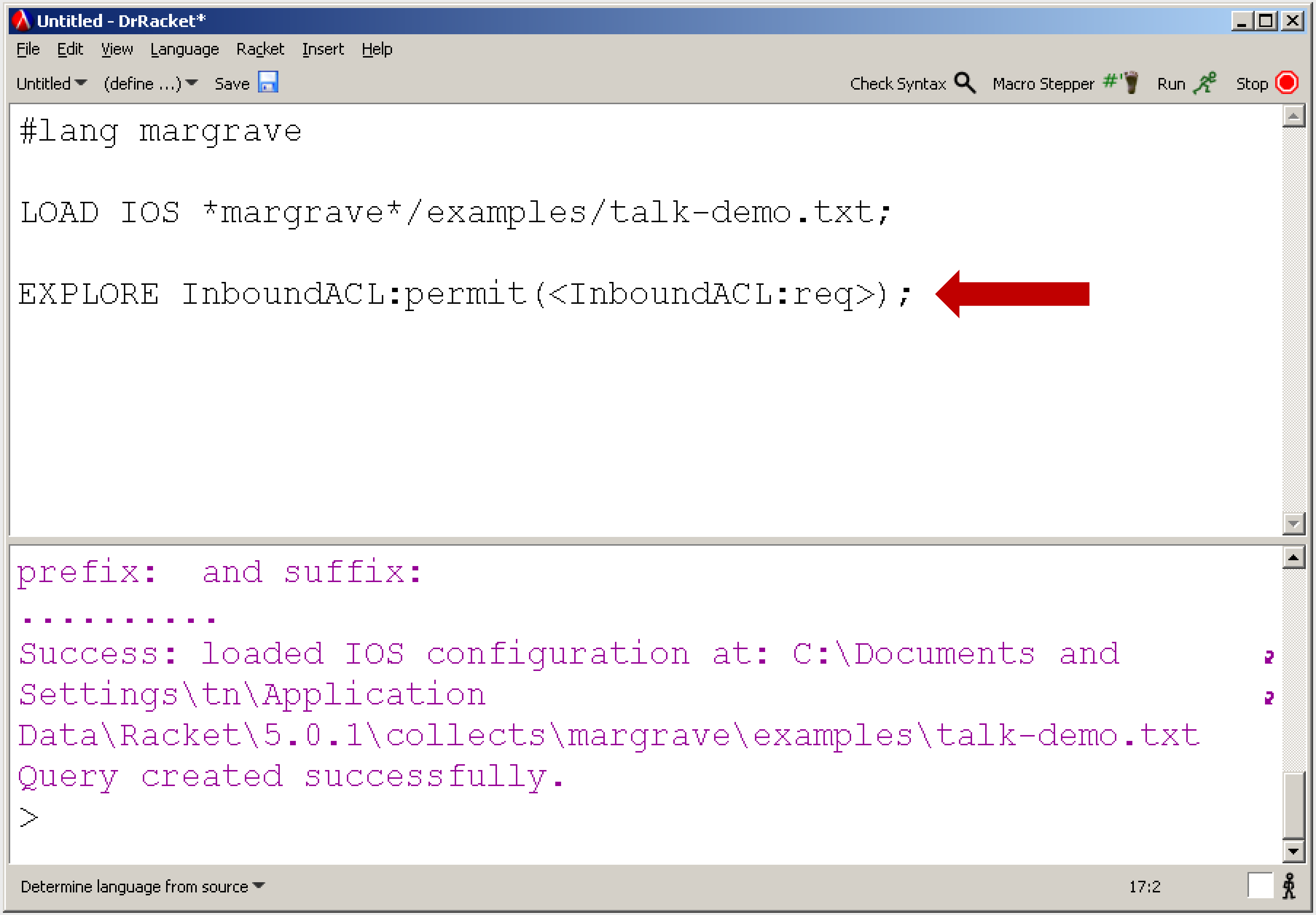
Determine language from source
16:46



Untitled - DrRacket*
File Edit View Language Racket Insert Help
Untitled (define ...) Save
Check Syntax Macro Stepper Run Stop
Determine language from source
18:2

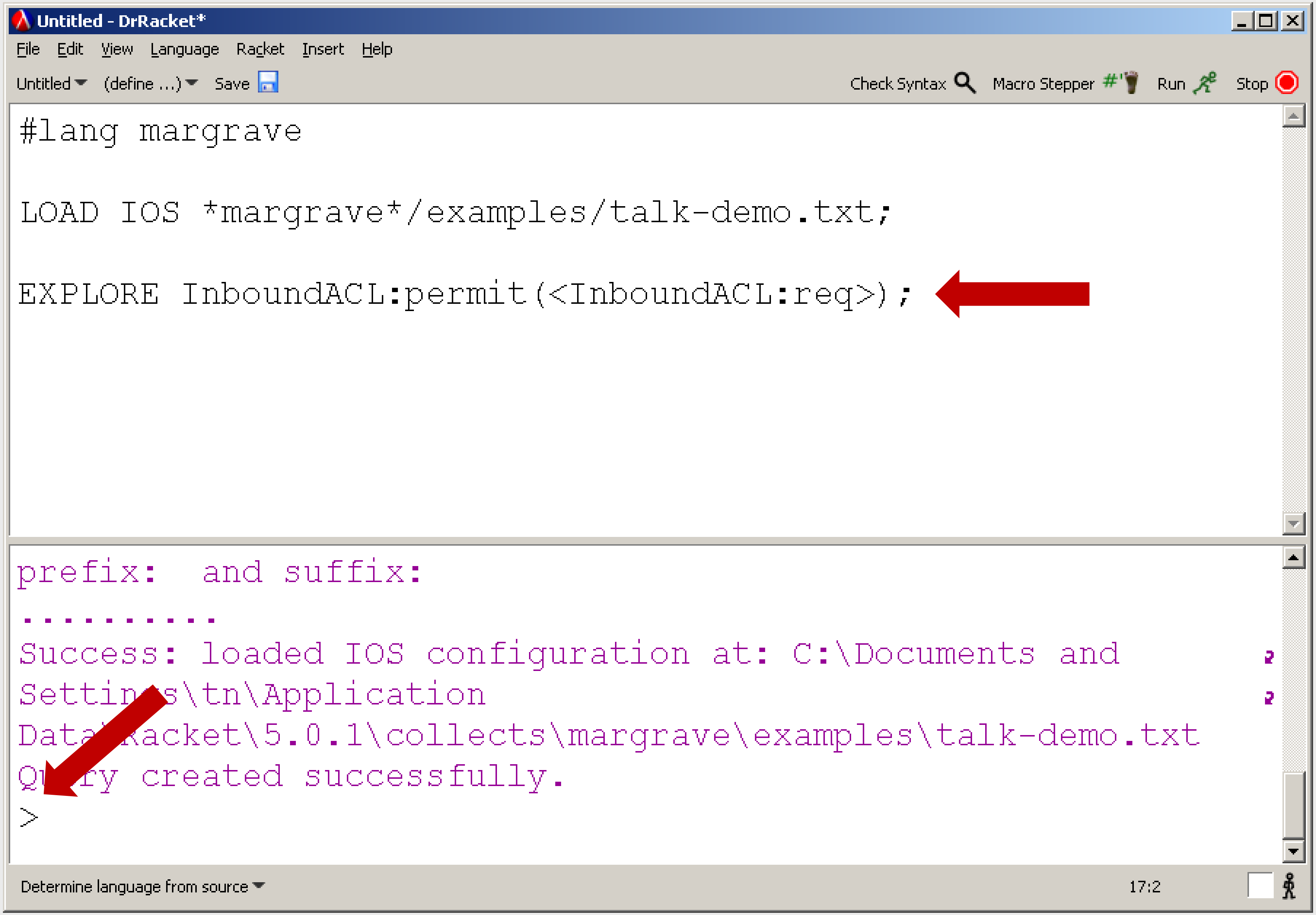
```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
...........
Success: loaded IOS configuration at: C:\Documents and
Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
> EXPLORE InboundACL:permit(<InboundACL:req>);
Query created successfully.
> 
```



```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;

EXPLORE InboundACL:permit(<InboundACL:req>);
```

```
prefix:  and suffix:
..........
Success: loaded IOS configuration at: C:\Documents and
Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
Query created successfully.
>
```

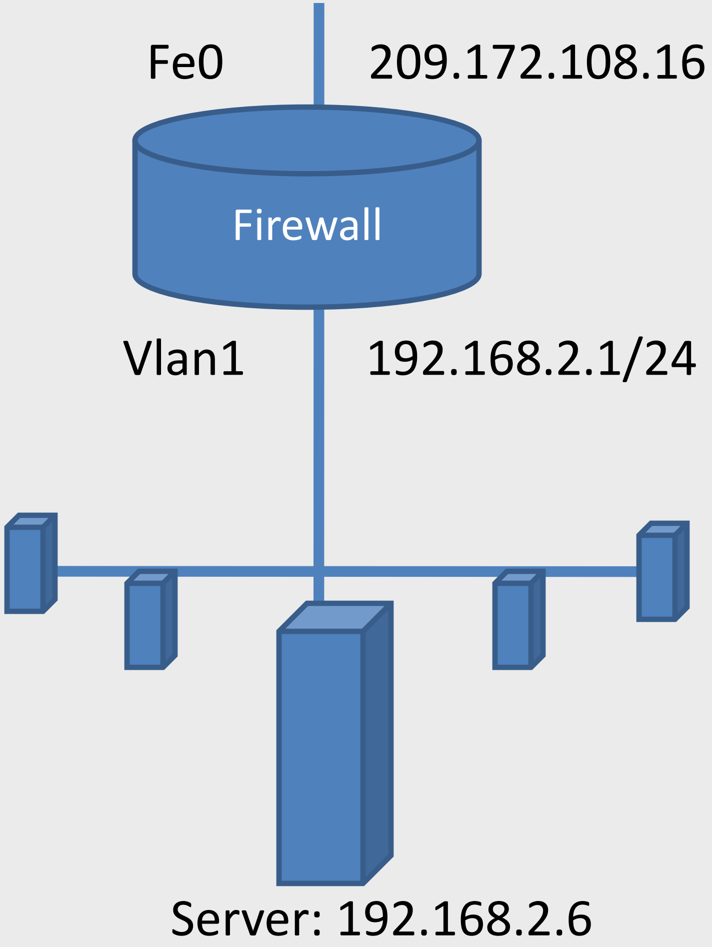

Untitled - DrRacket*
File Edit View Language Racket Insert Help
Untitled (define ...) Save
Check Syntax Macro Stepper Run Stop
Determine language from source
17:2

```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;

EXPLORE InboundACL:permit(<InboundACL:req>);
```

```
prefix:  and suffix:
..........
Success: loaded IOS configuration at: C:\Documents and
Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
Query created successfully.
>
```

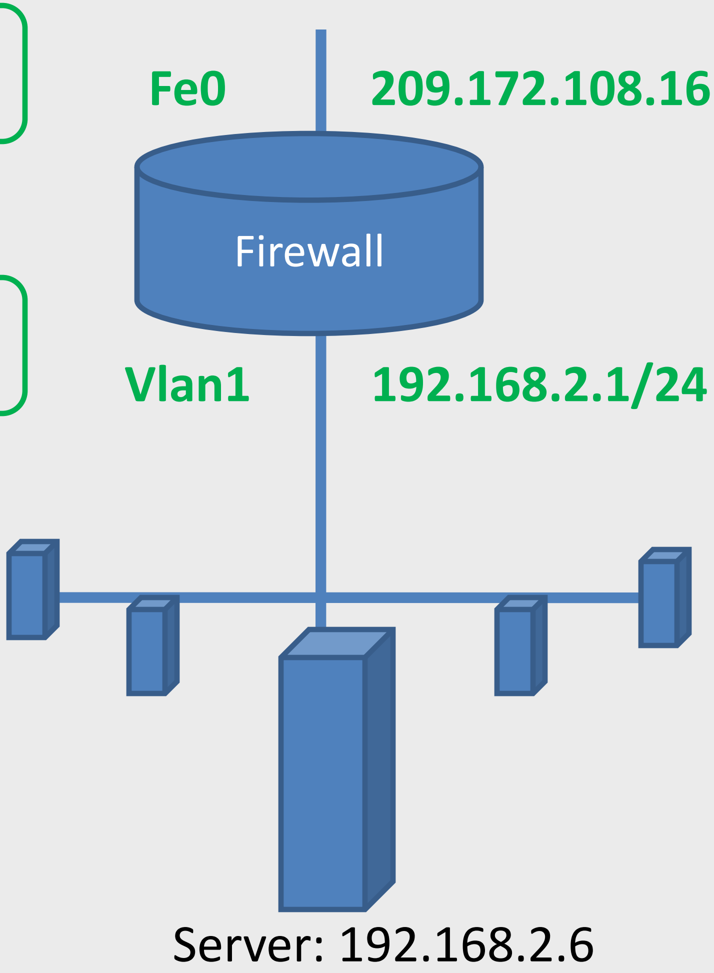
“The web can access my server, but my server can’t access the web.”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```



“The web can access my server, but my server can’t access the web.”

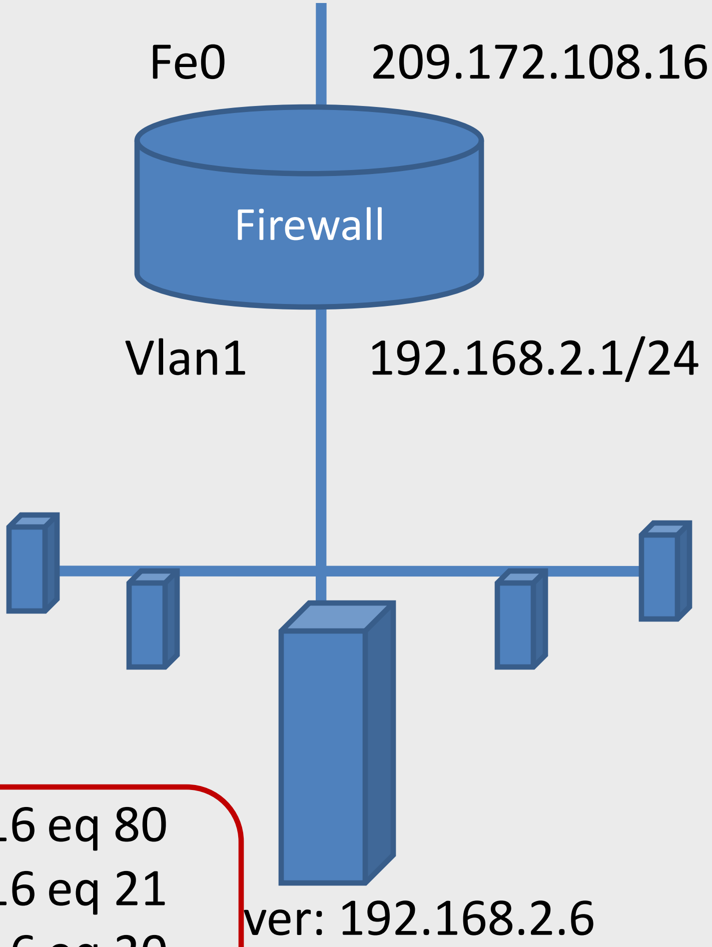
```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```



“The web can access my server, but my server can’t access the web.”

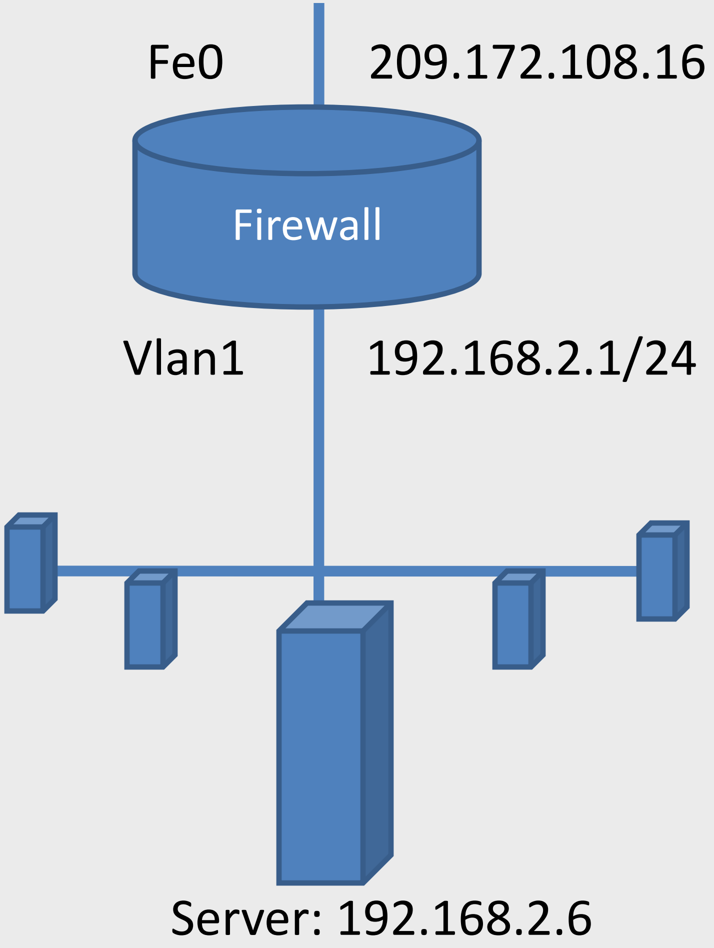
```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```



