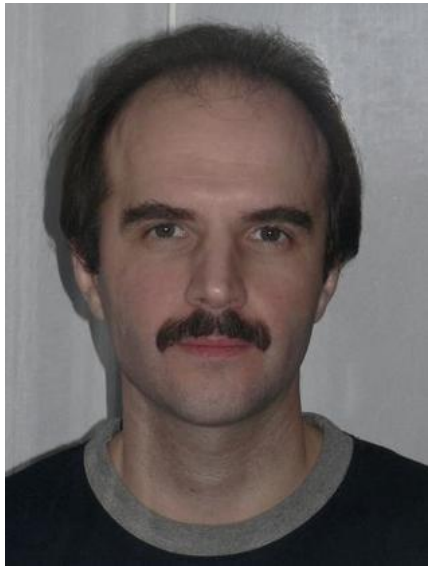
Cisco Support Community
Expert Series Webcasts in
Russian:

Understanding and Troubleshooting ASA NAT

Created by Oleg Tipisov, Cisco TAC.
Version 1.1. Cisco Public

Cisco Support Community – Expert Series Webcasts in Russian

Сегодня на семинаре эксперт Cisco TAC



Олег Типисов

CCIE in Routing and Switching

Спасибо, что посетили наш семинар сегодня

Сегодняшняя презентация включает опросы аудитории

Пожалуйста, участвуйте!

Спасибо, что посетили наш семинар сегодня

Если Вы хотите получить копию слайдов сегодняшнего семинара, пожалуйста, используйте следующие ссылки:

https://supportforums.cisco.com/community/russian/security

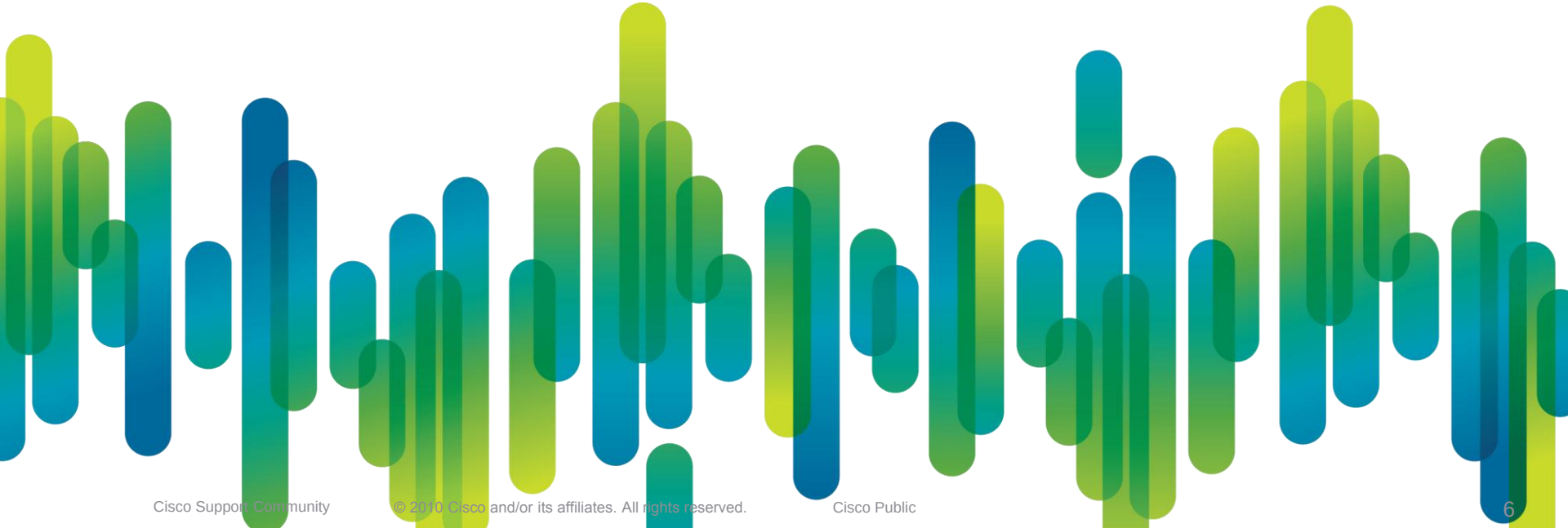
или, https://supportforums.cisco.com/docs/DOC-27135

Опрос #1
Каков уровень ваших знаний о ASA NAT?

1. Я представляю, что такое NAT, но не работал с ним
2. Мне приходилось настраивать NAT на ASA с помощью графического интерфейса ASDM
3. Я владею настройкой NAT из CLI и ASDM и применяю эту технологию в своей сети
4. Я неоднократно настраивал различные варианты NAT на ASA во многих версиях ПО

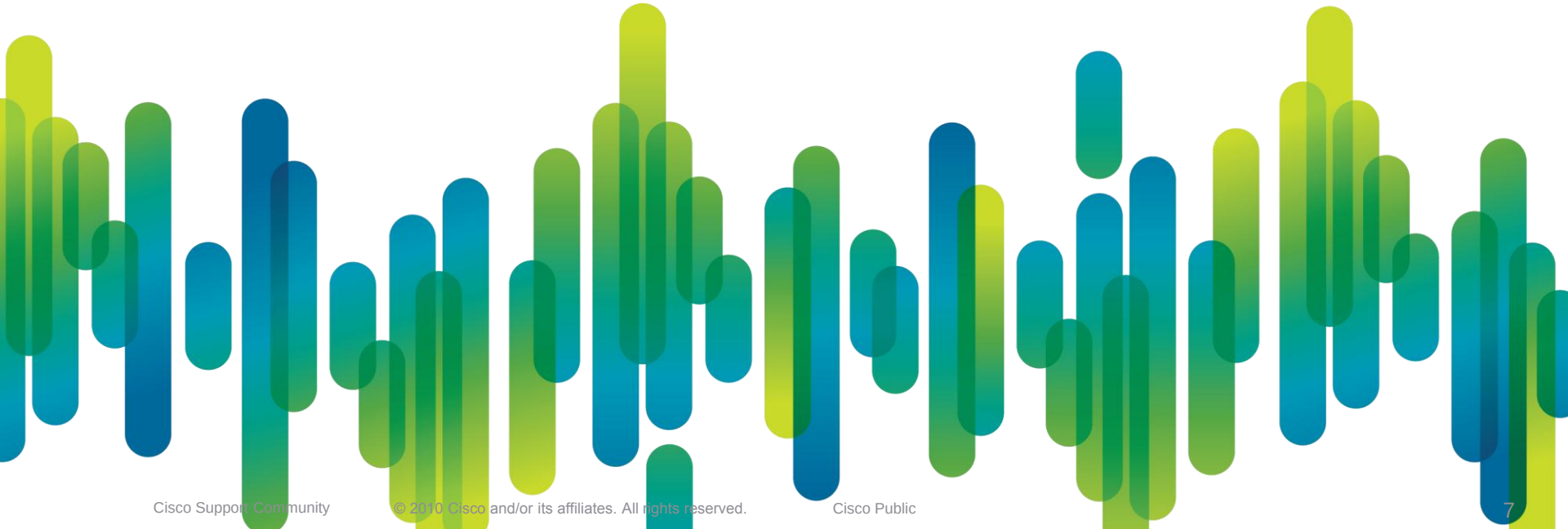
Задавайте Ваши вопросы!

Используйте Q&A панель, чтобы послать вопрос. Наши эксперты ответят на них



Understanding and Troubleshooting ASA NAT

Created by Oleg Tipisov, Cisco TAC.
Version 1.1. Cisco Public



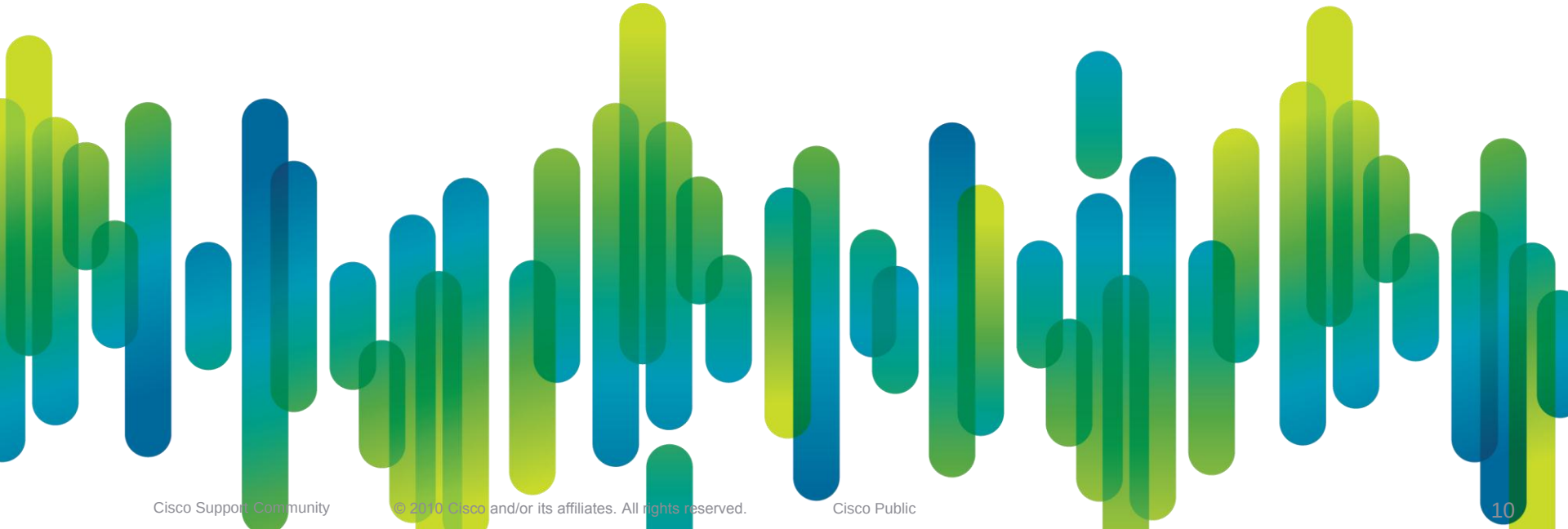
Introduction

- This session is mostly about ASA 8.3+ NAT
- ASA 8.2 configuration example is given, but slides are hidden to save time
- Two real-world troubleshooting scenarios are given
- Students are expected to understand ASA NAT CLI
- We will not discuss:
  - 8.2 -> 8.3 Configuration migration
  - NAT and Routing integration
  - NAT RPF Check and associated issues
- Separate presentation is needed for each of the above

Agenda

- Introduction
- NAT Terminology
- ASA 8.2 Configuration Example
- ASA 8.3+ Configuration Example
- Troubleshooting Scenario #1
- Troubleshooting Scenario #2
- Final Recommendations

Introduction



ASA Features

- Stateful packet filter
- Security policy is based on “interface security levels”
- Application inspection
- NAT/PAT, NAT ALG
- Static & Dynamic IPv4 & IPv6 routing
- Integration with IPS, CSC and CX modules
- L2L & RA VPN (IPSec IKEv1, IPSec IKEv2, SSL)
- Redundancy features and failover

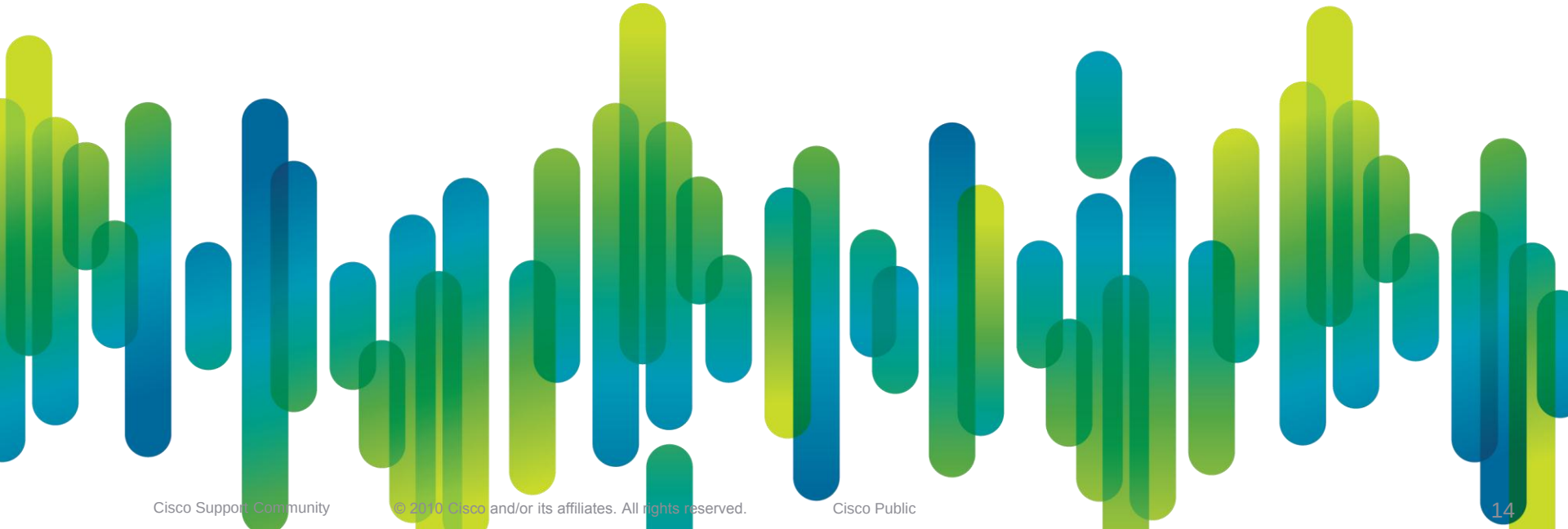
ASA Features

- Virtualization (multiple context mode)
- Transparent mode
- NetFlow v9 for security monitoring
- Botnet traffic filtering (Ironport integration)
- Identity firewall
- ASA Phone Proxy and other UC integration features

Latest Releases

- 8.4 – 5505, 5510-5550, 5580, 5585-X
  - 8.4(4) is the latest version
- 8.5 – ASA SM
  - 8.4(1) with few other features
- 8.6 – 5500-X
  - 8.4(2) with few other features
- 8.7 – ASA 1000V
  - ASA in a Nexus 1000V switch
- 9.0 – To be released soon

