cisco Live!

Let's go

#CiscoLive

The bridge to possible

Firepower Cluster NAT and PAT Operation and Troubleshooting

Alejandra Páez Castro
Security Technical Leader, CX Americas
BRKSEC-2102

By understanding how Dynamic PAT works in Secure Firewall Cluster, network performance degradation can be avoided.

Agenda

NAT Types

Cluster Dynamic PAT Operation

- ASA 9.14 and Earlier
  FTD 6.6 and Earlier
- From ASA 9.15.1
  From FTD 6.7
- From ASA 9.16.1
  From FTD 7.0

Troubleshooting Walkthroughs

Demo

Conclusion

Cisco Webex App

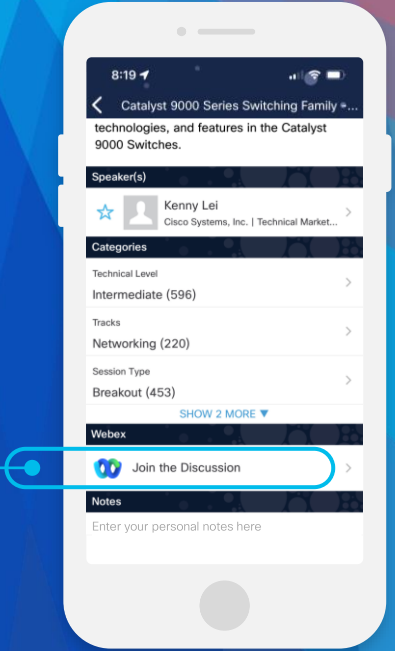
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 9, 2023.



8:19

Catalyst 9000 Series Switching Family •...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2102

Your Presenter

Alejandra Páez Castro

- Venezuela / Mexico
- Telecommunications Engineer
- 6 years as Technical Consulting Engineer in Firewall TAC
- 2 years+ as Security Technical Leader in CX
- Passionate about NGFW appliances

Secure Firewall Threat Defense
Día en la vida de un paquete

Alejandra Páez Castro
Security Technical Leader, CX Americas
BRKSEC-2321

Inclusive Future

Cisco's purpose is to power an inclusive future for all.

As a matter of policy, Cisco content should be free of offensive or suggestive language, graphics, and scenarios. We are changing terms, as noted below, to more appropriate alternatives.

Master – Control Unit

Slave – Data Unit

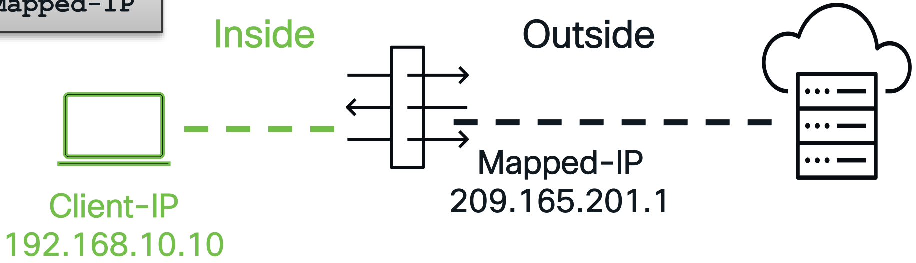
NAT Types

Static NAT

- Fixed translation of a real address to a mapped address
- It allows bidirectional connection initiation
- Static NAT Scenarios
  - Static NAT with Port Translation: Allows translating a well-known port to a non-standard port

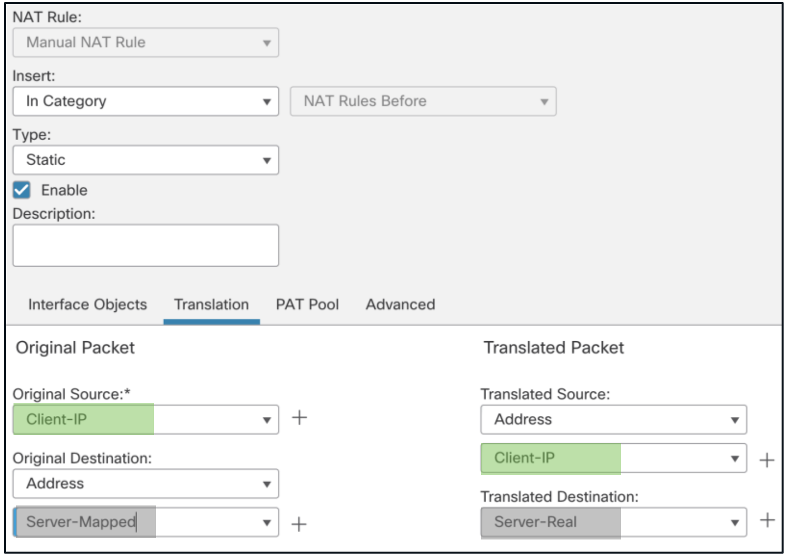
```
> show running-config nat
nat (Inside,Outside) source static Client-IP Mapped-IP
```

```
> show running-config object
object network Client-IP
 host 192.168.10.10
object network Mapped-IP
 host 209.165.201.1
```



Identity NAT

- A real address is statically translated to itself
- Used to exempt traffic from NAT



NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static

☑ Enable

Description:

Original Packet

Original Source:* Client-IP

Original Destination: Address

Server-Mapped

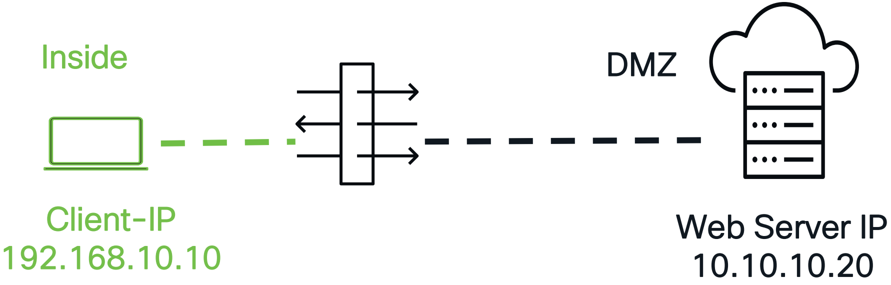
Translated Packet

Translated Source: Address

Client-IP

Translated Destination: Server-Real

```
> show running-config nat
nat (Inside,DMZ) source static Client-IP Client-IP
destination static Server-IP Server-IP
```

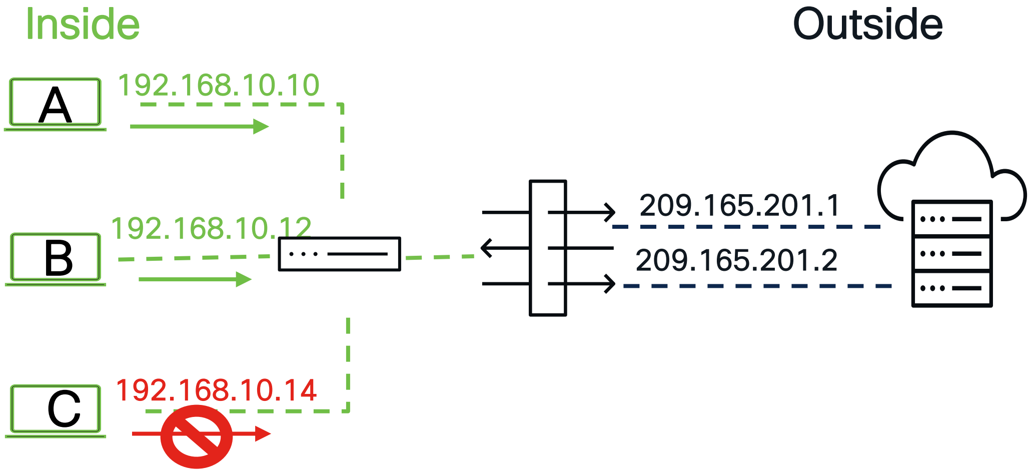


Dynamic NAT

- A group of real IP addresses are mapped to a (usually smaller) **group of mapped IP addresses**
- The translation is created only when the real host initiates the connection

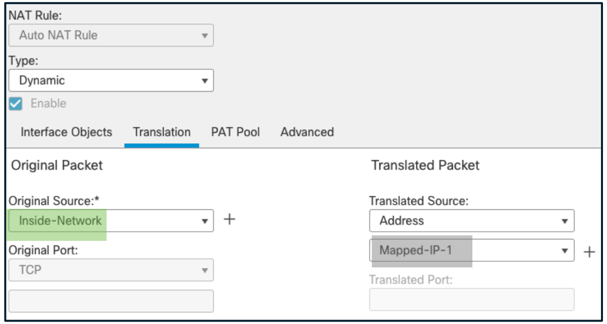
```
object network Inside-Network
 nat (Inside,Outside) static Mapped-IPGroup
```

```
> show running-config object
object network Inside-Network
 subnet 192.168.10.0 255.255.255.0
object network Mapped-IPGroup
 range 209.165.201.1 209.165.201.2
```



Dynamic PAT

- A group of real IP addresses are mapped to a **single IP address** using a unique source port of that IP address



NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Interface Objects | Translation | PAT Pool | Advanced

Original Packet

Original Source:* Inside-Network

Original Port: TCP

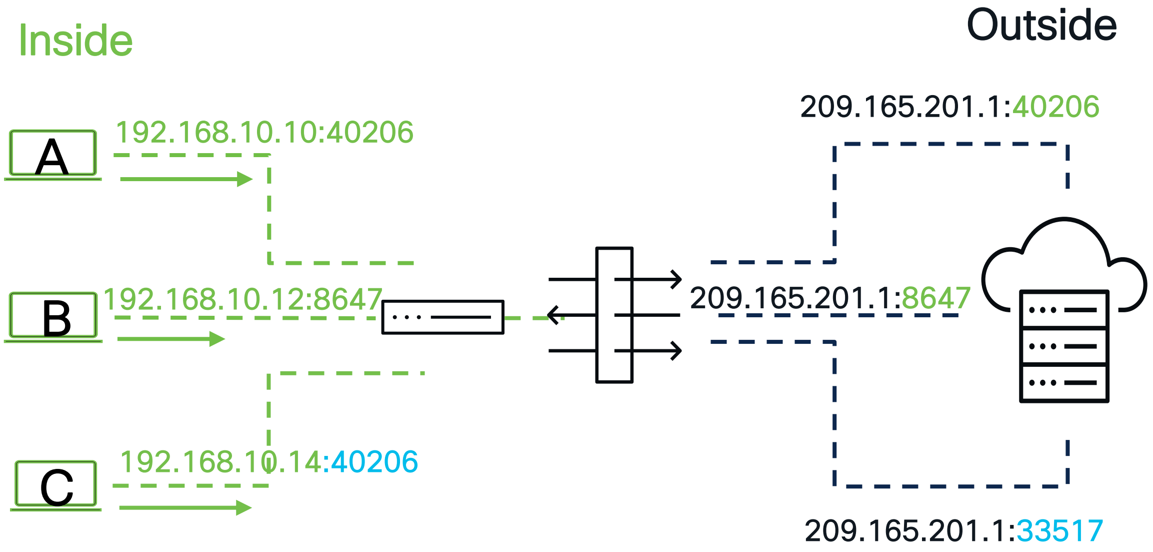
Translated Packet

Translated Source: Address

Mapped-IP-1

Translated Port:

```
> show running-config nat
object network Inside-Network
 nat (Inside,Outside) dynamic
Mapped-IP-1
```



Dynamic PAT

FTD 6.6 and Earlier / ASA 9.14 and Earlier

- If available, the mapped source port will be the same as the real source port
    - In case it is not available, the mapped port is chosen from the same range of ports as the real port number

Real Source Port	Mapped Source Port
1-511	1-511
512-1023	512-1023
1024-65535	1024-65535

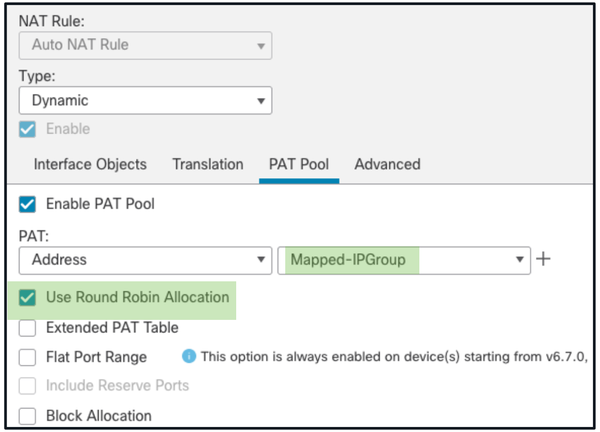
```
> show nat pool
TCP PAT pool Outside, address 209.165.201.1, range 1-511, allocated 0
TCP PAT pool Outside, address 209.165.201.1, range 512-1023, allocated 0
TCP PAT pool Outside, address 209.165.201.1, range 1024-65535, allocated 3
```

```
> show xlate
1 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
                                                  […]
TCP PAT from Inside:192.168.10.10/40206 to Outside:209.165.201.1/40206
flags ri idle 0:03:01 timeout 0:00:30
TCP PAT from Inside:192.168.10.14/40206 to Outside:209.165.201.1/33517
flags ri idle 0:02:01 timeout 0:00:30
```

Pat-Pool Options

Round-Robin

- It assigns an IP address/port from each PAT address in the pool before returning to use the first address again
  - Not supported in Cluster



NAT Rule:
Auto NAT Rule ▾

Type:
Dynamic ▾

☑ Enable

Interface Objects | Translation | PAT Pool | Advanced

☑ Enable PAT Pool

PAT:
Address ▾ | Mapped-IPGroup ▾ +

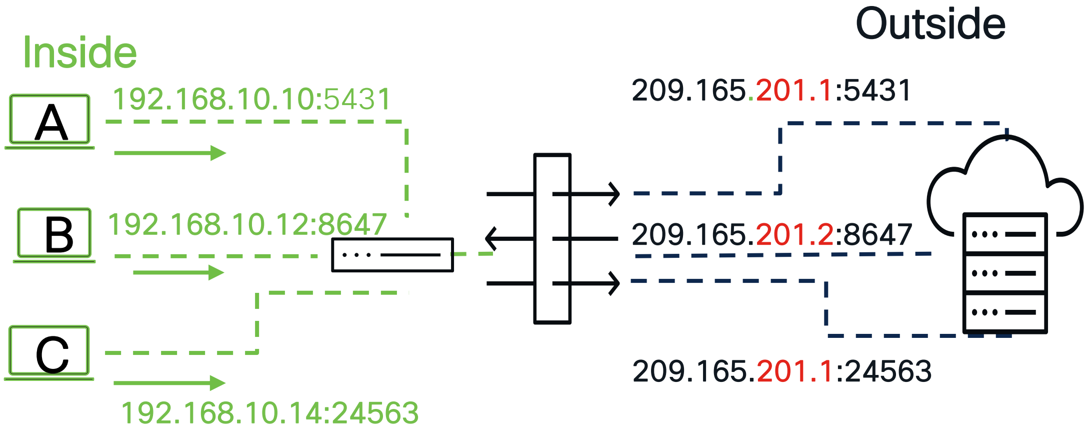
☑ Use Round Robin Allocation

□ Extended PAT Table

□ Flat Port Range — This option is always enabled on device(s) starting from v6.7.0,

□ Include Reserve Ports

□ Block Allocation

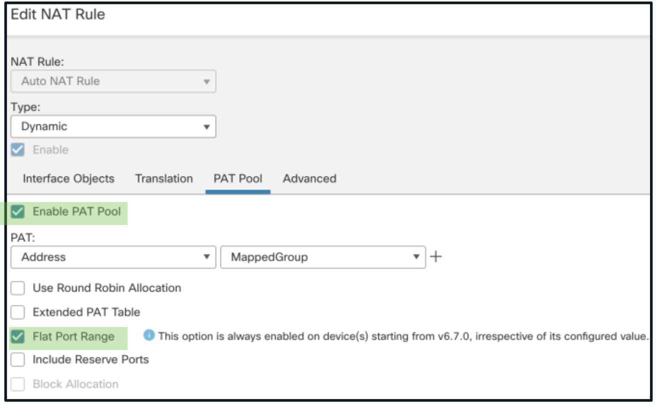


```
> show running-config nat
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool Mapped-IPGroup round-robin
```

```
object network Mapped-IPGroup
 range 209.165.201.1 209.165.201.2
```

Flat

- PAT Xlates are built by using the ephemeral port range 1024-65535, regardless of the source port range



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Interface Objects | Translation | PAT Pool | Advanced

☑ Enable PAT Pool

PAT: Address | MappedGroup +

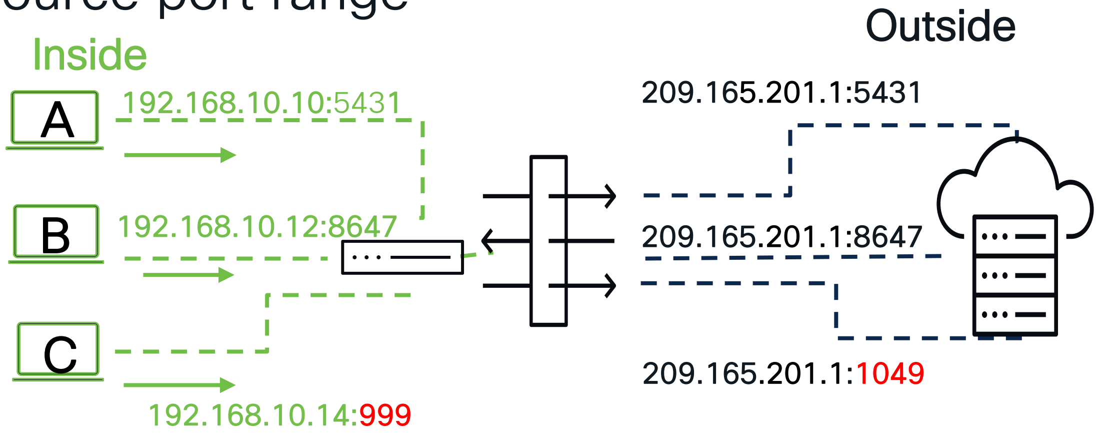
□ Use Round Robin Allocation

□ Extended PAT Table

☑ Flat Port Range — This option is always enabled on device(s) starting from v6.7.0, irrespective of its configured value.