“The web can access my server, but my server can’t access the web.”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1

ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

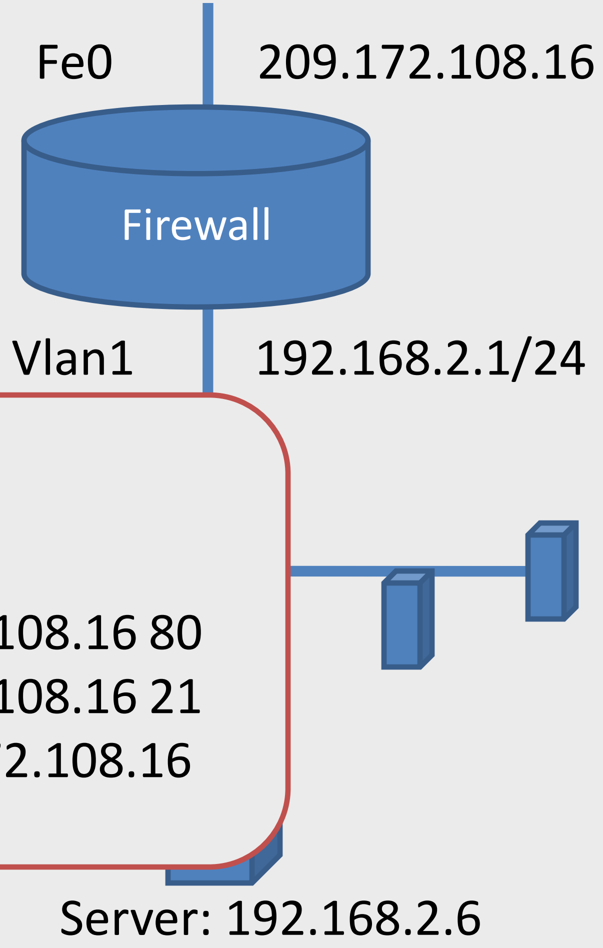


“The web can access my server, but my server can’t access the web.”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
 ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
 ip nat inside
!
```

```
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16
   3389
```

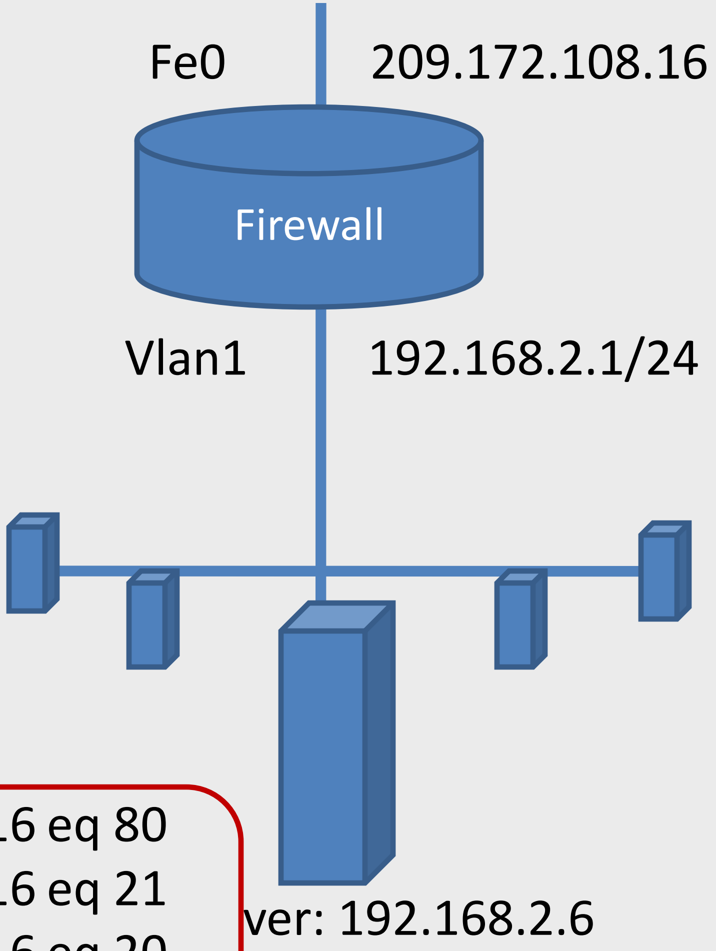
```
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```



“The web can access my server, but my server can’t access the web.”

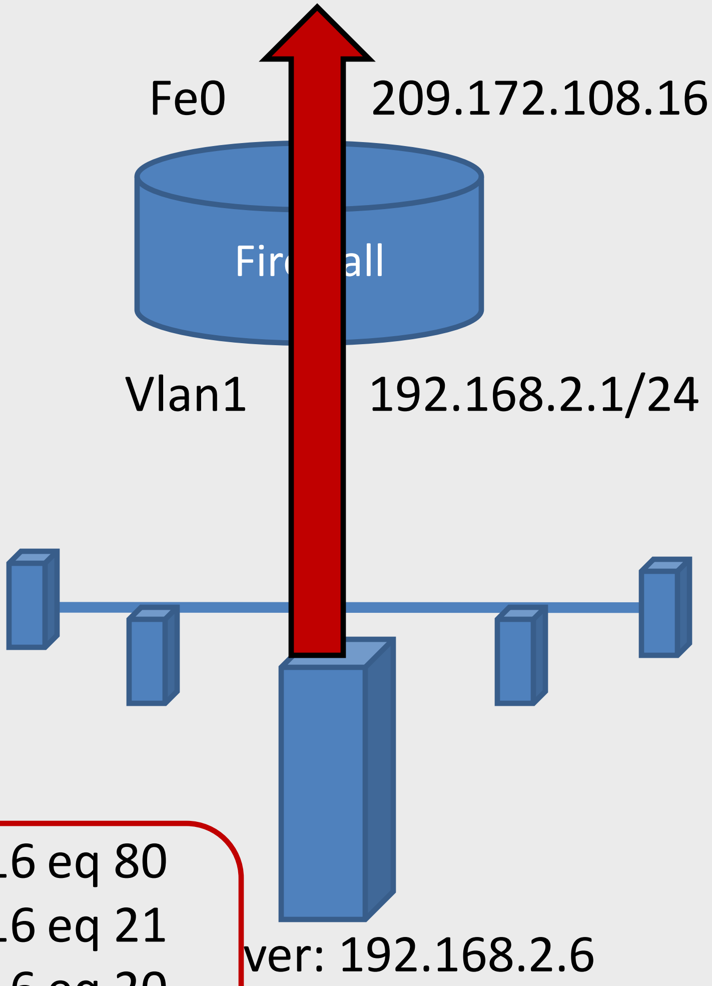
```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```



“The web can access my server, but my server can’t access the web.”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
```

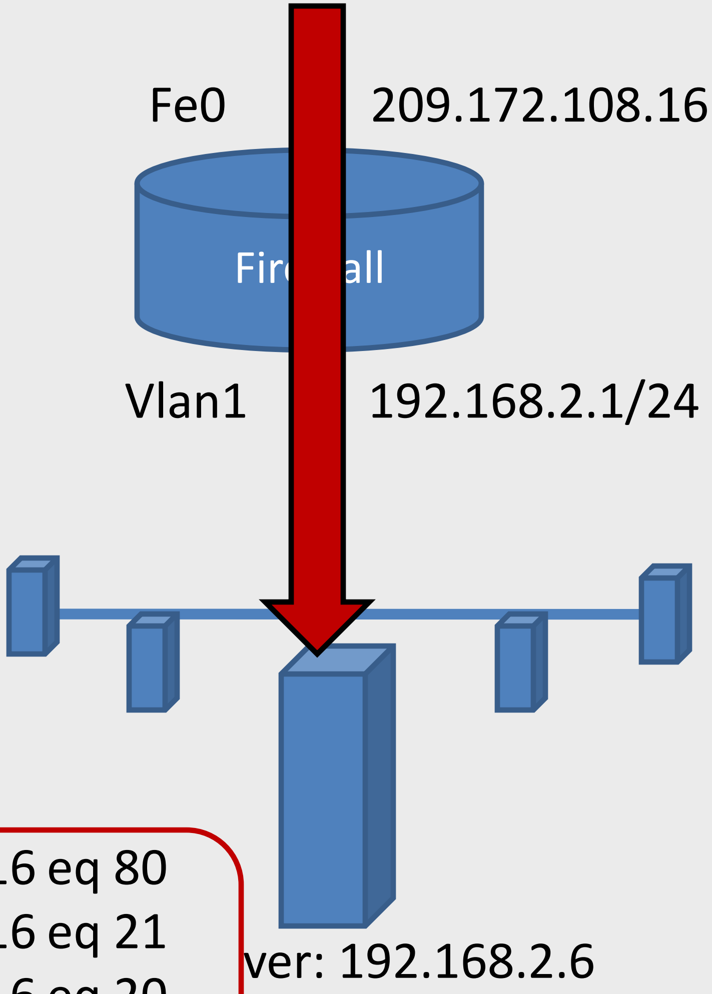


```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

“The web can access my server, but my server can’t access the web.”

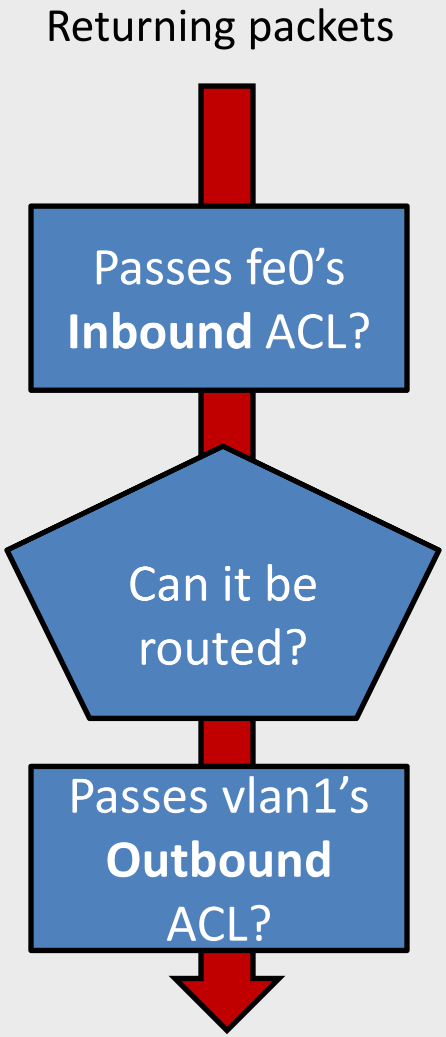
```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

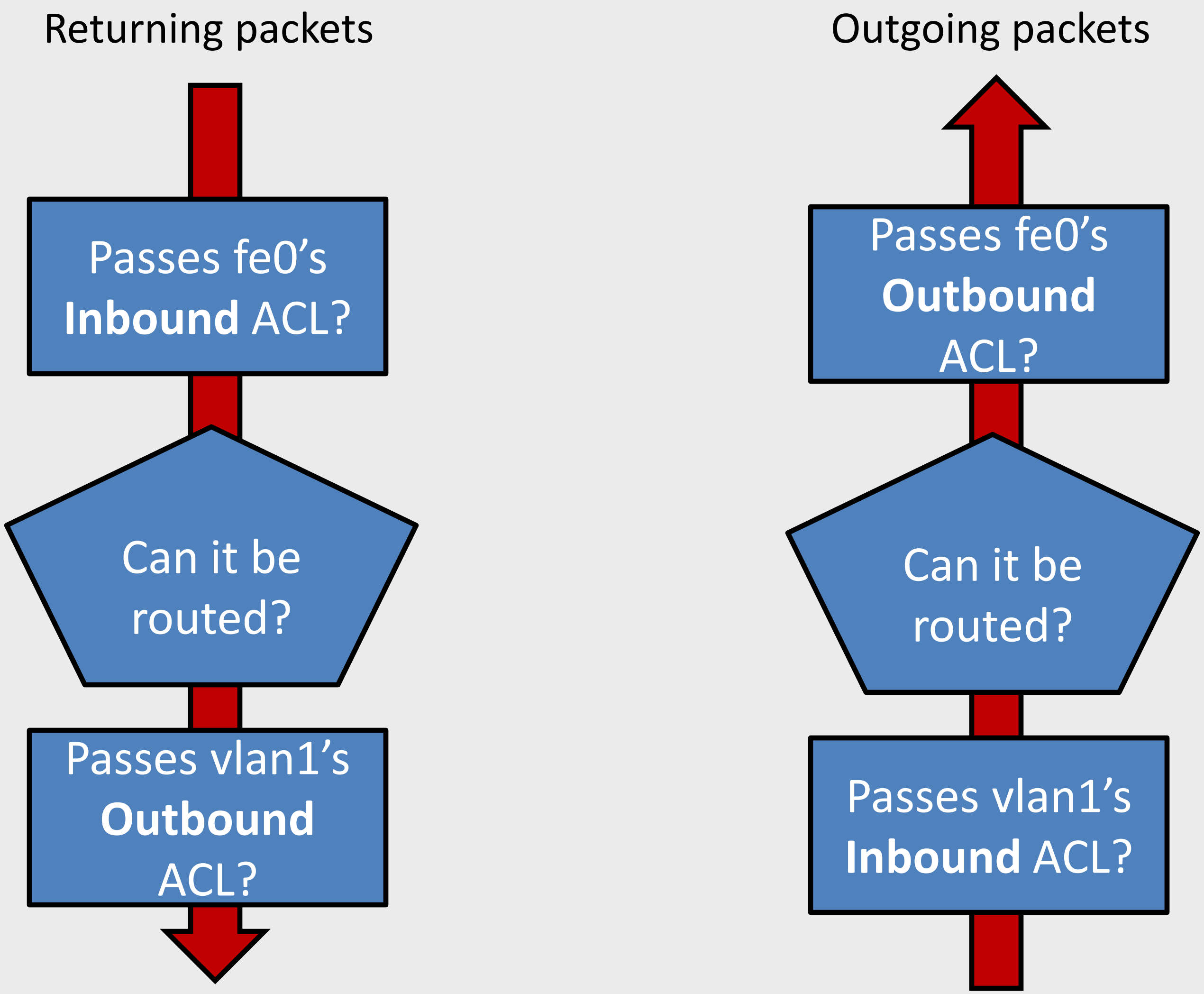


“The web can access my server, but my server can’t access the web.”

“The web can access my server, but my server can’t access the web.”


Returning packets
Passes fe0’s **Inbound** ACL?
Can it be routed?
Passes vlan1’s **Outbound** ACL?

“The web can access my server, but my server can’t access the web.”


Returning packets
Passes fe0’s **Inbound** ACL?
Can it be routed?
Passes vlan1’s **Outbound** ACL?
Outgoing packets
Passes fe0’s **Outbound** ACL?
Can it be routed?
Passes vlan1’s **Inbound** ACL?