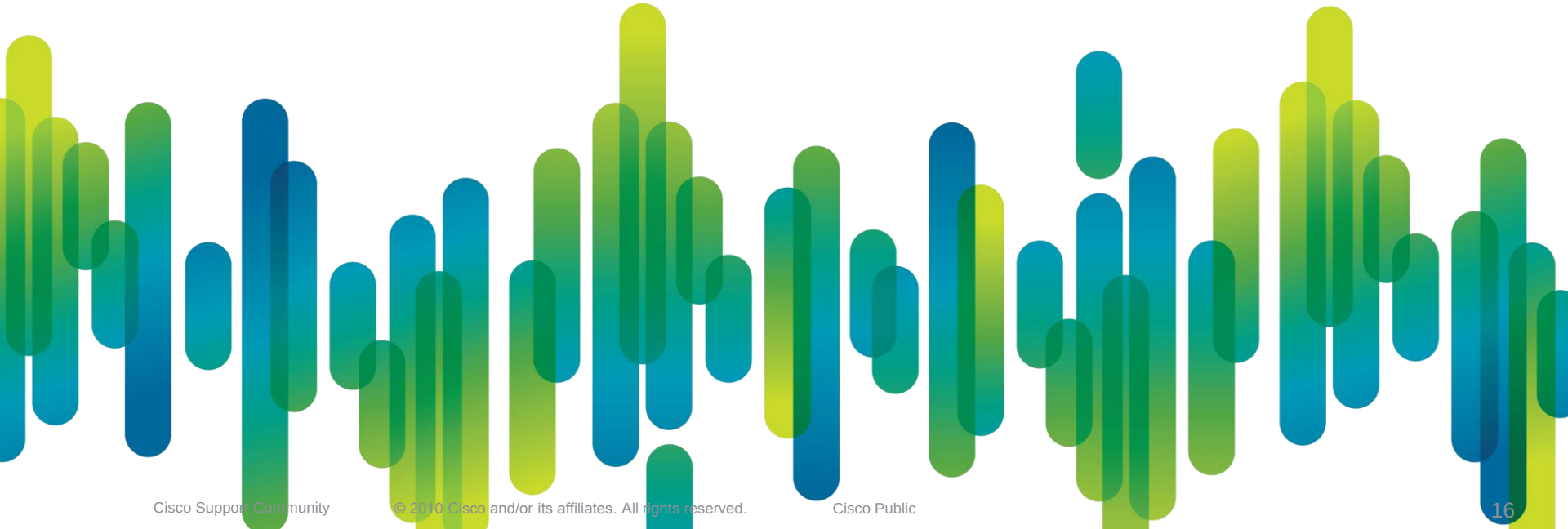
NAT Terminology



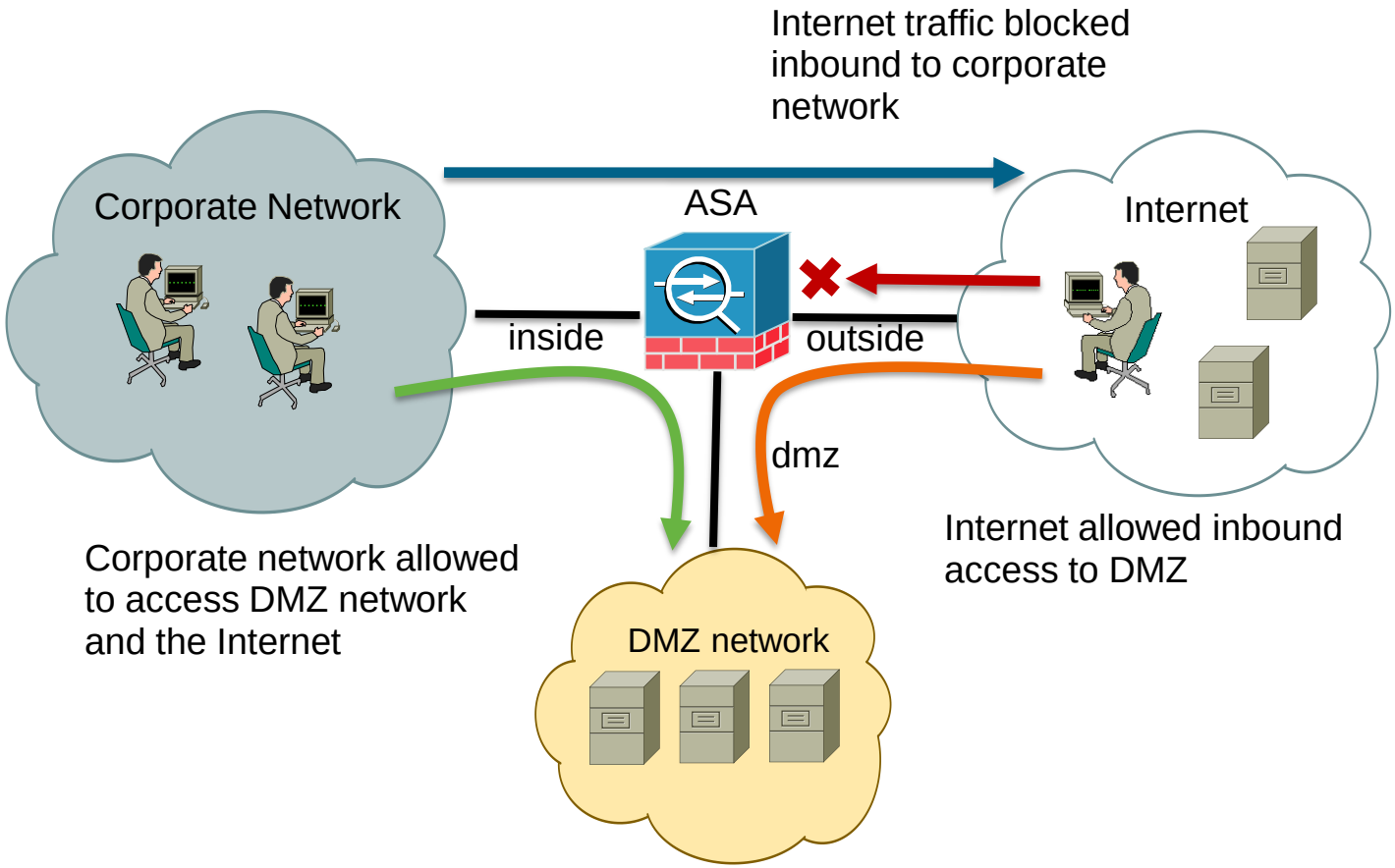
NAT Terminology

- Real Address vs. Mapped Address
- Connection vs. xlate
- Source Translation vs. Destination Translation (UN-NAT)
- Bidirectional NAT
- Dynamic NAT vs. Static NAT
- NAT vs. PAT
- Identity NAT
- NAT exemption or “NAT 0 ACL” (8.2- only)
- Policy NAT

ASA 8.2 Configuration Example



Security Policy Example

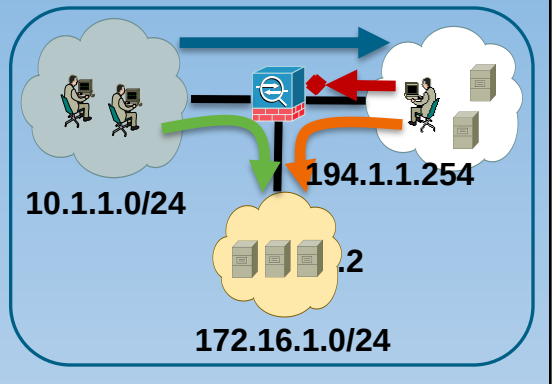


ASA Interface Configuration

```
interface GigabitEthernet0/0.1
 vlan 99
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/0.2
 vlan 98
 nameif dmz
 security-level 50
 ip address 172.16.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 194.1.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 194.1.1.2 1
```

ASA NAT and ACL Configuration – 8.2

```
no nat-control

! Dynamic PAT to "outside" interface IP
global (outside) 1 interface
nat (inside) 1 10.1.1.0 255.255.255.0

! Static PAT
static (dmz,outside) 194.1.1.254 172.16.1.2 netmask 255.255.255.255

! No NAT between "inside" and "dmz" interfaces
access-list nonat extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0

nat (inside) 0 access-list nonat

! Allow HTTP to DMZ server
access-list outside_in extended permit tcp any host 194.1.1.254 eq www
access-group outside_in in interface outside
```



"host 194.1.1.254 eq www" public IP in this release!

ASA Dynamic NAT – 8.2

```
%ASA-6-305011: Built dynamic TCP translation from inside:10.1.1.2/64253 to
outside:194.1.1.1/33627

%ASA-6-302013: Built outbound TCP connection 0 for outside:207.1.1.2/80
(207.1.1.2/80) to inside:10.1.1.2/64253 (194.1.1.1/33627)


ASA# show conn long

TCP outside:207.1.1.2/80 (207.1.1.2/80) inside:10.1.1.2/64253
(194.1.1.1/33627), flags U, idle 30s, uptime 30s, timeout 1h0m, bytes 0


ASA# show xlate debug

2 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static

TCP PAT from inside:10.1.1.2/64253 to outside:194.1.1.1/33627 flags ri idle
0:00:36 timeout 0:00:30
```

Source port is always changed as of CSCsr28008
https://supportforums.cisco.com/docs/DOC-9233

ASA Static NAT – 8.2

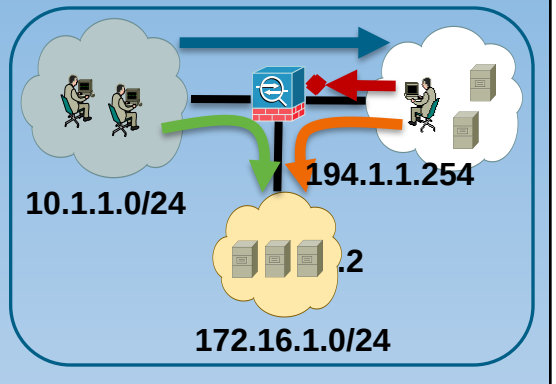
```
%ASA-6-302013: Built inbound TCP connection 1 for outside:207.1.1.2/63715
(207.1.1.2/63715) to dmz:172.16.1.2/80 (194.1.1.254/80)


ASA# show conn long

TCP outside:207.1.1.2/63715 (207.1.1.2/63715) dmz:172.16.1.2/80
(194.1.1.254/80), flags UB, idle 26s, uptime 26s, timeout 1h0m, bytes 0


ASA# show xlate debug

1 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static

NAT from dmz:172.16.1.2 to outside:194.1.1.254 flags s idle 0:08:00 timeout
0:00:00


ASA# show access-list
access-list outside_in line 1 extended permit tcp any host 194.1.1.254 eq www
(hitcnt=1) 0x24e3fc02
```

public IP

number of connections, not packets!

NAT Rules Order – 8.2

```
no nat-control

! Dynamic PAT to "outside" interface IP
global (outside) 1 interface
nat (inside) 1 10.1.1.0 255.255.255.0

! Static PAT
static (dmz,outside) 194.1.1.254 172.16.1.2 netmask 255.255.255.255

! No NAT between "inside" and "dmz" interfaces
access-list nonat extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0

nat (inside) 0 access-list nonat

! Allow HTTP to DMZ server
access-list outside_in extended permit tcp any host 194.1.1.254 eq www
access-group outside_in in interface outside
```



"host 194.1.1.254 eq www" public IP in this release!

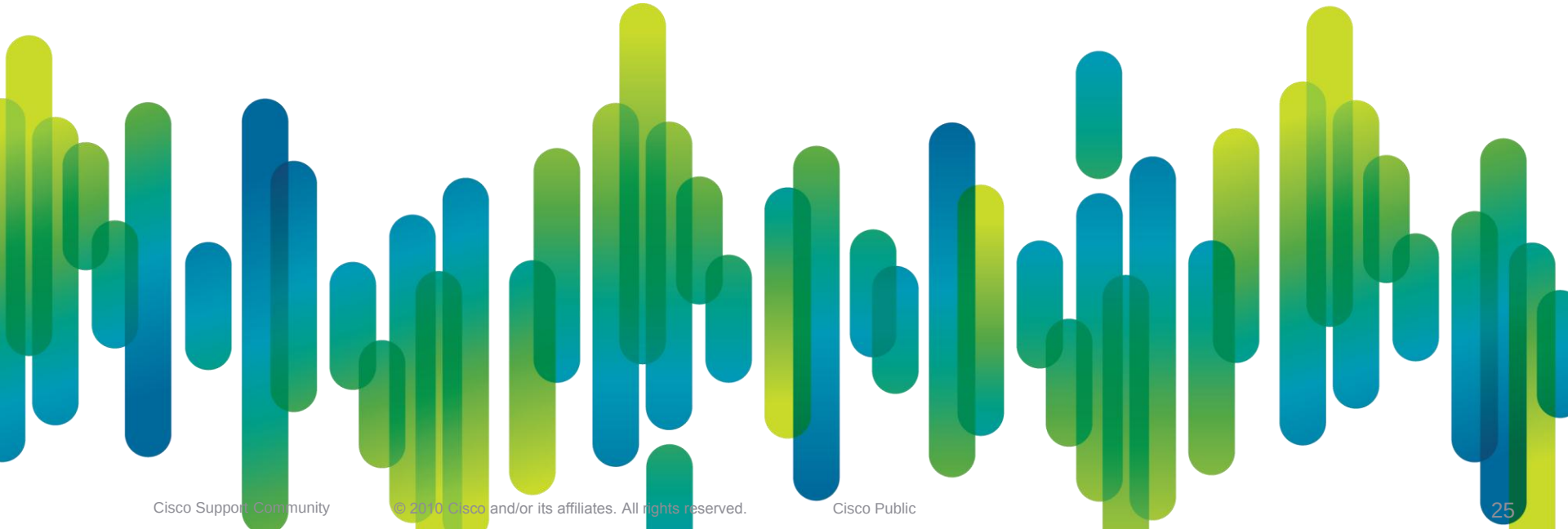
NAT Rules Order – 8.2

1. NAT Exemption (NAT 0 ACL)
2. Static NAT, Static PAT, Static Policy NAT/PAT
   - in order, until the first match
   - FWSM uses longest match for static NAT
3. Dynamic Policy NAT/PAT
   - in order, until the first match
4. Regular Dynamic NAT/PAT
   - longest match
   - identity NAT doesn’t have priority

NAT Pitfalls – 8.2

- “no nat-control” doesn’t help much…
- Policy NAT ACL doesn’t support “deny” statements
- NAT exemption ACL doesn’t support TCP/UDP ports
- Bidirectional NAT is difficult to configure
- Flexibility is limited
  - 64K xlates per PAT IP
  - port ranges cannot be configured (0-511, 512-1023, 1024-65535)
  - no support for “timeout pat-xlate”