□ Include Reserve Ports

□ Block Allocation

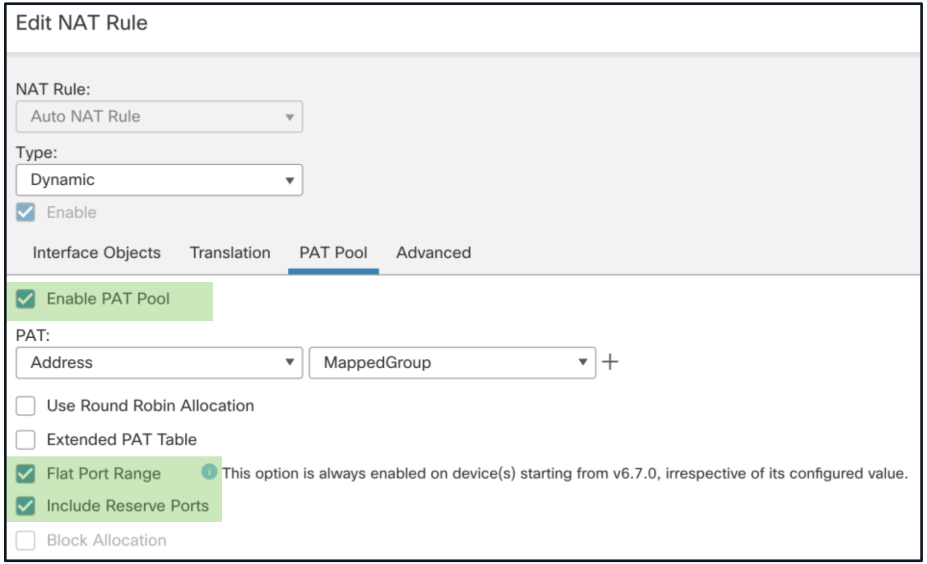


```
> show running-config nat
!
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool
MappedGroup flat
```

```
> show nat pool
TCP PAT pool Outside, address 209.165.201.1,
range 1-1023, allocated 0
TCP PAT pool Outside, address 209.165.201.1,
range 1024-65535, allocated 3
```

Include-reserve

- To use the entire range of 1 to 65535, specify the **include-reserve** keyword



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Interface Objects | Translation | PAT Pool | Advanced

☑ Enable PAT Pool

PAT: Address | MappedGroup +

□ Use Round Robin Allocation

□ Extended PAT Table

☑ Flat Port Range   This option is always enabled on device(s) starting from v6.7.0, irrespective of its configured value.

☑ Include Reserve Ports

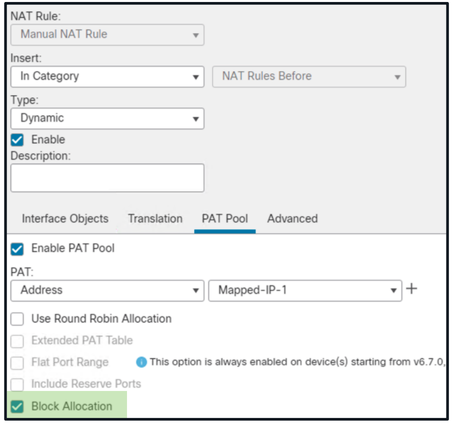
□ Block Allocation

```
> show running-config nat
!
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool
MappedGroup flat include-reserve
```

```
> show nat pool
TCP PAT pool Outside, address 209.165.201.1,
range 1-65535, allocated 1
```

Block-Allocation

- Enables port block allocation per host
  - Port blocks are allocated in the 1024-65535 range only



NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Dynamic

☑ Enable

Description:

Interface Objects | Translation | PAT Pool | Advanced

☑ Enable PAT Pool

PAT: Address | Mapped-IP-1 +

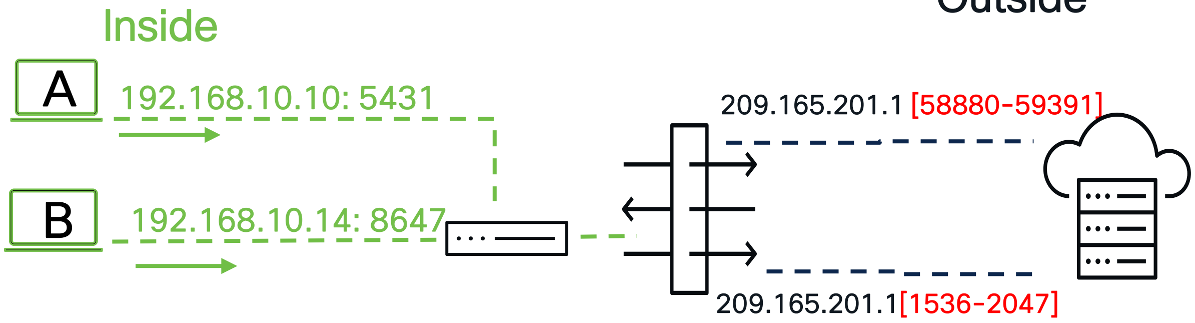
☐ Use Round Robin Allocation

☐ Extended PAT Table

☐ Flat Port Range — This option is always enabled on device(s) starting from v6.7.0,

☐ Include Reserve Ports

☑ Block Allocation



```
> show running-config nat
nat (Inside,Outside) source dynamic Inside-
Network pat-pool Mapped-IP-1 block-allocation
```

```
> show local-host 192.168.10.10
[…]
Port Block Allocation:
Block 1: IP 209.165.201.1, TCP port range 58880-59391, in
use 10
```

PAT Xlate termination

- Multi-Session PAT → PAT Xlate timeout is 30 seconds, by default

```
> show running-config timeout
timeout pat-xlate 0:00:30
```

- Per-session PAT → PAT xlate is immediately removed from the xlate table when the connection is closed
- Per-Session PAT improves the scalability of PAT

```
> show running-config all xlate
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

```
> show conn
9 in use, 191 most used
Inspect Snort:
        preserve-connection: 1 enabled, 0 in
effect, 183 most enabled, 13 most in effect

TCP Outside  209.165.201.10:22 Inside
192.168.10.10:40208, idle 0:00:07, bytes 7818,
flags UxIO N1
```

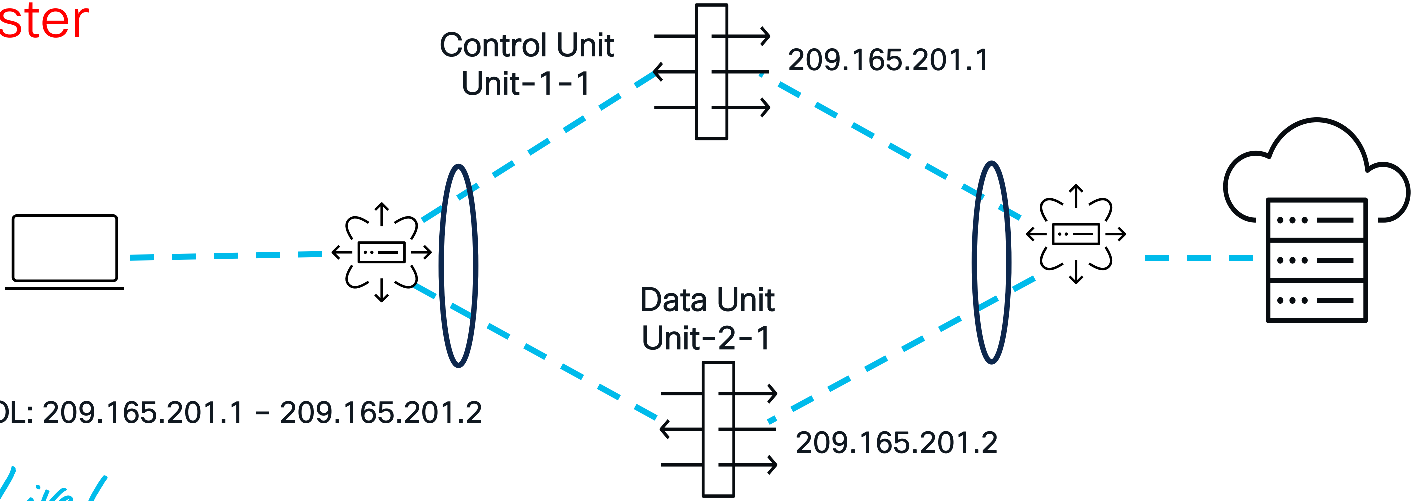
Cluster Dynamic PAT Operation

ASA 9.14 and Earlier
FTD 6.6 and Earlier

Cluster Dynamic PAT Operation

FTD 6.6 and Earlier / ASA 9.14 and Earlier

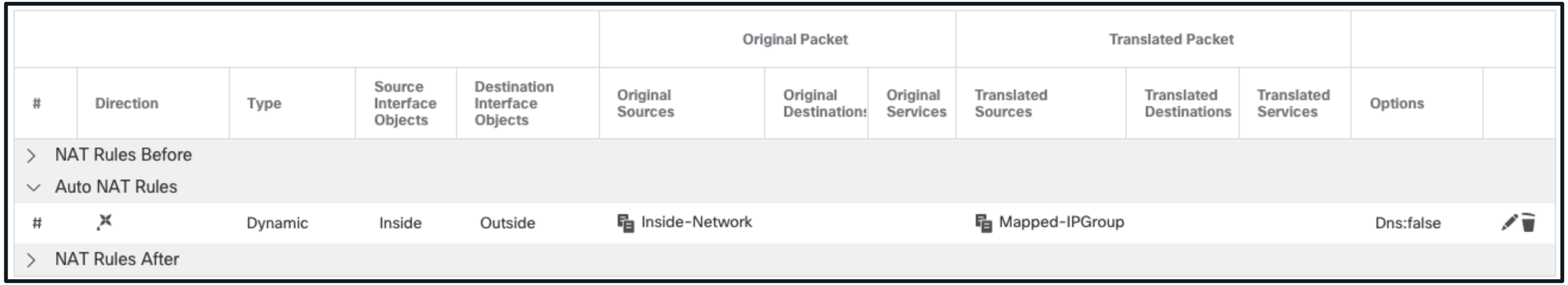
- Control Unit distributes PAT Pool IP addresses across the cluster nodes
- PAT pool of size at least equal to the number of members in the cluster



PAT POOL: 209.165.201.1 – 209.165.201.2

Cluster Dynamic PAT Operation

FTD 6.6 and Earlier / ASA 9.14 and Earlier



					Original Packet			Translated Packet				
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
> NAT Rules Before												
∨ Auto NAT Rules												
#		Dynamic	Inside	Outside	Inside-Network			Mapped-IPGroup			Dns:false	
> NAT Rules After												

FTD CLI