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

EXPLORE

“Find me scenarios where…”

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

EXPLORE
NOT passes-firewall(<pkt>);

“Dropped or rejected”

<pkt> =

entry-interface
src-addr-in
protocol
…

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

EXPLORE

NOT passes-firewall(<pkt>)

AND **internal-result**(<pktplus>) ;

“Compute next hop and NAT”

<pktplus> =

<pkt>

+

temporary variables

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

EXPLORE
NOT passes-firewall(<pkt>)
AND **internal-result**(<pktplus>)
AND **FastEthernet0** = **entry-interface**;

“Arriving at FastEthernet0”

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-leng
ip nat inside source list 1 pool localnet overlo
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.1
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

EXPLORE

NOT passes-firewall(<pkt>)

AND **internal-result**(<pktplus>)

AND **FastEthernet0** = **entry-interface**

AND

  NOT **src-addr-in** IN **192.168.2.0/255.255.255.0**;

“Reasonable source”

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 8
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

```
EXPLORE
NOT passes-firewall(<pkt>)
AND internal-result(<pktplus>)
AND FastEthernet0 = entry-interface
AND
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
AND prot-TCP = protocol
AND port-80 = src-port-in;
```

“TCP from port 80”

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

```
EXPLORE
NOT passes-firewall(<pkt>)
AND internal-result(<pktplus>)
AND FastEthernet0 = entry-interface
AND
 NOT src-addr-in IN 192.168.2.0/255.255.255.0
AND prot-TCP = protocol
AND port-80 = src-port-in;
AND dest-addr-in = 209.172.108.16;
```

“To public address”

“Can **returning** packets be lost?”

```
interface FastEthernet0
ip address 209.172.108.16 255.255.255.224
ip access-group 102 in
ip nat outside
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 209.172.108.1
!
ip nat pool localnet 209.172.108.16 prefix-length 24
ip nat inside source list 1 pool localnet overload
ip nat inside source list 1 interface FastEthernet0
ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
ip nat inside source static tcp 192.168.2.6 21 209.172.108.16
ip nat inside source static tcp 192.168.2.6 3389 209.172.108.
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

EXPLORE
NOT passes-firewall(<pkt>)
AND **internal-result**(<pktplus>)
AND **FastEthernet0** = **entry-interface**
AND
NOT **src-addr-in** IN **192.168.2.0/255.255.255.0**
AND **prot-TCP** = **protocol**
AND **port-80** = **src-port-in**;
AND **dest-addr-in** = **209.172.108.16**;

Here, a scenario is:

Data about a packet’s contents & handling

“Can **returning** packets be lost?”

Check for denied return packets:

```
> EXPLORE
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
  AND FastEthernet0 = entry-interface
  AND prot-TCP = protocol
  AND port-80 = src-port-in
  AND dest-addr-in = 209.172.108.16
  AND internal-result(<pktplus>)
  AND NOT passes-firewall(<pkt>);

> IS POSSIBLE?;
```

“Can **returning** packets be lost?”

Check for denied return packets:

```
> EXPLORE
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
  AND FastEthernet0 = entry-interface
  AND prot-TCP = protocol
  AND port-80 = src-port-in
  AND dest-addr-in = 209.172.108.16
  AND internal-result(<pktplus>)
  AND NOT passes-firewall(<pkt>);

> IS POSSIBLE?;
true
>
```

Some return packets will be dropped.

“Can **returning** packets be lost?”

Check for denied return packets:

```
> EXPLORE
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
  AND FastEthernet0 = entry-interface
  AND prot-TCP = protocol
  AND port-80 = src-port-in
  AND dest-addr-in = 209.172.108.16
  AND internal-result(<pktplus>)
  AND NOT passes-firewall(<pkt>);

> IS POSSIBLE?;
true
>
```

Some return packets will be dropped.

Similar query: **outgoing** packets all pass the firewall.

“Which rule(s) were responsible?”

```
> EXPLORE
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
  AND FastEthernet0 = entry-interface
  AND prot-TCP = protocol
  AND port-80 = src-port-in
  AND dest-addr-in = 209.172.108.16
  AND internal-result(<pktplus>)
  AND NOT passes-firewall(<pkt>);

> SHOW REALIZED
  InboundACL:router-FastEthernet0-line22_applies(<pkt>),
  InboundACL:router-FastEthernet0-line23_applies(<pkt>),
  InboundACL:router-FastEthernet0-line24_applies(<pkt>),
  InboundACL:router-FastEthernet0-line25_applies(<pkt>),
  InboundACL:router-FastEthernet0-line26_applies(<pkt>);
```

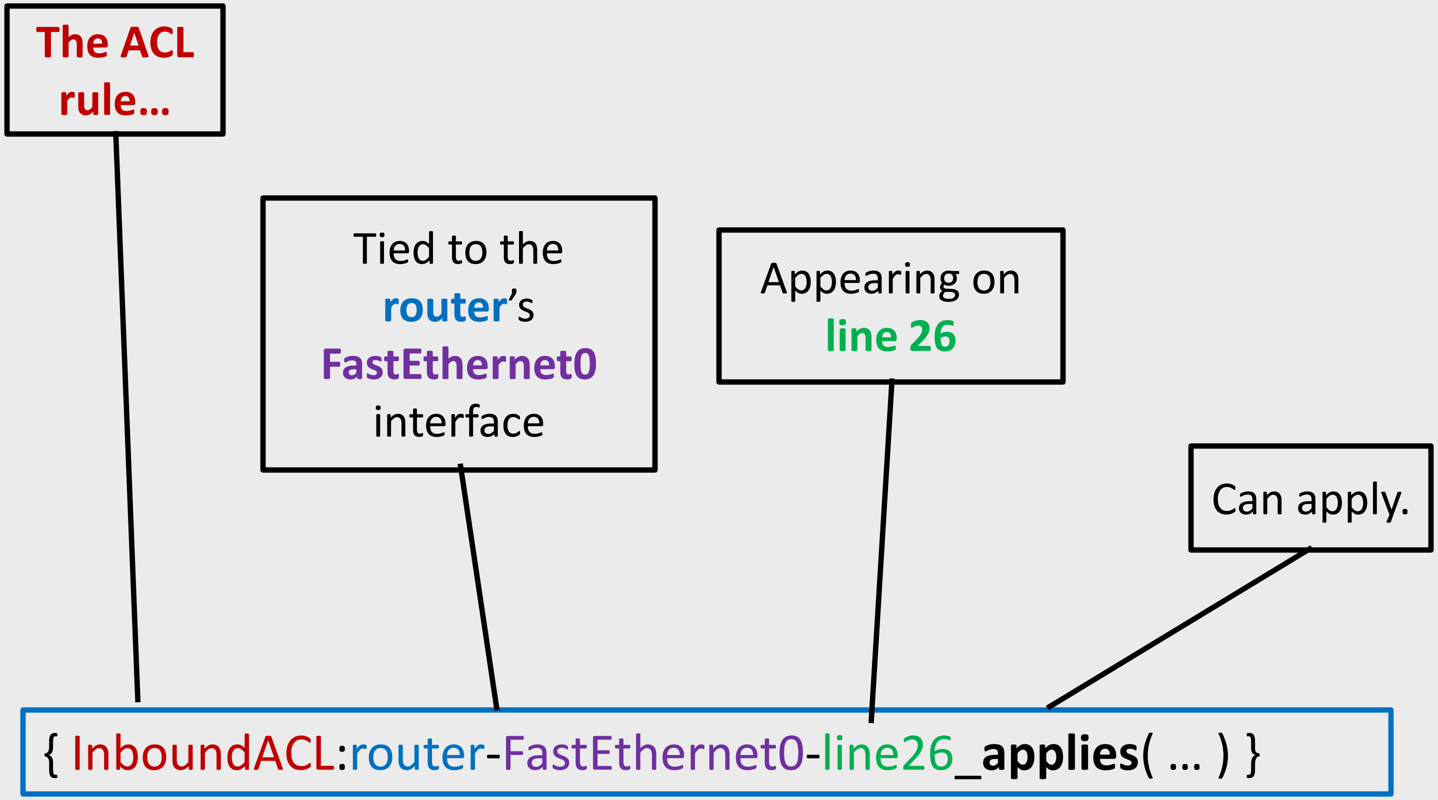
“Which rule(s) were responsible?”

```
> EXPLORE
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
  AND FastEthernet0 = entry-interface
  AND prot-TCP = protocol
  AND port-80 = src-port-in
  AND dest-addr-in = 209.172.108.16
  AND internal-result(<pktplus>)
  AND NOT passes-firewall(<pkt>);

> SHOW REALIZED
  InboundACL:router-FastEthernet0-line22_applies(<pkt>),
  InboundACL:router-FastEthernet0-line23_applies(<pkt>),
  InboundACL:router-FastEthernet0-line24_applies(<pkt>),
  InboundACL:router-FastEthernet0-line25_applies(<pkt>),
  InboundACL:router-FastEthernet0-line26_applies(<pkt>);
```

The ACL rules tied to FastEthernet0

“Which rule(s) were responsible?”

```
> EXPLORE
  NOT src-addr-in IN 192.168.2.0/255.255.255.0
  AND FastEthernet0 = entry-interface
  AND prot-TCP = protocol
  AND port-80 = src-port-in
  AND dest-addr-in = 209.172.108.16
  AND internal-result(<pktplus>)
  AND NOT passes-firewall(<pkt>);

> SHOW REALIZED
  InboundACL:router-FastEthernet0-line22_applies(<pkt>),
  InboundACL:router-FastEthernet0-line23_applies(<pkt>),
  InboundACL:router-FastEthernet0-line24_applies(<pkt>),
  InboundACL:router-FastEthernet0-line25_applies(<pkt>),
  InboundACL:router-FastEthernet0-line26_applies(<pkt>);

{ InboundACL:router-FastEthernet0-line26_applies( … ) }
>
```



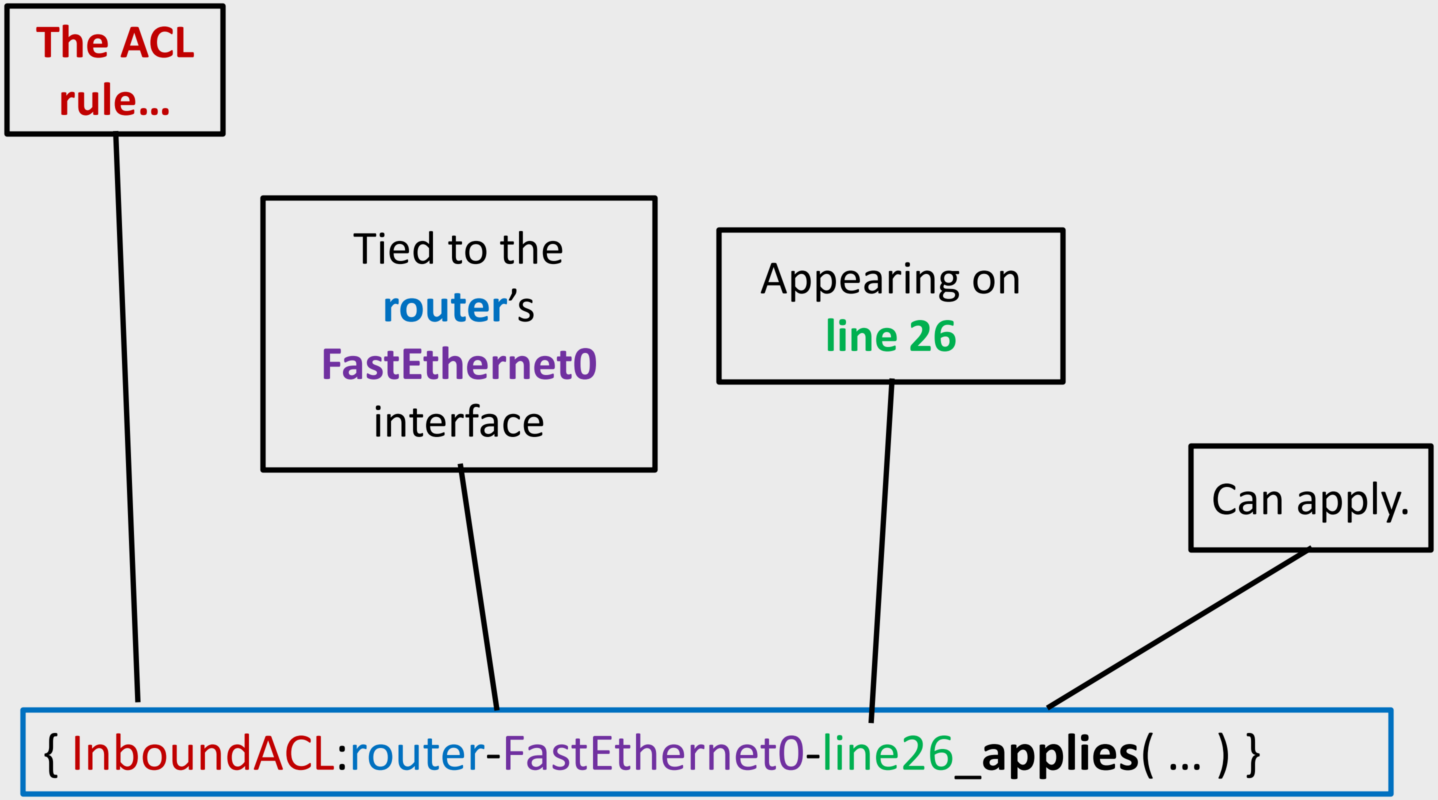
The ACL rule…

Tied to the **router**’s **FastEthernet0** interface

Appearing on **line 26**

Can apply.

{ InboundACL:router-FastEthernet0-line26_**applies**(…) }



The ACL rule…

Tied to the **router**’s **FastEthernet0** interface

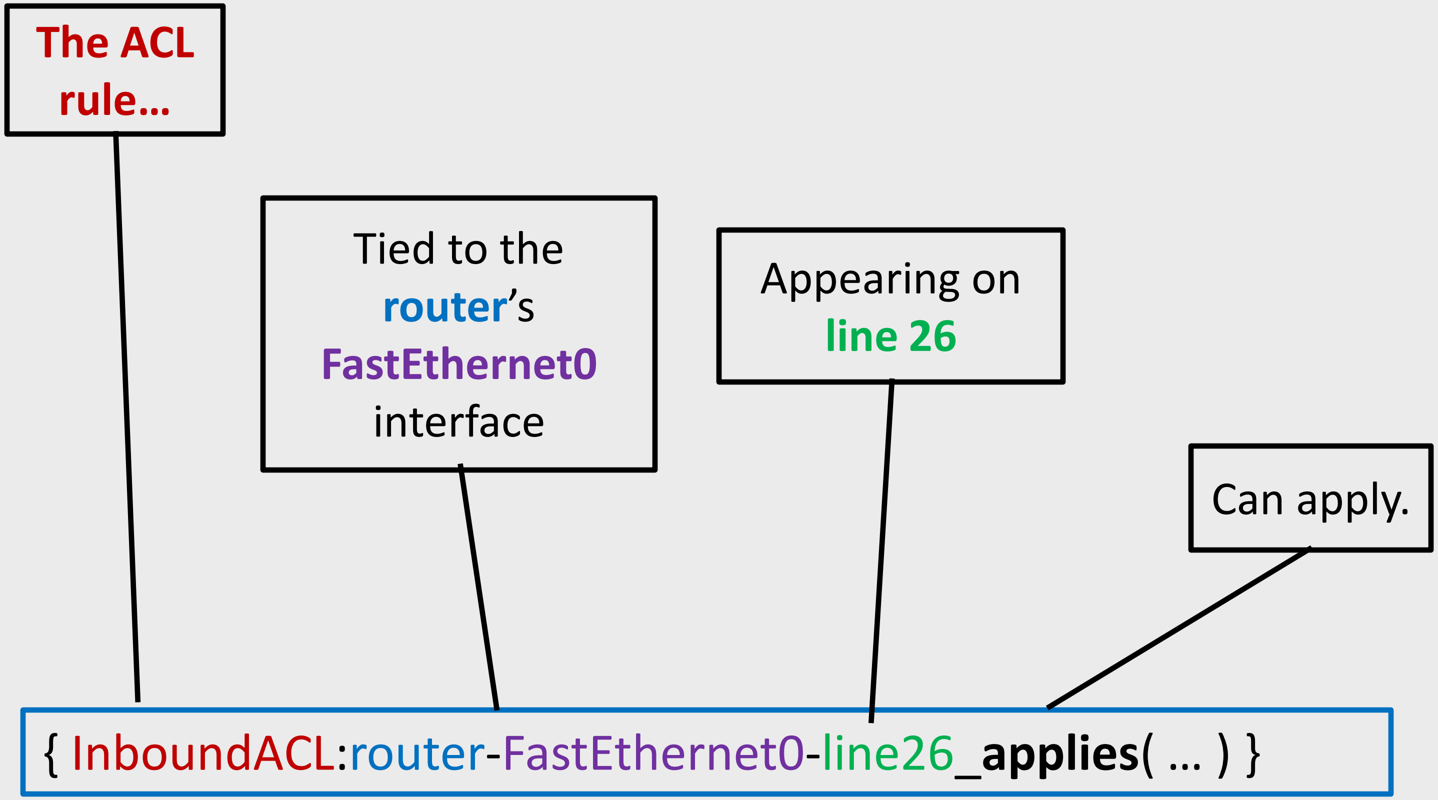
Appearing on **line 26**

Can apply.