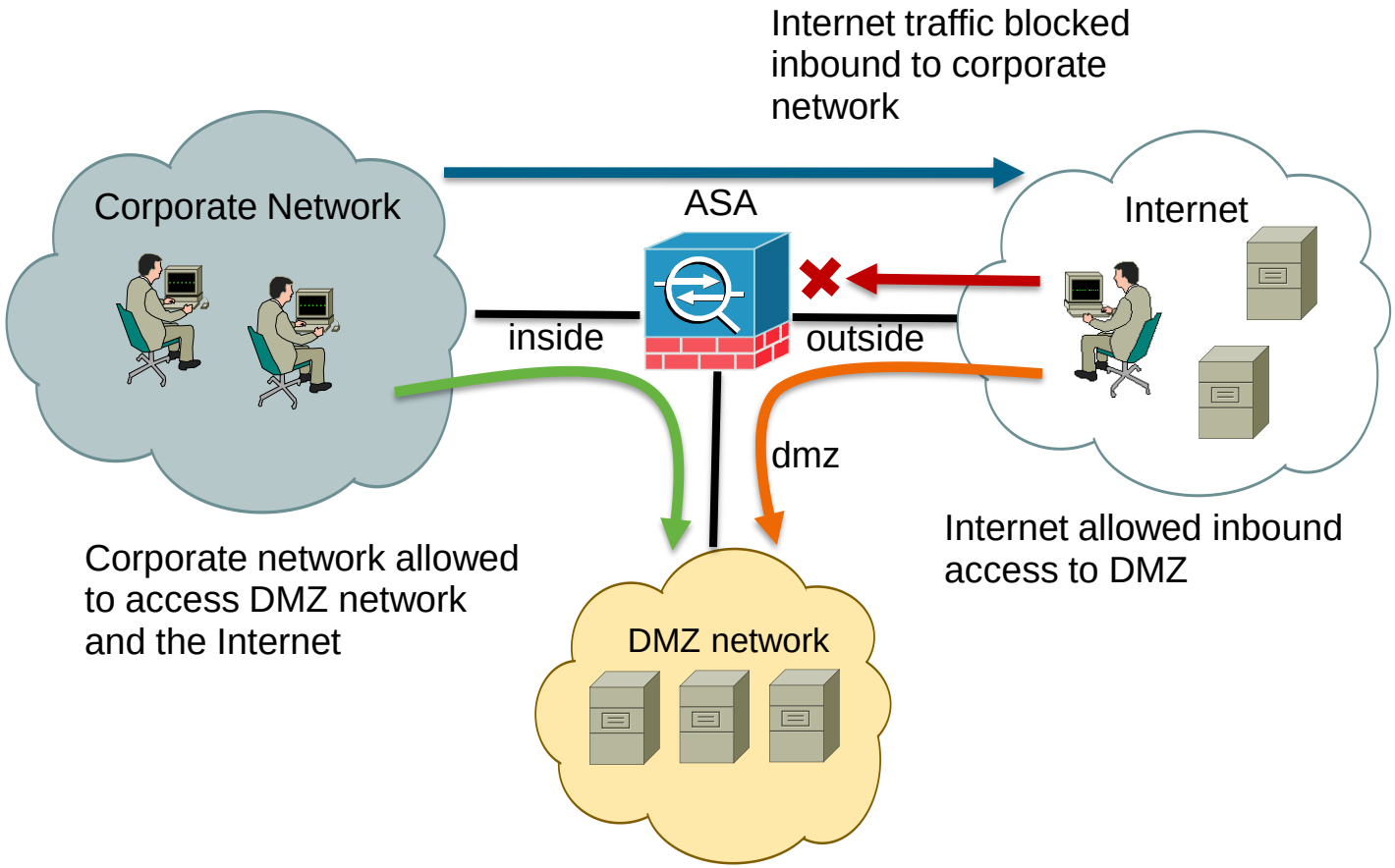
ASA 8.3+ Configuration Example



NAT in 8.3+

- Completely new implementation
- “NAT simplification”
- Object NAT (Auto NAT)
- Twice NAT (Manual NAT)
- Bidirectional NAT is very easy to configure
- Flexibility is higher, new features are being implemented

Security Policy Example



Configuration Migration (8.2 –> 8.3)

```
INFO: MIGRATION - Saving the startup configuration to file

INFO: MIGRATION - Startup configuration saved to file
'flash:8_2_1_0_startup_cfg.sav'
*** Output from config line 4, "ASA Version 8.2(1) "
.
Cryptochecksum (unchanged): 66abf6f4 1b22b1c8 2f06d057 62b2e46a
NAT migration logs:
The following 'nat' command didn't have a matching 'global' rule on interface
'dmz' and was not migrated.
nat (inside) 1 10.1.1.0 255.255.255.0

INFO: NAT migration completed.
Real IP migration logs:
        ACL <outside_in> has been migrated to real-ip version

INFO: MIGRATION - Saving the startup errors to file
'flash:upgrade_startup_errors_200503292016.log'
```

See this article about 8.2 -> 8.3+ software upgrade and configuration migration:

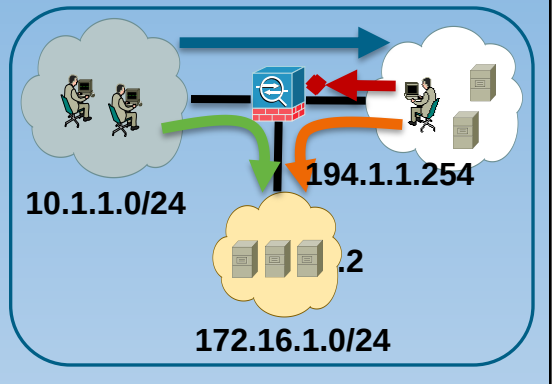
https://supportforums.cisco.com/docs/DOC-12690

ASA Interface Configuration

```
interface GigabitEthernet0/0.1
 vlan 99
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/0.2
 vlan 98
 nameif dmz
 security-level 50
 ip address 172.16.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 194.1.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 194.1.1.2 1
```

ASA Object NAT – 8.3+

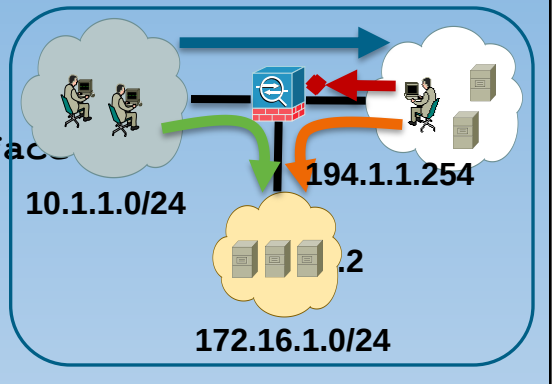
```
object network obj-10.1.1.0
 subnet 10.1.1.0 255.255.255.0

object network obj-172.16.1.2
 host 172.16.1.2

object network obj-10.1.1.0
 nat (inside,outside) dynamic interface

object network obj-172.16.1.2
 nat (dmz,outside) static 194.1.1.254

access-list outside_in extended permit tcp any host 172.16.1.2 eq www
access-group outside_in in interface outside
```



"host 172.16.1.2 eq www"
real IP in this release!

ASA Twice NAT – 8.3+

```
object network obj-10.1.1.0
 subnet 10.1.1.0 255.255.255.0

nat (inside,outside) source dynamic obj-10.1.1.0 interfac


object network obj-172.16.1.2
 host 172.16.1.2

object network obj-194.1.1.254
 host 194.1.1.254

nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254

access-list outside_in extended permit tcp any host 172.16.1.2 eq www
access-group outside_in in interface outside
```



"host 172.16.1.2 eq www"
real IP in this release!

ASA Dynamic NAT – 8.3+

```
%ASA-6-305011: Built dynamic TCP translation from inside:10.1.1.2/57126 to
outside:194.1.1.1/57126

%ASA-6-302013: Built outbound TCP connection 3 for outside:207.1.1.2/80
(207.1.1.2/80) to inside:10.1.1.2/57126 (194.1.1.1/57126)


ASA# show conn long

TCP outside:207.1.1.2/80 (207.1.1.2/80) inside:10.1.1.2/57126
(194.1.1.1/57126), flags U, idle 12s, uptime 12s, timeout 1h0m, bytes 0


ASA# show xlate

2 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended

TCP PAT from inside:10.1.1.2/57126 to outside:194.1.1.1/57126 flags ri idle
0:00:23 timeout 0:00:30
```

Newest software tries to preserve source port if possible

ASA Static NAT – 8.3+

```
%ASA-6-302013: Built inbound TCP connection 4 for outside:207.1.1.2/41506
(207.1.1.2/41506) to dmz:172.16.1.2/80 (194.1.1.254/80)


ASA# show conn long

TCP outside:207.1.1.2/41506 (207.1.1.2/41506) dmz:172.16.1.2/80
(194.1.1.254/80), flags UB, idle 41s, uptime 43s, timeout 1h0m, bytes 0


ASA# show xlate

1 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended

NAT from dmz:172.16.1.2 to outside:194.1.1.254
    flags s idle 0:00:47 timeout 0:00:00


ASA# show access-list
access-list outside_in line 1 extended permit tcp any host 172.16.1.2 eq www
(hitcnt=1) 0xdae674c0
```

public IP

number of connections, not packets!

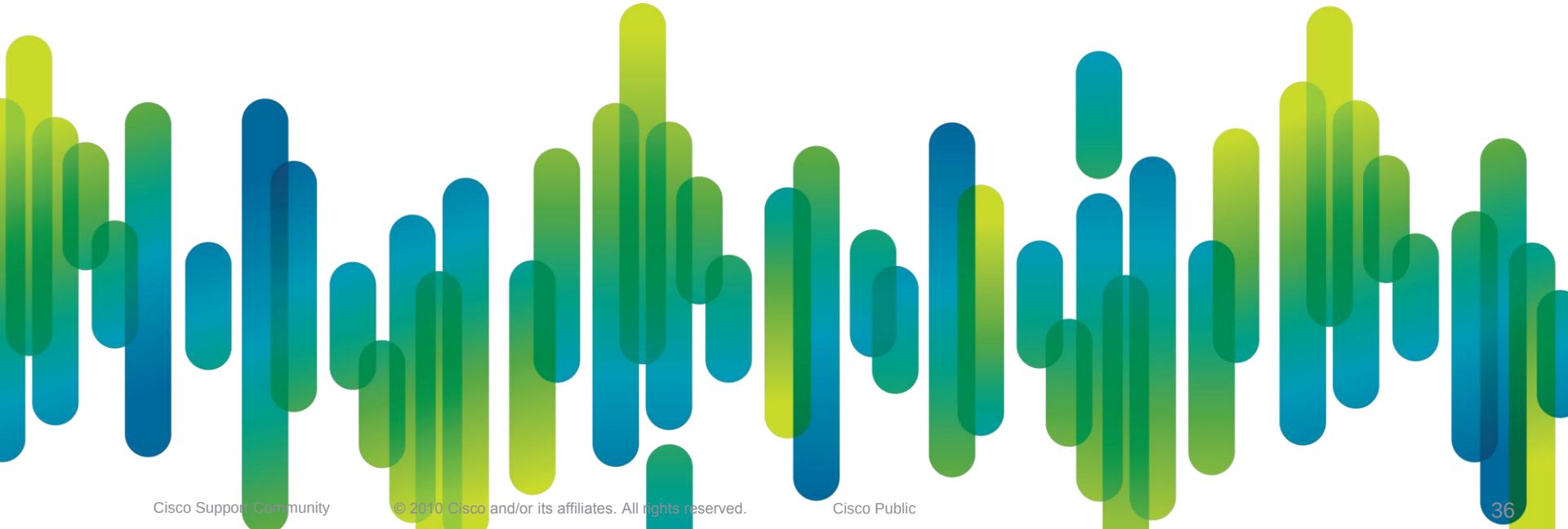
NAT Rules Order (8.3+)

1. Section 1: Twice NAT
   - default place for twice NAT rules
   - in order, until the first match
2. Section 2: Object NAT
   - static NAT (longest match)
   - dynamic NAT (longest match)
3. Section 3: Twice NAT
   - “after-auto” needs to be specified in “nat” command
   - in order, until the first match

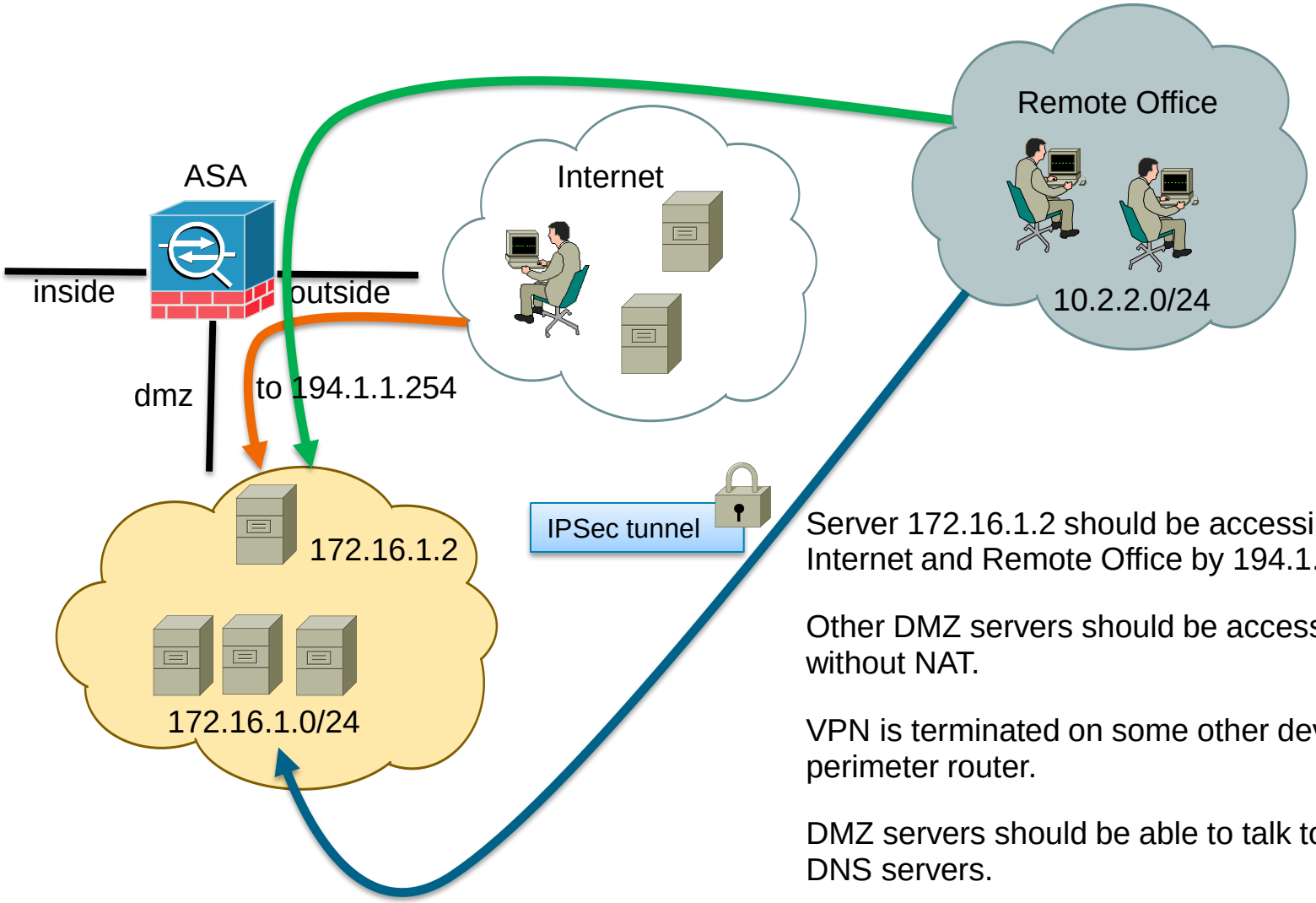
Опрос #2
Сталкивались ли Вы с проблемами при использовании NAT на ASA

1. Нет, никогда. Все отлично работает
2. Иногда бывало, но это были ошибки настройки
3. Проблемы встречались, но они легко решались переходом на новую версию
4. Проблемы возникали и их могли решить только инженеры Cisco TAC
5. Сплошные проблемы, не знаю, что делать
6. Я не использую NAT на ASA, потому что он не работает

Troubleshooting Scenario #1



Security Policy Example



Server 172.16.1.2 should be accessible from both Internet and Remote Office by 194.1.1.254.

Other DMZ servers should be accessible via VPN without NAT.

VPN is terminated on some other device, such as perimeter router.

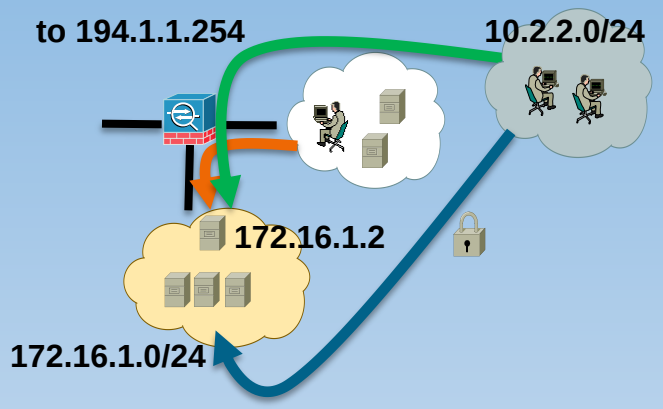
DMZ servers should be able to talk to Internet DNS servers.

