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...”
Policy-based routing

Static routing, NAT

ACLs, reflexive access-lists
Go to page 1, 2, 3, 4  Next

Previous topic  |  Next topic

Posted: Fri Aug 15, 2008 2:25 am
Try this!
Try this!

No! Try this!
Try this!

No! Try this!

No, no, try this.
Suggestions do not always agree.
Debugging Questions:
Debugging Questions:

Q: Which hop will SMTP packets take next?
Q: Which hop will SMTP packets take next?

A: 192.168.100.4

A: 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
A: 192.168.200.5

Q: Which configuration rules caused the incorrect routing?
A: Line 14 applied to...
A: Line 15 applied to...

...
Debugging Questions:

Q: Which hop will SMTP packets take next?

A: 192.168.100.4
A: 192.168.200.5

Q: Which configuration rules caused the incorrect routing?

A: Line 14 applied to...
A: Line 15 applied to...

Q: What packets will pass the firewall?
Debugging Questions:

Q: Which hop will SMTP packets take next?
A: 192.168.100.4
A: 192.168.200.5

Q: Which configuration rules caused the incorrect routing?
A: Line 14 applied to...
A: Line 15 applied to...

Q: What packets will pass the firewall?
A: TCP From X to Y

...
Debugging Questions:

Q: Which hop will SMTP packets take next?
A: 192.168.100.4
A: 192.168.200.5

Q: Which configuration rules caused the incorrect routing?
A: Line 14 applied to...
A: Line 15 applied to...

Q: How do a pair of configurations behave differently?

Q: What packets will pass the firewall?
A: TCP From X to Y
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: Time
Connection State
Debugging Questions:

Q: Which hop will SMTP packets take next?
A: 192.168.100.4
A: 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?
Q: How do a pair of configurations behave differently?
A: Line 14 applied to...
A: Line 15 applied to...

Scenarios

Time
Connection
State

...
Debugging Questions:

Q: Which hop will SMTP packets take next?
A: 192.168.100.4

Q: Which packets will pass the firewall?

Q: Which configuration rules caused the incorrect routing?

Q: Which hop will SMTP packets take next?

Q: How do a pair of configurations behave differently?

Scenarios

Margrave

TCP From X to Y
#lang margrave

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

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

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

> EXPLORE InboundACL:permit(<InboundACL:req>);
#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.
> |
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.

>
#lang margrave

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

EXPLORE InboundACL:permit(<InboundACL:req>);
“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.”

```
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
```
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
speed auto
full-duplex
!
interface Vlan1
ip address 192.168.2.1 255.255.255.0
!
access-list 1 permit 192.168.2.0 0.0.0.255
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

ip nat outside

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

Firewall

Server: 192.168.2.6

“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.”

```
1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
20. !
21. 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.

```plaintext
1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
20. !
21. 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."

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.”
“The web can access my server, but my server can’t access the web.”
“Can returning packets be lost?”

1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
20. !
21. access-list 1 permit 192.168.2.0 0.0.0.255
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
“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?”

EXPLOR

NOT passes-firewall(<pkt>);

“Dropped or rejected”

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

<pkt> =
entry-interface
src-addr-in
protocol
...
“Can returning packets be lost?”

1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
20. !
21. access-list 1 permit 192.168.2.0 0.0.0.255
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

EXPLORE
NOT passes-firewall(<pkt>)
AND internal-result(<pktplus>) ;

“Compute next hop and NAT”

<pktplus> = <pkt> + temporary variables
“Can returning packets be lost?”

1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
20. !
21. access-list 1 permit 192.168.2.0 0.0.0.255
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

EXPLORE

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

“Arriving at FastEthernet0”
“Can returning packets be lost?”

EXPLORE

\[\text{NOT passes-firewall(<pkt>) AND internal-result(<pktplus>) AND FastEthernet0 = entry-interface AND NOT src-addr-in IN 192.168.2.0/255.255.255.0;}\]

“Reasonable source”
“Can returning packets be lost?”

1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16
20. !
21. access-list 1 permit 192.168.2.0 0.0.0.255
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

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?”