```
{ InboundACL:router-FastEthernet0-line26_applies( … ) }
```

Use these in queries too:

```
EXPLORE InboundACL:router-FastEthernet0-line26_applies(<pkt>);
```



The ACL rule…

Tied to the **router**’s **FastEthernet0** interface

Appearing on **line 26**

Can apply.

```
{ InboundACL:router-FastEthernet0-line26_applies( … ) }
```

Use these in queries too:

```
EXPLORE InboundACL:router-FastEthernet0-line26_applies(<pkt>);
```

```
EXPLORE InboundACL:router-FastEthernet0-line26_matches (<pkt>);
```

“Add a rule allowing all returning traffic from port 80…”

“Add a rule allowing all returning traffic from port 80…”

networking
-forum.com
Think you know Cisco? *Think again.*

Will this change fix my problem?

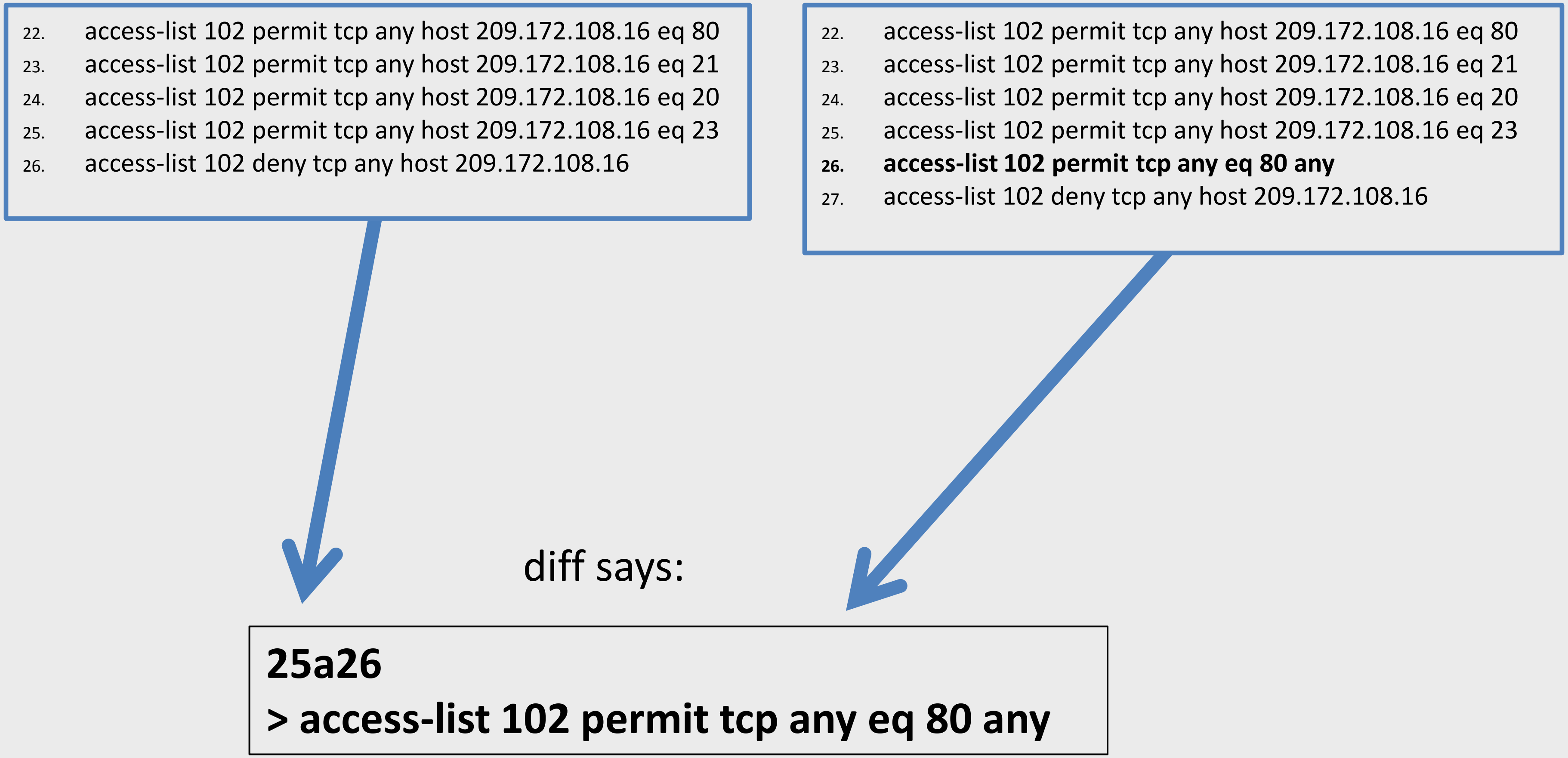
"Add a rule allowing all returning traffic from port 80…"

Will this change fix my problem?

Will it introduce new problems?

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 permit tcp any eq 80 any
access-list 102 deny tcp any host 209.172.108.16
```



```
22.  access-list 102 permit tcp any host 209.172.108.16 eq 80
23.  access-list 102 permit tcp any host 209.172.108.16 eq 21
24.  access-list 102 permit tcp any host 209.172.108.16 eq 20
25.  access-list 102 permit tcp any host 209.172.108.16 eq 23
26.  access-list 102 deny tcp any host 209.172.108.16
```

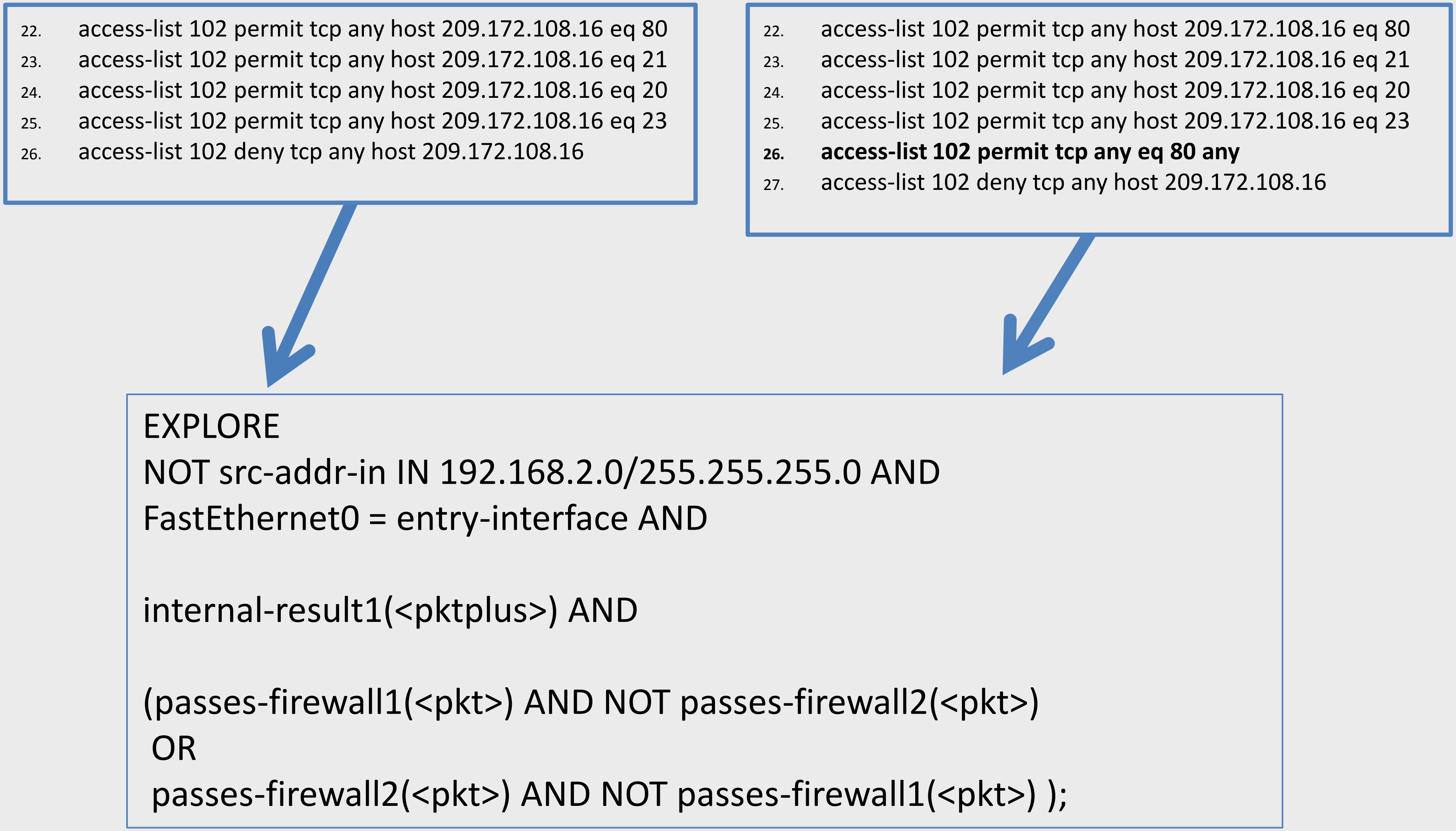
```
22.  access-list 102 permit tcp any host 209.172.108.16 eq 80
23.  access-list 102 permit tcp any host 209.172.108.16 eq 21
24.  access-list 102 permit tcp any host 209.172.108.16 eq 20
25.  access-list 102 permit tcp any host 209.172.108.16 eq 23
26.  access-list 102 permit tcp any eq 80 any
27.  access-list 102 deny tcp any host 209.172.108.16
```

diff says:

```
25a26
> access-list 102 permit tcp any eq 80 any
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

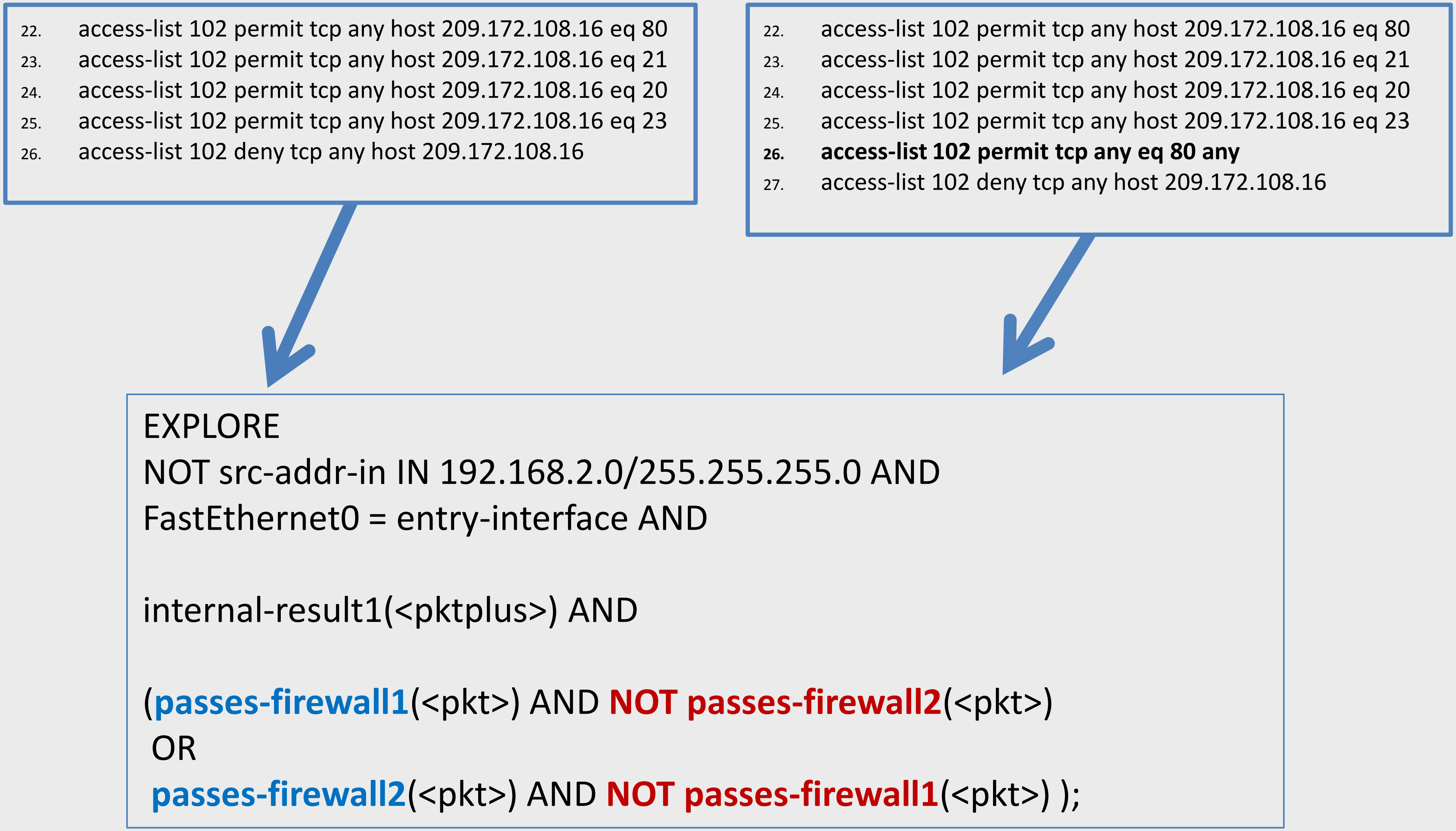
```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 permit tcp any eq 80 any
access-list 102 deny tcp any host 209.172.108.16
```



```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 permit tcp any eq 80 any
access-list 102 deny tcp any host 209.172.108.16
```

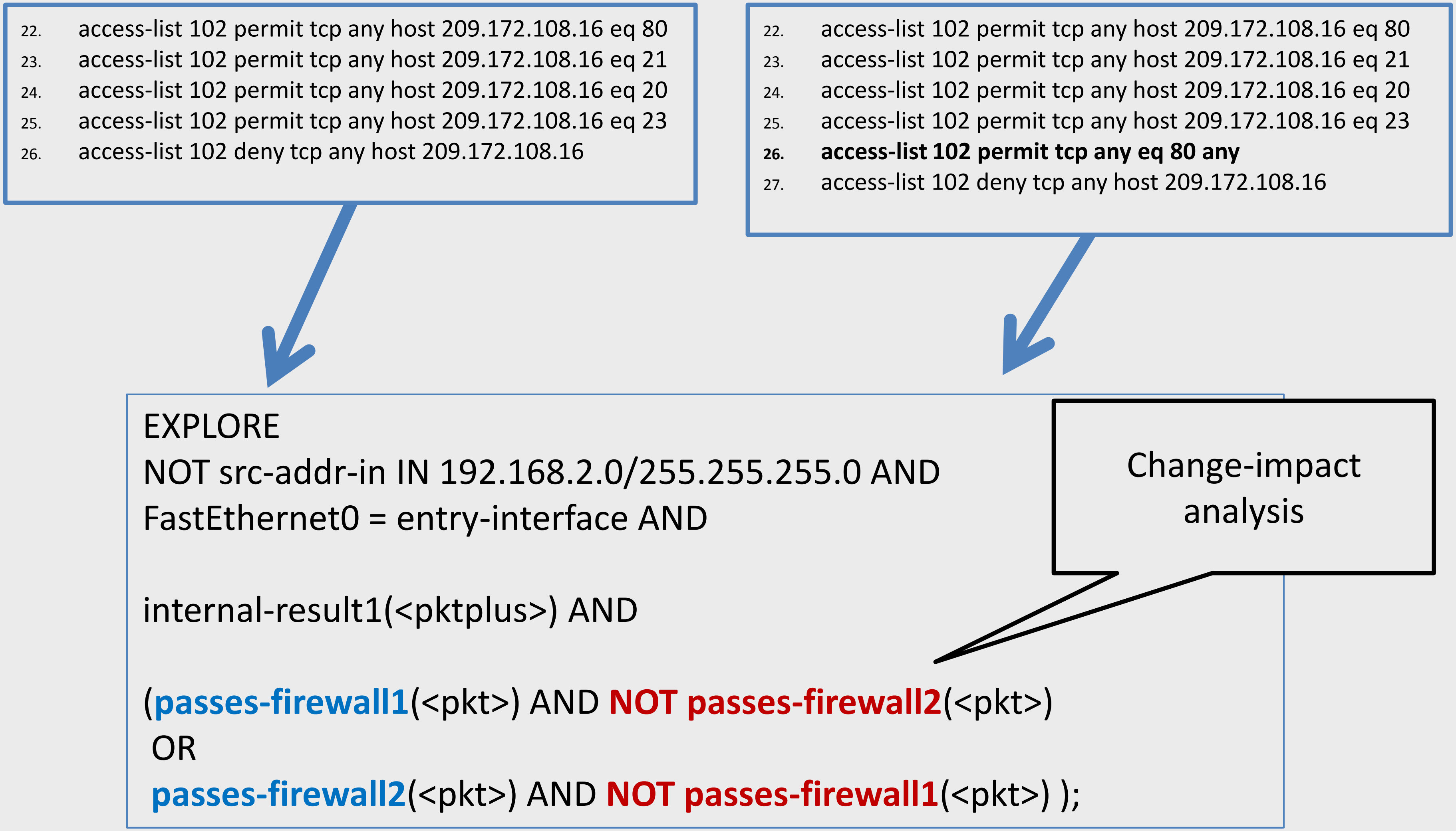
```
EXPLORE
NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
FastEthernet0 = entry-interface AND

internal-result1(<pktplus>) AND

(passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
 OR
 passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );
```