```
> show running-config nat
!
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool Mapped-IPGroup
```

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-2-1
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-2-1, backup unit-1-1
```

When a unit leaves the cluster

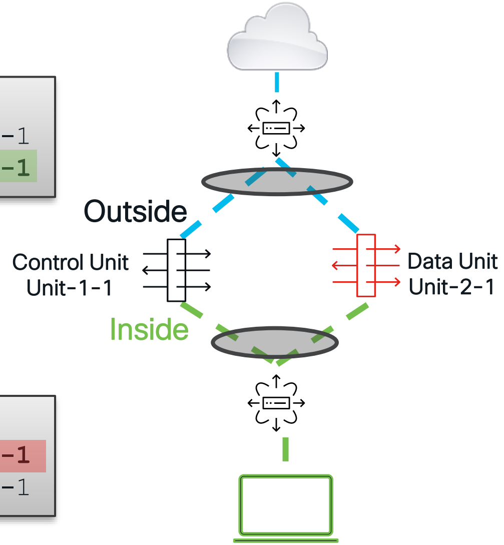
FTD 6.6 and Earlier / ASA 9.14 and Earlier

- The PAT IP assigned to that unit will be rebalanced to another unit in the cluster

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-2-1
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-2-1, backup unit-1-1
```

Unit-2-1 leaves the cluster:

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-1-1, backup unit-1-1
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-1-1
```



When a unit joins the cluster

FTD 6.6 and Earlier / ASA 9.14 and Earlier

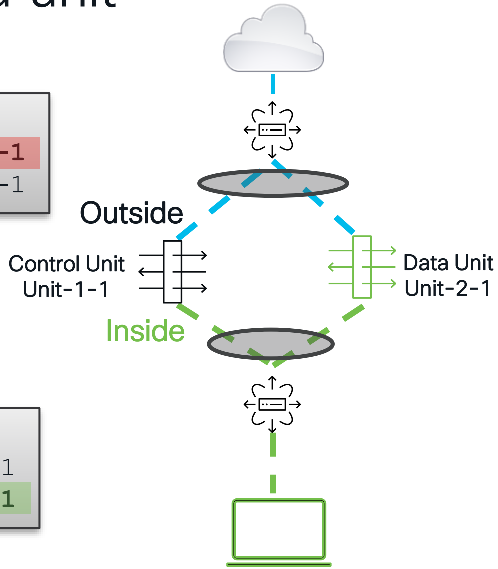
- The Control unit attempts to find one or more unused PAT IPs from the PAT pool and assign it to the newly joined unit

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-1-1, backup unit-1-1
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-1-1
```

Unit-2-1 re-joins the cluster

PAT IP Addresses are rebalanced:

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-2-1
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-2-1, backup unit-1-1
```



Cluster Dynamic PAT Limitations

FTD 6.6 and Earlier / ASA 9.14 and Earlier

1. Cluster PAT pool size

   PAT pool of size at least equal to the number of nodes in the cluster

2. PAT Pool redistribution

   PAT pool distribution becomes imbalanced as nodes leave/join the cluster

3. Lack of IP stickiness

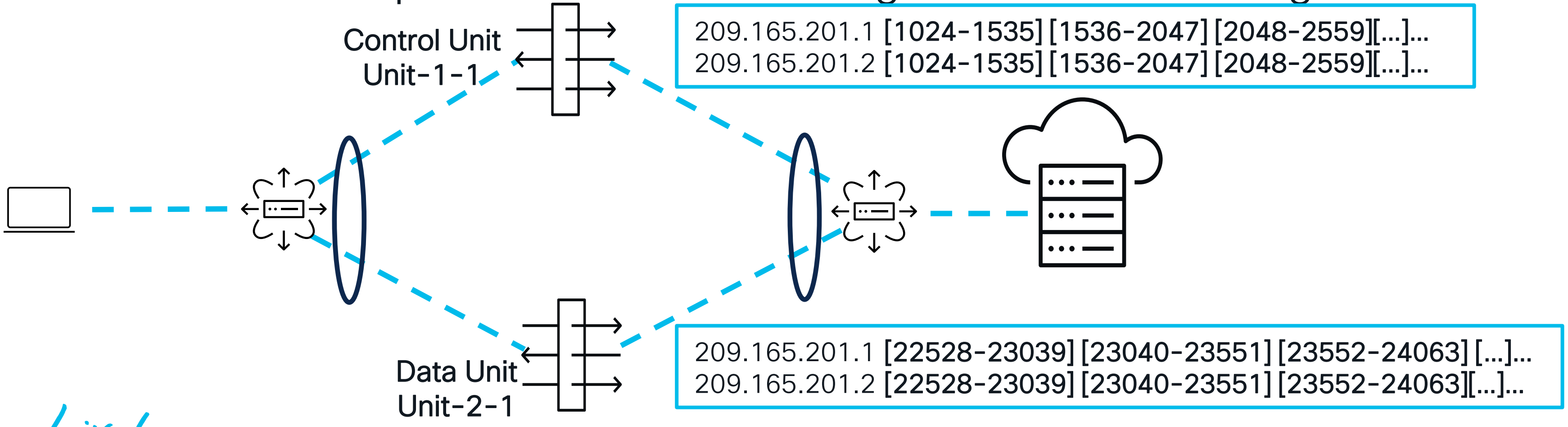
   Multi-session applications are affected due to a lack of cluster-wide IP stickiness

From ASA 9.15.1
From FTD 6.7

Cluster Dynamic PAT Operation

FROM ASA 9.15.1 / FTD 6.7

- Port Block-Based pool distribution
  - Port Block size = 512 ports by default
- PAT functionality with “flat” as the default behavior
  - ‘include-reserve’ option will extend this range to 1-65535 for regular PAT



Control Unit
Unit-1-1

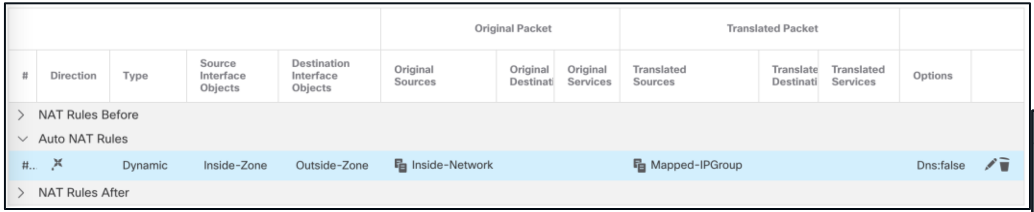
209.165.201.1 [1024-1535] [1536-2047] [2048-2559][...]...
209.165.201.2 [1024-1535] [1536-2047] [2048-2559][...]...

Data Unit
Unit-2-1

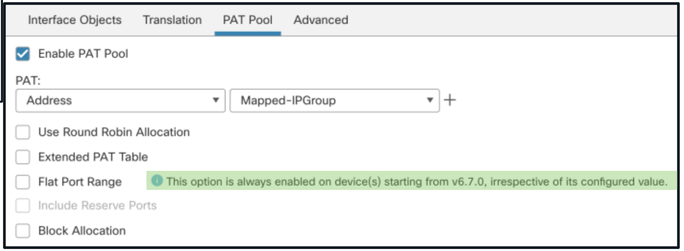
209.165.201.1 [22528-23039] [23040-23551] [23552-24063] [...]...
209.165.201.2 [22528-23039] [23040-23551] [23552-24063][...]...