ASA Interface Configuration

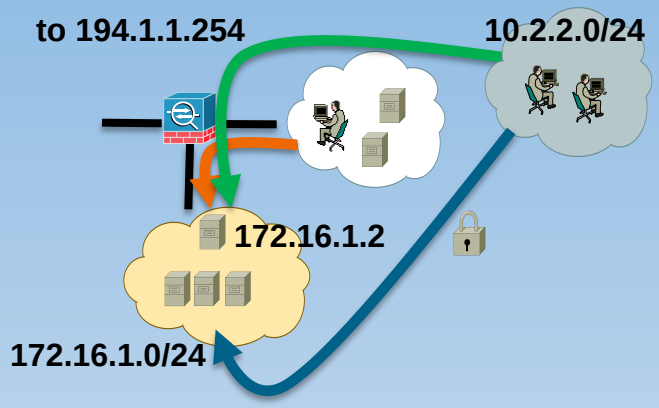
```
interface GigabitEthernet0/0.1
 vlan 99
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/0.2
 vlan 98
 nameif dmz
 security-level 50
 ip address 172.16.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 194.1.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 194.1.1.2 1
```

ASA NAT Configuration – 8.3+

```
object network obj-172.16.1.0
 subnet 172.16.1.0 255.255.255.0

object network obj-172.16.1.2
 host 172.16.1.2

object network obj-194.1.1.254
 host 194.1.1.254

object network RemoteOfficeNet
 subnet 10.2.2.0 255.255.255.0

object network RemoteOfficeNet-2
 subnet 10.2.2.0 255.255.255.0

nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254

nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination
static RemoteOfficeNet RemoteOfficeNet-2

nat (dmz,outside) source dynamic obj-172.16.1.0 interface
```



Customer Symptom



Everything works, but 172.16.1.2 gets wrong IP when goes to the Internet…

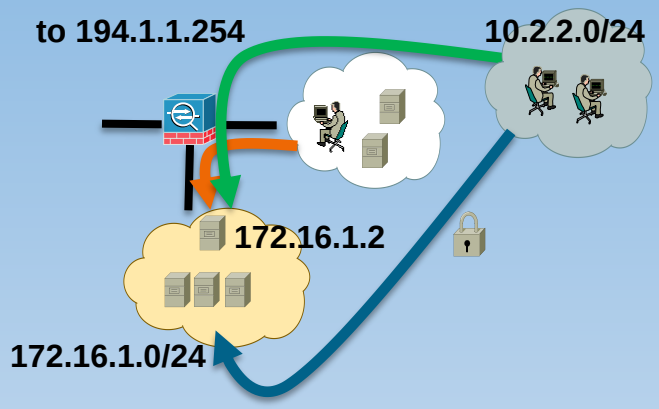
```
ASA# show conn long

TCP outside:207.1.1.2/80 (207.1.1.2/80) dmz:172.16.1.2/37116
(194.1.1.1/23384), flags U, idle 9s, uptime 9s, timeout 1h0m, bytes 0
```

At the same time inbound connections to 194.1.1.254 work as expected…

```
TCP outside:207.1.1.2/16123 (207.1.1.2/16123) dmz:172.16.1.2/80
(194.1.1.254/80), flags UB, idle 12s, uptime 12s, timeout 1h0m, bytes 0
```

Troubleshooting – Step #1

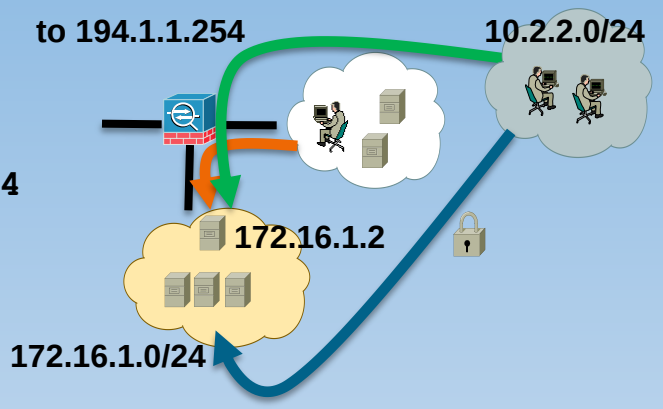
```
ASA# show run object
object network obj-172.16.1.0
 subnet 172.16.1.0 255.255.255.0
object network obj-172.16.1.2
 host 172.16.1.2
object network obj-194.1.1.254
 host 194.1.1.254
object network RemoteOfficeNet
 subnet 10.2.2.0 255.255.255.0
object network RemoteOfficeNet-2
 subnet 10.2.2.0 255.255.255.0
```




```
ASA# show run nat
nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination
static RemoteOfficeNet RemoteOfficeNet-2
nat (dmz,outside) source dynamic obj-172.16.1.0 interface
```

Troubleshooting – Step #2

```
%ASA-6-305011: Built dynamic TCP
translation from dmz:172.16.1.2/37116
to outside:194.1.1.1/23384

%ASA-6-302013: Built outbound TCP connection 54
for outside:207.1.1.2/80 (207.1.1.2/80)
to dmz:172.16.1.2/37116 (194.1.1.1/23384)
```

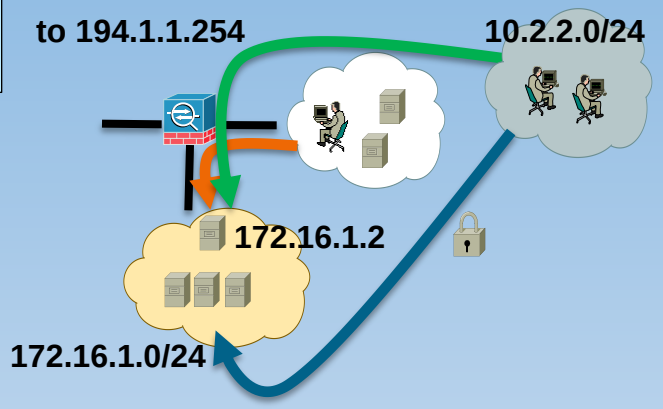



```
ASA# show conn long
TCP outside:207.1.1.2/80 (207.1.1.2/80) dmz:172.16.1.2/37116
(194.1.1.1/23384), flags U, idle 9s, uptime 9s, timeout 1h0m, bytes 0
```

```
ASA# show xlate local 172.16.1.2 global 194.1.1.1
4 in use, 4 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
TCP PAT from dmz:172.16.1.2/37116 to outside:194.1.1.1/23384 flags ri idle
0:02:03 timeout 0:00:30
```

Troubleshooting – Step #3

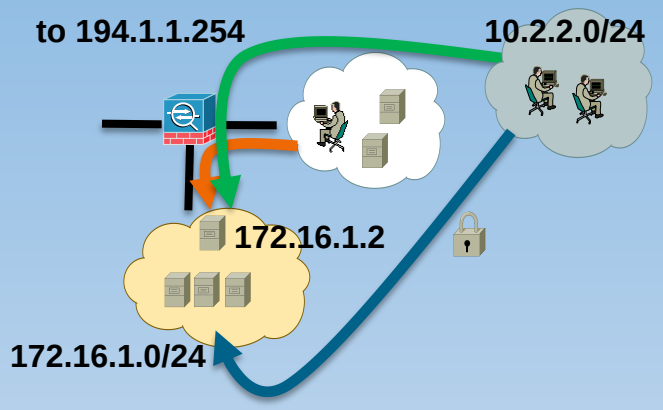
Hmm… This is strange. It seems that dynamic PAT (rule #3) takes precedence over static NAT (rule #1)




```
ASA# debug nat 255

nat: policy lock 0x73a1cb40, old count is 1
nat: translation - dmz:172.16.1.2/37116
to outside:194.1.1.1/23384

ASA# show nat detail
Manual NAT Policies (Section 1)
1 (dmz) to (outside) source static obj-172.16.1.2 obj-194.1.1.254
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 172.16.1.2/32, Translated: 194.1.1.254/32
2 (dmz) to (outside) source static obj-172.16.1.0 obj-172.16.1.0   destination
static RemoteOfficeNet RemoteOfficeNet-2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 172.16.1.0/24, Translated: 172.16.1.0/24
    Destination - Origin: 10.2.2.0/24, Translated: 10.2.2.0/24
3 (dmz) to (outside) source dynamic obj-172.16.1.0 interface
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 172.16.1.0/24, Translated: 194.1.1.1/24
```

Troubleshooting – Step #4

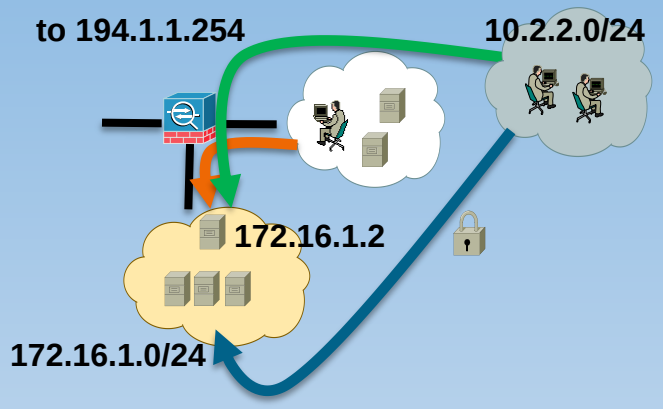
```
ASA# packet-tracer input dmz tcp 172.16.1.2 1234 207.1.1.2 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0          0.0.0.0          outside

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source dynamic obj-172.16.1.0 interface
Additional Information:
Dynamic translate 172.16.1.2/1234 to 194.1.1.1/40625
```



This again confirms that traffic is processed by dynamic PAT rule, instead of static NAT rule…

Troubleshooting – Step #5

```
ASA# packet-tracer input dmz tcp 172.16.1.2 1234 207.1.1.2 80 detail

Phase: 1
…

Phase: 2
…

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source dynamic obj-172.16.1.0 interface
Additional Information:
Dynamic translate 172.16.1.2/1234 to 194.1.1.1/12386
 Forward Flow based lookup yields rule:
 in  id=0x73a1de50, priority=6, domain=nat, deny=false
        hits=5, user_data=0x73a1cb40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=172.16.1.0, mask=255.255.255.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=dmz, output_ifc=outside
```

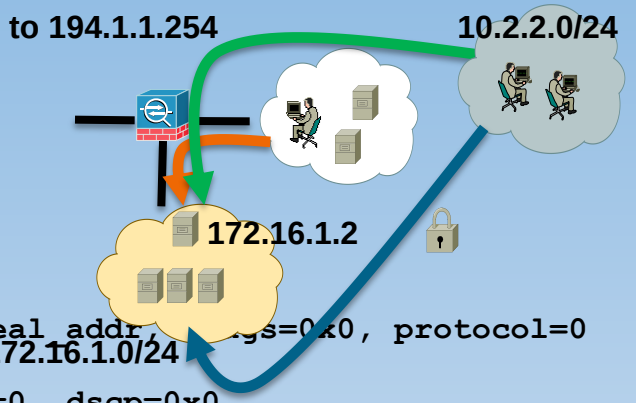


The following command can be used to look at this NAT rule in Accelerated Security Path (ASP) table:

show asp table classify domain nat

Troubleshooting – Step #6

ASP tables are used to classify traffic in data-path and apply different security policies to it




```
ASA# show asp table classify domain nat

Input Table
in   id=0x73984078, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1ca98, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=10.2.2.0, mask=255.255.255.0, port=0
         dst ip/id=172.16.1.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=outside, output_ifc=dmz
in   id=0x73a1de50, priority=6, domain=nat, deny=false
         hits=5, user_data=0x73a1cb40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x739f84d8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73980550, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.2, mask=255.255.255.255, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x73969338, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1c608, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=10.2.2.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
```

Troubleshooting – Step #6

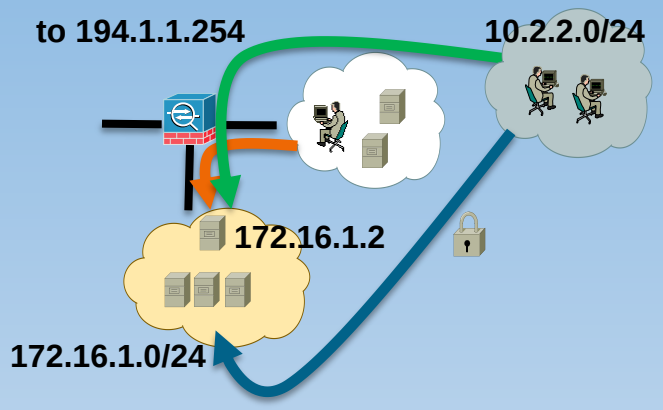
1 nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
2 nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static RemoteOfficeNet RemoteOfficeNet-2
3 nat (dmz,outside) source dynamic obj-172.16.1.0 interface

```
ASA# show asp table classify domain nat

Input Table
in   id=0x73984078, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1ca98, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=10.2.2.0, mask=255.255.255.0, port=0
         dst ip/id=172.16.1.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=outside, output_ifc=dmz
in   id=0x73a1de50, priority=6, domain=nat, deny=false
         hits=5, user_data=0x73a1cb40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x739f84d8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73980550, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.2, mask=255.255.255.255, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x73969338, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1c608, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=10.2.2.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
```

Incorrect order !

Incorrect order !

Troubleshooting – Root Cause



It was found that the problem was caused by editing of NAT lines as shown below

```
no nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
nat (dmz,outside) 1 source static obj-172.16.1.2 obj-194.1.1.254
```

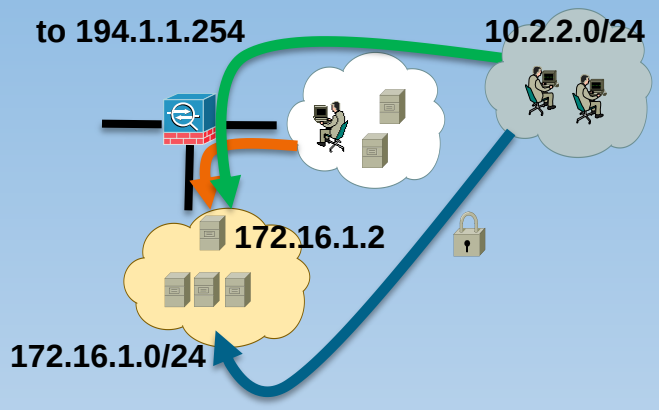
New bug was opened:

CSCtt11890 ASA: Manual NAT rules inserted above others may fail to match traffic

which was fixed in 8.4(4)

Troubleshooting – Solution

Clearing and re-entering configuration resolves the problem (see next slide)…




```
ASA(config)# clear conf nat

ASA(config)# nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
ASA(config)# nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination
static RemoteOfficeNet RemoteOfficeNet-2
ASA(config)# nat (dmz,outside) source dynamic obj-172.16.1.0 interface
ASA(config)# exit
ASA#
```

Troubleshooting – Solution Verification

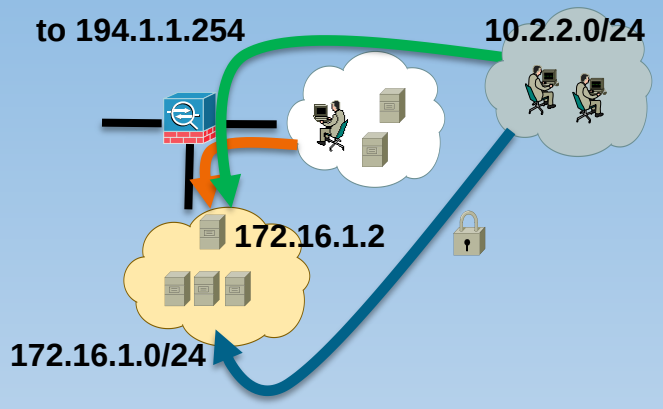
1 nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
2 nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static RemoteOfficeNet RemoteOfficeNet-2
3 nat (dmz,outside) source dynamic obj-172.16.1.0 interface

```
ASA# show asp table classify domain nat

Input Table
in   id=0x739f84d8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e480, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.2, mask=255.255.255.255, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x73982f98, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e8f8, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=10.2.2.0, mask=255.255.255.0, port=0
         dst ip/id=172.16.1.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=outside, output_ifc=dmz
in   id=0x73a1fbd8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e9a0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x739696a0, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e528, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=10.2.2.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
```

Order is now correct!