```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 permit tcp any eq 80 any
access-list 102 deny tcp any host 209.172.108.16
```

```
EXPLORE
NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
FastEthernet0 = entry-interface AND

internal-result1(<pktplus>) AND

(passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
 OR
 passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );
```



```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 deny tcp any host 209.172.108.16
```

```
access-list 102 permit tcp any host 209.172.108.16 eq 80
access-list 102 permit tcp any host 209.172.108.16 eq 21
access-list 102 permit tcp any host 209.172.108.16 eq 20
access-list 102 permit tcp any host 209.172.108.16 eq 23
access-list 102 permit tcp any eq 80 any
access-list 102 deny tcp any host 209.172.108.16
```

```
EXPLORE
NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
FastEthernet0 = entry-interface AND

internal-result1(<pktplus>) AND

(passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
 OR
 passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );
```

Change-impact analysis

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );

> SHOW ALL;
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );

> SHOW ALL;
```

```
protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1
```

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)

                              ND NOT passes-firewall1(<pkt>) );

> SHO          L;
```

Public address of server

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passe                          T passes-firewall1(<pkt>) );

> SHOW
```

protocol: pro

entry-interface: faste ernet0

dest-addr-in: 209.172 108.16

src-addr-in: ipaddress

dest-port-in: port

src-port-in: port-80

exit-interface: vlan1

"Some **other** address"

"Some **other** port"

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );

> SHOW ALL;
```

```
protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1
```

Packet is routed successfully

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-firewall1(<pkt>) );

> SHOW ALL;
```

```
protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1
```

```
protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: ipaddress
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1
```

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-

> SHOW ALL;
```

More than we intended?

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

protocol: p -tcp
entry-interface: fas ethernet0
dest-addr-in: ipaddress
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-

> SHOW ALL;
```

More than we intended?

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

protocol: p -tcp
entry-interface: fas ethernet0
dest-addr-in: ipaddress
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

…

```
> EXPLORE
   NOT src-addr-in IN 192.168.2.0/255.255.255.0 AND
   fastethernet0 = entry-interface AND
   internal-result1(<pktplus>) AND
   (passes-firewall1(<pkt>) AND NOT passes-firewall2(<pkt>)
    OR
    passes-firewall2(<pkt>) AND NOT passes-

> SHOW ALL;
```

More than we intended?

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

protocol: p -tcp
entry-interface: fas ethernet0
dest-addr-in: ipaddress
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

…

Query:

Query:

```
EXPLORE
passes-firewall(<pkt>)
```

Query:

EXPLORE
passes-firewall(**<pkt>**)

Variables for packet contents & handling

Query:

EXPLORE
passes-firewall(**<pkt>**)

entry-interface,
next-hop,
dest-addr-in,
…

Query:

EXPLORE
passes-firewall(**<pkt>**)

entry-interface,
next-hop,
dest-addr-in,
…

Scenario:

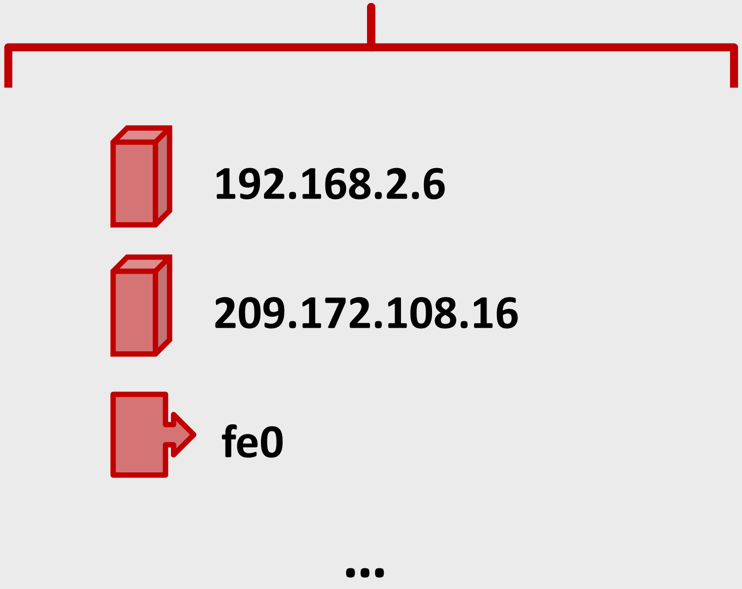
entry-interface: fe0
next-hop: 192.168.2.6
dest-addr-in: 209.172.108.16
…

Query:

EXPLORE
passes-firewall(**<pkt>**)

Scenario:

entry-interface: fe0
next-hop: 192.168.2.6
dest-addr-in: 209.172.108.16
…



192.168.2.6

209.172.108.16

fe0

…

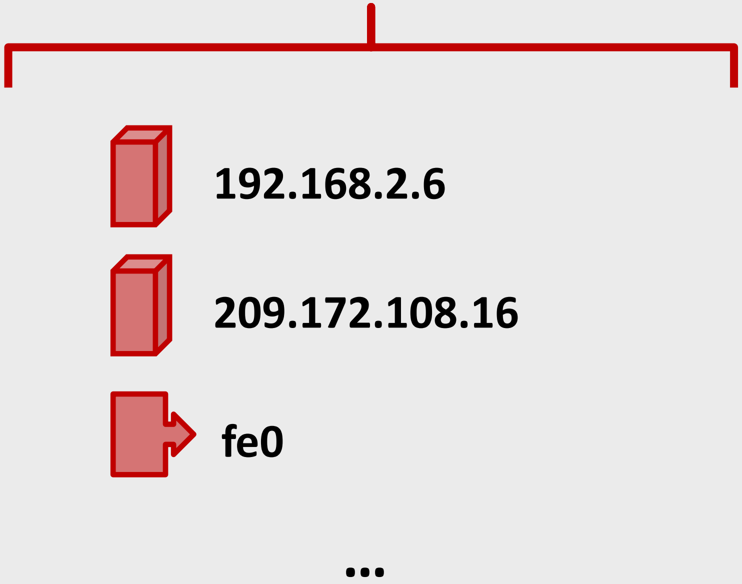
Query:

EXPLORE
passes-firewall(**<pkt>**)

How large a scenario do we need to check?

Scenario:

entry-interface: fe0
next-hop: 192.168.2.6
dest-addr-in: 209.172.108.16
…



192.168.2.6

209.172.108.16

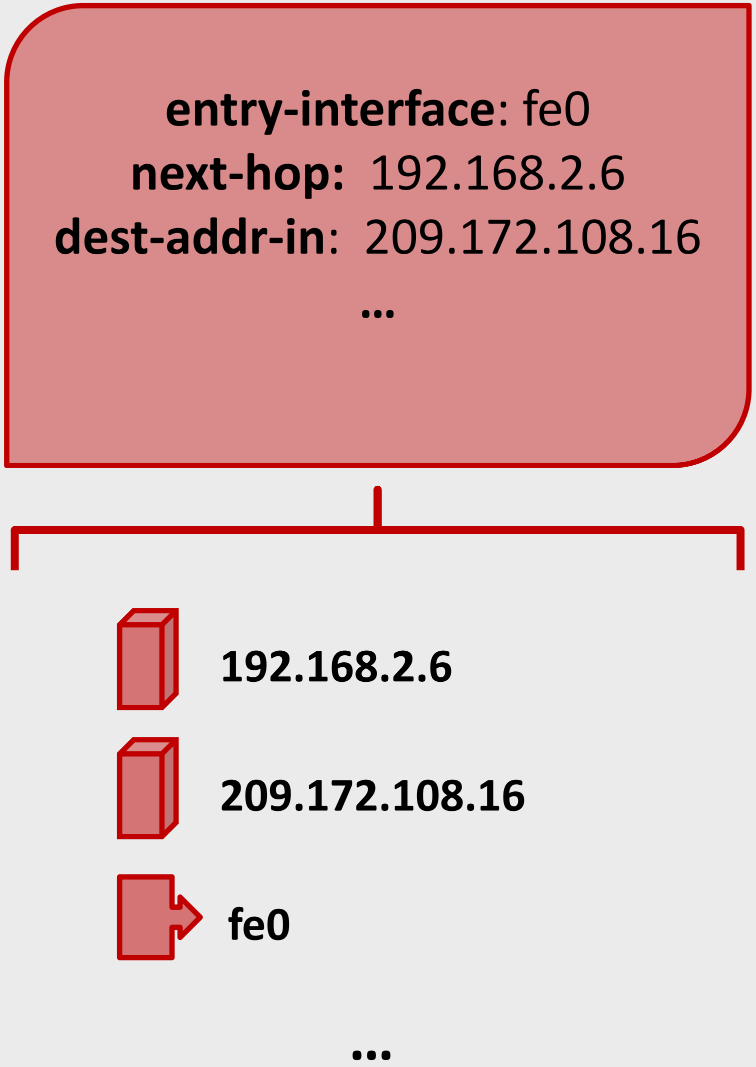
fe0

…

Query:

EXPLORE
passes-firewall(**<pkt>**)

Scenario:



entry-interface: fe0
next-hop: 192.168.2.6
dest-addr-in: 209.172.108.16
…

How large a scenario do we need to check?

Margrave computes a bound automatically, most of the time.

Let’s Recap:

Let’s Recap:

Do scenarios exist?

True/false

Let’s Recap:

Do scenarios exist?

True/false

Which scenarios exist?

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

Let’s Recap:

Do scenarios exist?

True/false

Which scenarios exist?

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

Which rules can take effect?

“InboundACL for FastEthernet0 on Line26”

Let’s Recap:

Do scenarios exist?

True/false

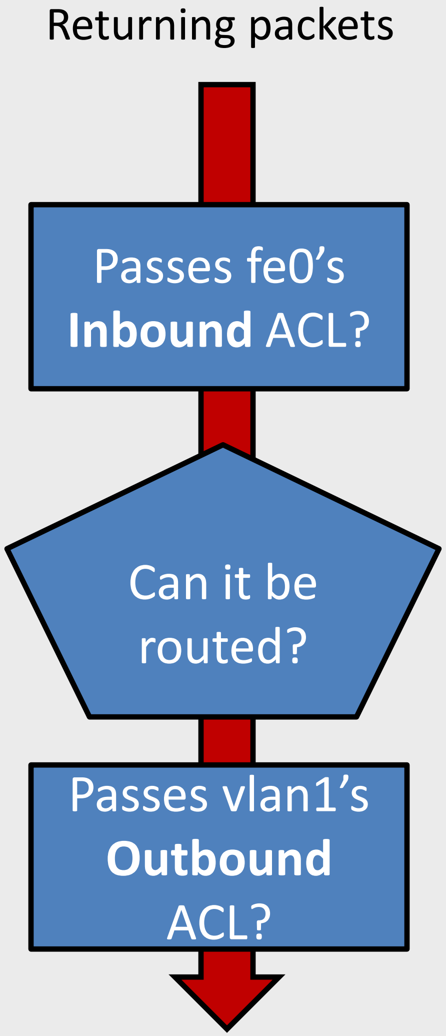
Which scenarios exist?

protocol: prot-tcp
entry-interface: fastethernet0
dest-addr-in: 209.172.108.16
src-addr-in: ipaddress
dest-port-in: port
src-port-in: port-80
exit-interface: vlan1

Which rules can take effect?

“InboundACL for FastEthernet0 on Line26”

Single-configuration
and
multi-configuration queries
(Change-impact analysis)

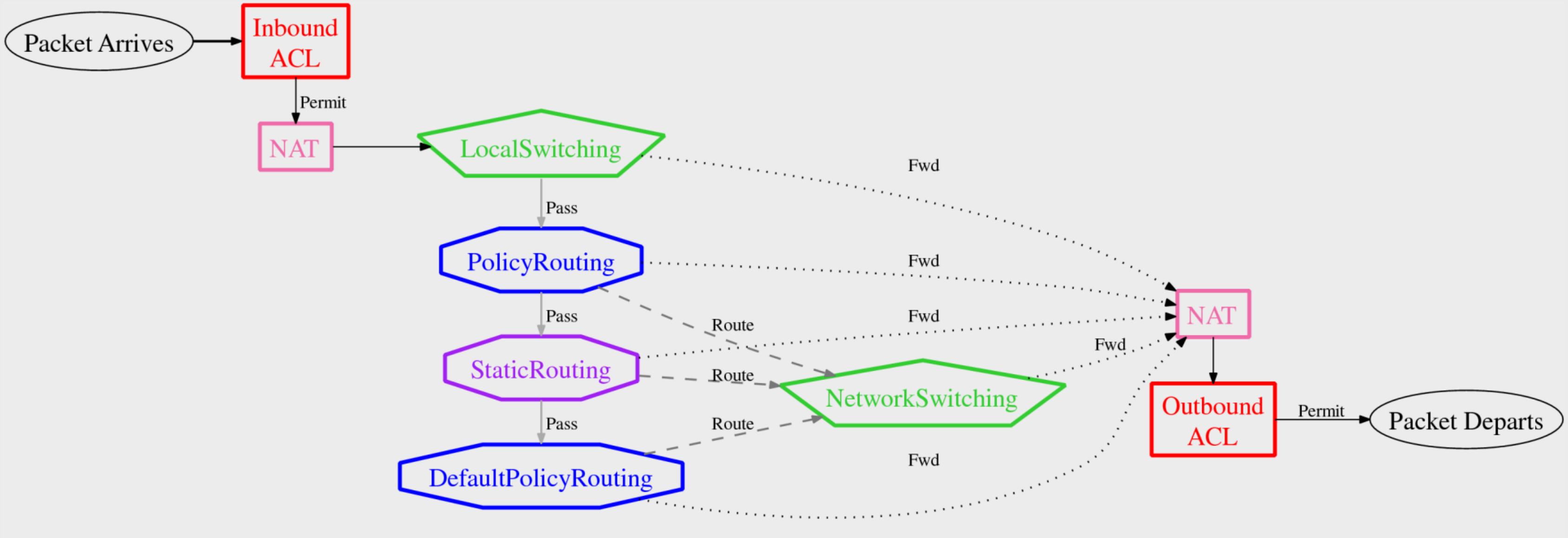

Returning packets
Passes fe0's **Inbound** ACL?
Can it be routed?
Passes vlan1's **Outbound** ACL?

```
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0
ip access-group 101 in
ip policy route-map internet
!
ip route 10.232.100.0 255.255.252.0 10.254.1.130
ip route 10.232.104.0 255.255.252.0 10.254.1.130
!
access-list 101 deny ip 10.232.0.0 0.0.3.255 10.232.4.0 0.0.3.255
access-list 101 deny ip 10.232.4.0 0.0.3.255 10.232.0.0 0.0.3.255
access-list 101 permit ip any any
!
access-list 10 permit 10.232.0.0 0.0.3.255
access-list 10 permit 10.232.100.0 0.0.3.255
!
route-map internet permit 10
match ip address 10
set ip next-hop 10.232.0.15
```