Cluster Dynamic PAT Operation

FROM ASA 9.15.1 / FTD 6.7



					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinati	Original Services	Translated Sources	Translate Destinati	Translated Services	Options
> NAT Rules Before											
∨ Auto NAT Rules											
#..	⤨	Dynamic	Inside-Zone	Outside-Zone	Inside-Network			Mapped-IPGroup			Dns:false
> NAT Rules After											



Interface Objects | Translation | PAT Pool | Advanced

☑ Enable PAT Pool

PAT:

Address ▾ | Mapped-IPGroup ▾ +

□ Use Round Robin Allocation

□ Extended PAT Table

□ Flat Port Range — ⓘ This option is always enabled on device(s) starting from v6.7.0, irrespective of its configured value.

□ Include Reserve Ports

□ Block Allocation

FTD CLI

```
> show running-config nat
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool Mapped-
IPGroup
```

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.1
   [1024-1535], owner unit-1-1, backup unit-2-1
   [1536-2047], owner unit-1-1, backup unit-2-1
   [2048-2559], owner unit-1-1, backup unit-2-1
                            […]
   [22528-23039], owner unit-2-1, backup unit-1-1
   [23040-23551], owner unit-2-1, backup unit-1-1
   [23552-24063], owner unit-2-1, backup unit-1-1
```

IP Stickiness

FROM ASA 9.15.1 / FTD 6.7

- Predictable IP Stickiness Algorithm
  - Each node will use an algorithm to select the Sticky PAT IP
- In case selected sticky PAT IP is exhausted, the next available PAT IP in the pool
  - Stickiness syslog will be generated

Cluster Dynamic PAT Enhancements Summary

ASA 9.14 and Earlier/ FTD 6.6 and Earlier

FROM ASA 9.15.1/ FTD 6.7.+

PAT Pool size at least equal to the number of nodes

IP Based distribution

→

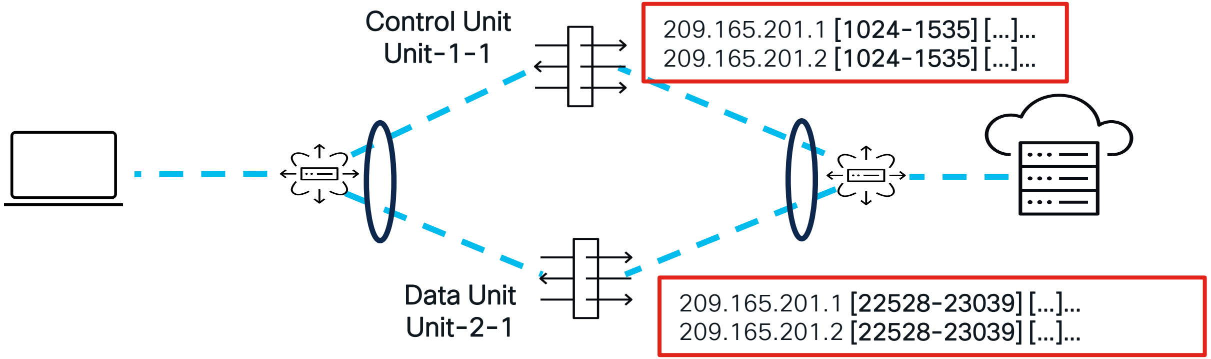
Ability to work with a single IP

Port Block Based distribution

Lack of IP Stickiness

→

Cluster-Wide IP Stickiness



Control Unit
Unit-1-1

209.165.201.1 [1024-1535] [...]...
209.165.201.2 [1024-1535] [...]...

Data Unit
Unit-2-1

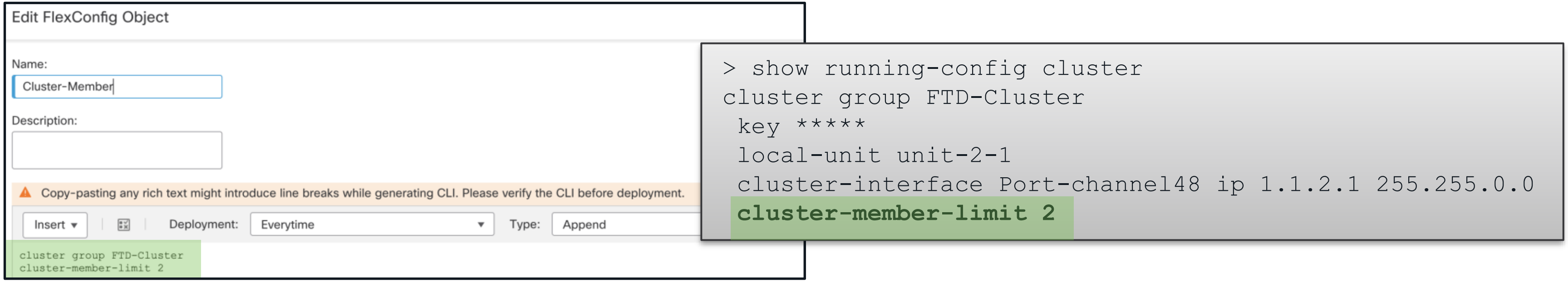
209.165.201.1 [22528-23039] [...]...
209.165.201.2 [22528-23039] [...]...

From ASA 9.16.1
From FTD 7.0

Cluster Member Limit

FROM ASA 9.16 / FTD 7.0

- Used to configure the maximum number of cluster members.
  - Cluster Member Limit by default = 16
  - When the Current Cluster Members = Cluster Member Limit, then the Cluster is marked as Full



Edit FlexConfig Object

Name: Cluster-Member

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Everytime

Type: Append

```
cluster group FTD-Cluster
cluster-member-limit 2
```

```
> show running-config cluster
cluster group FTD-Cluster
 key *****
 local-unit unit-2-1
 cluster-interface Port-channel48 ip 1.1.2.1 255.255.0.0
 cluster-member-limit 2
```

Port Blocks Reservation

FROM ASA 9.16 / FTD 7.0

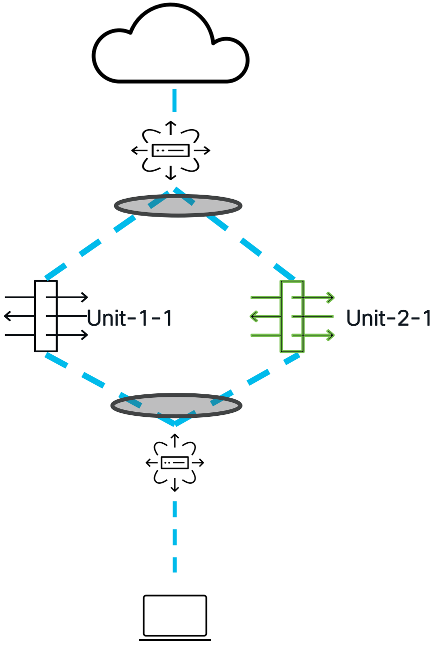
- If there are N units in the cluster, Control unit reserves port blocks for (N+1) nodes until the cluster is full

- On a cluster that is just being brought up, the Control unit will initially own 50% and the rest will be reserved
  - The number of port blocks owned per unit will get adjusted as nodes join the cluster
  - When the cluster is Full, all the port blocks are distributed across cluster members

Port Blocks Reservation

Examples

- Cluster Member Limit by default



```
> show running-config nat
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool Mapped-IPGroup
```

Available ports for a single IP
65535-1023 = 64512

Total port blocks per IP:
64512/512 = 126

Reserved port block:
126/2 = 63

```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 209.165.201.1 (126 - 63) ^ 63 # 0
IP Outside:Mapped-IPGroup 209.165.201.2 (126 - 63) ^ 63 # 0
```

Unit-2-1 joins the cluster

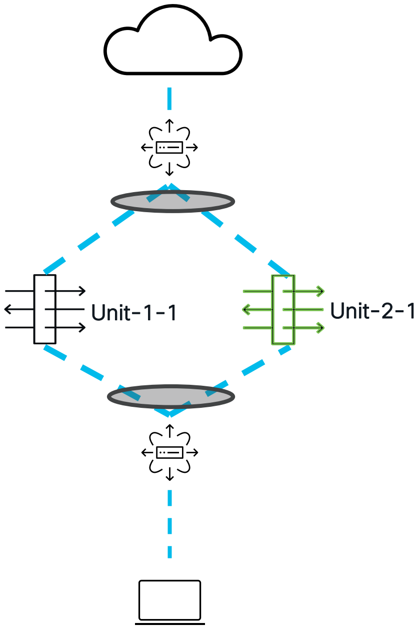
```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 209.165.201.1 (126 - 42 / 42) ^ 42 # 0
IP Outside:Mapped-IPGroup 209.165.201.2 (126 - 42 / 42) ^ 42 # 0
```

Port Blocks Reservation

Examples

- Cluster Member Limit = 2