Troubleshooting – Solution Verification

```
ASA# packet-tracer input dmz tcp 172.16.1.2 1234 207.1.1.2 80 detail

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0          0.0.0.0          outside
…
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
Additional Information:
Static translate 172.16.1.2/1234 to 194.1.1.254/1234
 Forward Flow based lookup yields rule:
 in  id=0x739f84d8, priority=6, domain=nat, deny=false
        hits=2, user_data=0x73a1e480, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=172.16.1.2, mask=255.255.255.255, port=0
   (1)  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=dmz, output_ifc=outside
```



Now the correct rule is hit and static NAT works as expected for traffic DMZ:172.16.1.2 -> Internet

Troubleshooting – Solution Verification

1 nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
2 nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static RemoteOfficeNet RemoteOfficeNet-2
3 nat (dmz,outside) source dynamic obj-172.16.1.0 interface

```
ASA# show asp table classify domain nat

Input Table
in   id=0x739f84d8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e480, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.2, mask=255.255.255.255, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x73982f98, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e8f8, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=10.2.2.0, mask=255.255.255.0, port=0
         dst ip/id=172.16.1.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=outside, output_ifc=dmz
in   id=0x73a1fbd8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e9a0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
in   id=0x739696a0, priority=6, domain=nat, deny=false
         hits=0, user_data=0x73a1e528, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
         src ip/id=172.16.1.0, mask=255.255.255.0, port=0
         dst ip/id=10.2.2.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=dmz, output_ifc=outside
```

Hmm… why was it placed here?

Will Identity NAT work?

Troubleshooting – Identity NAT

```
ASA# packet-tracer input dmz tcp 172.16.1.2 1234 10.2.2.2 80 detail

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static
RemoteOfficeNet RemoteOfficeNet-2
Additional Information:
NAT divert to egress interface outside
Untranslate 10.2.2.2/80 to 10.2.2.2/80
…
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
Additional Information:
Static translate 172.16.1.2/1234 to 172.16.1.2/1234
 Forward Flow based lookup yields rule:
 in  id=0x739f84d8, priority=6, domain=nat, deny=false
        hits=3, user_data=0x73a1e480, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
   (1)  src ip/id=172.16.1.2, mask=255.255.255.255, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=dmz, output_ifc=outside
```

Note that destination IP is 10.2.2.2 now, so Identity NAT rule (rule #2) should be hit…

…but we see that static NAT rule is hit instead at step 3, which doesn't look correct…

Troubleshooting – Identity NAT

```
ASA# packet-tracer input dmz tcp 172.16.1.2 1234 10.2.2.2 80 detail

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static
RemoteOfficeNet RemoteOfficeNet-2
Additional Information:
NAT divert to egress interface outside
Untranslate 10.2.2.2/80 to 10.2.2.2/80
…
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
Additional Information:
Static translate 172.16.1.2/1234 to 172.16.1.2/1234
 Forward Flow based lookup yields rule:
 in  id=0x739f84d8, priority=6, domain=nat, deny=false
        hits=3, user_data=0x73a1e480, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=172.16.1.2, mask=255.255.255.255, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=dmz, output_ifc=outside
```

but, on the other hand, syslog message confirms that Identity NAT rule #1 is hit…

%ASA-6-302013: Built outbound TCP connection 60 for outside:10.2.2.2/80 (10.2.2.2/80) to dmz:172.16.1.2/1234 (172.16.1.2/1234) ②

①

Troubleshooting – Identity NAT

```
ASA# packet-tracer input dmz tcp 172.16.1.2 1234 10.2.2.2 80 detail

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static
RemoteOfficeNet RemoteOfficeNet-2
Additional Information:
NAT divert to egress interface outside
Untranslate 10.2.2.2/80 to 10.2.2.2/80
…
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
Additional Information:
Static translate 172.16.1.2/1234 to 172.16.1.2/1234
 Forward Flow based lookup yields rule:
 in  id=0x739f84d8, priority=6, domain=nat, deny=false
        hits=3, user_data=0x73a1e480, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=172.16.1.2, mask=255.255.255.255, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=dmz, output_ifc=outside
```

In fact, NAT decision at step #3 is ignored as UN-NAT at step #1 takes precedence over NAT

Note this line…

Troubleshooting – Identity NAT

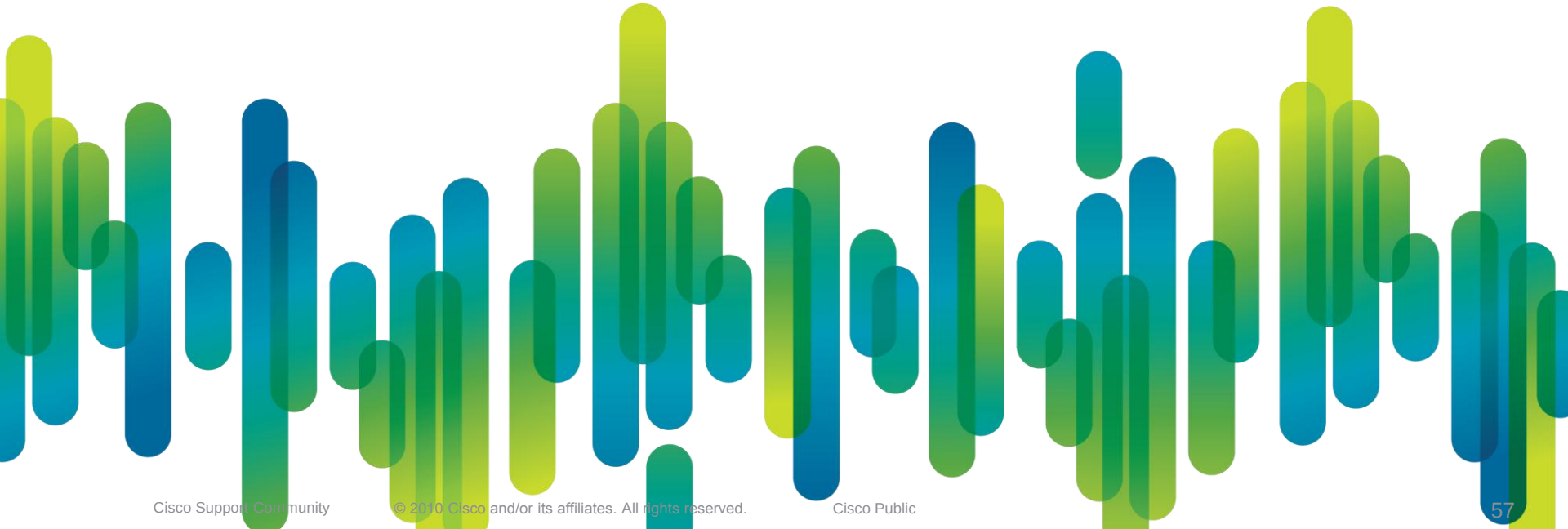
```
nat (dmz,outside) source static obj-172.16.1.2 obj-194.1.1.254
nat (dmz,outside) source static obj-172.16.1.0 obj-172.16.1.0 destination static RemoteOfficeNet RemoteOfficeNet-2
nat (dmz,outside) source dynamic obj-172.16.1.0 interface
```

UN-NAT uses “NAT divert table” to classify traffic

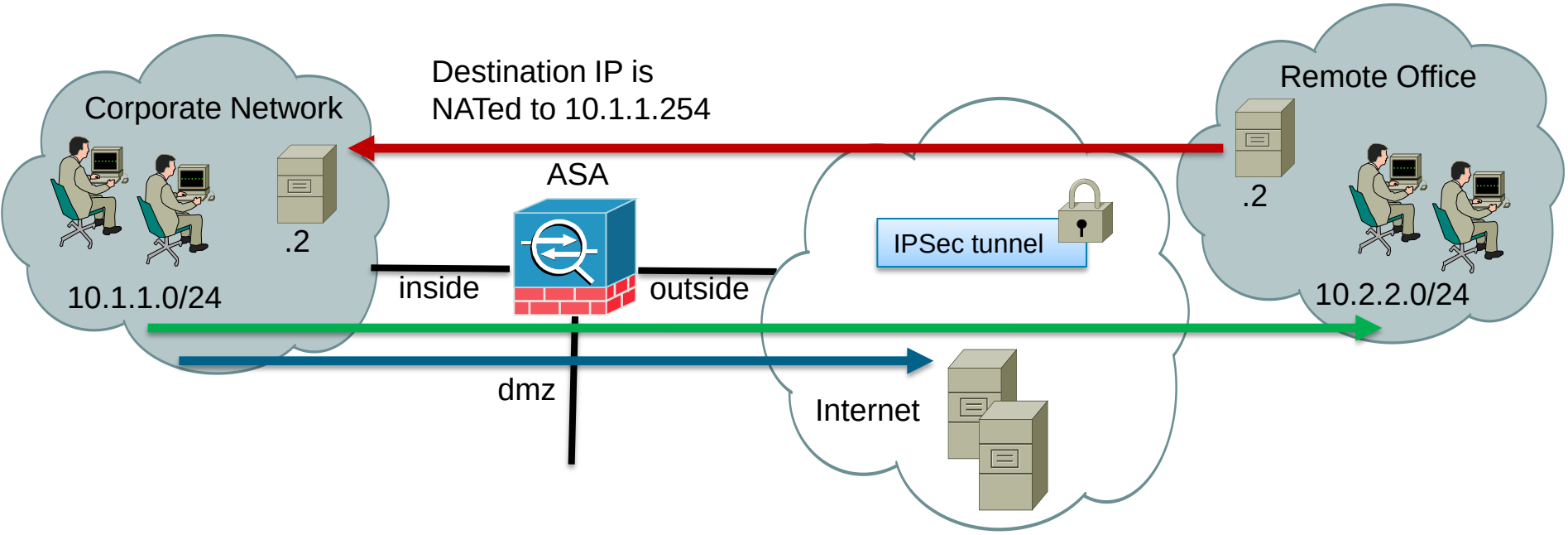
```
ASA# show nat divert-table

Divert Table
id=0x73aea970, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=194.1.1.254, mask=255.255.255.255 port=0-0
        input_ifc=outside, output_ifc=dmz
id=0x73aebc00, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=172.16.1.0, mask=255.255.255.0 port=0-0
        dst ip/id=10.2.2.0, mask=255.255.255.0 port=0-0
        input_ifc=dmz, output_ifc=outside
id=0x73aedbc8, domain=divert-route
        type=dynamic, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=194.1.1.1, mask=255.255.255.255 port=0-0
        input_ifc=outside, output_ifc=dmz
id=0x73aebb58, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=10.2.2.0, mask=255.255.255.0 port=0-0
        dst ip/id=172.16.1.0, mask=255.255.255.0 port=0-0
        input_ifc=outside, output_ifc=dmz
```

This rule classifies traffic and routes it to outside interface

Troubleshooting Scenario #2



Security Policy Example



Remote office server 10.2.2.2 needs to talk to inside server 10.1.1.2, but 10.1.1.2 has default route via some internal router 10.1.1.x and cannot have routes through the ASA due to security reasons.

So, the decision was made to NAT all incoming requests, coming from 10.2.2.2, to 10.1.1.254.

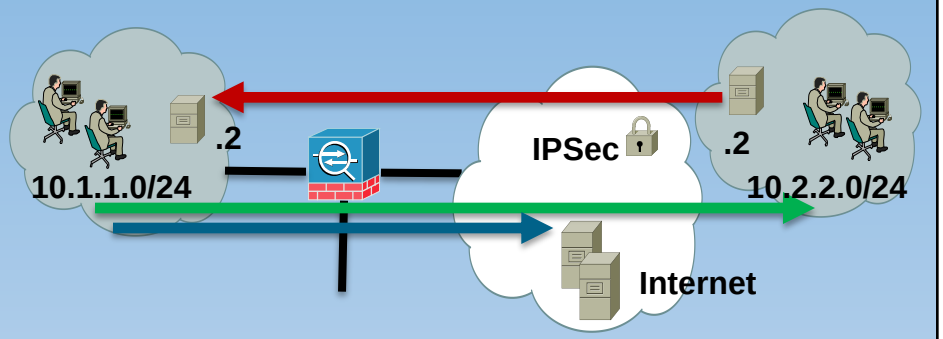
Other hosts in 10.1.1.0/24 and 10.2.2.0/24 should be able to communicate without NAT.

ASA Interface Configuration

```
interface GigabitEthernet0/0.1
 vlan 99
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/0.2
 vlan 98
 nameif dmz
 security-level 50
 ip address 172.16.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 194.1.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 194.1.1.2 1
```

ASA NAT Configuration – 8.3+

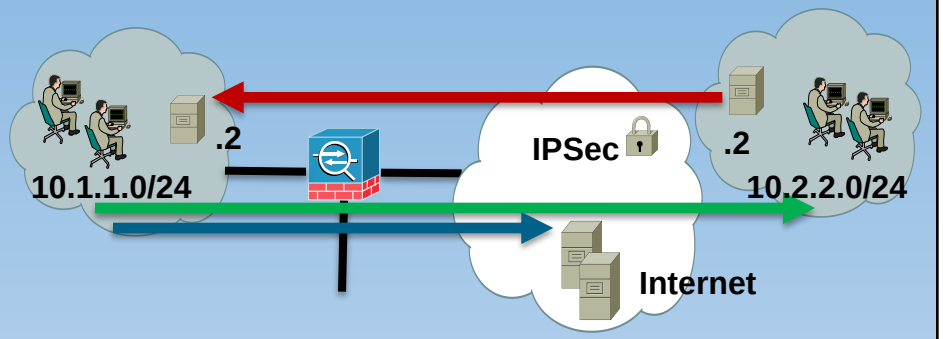
```
object network obj-10.1.1.0
 subnet 10.1.1.0 255.255.255.0

object network obj-10.1.1.254
 host 10.1.1.254

object network RemoteOfficeNet
 subnet 10.2.2.0 255.255.255.0

object network RemoteServer
 host 10.2.2.2

nat (outside,inside) source static RemoteServer obj-10.1.1.254

nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination
static RemoteOfficeNet RemoteOfficeNet

nat (inside,outside) source dynamic any interface
```



Customer Symptom

Remote office server 10.2.2.2 cannot access inside server 10.1.1.2.