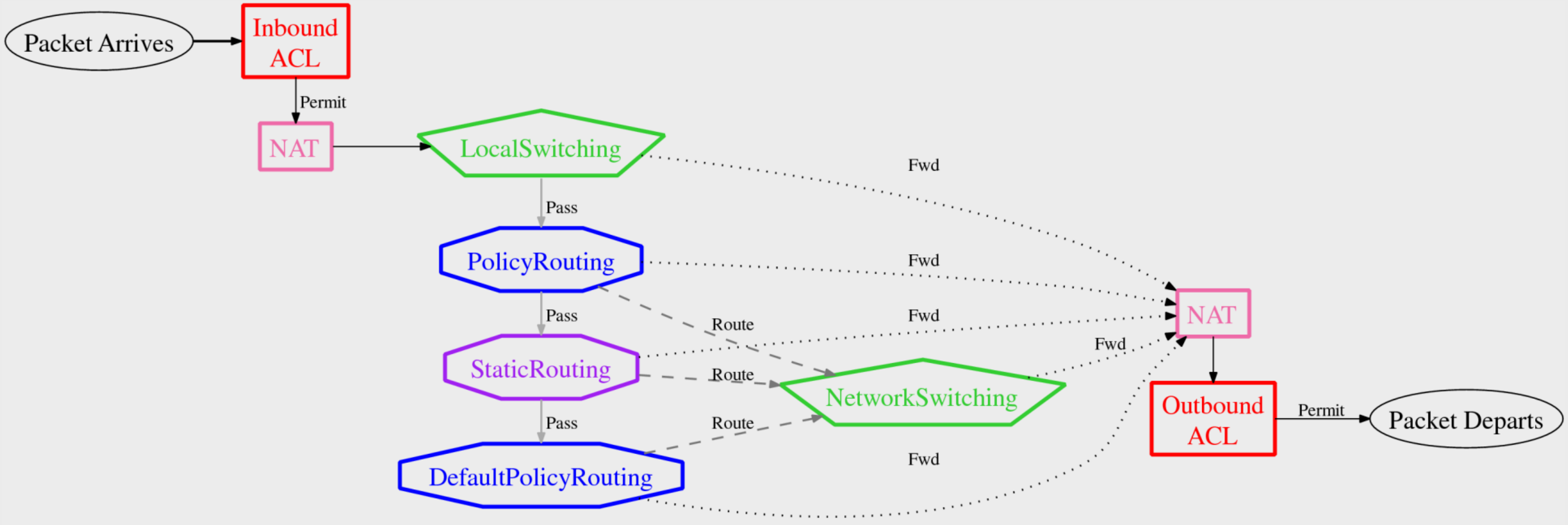
Can it be routed?

```
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0
ip access-group 101 in
ip policy route-map internet
!
ip route 10.232.100.0 255.255.252.0 10.254.1.130
ip route 10.232.104.0 255.255.252.0 10.254.1.130
!
access-list 101 deny ip 10.232.0.0 0.0.3.255 10.232.4.0 0.0.3.255
access-list 101 deny ip 10.232.4.0 0.0.3.255 10.232.0.0 0.0.3.255
access-list 101 permit ip any any
!
access-list 10 permit 10.232.0.0 0.0.3.255
access-list 10 permit 10.232.100.0 0.0.3.255
!
route-map internet permit 10
match ip address 10
set ip next-hop 10.232.0.15
```

How is it routed?


Packet Arrives
Inbound ACL
Permit
NAT
LocalSwitching
Fwd
Pass
PolicyRouting
Fwd
Pass
Route
Fwd
NAT
StaticRouting
Route
Fwd
NetworkSwitching
Pass
Route
Outbound ACL
Permit
Packet Departs
DefaultPolicyRouting
Fwd

ip access-group 102 in

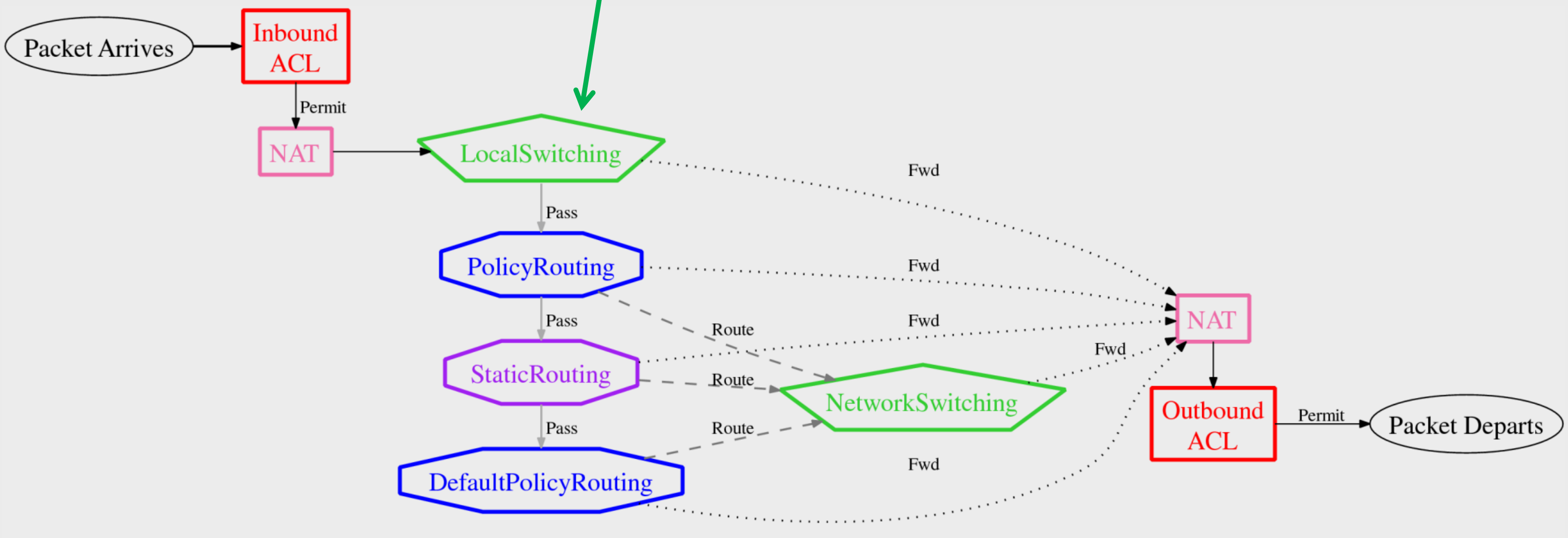


Provides these query terms:

InboundACL:Permit
InboundACL:Deny

```
ip access-group 102 in
```

```
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0
```

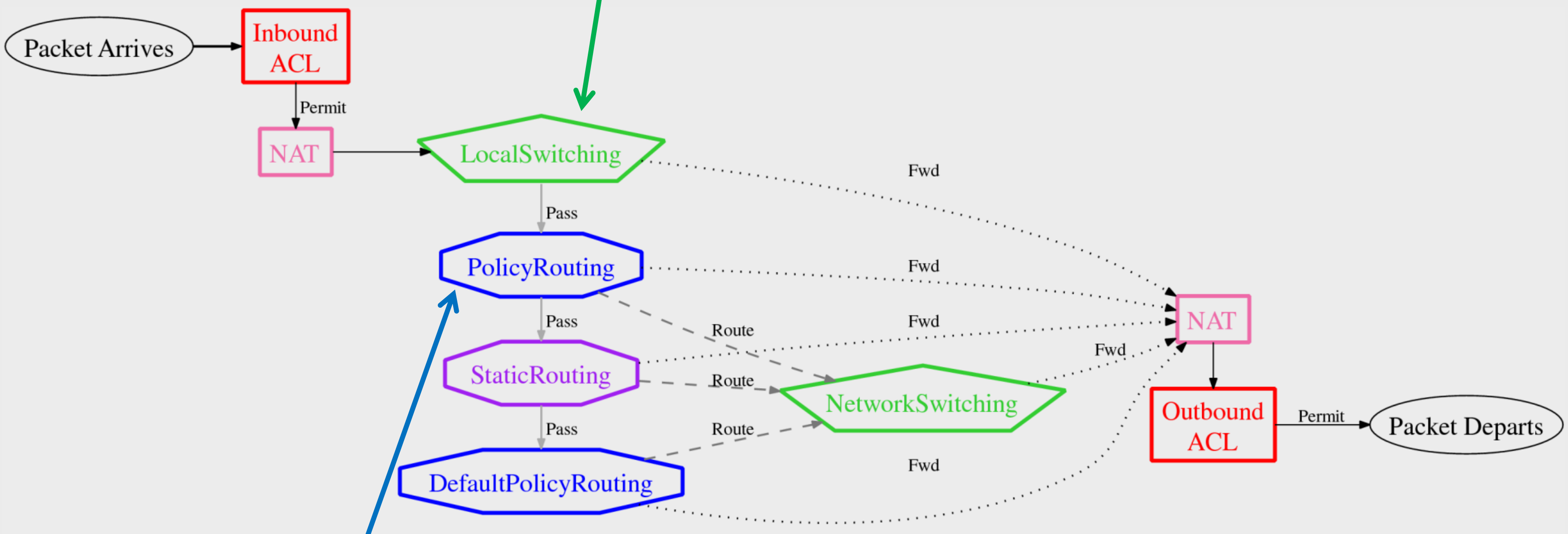


Provides these query terms:

LocalSwitching:Forward
LocalSwitching:Pass

```
ip access-group 102 in
```

```
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0
```



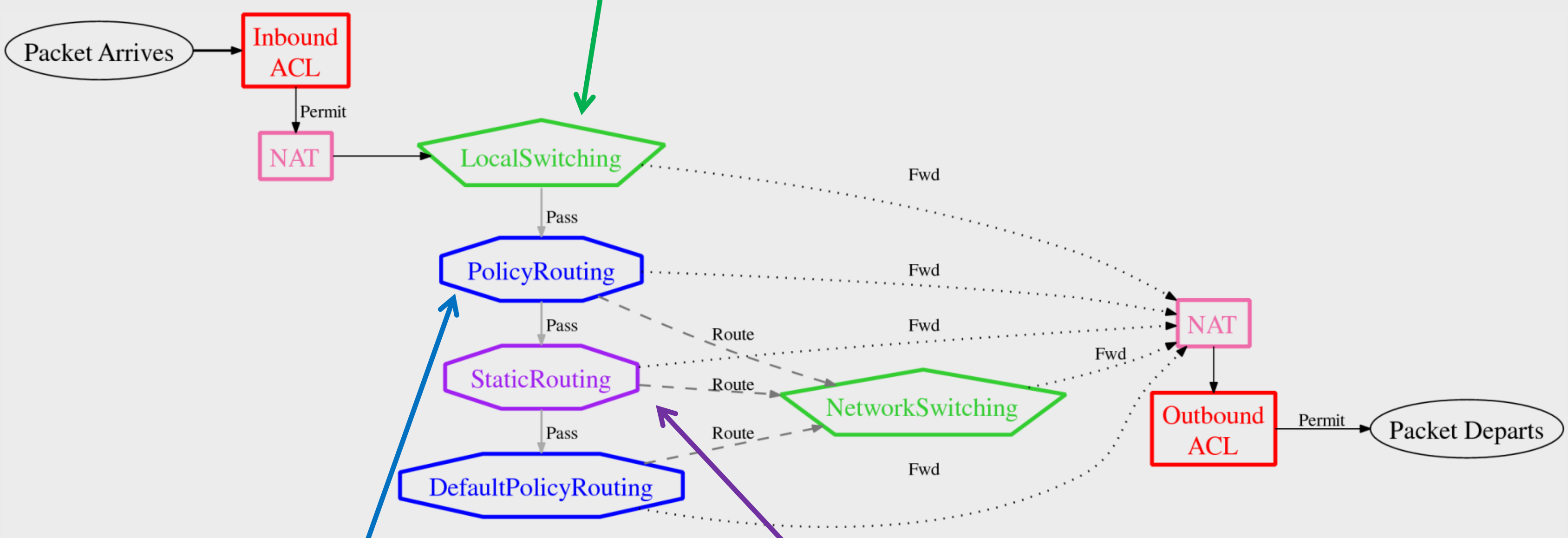
```
ip policy route-map internet

route-map internet permit 10
match ip address 10
set ip next-hop 10.232.0.15
```

Provides these query terms:

PolicyRouting:Forward
PolicyRouting:Route
PolicyRouting:Pass

ip access-group 102 in

interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0



ip policy route-map internet

route-map internet permit 10
match ip address 10
set ip next-hop 10.232.0.15

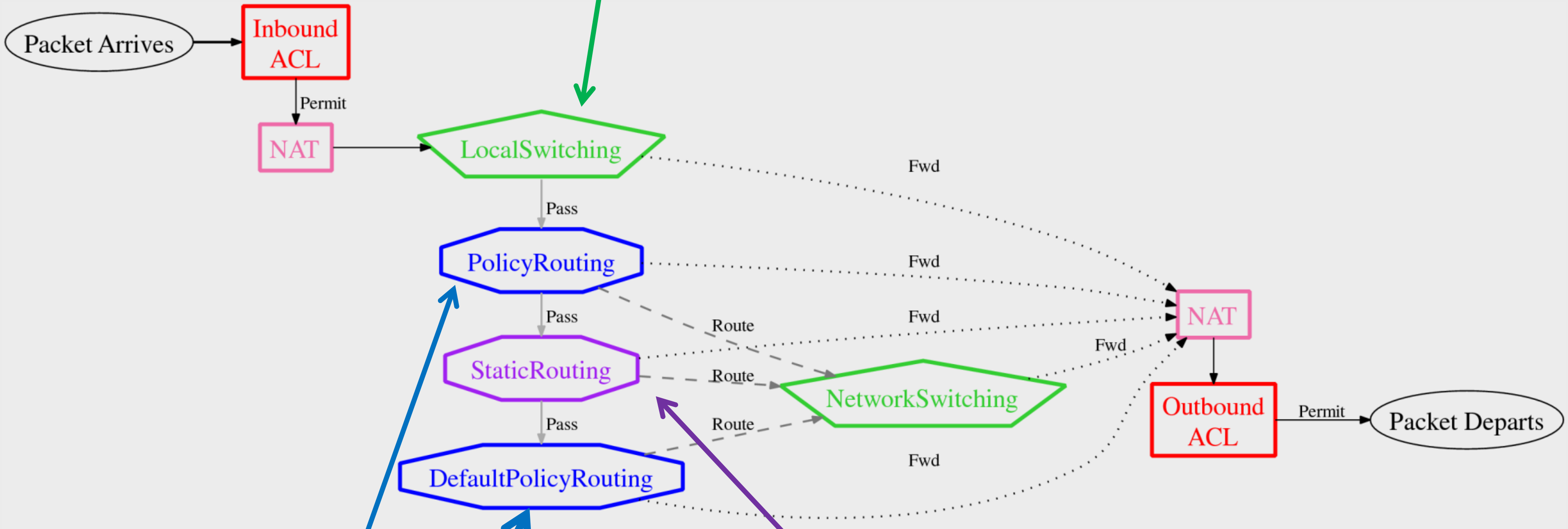
ip route 10.232.100.0 255.255.252.0 10.254.1.130
ip route 10.232.104.0 255.255.252.0 10.254.1.130

Provides these query terms:

StaticRouting:Forward
StaticRouting:Route
StaticRouting:Pass

ip access-group 102 in

interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0



ip policy route-map internet

route-map internet permit 10
match ip address 10
set ip [**default]** next-hop 10.232.0.15

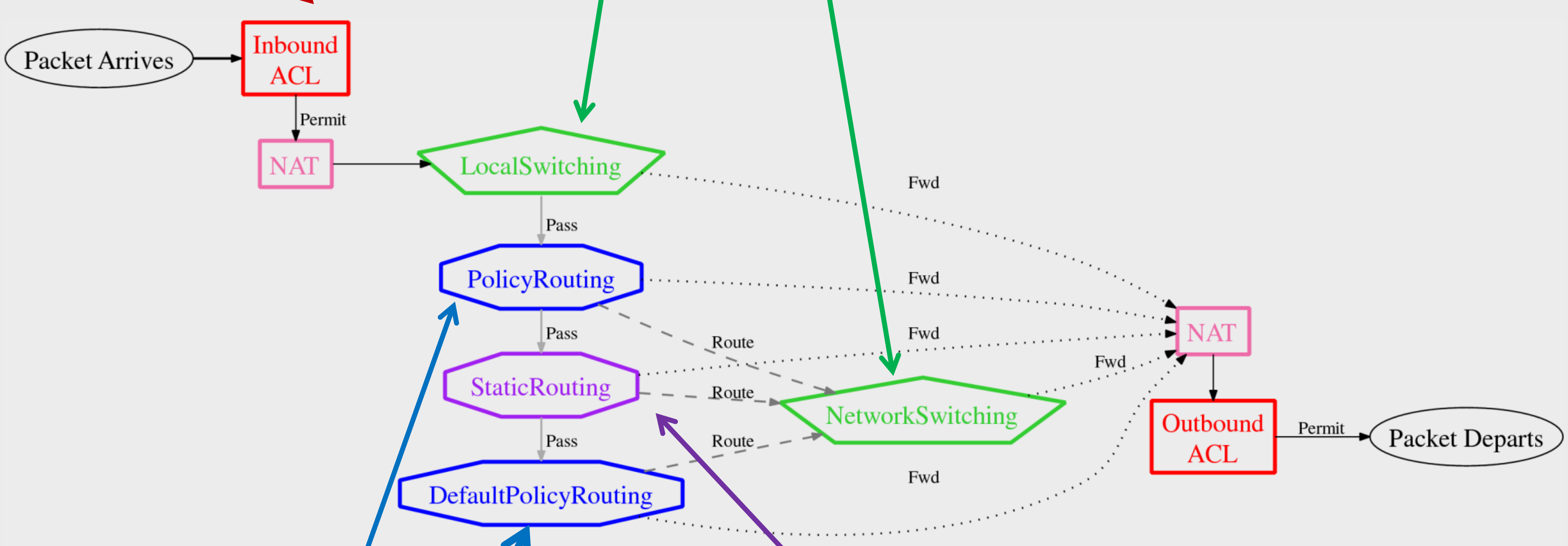
ip route 10.232.100.0 255.255.252.0 10.254.1.130
ip route 10.232.104.0 255.255.252.0 10.254.1.130