```
> show running-config nat
object network Inside-Network
 nat (Inside,Outside) dynamic pat-pool Mapped-IPGroup
```



Available ports for a single IP
65535-1023 = 64512

Total port blocks per IP:
64512/512 = 126

Reserved port block:
126/2 = 63

```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 209.165.201.1 (126 - 63) ^ 63 # 0
IP Outside:Mapped-IPGroup 209.165.201.2 (126 - 63) ^ 63 # 0
```

Unit-2-1 joins the cluster

```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 209.165.201.1 (126 - 63 / 63) ^ 0 # 0
IP Outside:Mapped-IPGroup 209.165.201.2 (126 - 63 / 63) ^ 0 # 0
```

Port Blocks Reclamation

FROM ASA 9.16.1 / FTD 7.0

- When a unit is joining or leaving, reclamation of Port Blocks is initiated in each unit
  - Excess port blocks from all units must be released to the control unit
  - New connections are not allowed on reclaimed port blocks. They are released to the control unit when the last port is cleared

```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 209.165.201.1 (126 - 80 / 46) ^ 0 # 17
IP Outside:Mapped-IPGroup 209.165.201.2 (126 - 63 / 63) ^ 0 # 0
```

```
> show nat pool ip 209.165.201.1 detail
TCP PAT pool Outside, address 209.165.201.1
        range 1024-1535, allocated 512 #
```

Cluster Dynamic PAT Enhancements Summary

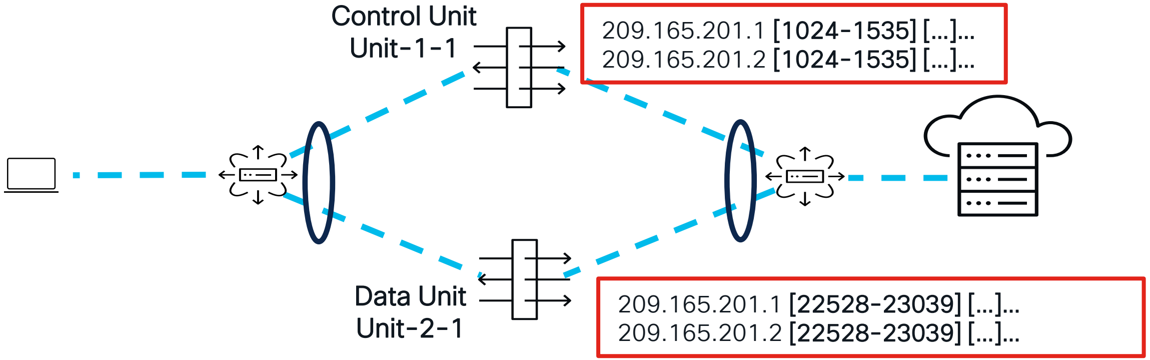
ASA 9.14 and Earlier/
FTD 6.6 and Earlier

FROM ASA 9.16.1/
FTD 7.0

PAT Pool distribution could become imbalanced. →

Improved PAT IP Address port-block redistribution:

- Cluster-member-limit
- Port Blocks Reservation
- Port Blocks Reclamation



209.165.201.1 [1024-1535] [...]...
209.165.201.2 [1024-1535] [...]...

209.165.201.1 [22528-23039] [...]...
209.165.201.2 [22528-23039] [...]...

Troubleshooting Walkthroughs

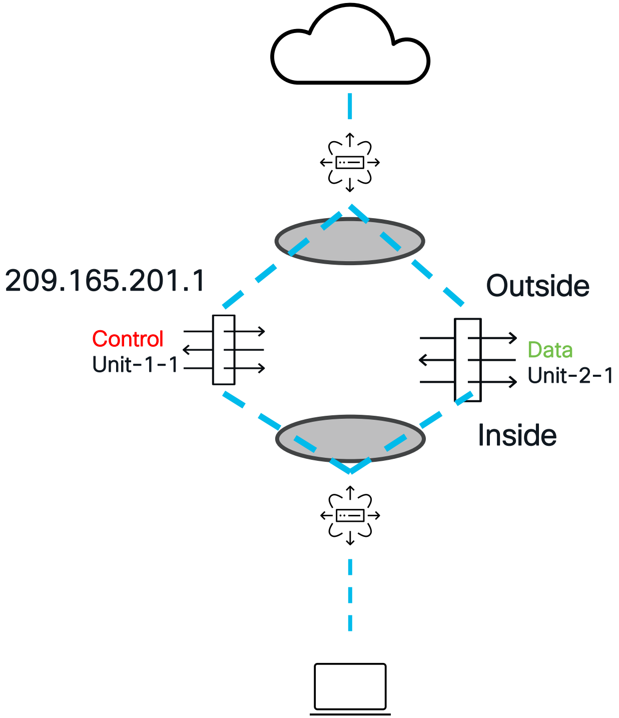
Scenario 1: PAT pool configured with a single IP

FTD 6.6 and Earlier / ASA 9.14 and Earlier

- The IP is assigned to the Control Unit and the Data units have none available

- All traffic subjected to PAT in the Data unit is forwarded over the CCL to the Control node for processing

- This may result in CCL congestion and high conn/xlate load on the Control unit which may limit cluster throughput



Scenario 1: PAT Configured with a single IP

FTD 6.6 and Earlier / ASA 9.14 and Earlier

1. Syn goes trough the Control Unit

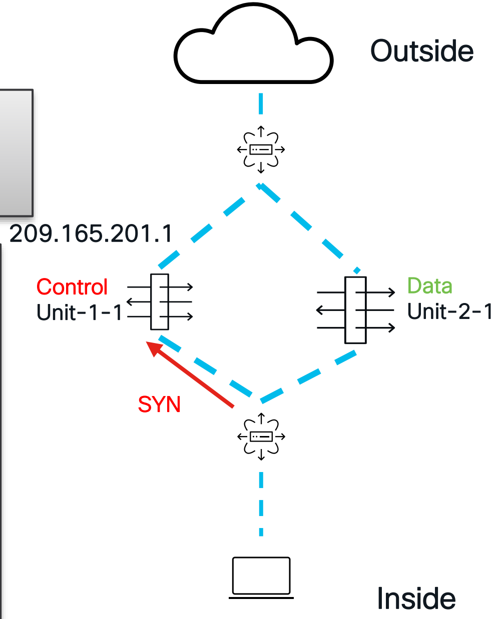
```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-2-1
```

```
firepower# show xlate

TCP PAT from Inside:192.168.10.10/37564 to Outside:209.165.201.1/37564 flags ri idle 0:00:04 timeout
0:00:30
```

SYN Capture Trace from Control Unit

```
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (0) am becoming owner
```



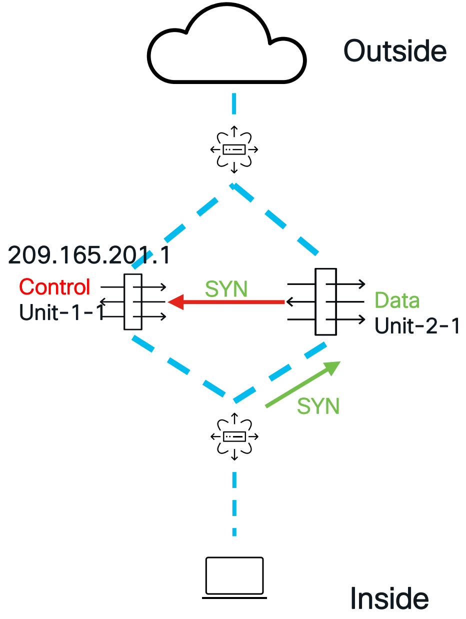
Scenario 1: PAT Configured with a single IP

FTD 6.6 and Earlier / ASA 9.14 and Earlier

2. Syn goes through the Data Unit

```
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (1) got initial, attempting ownership.
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
I (1) am becoming owner
```