1. interface FastEthernet0
2. ip address 209.172.108.16 255.255.255.224
3. ip access-group 102 in
4. ip nat outside
5. speed auto
6. full-duplex
7. !
8. interface Vlan1
9. ip address 192.168.2.1 255.255.255.0
10. ip nat inside
11. !
12. ip route 0.0.0.0 0.0.0.0 209.172.108.1
13. !
14. ip nat pool localnet 209.172.108.16 prefix-length 24
15. ip nat inside source list 1 pool localnet overload
16. ip nat inside source list 1 interface FastEthernet0
17. ip nat inside source static tcp 192.168.2.6 80 209.172.108.16 80
18. ip nat inside source static tcp 192.168.2.6 21 209.172.108.16 21
19. ip nat inside source static tcp 192.168.2.6 3389 209.172.108.16 3389
20. !
21. access-list 1 permit 192.168.2.0 0.0.0.255
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

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?”

EXPLORE

**NOT** passes-firewall(<pkt>)
AND **internal-result**(pkt+)
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
>
“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...”
Will this change fix my problem?

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

Will this change fix my problem?

Will it introduce new problems?
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

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
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
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>));
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>));

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

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>))

Public address of server
AND NOT passes-firewall1(<pkt>)

> SHOW

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(pkt+) AND
(passes-firewall1(pkt) AND NOT passes-firewall2(pkt))
OR
passes-firewall2(pkt) AND NOT passes-firewall1(pkt) );

> SHOW ALL;

protocol: prot
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

“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-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

More than we intended?
> 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

More than we intended?
> 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;

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: 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

...
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
  - 209.172.108.16
  - 192.168.2.6
  - ...
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>)

How large a scenario do we need to check?

Margrave computes a bound automatically, most of the time.

Scenario:

entry-interface: fe0
next-hop: 192.168.2.6
dest-addr-in: 209.172.108.16
...
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: ipaddr
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)
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?
ip access-group 102 in

Provides these query terms:

- InboundACL:Permit
- InboundACL:Deny
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0

Provides these query terms:

LocalSwitching:Forward
LocalSwitching:Pass
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
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:
StaticRouting:Forward
StaticRouting:Route
StaticRouting:Pass
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0

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

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
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0

Packet Arrives

Inbound ACL

IP access-group 102 in

LocalSwitching

PolicyRouting

StaticRouting

DefaultPolicyRouting

Packet Departs

Outbound ACL

NetworkSwitching:Forward

NetworkSwitching:Pass

Provides these query terms:

NetworkSwitching:Forward
NetworkSwitching:Pass

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
interface GigabitEthernet0/0
ip address 10.232.0.1 255.255.252.0

Packet Arrives

Inbound ACL

Permit

NAT

LocalSwitching

Pass

PolicyRouting

Pass

StaticRouting

Pass

DefaultPolicyRouting

Route

NetworkSwitching

Fwd

Outbound ACL

Permit

Packet Departs

NAT

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
Scenario-finding logic engine

General Policy Language

Kodkod & SAT Solving
Scenario-finding logic engine

General Policy Language

Query Language

Kodkod & SAT Solving
Scenario - finding logic engine

General Policy Language

Query Language

Scenario-finding logic engine

Kodkod & SAT Solving
Supported subset of Cisco IOS

General Policy Language

Query Language

Scenario-finding logic engine

Kodkod & SAT Solving
Supported subset of Cisco IOS

Iptables (in progress)

General Policy Language

Query Language

Scenario-finding logic engine

Kodkod & SAT Solving

XACML

Amazon SQS
<table>
<thead>
<tr>
<th>Feature</th>
<th>ITVal</th>
<th>Fireman</th>
<th>Prometheus</th>
<th>ConfigChecker</th>
<th>Fang/AlgoSec</th>
<th>Vantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which packets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User-defined queries</td>
<td>✓</td>
<td>?</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Rule Responsibility</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Rule Relationships</td>
<td>?</td>
<td>✓ nip</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Change-impact</td>
<td>?</td>
<td>✓ nip</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Support NAT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Support Routing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Firewall Networks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ nip</td>
</tr>
<tr>
<td>Language integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Commercial Tool?</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
Future Work
Future Work

192.168.1.5
Port 25

192.168.1.5
Port 80
Future Work

192.168.1.5
Port 25

192.168.1.5
Port 80

192.168.1.5
Ports 25, 80
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)