Provides these query terms:

DefaultPolicyRouting:Forward
DefaultPolicyRouting:Route
DefaultPolicyRouting:Pass

```
ip access-group 102 in
```

```
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0
```



```
ip route 10.232.100.0 255.255.252.0 10.254.1.130
ip route 10.232.104.0 255.255.252.0 10.254.1.130
```

```
ip policy route-map internet

route-map internet permit 10
match ip address 10
set ip [default] next-hop 10.232.0.15
```

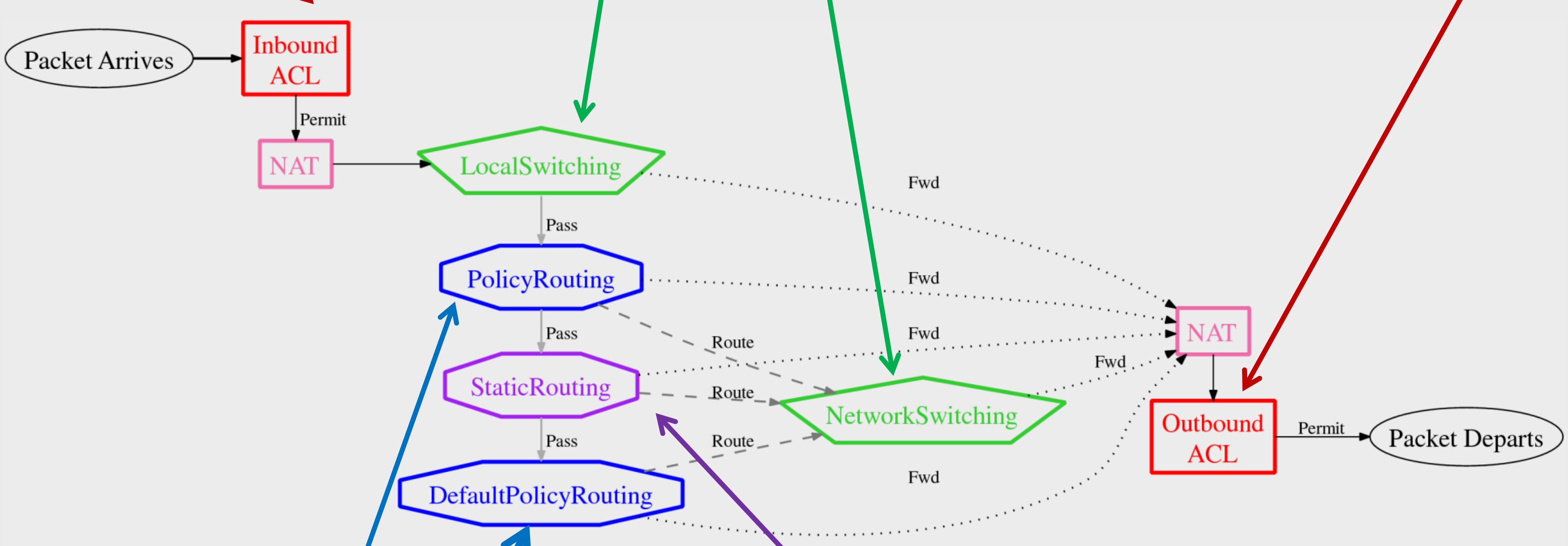
Provides these query terms:

NetworkSwitching:Forward
NetworkSwitching:Pass

```
ip access-group 102 in
```

```
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0
```

```
ip access-group 102 out
```



```
ip policy route-map internet

route-map internet permit 10
match ip address 10
set ip [default] next-hop 10.232.0.15
```

```
ip route 10.232.100.0 255.255.252.0 10.254.1.130
ip route 10.232.104.0 255.255.252.0 10.254.1.130
```

Provides these query terms:

OutboundACL:Permit
OutboundACL:Deny

EXPLORE

entry-interface = fastethernet0

AND **NOT** **LocalSwitching:Forward**(<pkt>)

I only want packets that don’t have a local destination.

EXPLORE

entry-interface = fastethernet0

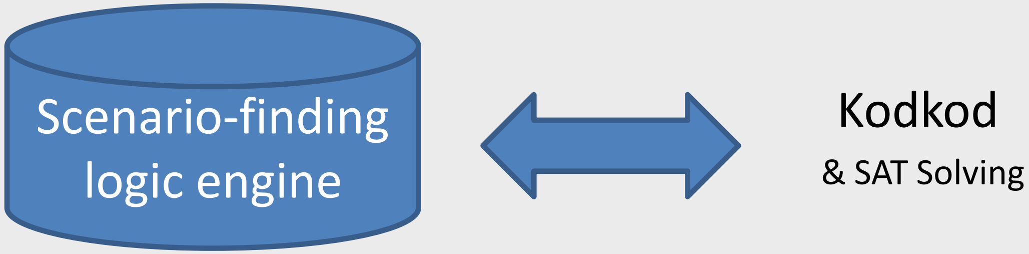
AND **NOT** **LocalSwitching:Forward**(<pkt>)

I only want packets that don’t have a local destination.

Does the static route ever apply to WWW packets?

Which permitted packets are handled by policy routing?

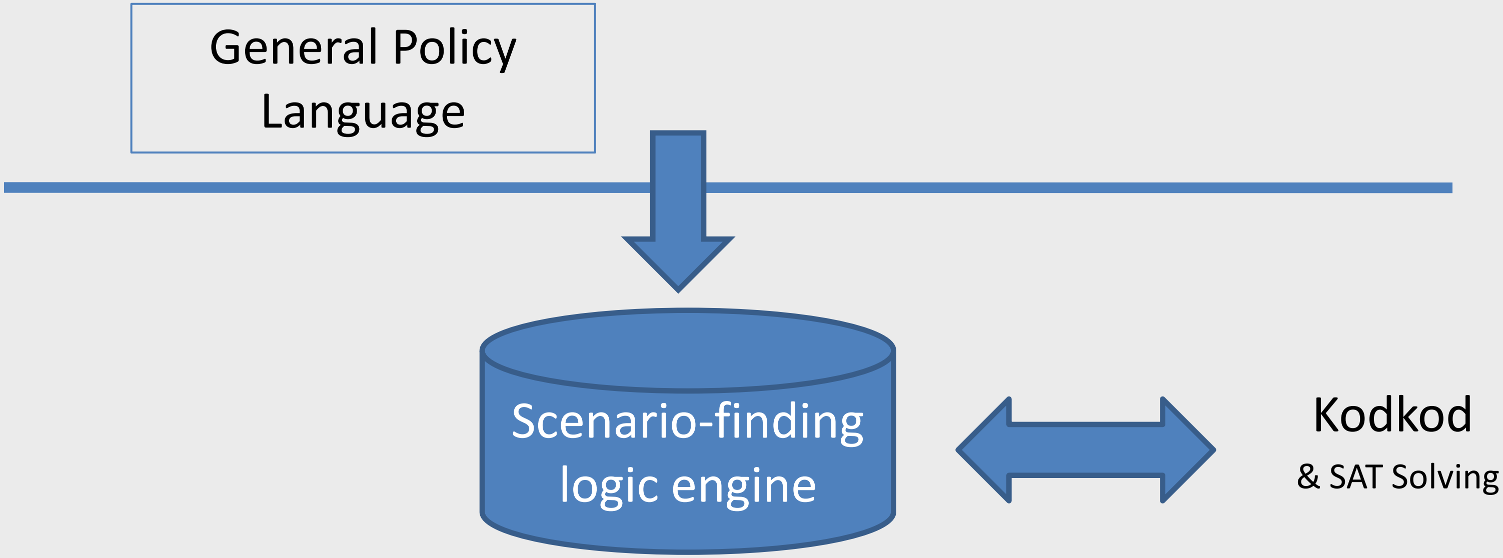
Scenario-finding
logic engine



Scenario-finding logic engine

Kodkod

& SAT Solving

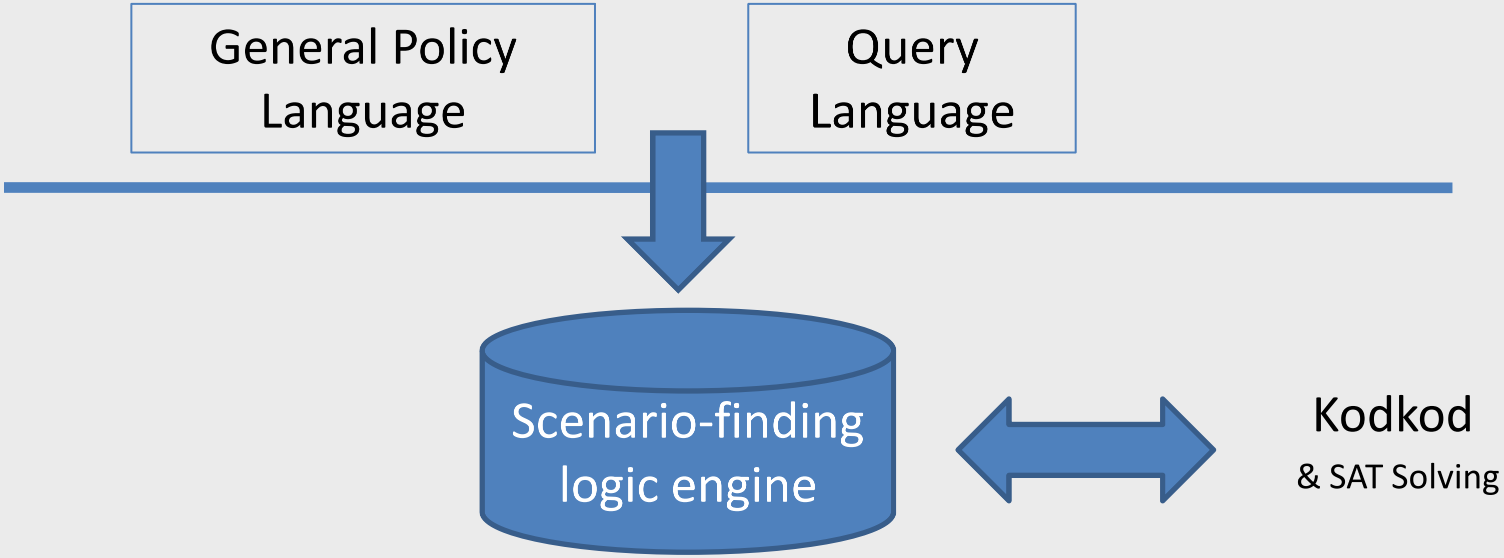


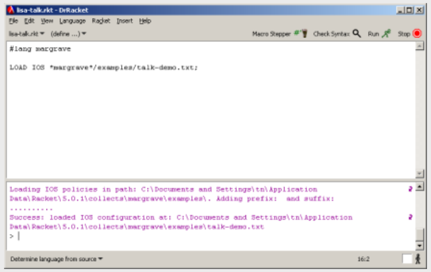
General Policy Language

Scenario-finding logic engine

Kodkod

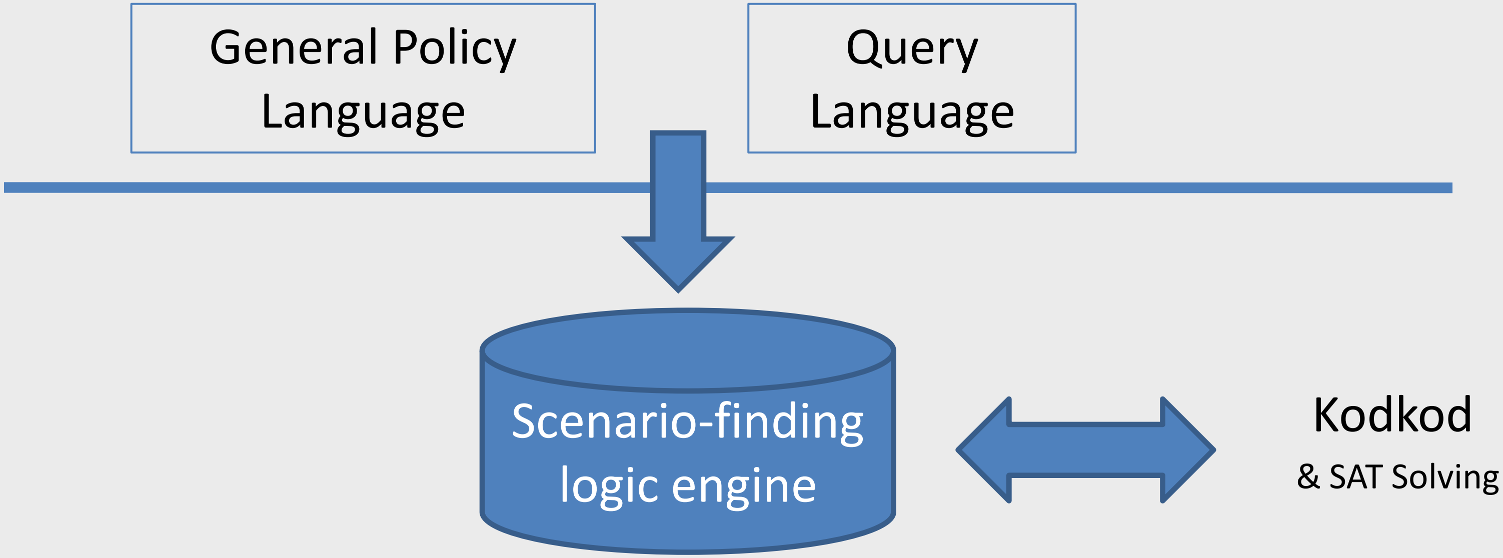
& SAT Solving


General Policy Language
Query Language
Scenario-finding logic engine
Kodkod
& SAT Solving


lisa-talk.rkt - DrRacket
File Edit View Language Racket Insert Help
lisa-talk.rkt (define ...)
Macro Stepper Check Syntax Run Stop
Determine language from source
16:2

```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
Loading IOS policies in path: C:\Documents and Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\. Adding prefix:  and suffix:
..........
Success: loaded IOS configuration at: C:\Documents and Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
> |
```



General Policy Language

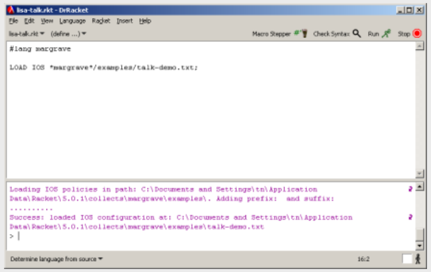
Query Language

Scenario-finding logic engine

Kodkod

& SAT Solving

Supported subset of Cisco IOS



lisa-talk.rkt - DrRacket
File Edit View Language Racket Insert Help
lisa-talk.rkt (define ...)
Macro Stepper Check Syntax Run Stop

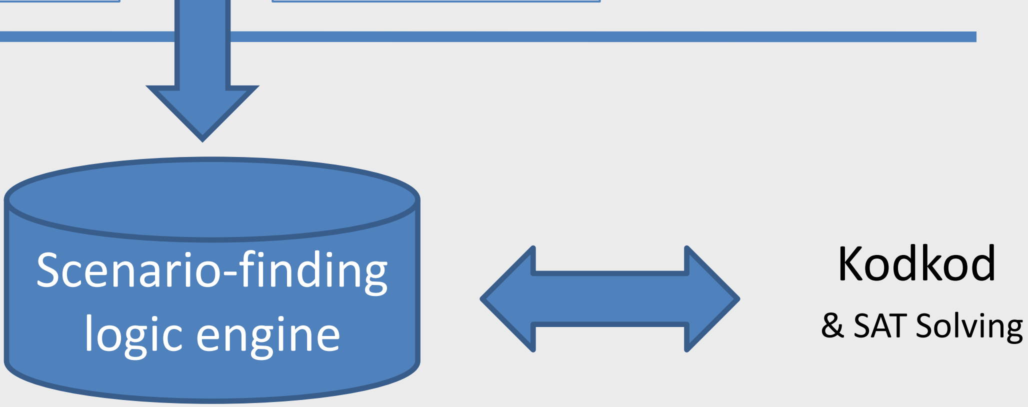
```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
Loading IOS policies in path: C:\Documents and Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\. Adding prefix:  and suffix:
..........
Success: loaded IOS configuration at: C:\Documents and Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
> |
```