Connection is created, but 10.2.2.2 is not NATed to 10.1.1.254

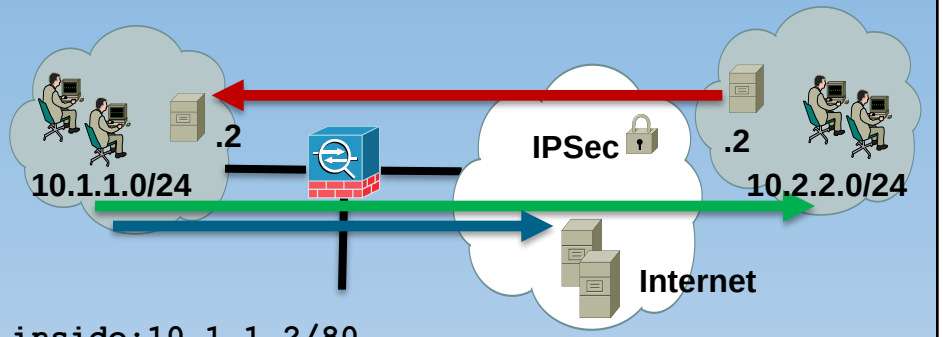



```
ASA# show conn long

TCP outside:10.2.2.2/31444 (10.2.2.2/31444) inside:10.1.1.2/80 (10.1.1.2/80),
flags SaAB, idle 6s, uptime 12s, timeout 30s, bytes 0
```

%ASA-6-302013: Built inbound TCP connection 198 for outside:10.2.2.2/31444 (10.2.2.2/31444) to inside:10.1.1.2/80 (10.1.1.2/80)

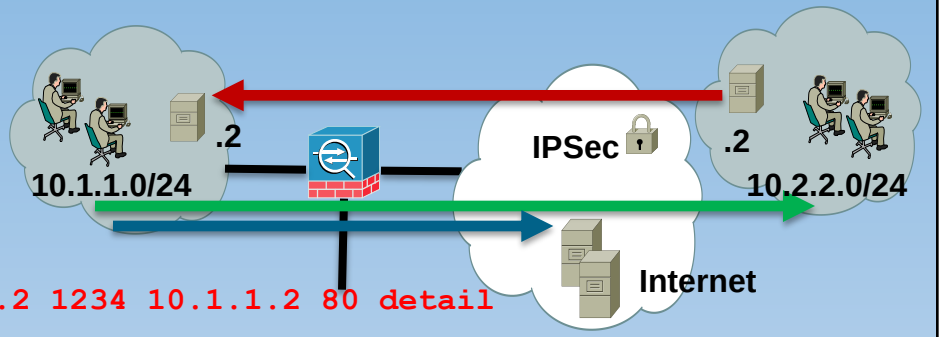
Troubleshooting – Step #1

It seems that first NAT rule is not hit




```
ASA# debug nat 255

nat: untranslation - outside:10.1.1.2/80 to inside:10.1.1.2/80


ASA# show nat detail
Manual NAT Policies (Section 1)
1 (outside) to (inside) source static RemoteServer obj-10.1.1.254
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.2.2.2/32, Translated: 10.1.1.254/32
2 (inside) to (outside) source static obj-10.1.1.0 obj-10.1.1.0   destination static
RemoteOfficeNet RemoteOfficeNet
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
    Destination - Origin: 10.2.2.0/24, Translated: 10.2.2.0/24
3 (inside) to (outside) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 194.1.1.1/24
```

Troubleshooting – Step #2

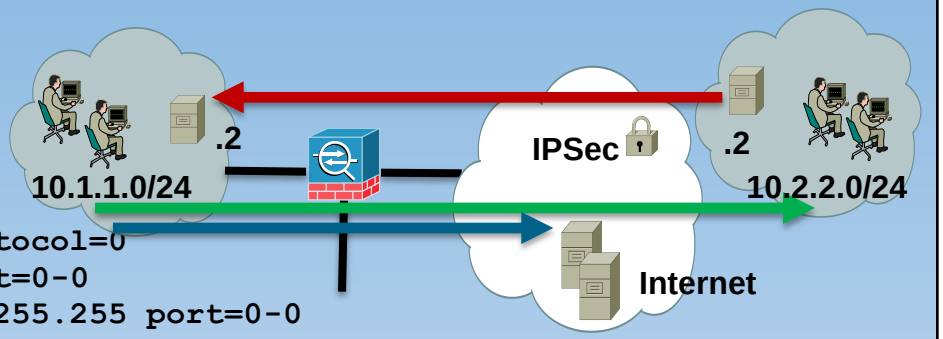



```
ASA# packet-tracer input outside tcp 10.2.2.2 1234 10.1.1.2 80 detail

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
RemoteOfficeNet RemoteOfficeNet
Additional Information:
NAT divert to egress interface inside
Untranslate 10.1.1.2/80 to 10.1.1.2/80
…
Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,inside) source static RemoteServer obj-10.1.1.254
…
```

UN-NAT chose another rule at step #1, so static NAT rule was ignored and NAT at step #4 wasn't performed

Troubleshooting – Step #3

```
ASA# show nat divert-table

Divert Table
id=0x73a92fc0, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=10.1.1.254, mask=255.255.255.255 port=0-0
        input_ifc=inside, output_ifc=outside
id=0x73a944a0, domain=divert-route
        type=static, hits=3, flags=0x1, protocol=0
        src ip/id=10.2.2.0, mask=255.255.255.0 port=0-0
        dst ip/id=10.1.1.0, mask=255.255.255.0 port=0-0
        input_ifc=outside, output_ifc=inside


ASA# show run nat
nat (outside,inside) source static RemoteServer obj-10.1.1.254
nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
RemoteOfficeNet RemoteOfficeNet
nat (inside,outside) source dynamic any interface
```

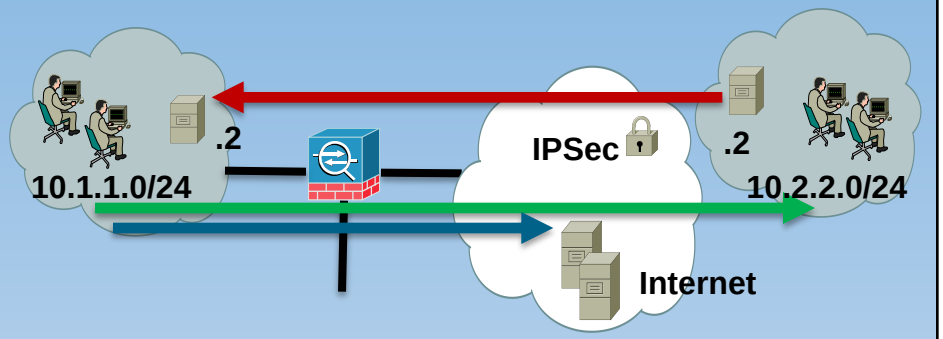


There is only one rule for outside interface in “NAT divert table”.

This rule was created from NAT rule #2 and blocked execution of NAT rule #1…

Troubleshooting – Workaround

```
object network obj-10.1.1.0
 subnet 10.1.1.0 255.255.255.0

object network obj-10.1.1.254
 host 10.1.1.254

object network RemoteOfficeNet
 subnet 10.2.2.0 255.255.255.0

object network RemoteServer
 host 10.2.2.2

object network LocalServer
 host 10.1.1.2

object network LocalServer-2
 host 10.1.1.2
```



The root cause of the problem is that “NAT divert table” is not populated with an entry for 1st NAT rule.

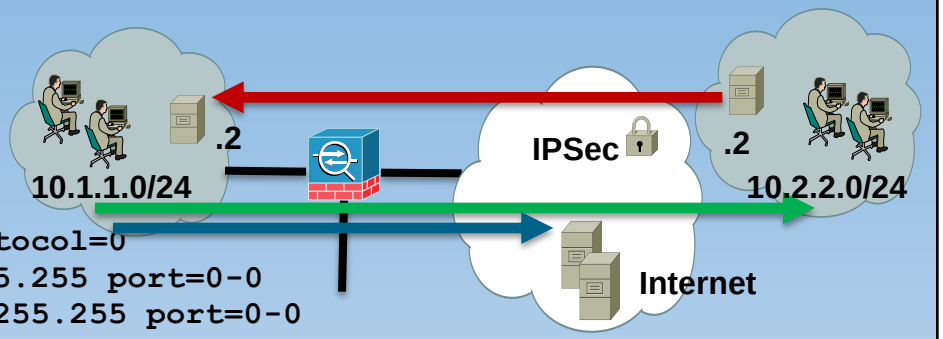
So, we can try to reconfigure 1st NAT rule and correct entry will be installed into the “NAT divert table”.

```
nat (outside,inside) source static RemoteServer obj-10.1.1.254 destination static
LocalServer LocalServer-2
nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
RemoteOfficeNet RemoteOfficeNet
nat (inside,outside) source dynamic any interface
```

Note that it is necessary to use two different object names here: LocalServer and LocalServer-2, otherwise “NAT divert” rule will not be installed

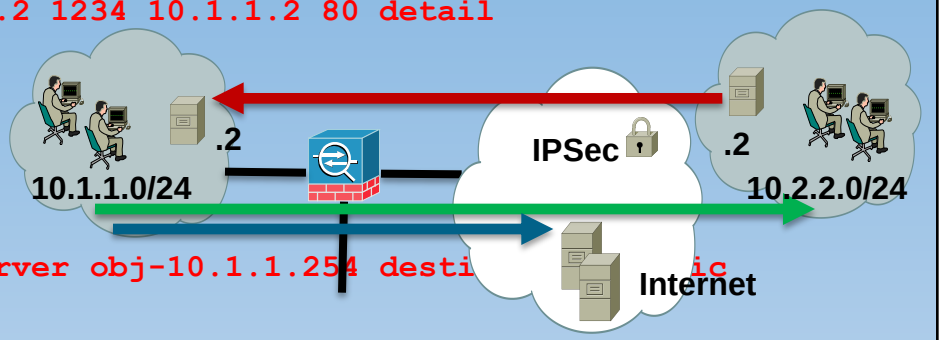
Troubleshooting – Verification

```
ASA# show nat divert-table

Divert Table
id=0x739f6ea8, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=10.1.1.2, mask=255.255.255.255 port=0-0
        dst ip/id=10.1.1.254, mask=255.255.255.255 port=0-0
        input_ifc=inside, output_ifc=outside
id=0x73a92fc0, domain=divert-route
        type=static, hits=1, flags=0x1, protocol=0
        src ip/id=10.2.2.2, mask=255.255.255.255 port=0-0
        dst ip/id=10.1.1.2, mask=255.255.255.255 port=0-0
        input_ifc=outside, output_ifc=inside
id=0x72f21768, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=10.2.2.0, mask=255.255.255.0 port=0-0
        dst ip/id=10.1.1.0, mask=255.255.255.0 port=0-0
        input_ifc=outside, output_ifc=inside

ASA# show run nat
nat (outside,inside) source static RemoteServer obj-10.1.1.254 destination static
LocalServer LocalServer-2
nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
RemoteOfficeNet RemoteOfficeNet
nat (inside,outside) source dynamic any interface
```



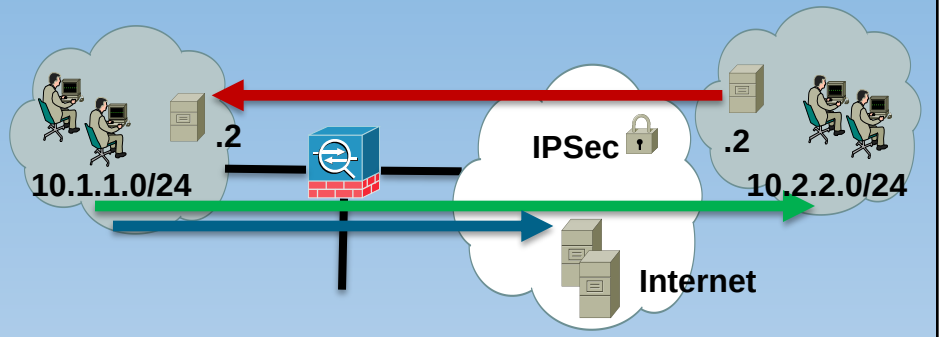
Troubleshooting – Verification

```
ASA# packet-tracer input outside tcp 10.2.2.2 1234 10.1.1.2 80 detail

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,inside) source static RemoteServer obj-10.1.1.254 desti                ic
LocalServer LocalServer-2
Additional Information:
NAT divert to egress interface inside
Untranslate 10.1.1.2/80 to 10.1.1.2/80
…
Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,inside) source static RemoteServer obj-10.1.1.254 destination static
LocalServer LocalServer-2
Additional Information:
Static translate 10.2.2.2/1234 to 10.1.1.254/1234
 Forward Flow based lookup yields rule:
 in  id=0x6dec91a0, priority=6, domain=nat, deny=false
        hits=1, user_data=0x739f6ea8, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.2.2.2, mask=255.255.255.255, port=0
        dst ip/id=10.1.1.2, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=outside, output_ifc=inside
```



Correct rule is hit at both UN-NAT and NAT steps

Troubleshooting – Verification



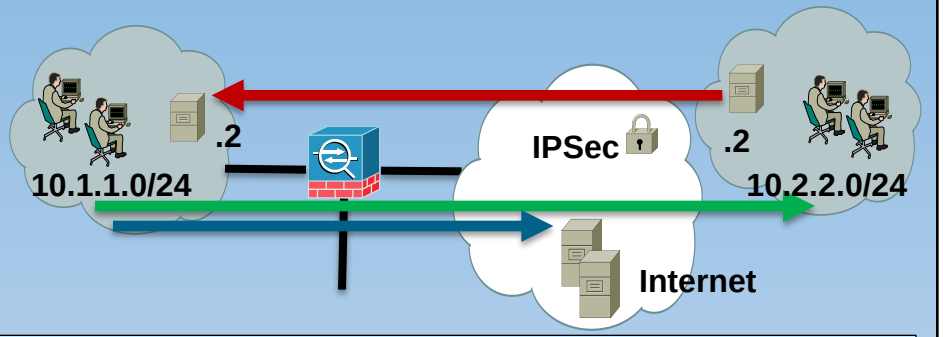
Correct rule is hit at both UN-NAT and NAT steps

```
ASA# show nat detail
Manual NAT Policies (Section 1)
1 (outside) to (inside) source static RemoteServer obj-10.1.1.254   destination static
LocalServer LocalServer-2
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 10.2.2.2/32, Translated: 10.1.1.254/32
    Destination - Origin: 10.1.1.2/32, Translated: 10.1.1.2/32
2 (inside) to (outside) source static obj-10.1.1.0 obj-10.1.1.0   destination static
RemoteOfficeNet RemoteOfficeNet
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
    Destination - Origin: 10.2.2.0/24, Translated: 10.2.2.0/24
3 (inside) to (outside) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 194.1.1.1/24
```

Troubleshooting – Permanent Fix

Permanent fix is available in 8.4(4.2)