```
Phase: 10
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'Inside'
Flow type: NO FLOW
NAT: I (1) am redirecting packet to
master (0) for PAT.
```



MITIGATION
Ensure you have a PAT pool size equal to the number of nodes in the cluster

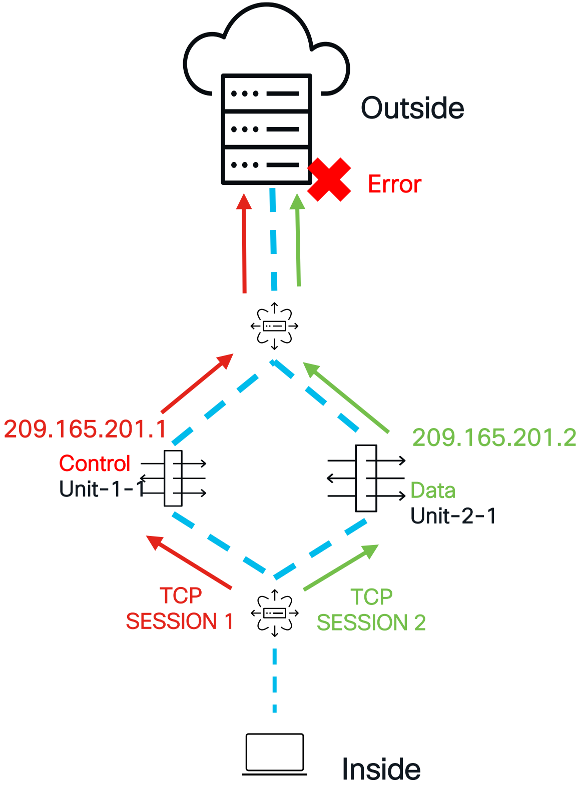
Scenario 2: Distributed PAT Xlates in Cluster for Multisession connections

FTD 6.6 and Earlier / ASA 9.14 and Earlier

- Multisession connections could be load-balanced across different cluster members
  - If this traffic is subjected to PAT, then each FTD translates each connection using its own PAT IP address

MITIGATION 1 (FTD 6.6 and earlier):

1. Configuring Static NAT for specific destination IP addresses.

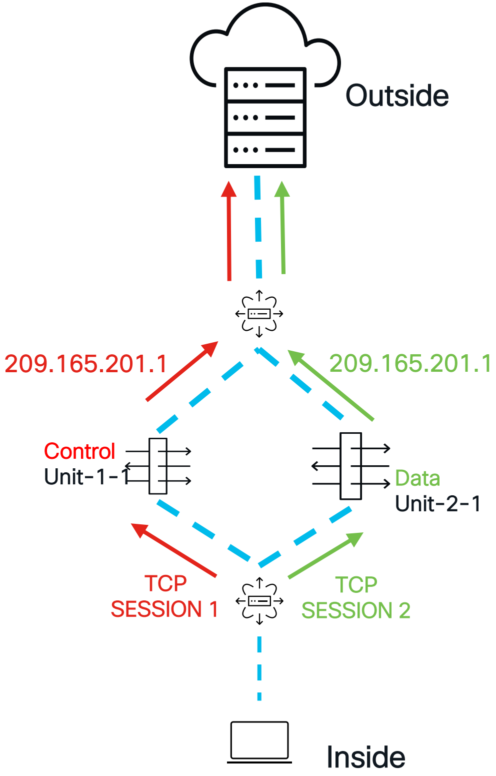


Scenario 2: Distributed PAT Xlates in Cluster for Multisession connections

FROM ASA 9.15.1 / FTD 6.7

MITIGATION 2 (From FTD 6.7.+):

FTD 6.7.+ supports IP Stickiness



Scenario 3: PAT IP allocation becomes imbalanced

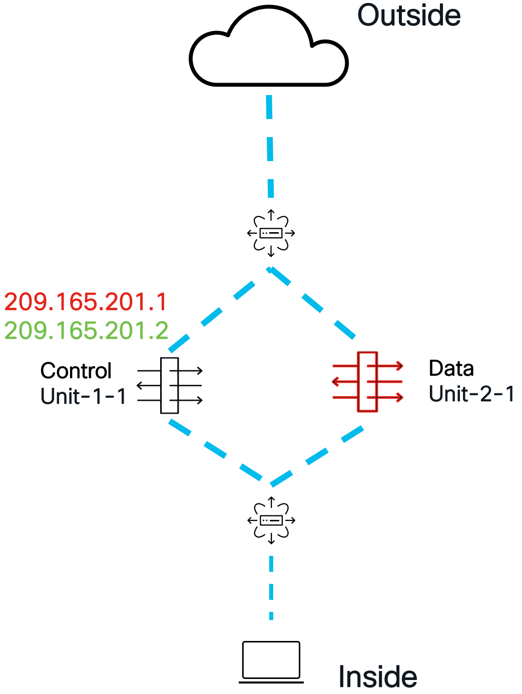
FTD 6.6 and Earlier / ASA 9.14 and Earlier

- As units join and leave the cluster, PAT IP Allocation could become imbalanced.
- Initially, PAT IP addresses are evenly distributed across cluster nodes

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-2-1
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-2-1, backup unit-1-1
```

- Unit-2-1 Leaves the cluster – PAT IP is rebalanced to the backup unit

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-1-1, backup unit-1-1
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-1-1
```



Scenario 3: PAT IP allocation becomes imbalanced

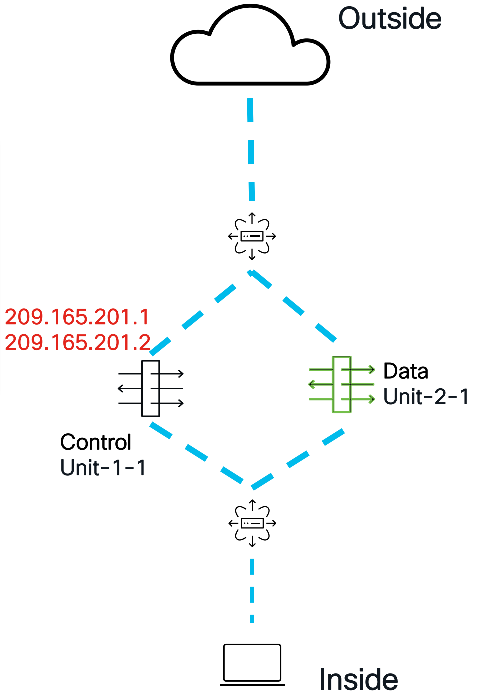
FTD 6.6 and Earlier / ASA 9.14 and Earlier

- The PAT IP 209.165.201.2 starts to be used by unit-1-1

```
> show nat pool
TCP PAT pool Outside, address 209.165.201.1, range 1-511, allocated 1
TCP PAT pool Outside, address 209.165.201.1, range 512-1023, allocated 2
TCP PAT pool Outside, address 209.165.201.1, range 1024-65535, allocated 12312
TCP PAT pool Outside, address 209.165.201.2, range 1-511, allocated 3
TCP PAT pool Outside, address 209.165.201.2, range 512-1023, allocated 10
TCP PAT pool Outside, address 209.165.201.2, range 1024-65535, allocated 453
```

- Unit-2-1 returns to the cluster but does not get a PAT IP address assigned

```
> show nat pool cluster
IP Outside:Mapped-IPGroup 209.165.201.2, owner unit-1-1, backup unit-2-1
IP Outside:Mapped-IPGroup 209.165.201.1, owner unit-1-1, backup unit-2-1
```



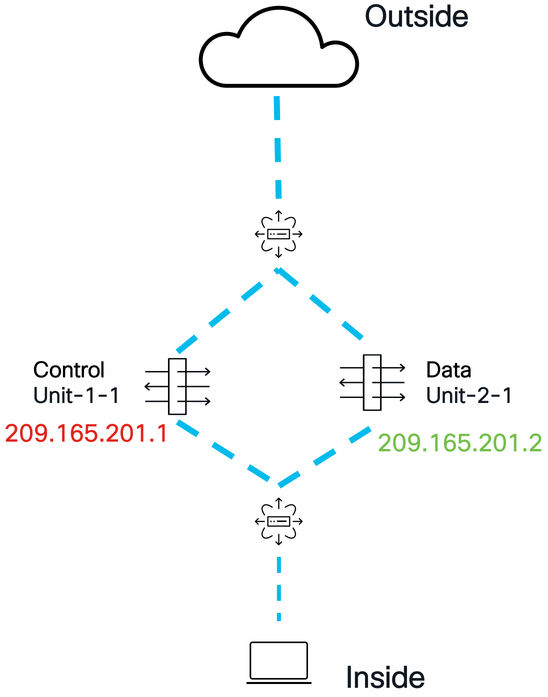
Scenario 3: PAT IP allocation becomes imbalanced

FTD 6.6 and Earlier / ASA 9.14 and Earlier

MITIGATIONS:

1. Add More IP Addresses to the PAT Pool
2. Manually clear xlates for one of the addresses in the pool