Determine language from source
16:2

General Policy Language

Query Language



Scenario-finding logic engine

Kodkod

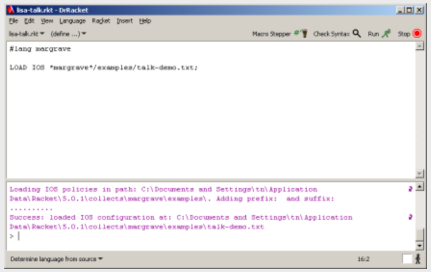
& SAT Solving

Iptables
(in progress)

<u>Supported subset of Cisco IOS</u>

XACML

Amazon SQS



```
#lang margrave

LOAD IOS *margrave*/examples/talk-demo.txt;
```

```
Loading IOS policies in path: C:\Documents and Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\. Adding prefix:  and suffix:
..........
Success: loaded IOS configuration at: C:\Documents and Settings\tn\Application
Data\Racket\5.0.1\collects\margrave\examples\talk-demo.txt
> |
```

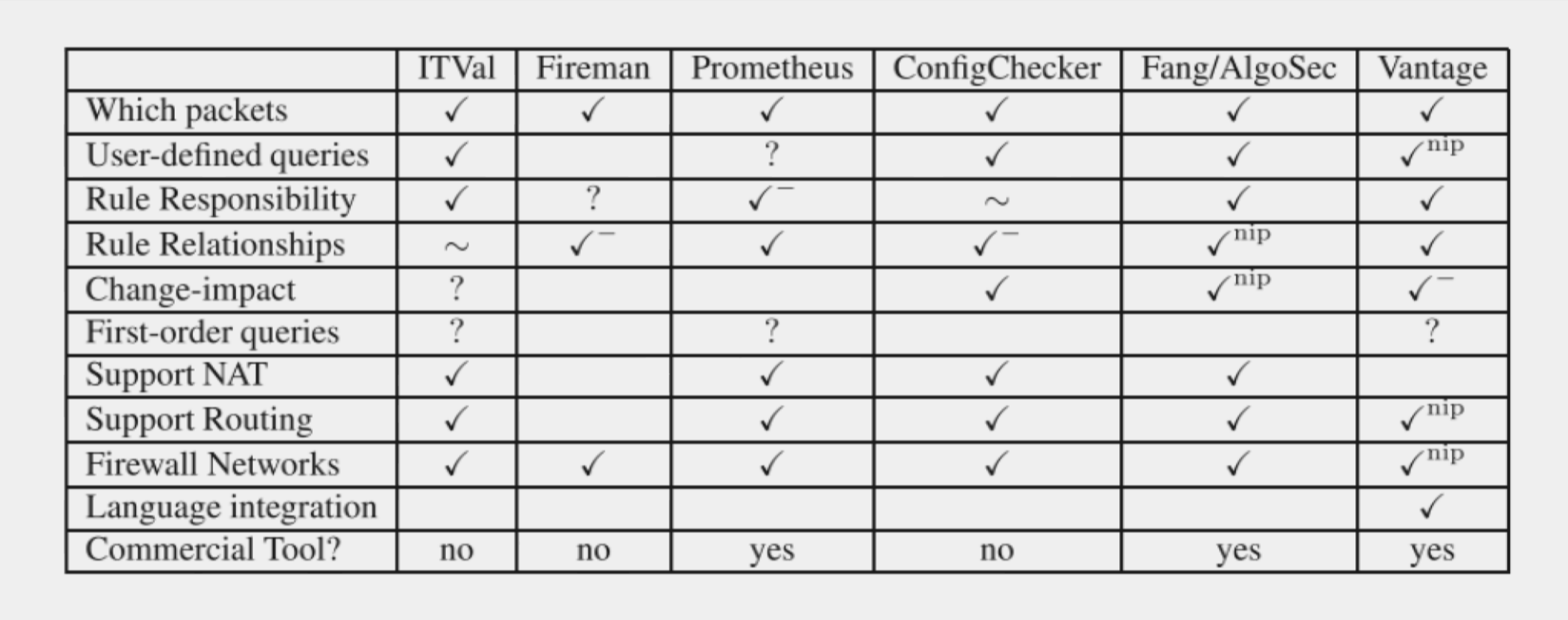
General Policy Language

Query Language

Scenario-finding logic engine

Kodkod

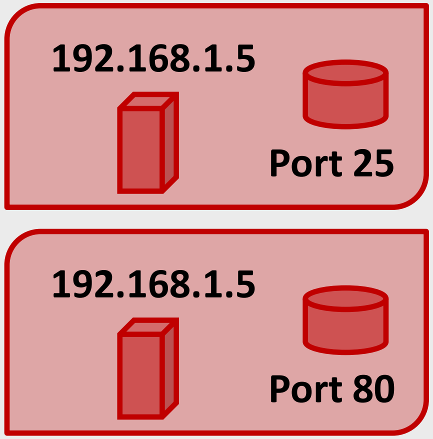
& SAT Solving



	ITVal	Fireman	Prometheus	ConfigChecker	Fang/AlgoSec	Vantage
Which packets	✓	✓	✓	✓	✓	✓
User-defined queries	✓		?	✓	✓	$\checkmark^{\mathrm{nip}}$
Rule Responsibility	✓	?	$\checkmark^{-}$	$\sim$	✓	✓
Rule Relationships	$\sim$	$\checkmark^{-}$	✓	$\checkmark^{-}$	$\checkmark^{\mathrm{nip}}$	✓
Change-impact	?			✓	$\checkmark^{\mathrm{nip}}$	$\checkmark^{-}$
First-order queries	?		?			?
Support NAT	✓		✓	✓	✓	
Support Routing	✓		✓	✓	✓	$\checkmark^{\mathrm{nip}}$
Firewall Networks	✓	✓	✓	✓	✓	$\checkmark^{\mathrm{nip}}$
Language integration						✓
Commercial Tool?	no	no	yes	no	yes	yes

Future Work

Future Work



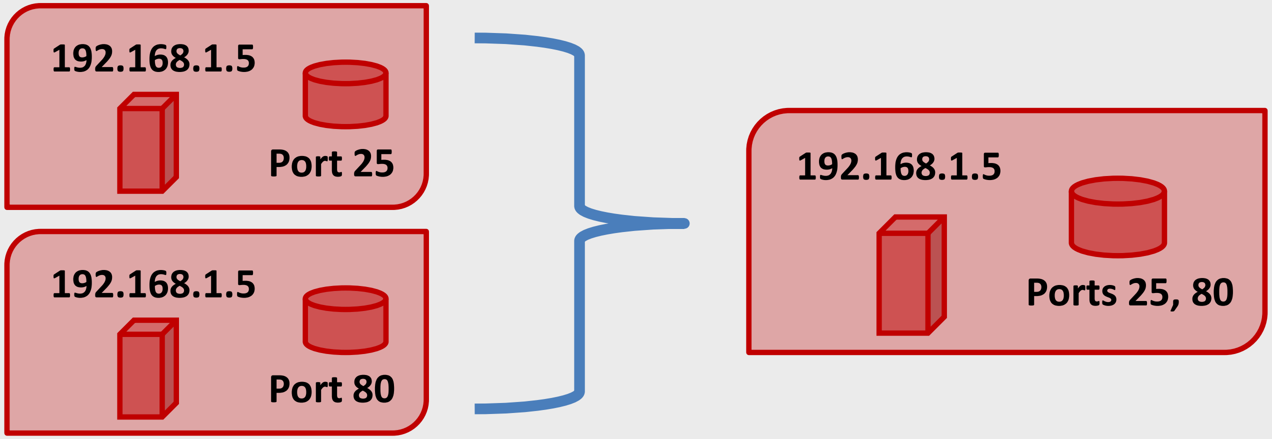
192.168.1.5

Port 25

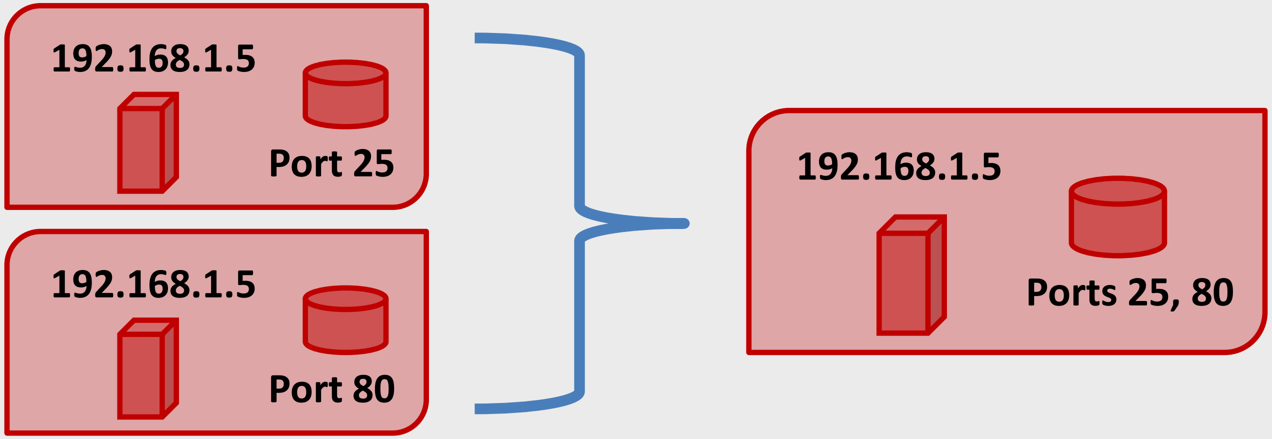
192.168.1.5

Port 80

Future Work



Future Work



192.168.1.5

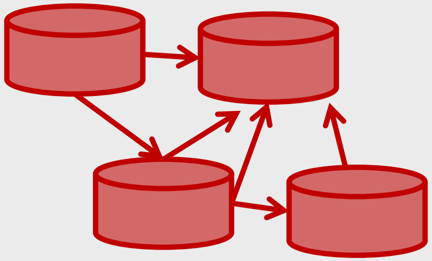
Port 25

192.168.1.5

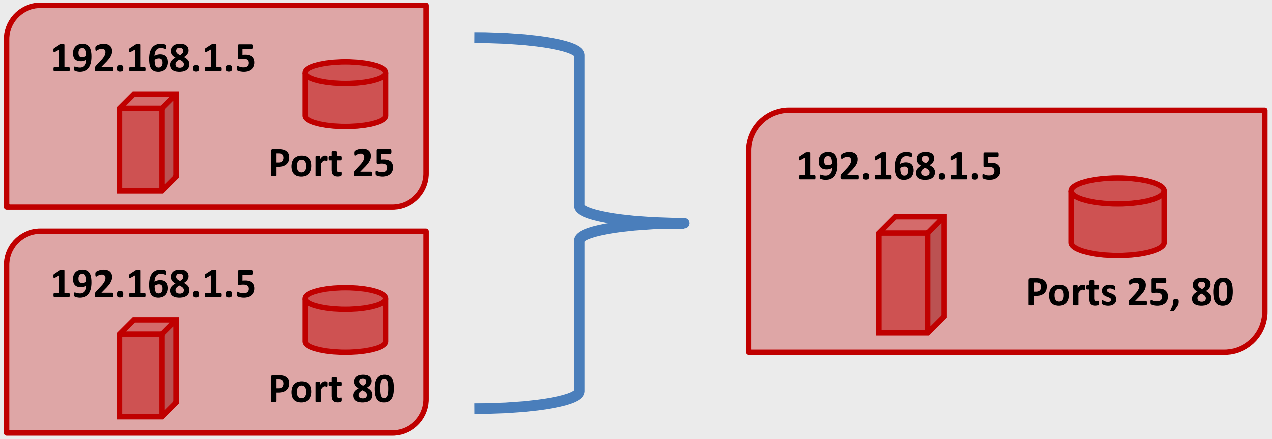
Port 80

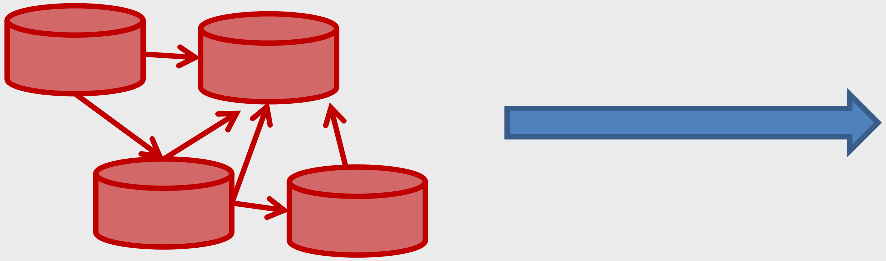
192.168.1.5

Ports 25, 80



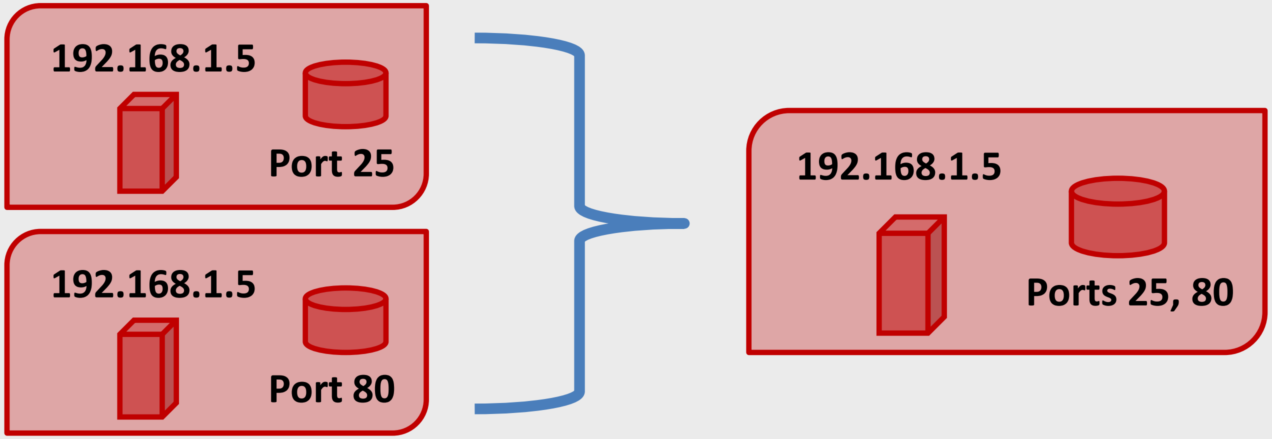
Future Work

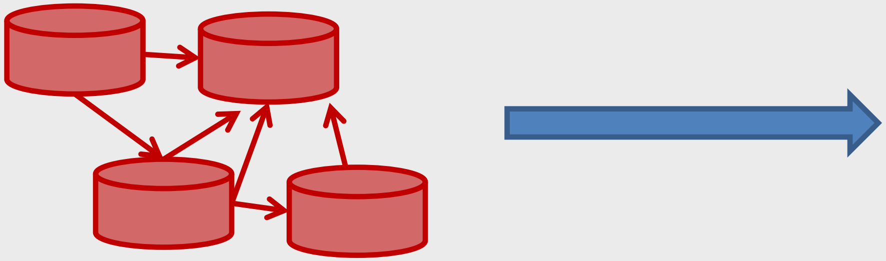




EXPLORE
FastEthernet0 = entry-interface
AND prot-TCP = protocol
AND port-80 = src-port-in

Future Work





EXPLORE
FastEthernet0 = entry-interface
AND prot-TCP = protocol
AND port-80 = src-port-in

“Try stateful inspection.”

What configuration problems do **you** face?

Come talk to me! (I’m here until Friday.)

Text me: (774) 314-1128

Email me: tn@cs.wpi.edu

Download the tool:

www.margrave-tool.org

Thank you to:

Varun Singh (Brown), Morgan Quirk (WPI), Emina Torlak (IBM Watson)