CSCtq47028 ASA: Manual NAT rules are not processed in order

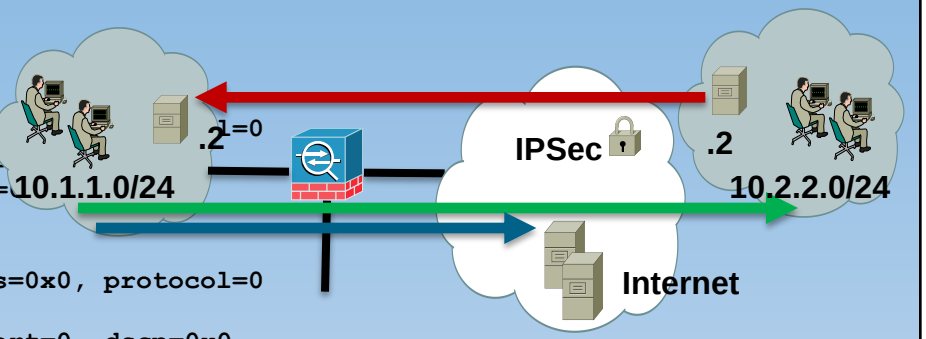


The CSCtq47028 fix made above workaround unnecessary. NAT rules are installed automatically into both “NAT divert” and NAT tables. This is a huge change in NAT implementation!

```
ASA# show run nat

nat (outside,inside) source static RemoteServer obj-10.1.1.254 (1)
nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
RemoteOfficeNet RemoteOfficeNet
nat (inside,outside) source dynamic any interface
```

Troubleshooting – Permanent Fix

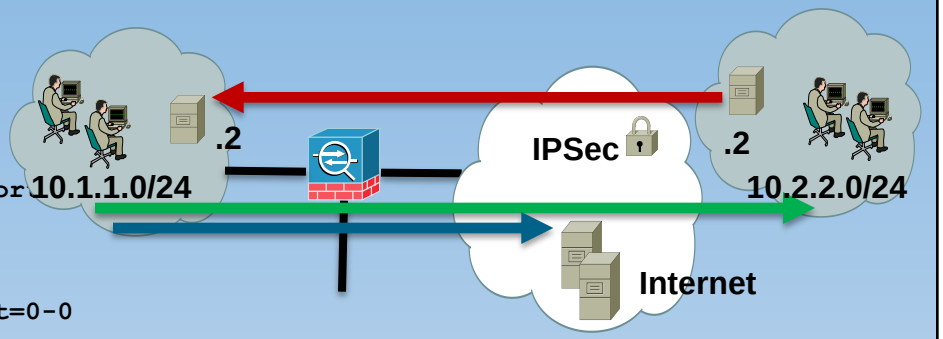
```
ASA# show asp table classify domain nat

Input Table
in   id=0x6decad08, priority=6, domain=nat, deny=false
         hits=0, user_data=0x6deca528, cs_id=0x0, flag                l=0
         src ip/id=10.2.2.2, mask=255.255.255.255, port
 (1)     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=
         input_ifc=outside, output_ifc=inside
in   id=0x6decaf80, priority=6, domain=nat, deny=false
         hits=0, user_data=0x6deca5d0, cs_id=0x0, flags=0x0, protocol=0
         src ip/id=0.0.0.0, mask=0.0.0.0, port=0
         dst ip/id=10.1.1.254, mask=255.255.255.255, port=0, dscp=0x0
         input_ifc=inside, output_ifc=outside
in   id=0x739c64f8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x739c0378, cs_id=0x0, flags=0x0, protocol=0
         src ip/id=10.1.1.0, mask=255.255.255.0, port=0
         dst ip/id=10.2.2.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=inside, output_ifc=outside
in   id=0x739c6770, priority=6, domain=nat, deny=false
         hits=0, user_data=0x6decd9f8, cs_id=0x0, flags=0x0, protocol=0
         src ip/id=10.2.2.0, mask=255.255.255.0, port=0
         dst ip/id=10.1.1.0, mask=255.255.255.0, port=0, dscp=0x0
         input_ifc=outside, output_ifc=inside
in   id=0x6decc5f0, priority=6, domain=nat, deny=false
         hits=0, user_data=0x7307e530, cs_id=0x0, flags=0x0, protocol=0
         src ip/id=0.0.0.0, mask=0.0.0.0, port=0
         dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
         input_ifc=inside, output_ifc=outside
in   id=0x6decc9d8, priority=6, domain=nat, deny=false
         hits=0, user_data=0x7307e3e0, cs_id=0x0, flags=0x0, protocol=0
         src ip/id=0.0.0.0, mask=0.0.0.0, port=0
         dst ip/id=194.1.1.1, mask=255.255.255.255, port=0, dscp=0x0
         input_ifc=outside, output_ifc=inside
```



Rule (1) in ASP NAT table is used to classify traffic, coming from 10.2.2.2, and translate source IP from 10.2.2.2 to 10.1.1.254

Troubleshooting – Permanent Fix

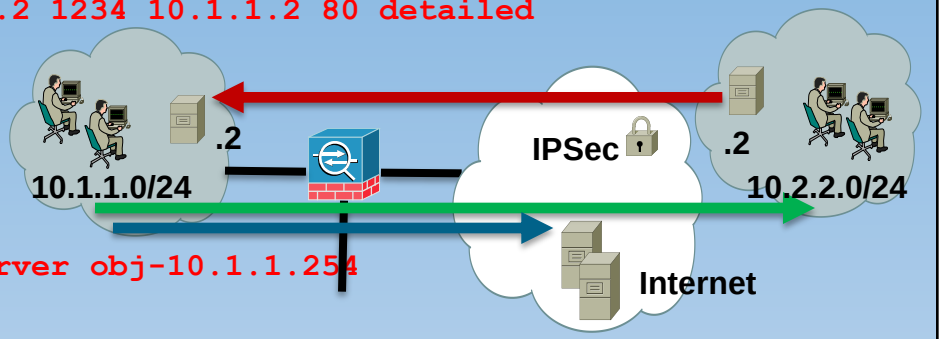
```
ASA# show nat divert-table

Divert Table
id=0x6deca528, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=10.1.1.254, mask=255.255.255.255 por
        input_ifc=inside, output_ifc=outside
id=0x6deca5d0, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=10.2.2.2, mask=255.255.255.255 port=0-0
  (1)   dst ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        input_ifc=outside, output_ifc=inside
id=0x739c0378, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=10.2.2.0, mask=255.255.255.0 port=0-0
        dst ip/id=10.1.1.0, mask=255.255.255.0 port=0-0
        input_ifc=outside, output_ifc=inside
id=0x6decd9f8, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=10.1.1.0, mask=255.255.255.0 port=0-0
        dst ip/id=10.2.2.0, mask=255.255.255.0 port=0-0
        input_ifc=inside, output_ifc=outside
id=0x7307e530, domain=divert-route
        type=dynamic, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=194.1.1.1, mask=255.255.255.255 port=0-0
        input_ifc=outside, output_ifc=inside
id=0x7307e3e0, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        input_ifc=inside, output_ifc=outside
```



Rule (1) in ASP “NAT divert” table is used to classify traffic, coming from 10.2.2.2, and translate destination IP from a.b.c.d (i.e. any IP) to itself

Troubleshooting – Permanent Fix

```
ASA# packet-tracer input outside tcp 10.2.2.2 1234 10.1.1.2 80 detailed
…
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,inside) source static RemoteServer obj-10.1.1.254
Additional Information:
NAT divert to egress interface inside
Untranslate 10.1.1.2/80 to 10.1.1.2/80
…
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,inside) source static RemoteServer obj-10.1.1.254
Additional Information:
Static translate 10.2.2.2/1234 to 10.1.1.254/1234
 Forward Flow based lookup yields rule:
 in  id=0x6decad08, priority=6, domain=nat, deny=false
        hits=1, user_data=0x6deca528, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.2.2.2, mask=255.255.255.255, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=inside
```



Correct rule is hit at both UN-NAT and NAT steps

CSCtq47028 Fix – More Info

- In many customer cases problems were seen when *asymmetric* or *overlapping* NAT rules were configured
- Definition of “asymmetric”
  - If an outbound packet matches a specific NAT rule and the return packet matches a different NAT rule in the table, then they are called *asymmetric* NAT rules. Most common with usage of 'dynamic' or 'unidirectional' NAT.
- Definition of “overlapping”
  - If two or more NAT rules matches **both** source and destination (ports included) in the table, then they are called *overlapping* rules. This also involves usage of 'any' keyword as source or destination network.
- In this case Twice NAT rules may not be processed in order

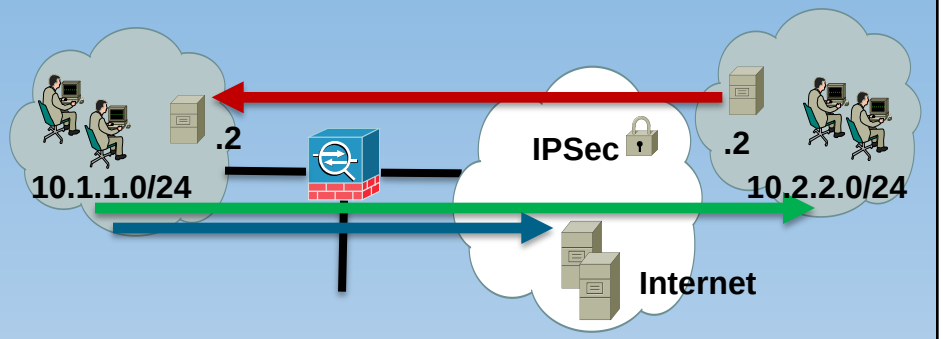
CSCtq47028 Fix – More Info

- This behavior is fixed by CSCtq47028 in 8.4(4.2)
- For a Twice NAT rule, if the destination is not explicitly specified, ASA implicitly adds “destination static any any”
- This populates “NAT divert” table with required rules and NAT rules order is strictly enforced

This change may affect existing configurations!

Impact on Existing Configurations

```
object network obj-10.1.1.254
 host 10.1.1.254

object network RemoteServer
 host 10.2.2.2

nat (inside,outside) source dynamic obj-10.1.1.0 interface
nat (outside,inside) source static RemoteServer obj-10.1.1.254
```

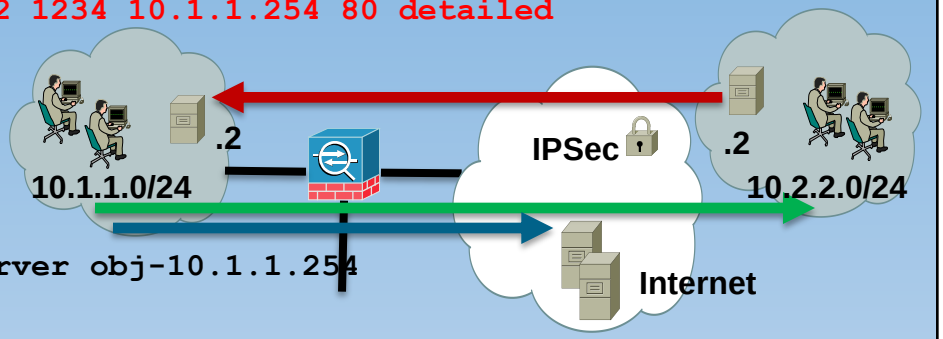


Dynamic PAT is placed above static NAT and Identity NAT is removed. In 8.4(3) this works (unidirectionally). I.e. it's possible to connect to 10.1.1.254 from inside host 10.1.1.2. Destination IP 10.1.1.254 is UN-NATed to 10.2.2.2 according to 2nd NAT rule:

%ASA-6-302013: Built outbound TCP connection 3 for outside:10.2.2.2/80 (10.1.1.254/80) to inside:10.1.1.2/1234 (10.1.1.2/1234)

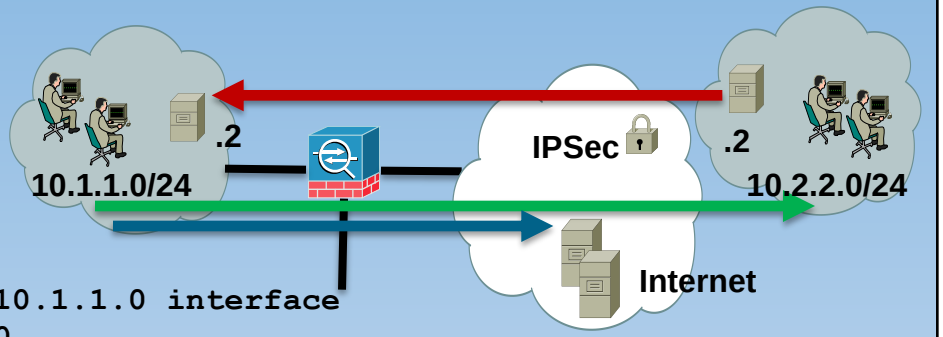
Impact on Existing Configurations

```
ASA# packet-tracer input inside tcp 10.1.1.2 1234 10.1.1.254 80 detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,inside) source static RemoteServer obj-10.1.1.254
Additional Information:
NAT divert to egress interface outside
Untranslate 10.1.1.254/80 to 10.2.2.2/80
…

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic obj-10.1.1.0 interface
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x6e1f6bf8, priority=6, domain=nat, deny=false
        hits=2, user_data=0x73433dc0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.1.1.0, mask=255.255.255.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=inside, output_ifc=outside
```



UN-NAT chose static NAT rule at step #1 and NAT decision at step #3 was ignored. So, order of NAT rules is violated, but customer configuration works.

Impact on Existing Configurations

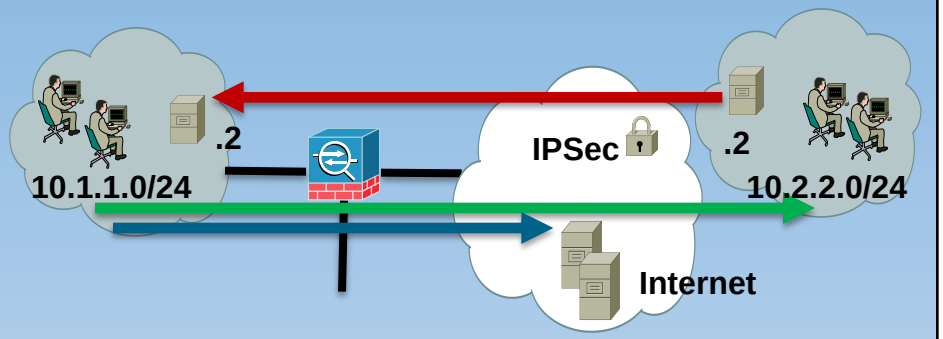



```
ASA# show nat detail
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.1.1.0 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 194.1.1.1/24
2 (outside) to (inside) source static RemoteServer obj-10.1.1.254
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 10.2.2.2/32, Translated: 10.1.1.254/32

ASA# show nat divert-table

Divert Table
id=0x73433dc0, domain=divert-route
        type=dynamic, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=194.1.1.1, mask=255.255.255.255 port=0-0
        input_ifc=outside, output_ifc=inside
id=0x73addc00, domain=divert-route
        type=static, hits=1, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=10.1.1.254, mask=255.255.255.255 port=0-0
        input_ifc=inside, output_ifc=outside
```

Root cause: dynamic PAT didn't create a rule in "NAT Divert" table. Rule, created by static NAT, is there.