```
Clear xlate global x.x.x.x
```



Demo Section

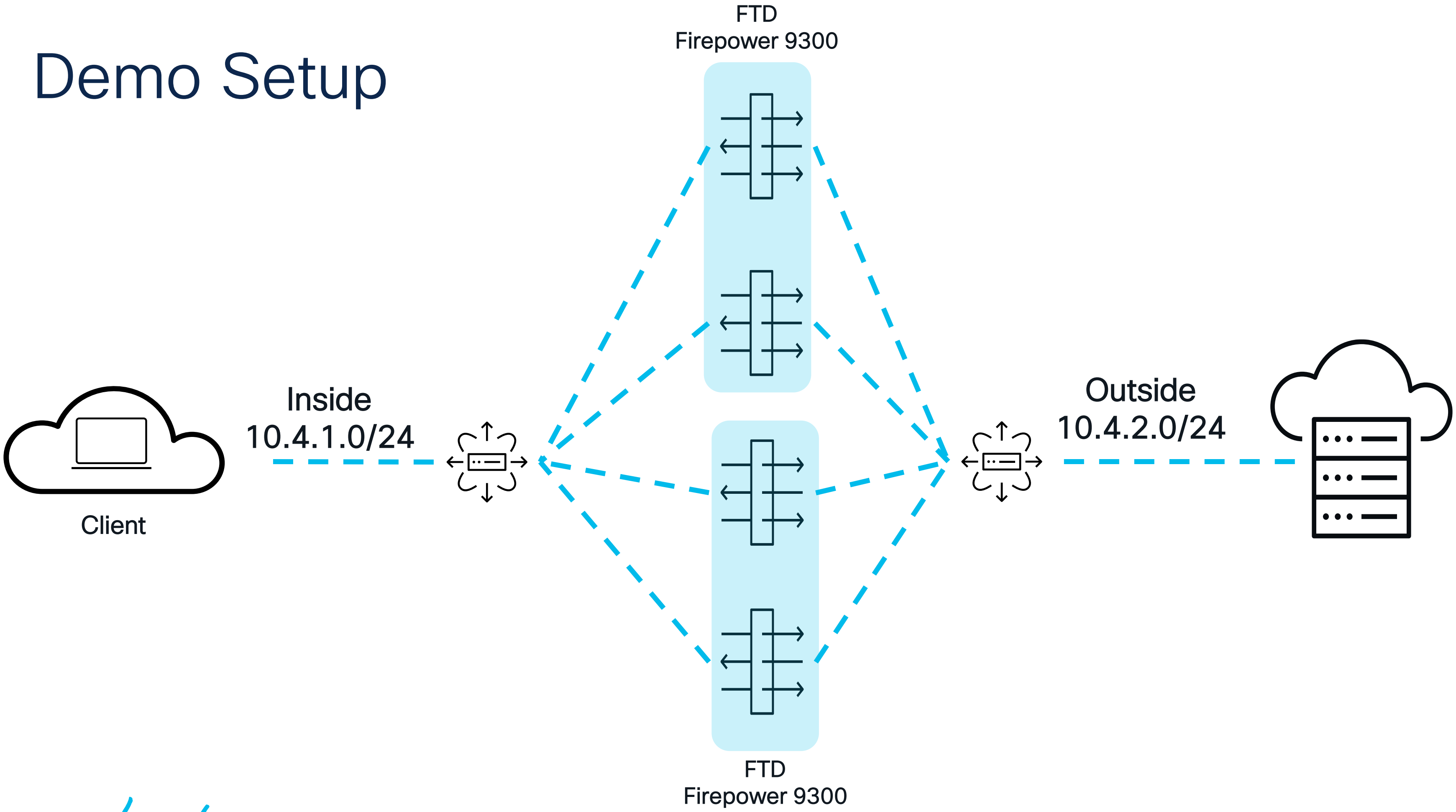
Demo 1

In this Demo, we will...

SHOW GENERAL CLUSTER CONFIGURATION

SHOW THE TROUBLESHOOTING COMMANDS

Demo Setup


FTD
Firepower 9300
Inside
10.4.1.0/24
Client
Outside
10.4.2.0/24
FTD
Firepower 9300

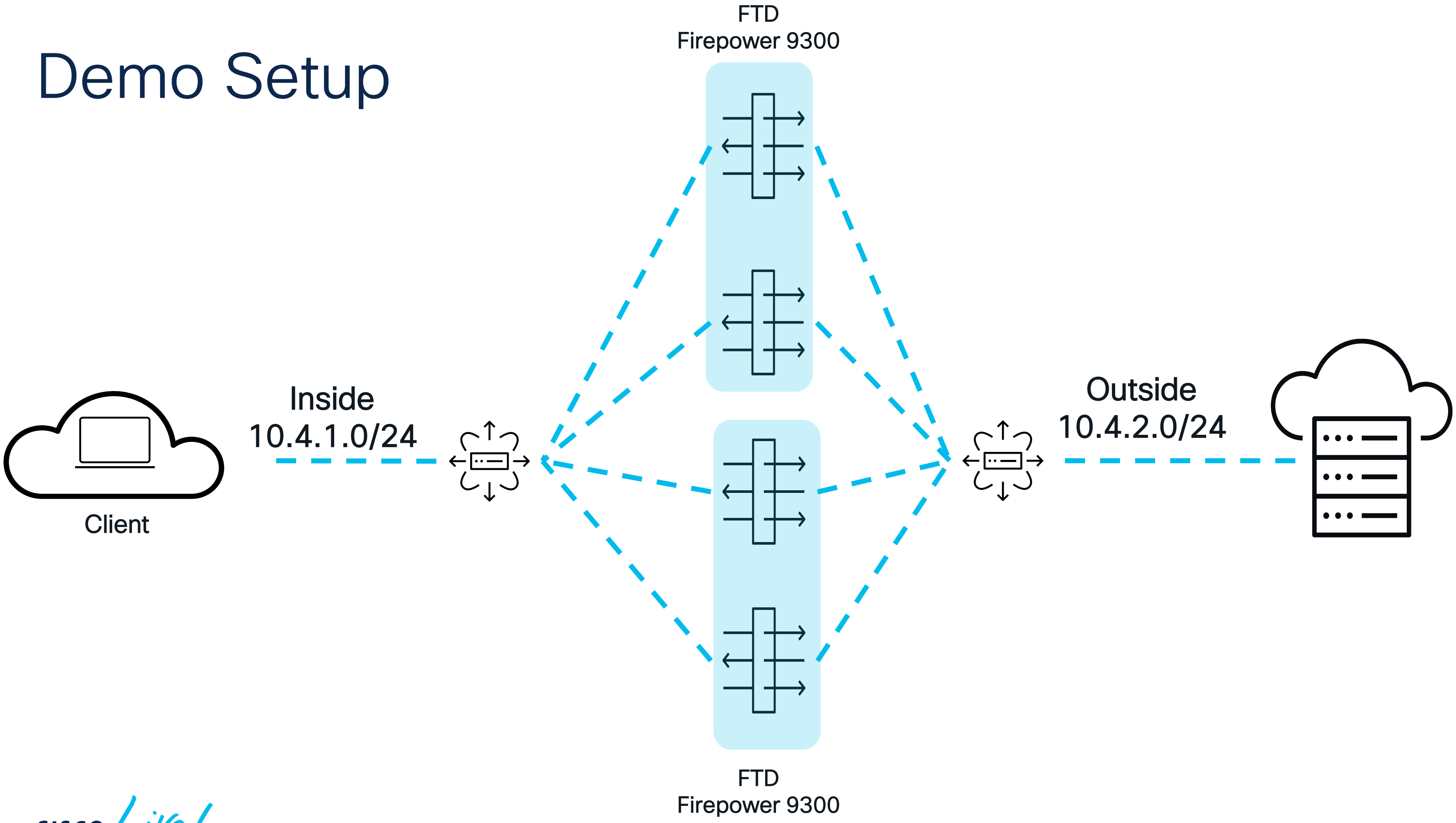
Demo 2

In this Demo, we will...

Demonstrate how IP Stickiness works, based on below traffic profile:

- Multiple TCP connections from a single host
- Multiple TCP Connections from multiple hosts
- Multiple UDP connections from a single host

Demo Setup


FTD
Firepower 9300
Inside
10.4.1.0/24
Client
Outside
10.4.2.0/24
FTD
Firepower 9300

Conclusion

Conclusion

Cluster Dynamic PAT Limitations in FTD 6.6 and Earlier/ASA 9.14 and earlier

- PAT pool of size at least equal to the number of nodes in the cluster
- PAT Pool distribution could become imbalanced
- Lack of IP Stickiness

Dynamic PAT Enhancements in Cluster From FTD 6.7 / ASA 9.15:

- Enhanced PAT Pool distribution across cluster nodes
- Cluster Wide IP Stickiness

Port-block Distribution Enhancements in Cluster From FTD 7.0 / ASA 9.16:

- Cluster Member Limit
- Port blocks Reservation
- Port blocks Reclamation

By understanding how Dynamic PAT works in Secure Firewall Cluster, network performance degradation can be avoided.

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

#CiscoLive

cisco Live!

Let’s go

#CiscoLive

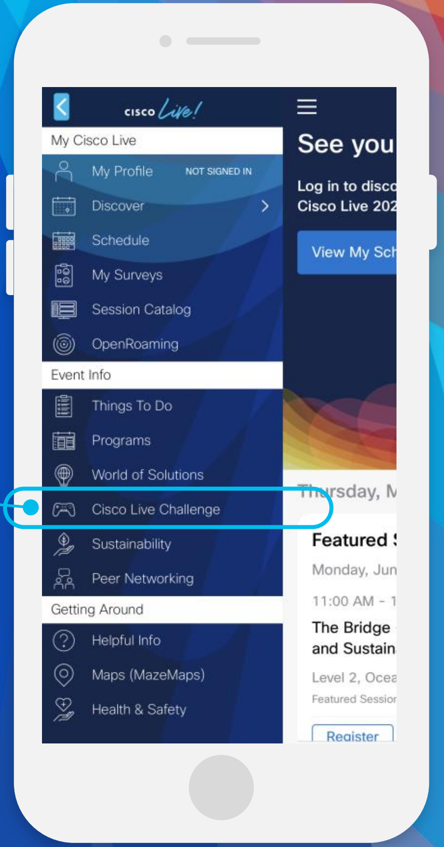
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!