Impact on Existing Configurations

```
object network obj-10.1.1.254
 host 10.1.1.254

object network RemoteServer
 host 10.2.2.2

nat (inside,outside) source dynamic obj-10.1.1.0 interface
nat (outside,inside) source static RemoteServer obj-10.1.1.254
```



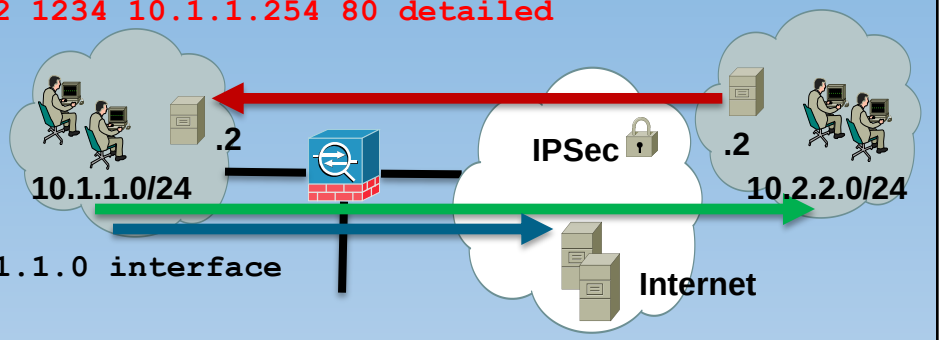
This configuration no longer works after upgrade, as dynamic PAT installs its own rule into the “NAT divert” table for inside interface

%ASA-6-305011: Built dynamic TCP translation from inside:10.1.1.2/1234 to outside:194.1.1.1/1234

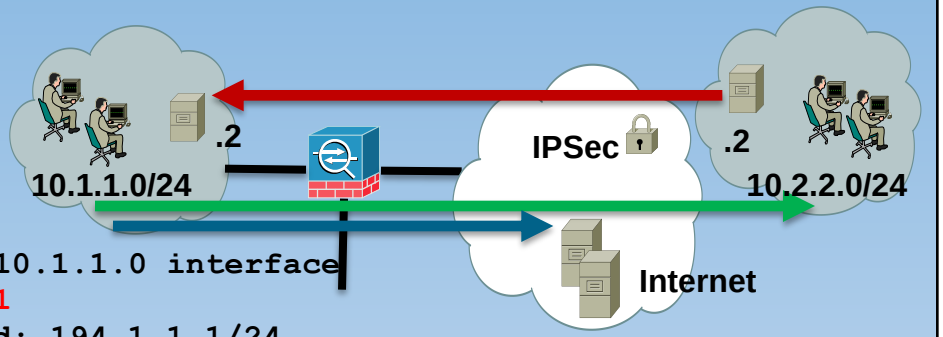
%ASA-6-302013: Built outbound TCP connection 1 for outside:10.1.1.254/80 (10.1.1.254/80) to inside:10.1.1.2/1234 (194.1.1.1/1234)

Impact on Existing Configurations

```
ASA# packet-tracer input inside tcp 10.1.1.2 1234 10.1.1.254 80 detailed

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source dynamic obj-10.1.1.0 interface
Additional Information:
NAT divert to egress interface outside
Untranslate 10.1.1.254/80 to 10.1.1.254/80
…

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic obj-10.1.1.0 interface
Additional Information:
Dynamic translate 10.1.1.2/1234 to 194.1.1.1/1234
 Forward Flow based lookup yields rule:
 in  id=0x739a6878, priority=6, domain=nat, deny=false
        hits=1, user_data=0x7324c4e0, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.1.1.0, mask=255.255.255.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=inside, output_ifc=outside
```

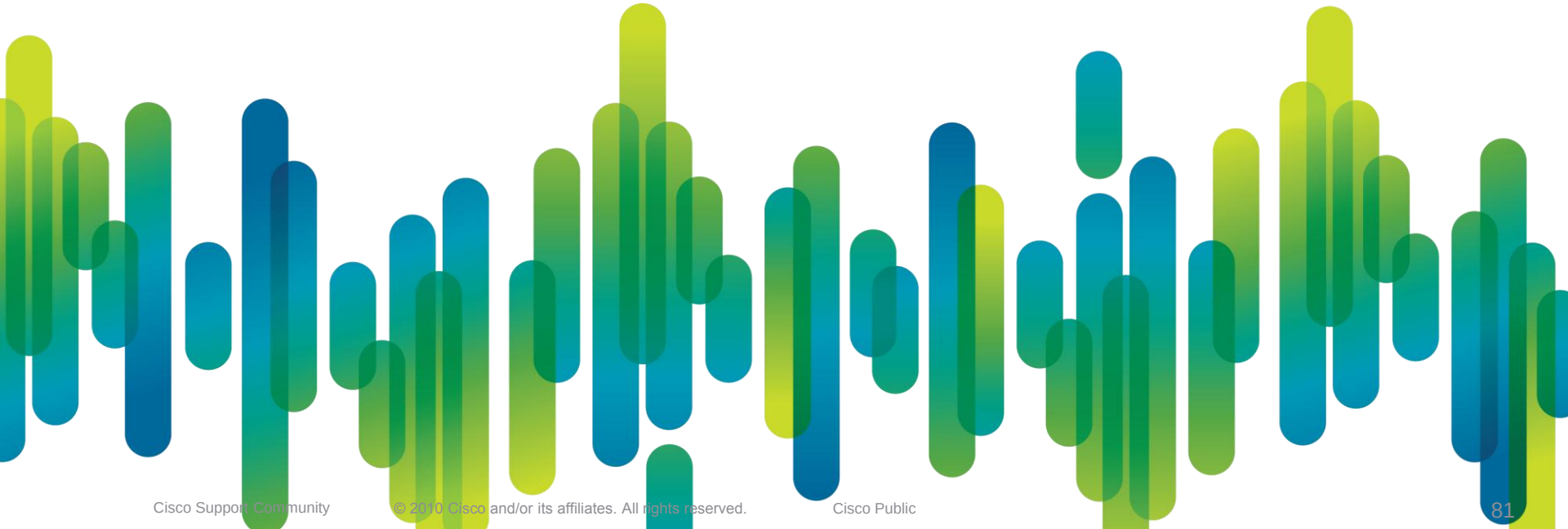


Impact on Existing Configurations




```
ASA# show nat detail
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.1.1.0 interface
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 10.1.1.0/24, Translated: 194.1.1.1/24
2 (outside) to (inside) source static RemoteServer obj-10.1.1.254
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.2.2.2/32, Translated: 10.1.1.254/32

ASA# show nat divert-table

Divert Table
…
id=0x7324c588, domain=divert-route
        type=static, hits=1, flags=0x1, protocol=0
        src ip/id=10.1.1.0, mask=255.255.255.0 port=0-0
        dst ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        input_ifc=inside, output_ifc=outside
id=0x739a80d8, domain=divert-route
        type=static, hits=0, flags=0x1, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0 port=0-0
        dst ip/id=10.1.1.254, mask=255.255.255.255 port=0-0
        input_ifc=inside, output_ifc=outside
```

Final Recommendations



Final Recommendations

- KISS: Keep It Simple, Stupid
- Use Object NAT whenever possible, use Twice NAT when Policy NAT is really needed
- Design your network carefully, don’t use NAT to workaround routing problems
- Don’t use NAT for policy control, use ACLs instead
- Remember that ASA is not a IOS router; learn how NAT and routing interoperate on this platform

Final Recommendations

- Always issue “no nat-control” prior to upgrading to 8.3+
- Don’t upgrade to 8.3 on a Friday night just as you are getting ready to go out of town for the weekend
- Test upgrade in a lab first (if you have one)
- Read documentation and Cisco Support Community documents with ‘ASA’ and ‘nat’ tags
- Call in to the TAC in case of a trouble

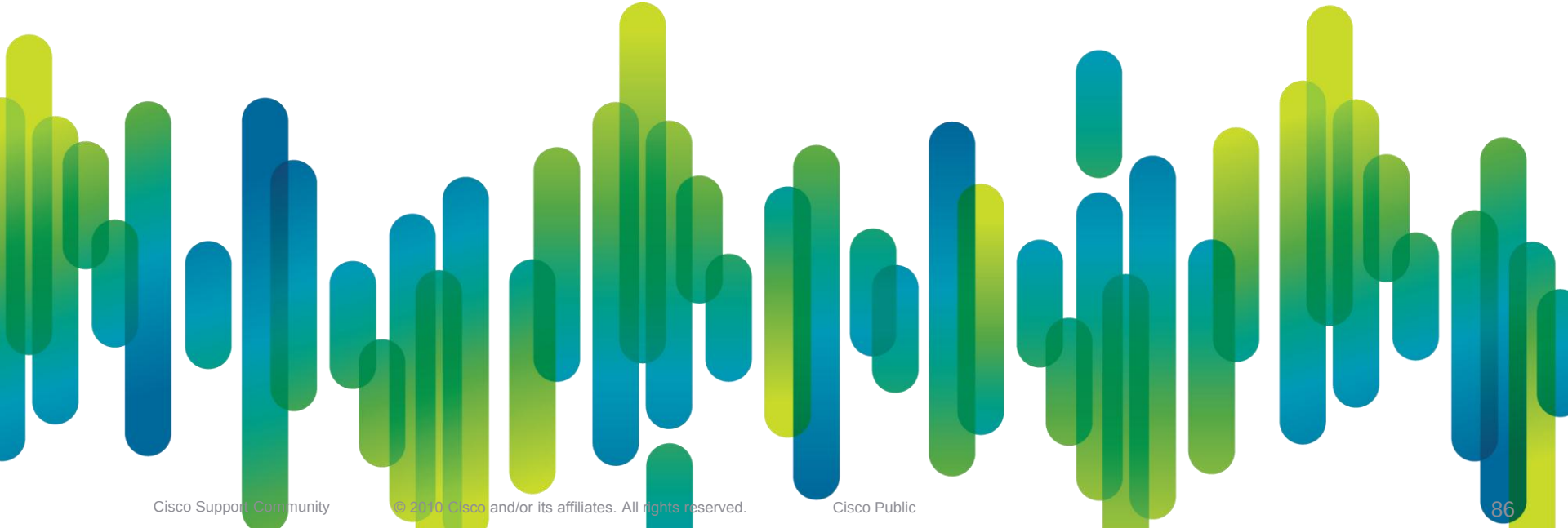
FIN, ACK [Thank you !]

Опрос #3
Какие темы семинаров по безопасности Вам интересны?

1. Построение Remote Access VPN с помощью ASA
2. Построение Site-to-Site VPN на маршрутизаторах
3. DMVPN и GETVPN на маршрутизаторах Cisco
4. Использование платформы ASR1k для VPN
5. Любые вопросы использования Cisco ASA в качестве межсетевого экрана
6. IOS Zone-based Firewall
7. Система обнаружения атак IPS 4200
8. Продукты IronPort

Q & A

Эксперт ответит на некоторые Ваши вопросы. Используйте Q&A панель, чтобы задать еще вопросы



Вебинар с экспертом на английском

Тема: Licensing Architecture: Cisco Unified Call Manager Version 9.x

Вторник, 9 октября

10:00 по московскому времени

Эксперт Cisco:

Amit Singh

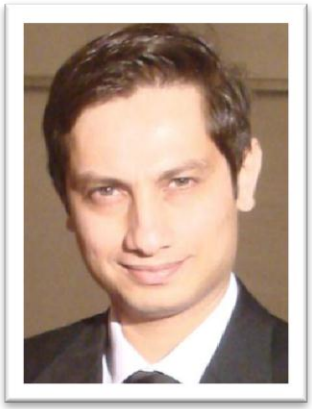
Расскажет об архитектуре лицензирования Cisco Unified Call Manager (CUCM) версии 9.0x.

Регистрация:

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=E&PRIORITY_CODE=4&SEMINAR_CODE=S17111

Вебинар с экспертом на английском

Тема: Troubleshooting SSL VPN on ASA



Вторник, 30 октября

18:00 по московскому времени

Эксперт Cisco:

Jazib Frahim

Расскажет о том как решать проблемы с SSL VPN на Cisco Adaptive Security Appliance (ASA)

Регистрация

https://supportforums.cisco.com/community/netpro/expert-corner#view=webcasts

Сессия «Спросить Эксперта»

Получить дополнительную информацию, а также задать вопросы экспертам в рамках данной темы вы можете в течение двух недель, на странице, доступной по ссылке

https://supportforums.cisco.com/community/russian/expert-corner/ask-the-experts

Вы можете получить видеозапись данного семинара и текст сессии Q&A в течение ближайших 5 дней по следующей ссылке

https://supportforums.cisco.com/community/russian/expert-corner/webcast

Приглашаем Вас активно участвовать в Cisco Support Community и социальных сетях

https://supportforms.cisco.com/community/russian

http://www.facebook.com/CiscoRu

http://twitter.com/CiscoRussia

http://www.youtube.com/user/CiscoRussiaMedia

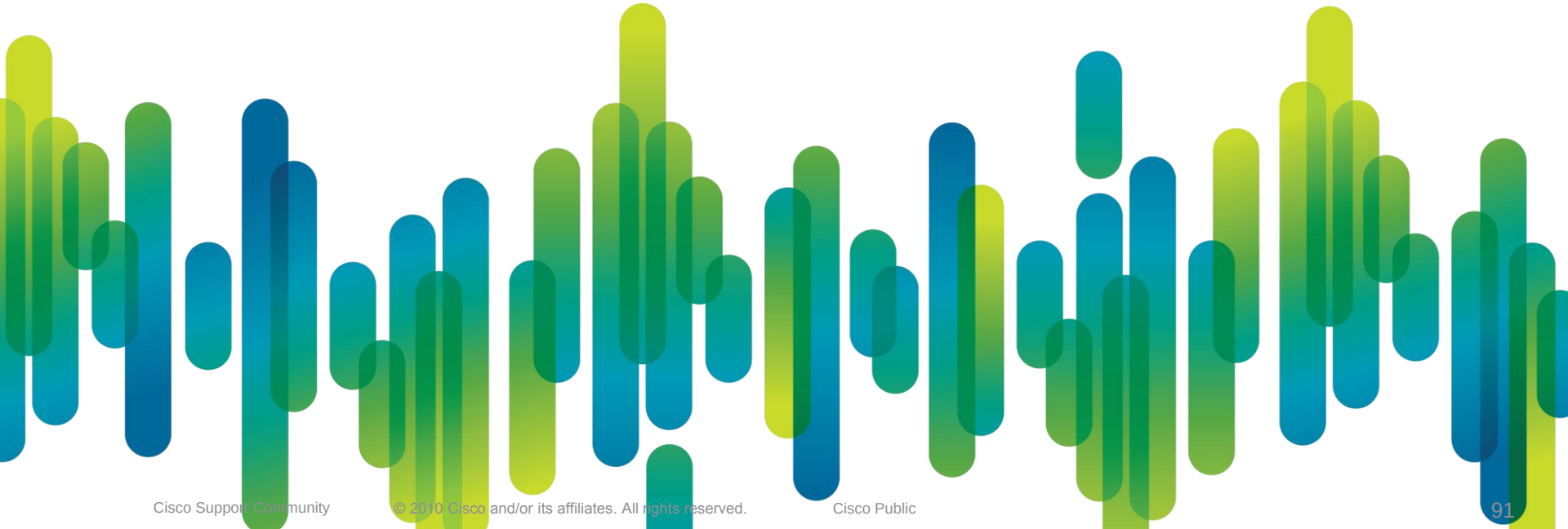
http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8

http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019

Newsletter Subscription:
https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=589&keyCode=146298_2&PHYSICAL%20FULFILLMENT%20Y/N=NO&SUBSCRIPTION%20CENTER=YES

Спасибо за Ваше время

Пожалуйста, участвуйте в опросе




CISCO