Cisco Support Community Expert Series Webcast:

Troubleshooting Adaptive Security Appliances (ASA), Private Internet Exchange (PIX), and Firewall Service Modules (FWSM)

Kureli Sankar
Customer Support Engineer

January 15, 2013

Cisco Support Community – Expert Series Webcast

- Today's featured expert is Cisco Support Engineer **Kureli Sankar**
- Ask Her questions now Firewalls

Kureli Sankar

Customer Support Engineer

CCIE

Topic: Troubleshooting Adaptive Security Appliances (ASA), Private Internet Exchange (PIX), and Firewall Service Modules (FWSM)

Event Date: January 15th, 2013

Panel of Experts

ElMehdi Babzine
CSE. CCIE

Michael Robertson
CSE, CCIE

Aniket Rodrigues
CSE, CCIE

Thank You for Joining Us Today

Today's presentation will include audience polling questions

We encourage you to participate!

Thank You for Joining Us Today

If you would like a copy of the presentation slides, click the PDF link in the chat box on the right or go to

https://supportforums.cisco.com/community/netpro/security/firewall

Or, https://supportforums.cisco.com/docs/DOC-29170

Thank You for Joining Us Today

Everyone who joins today's webcast will receive:

125 Cisco Preferred Access Points!

Polling Question 1

What is the most common issue that you have encountered in your firewall in last few months?

a) Basic Configuration Issue

b) Latency Issues

c) Translation issues

d) Failover problems

e) Other

Submit Your Questions Now!

Use the Q&A panel to submit your questions. Experts will start responding those

Cisco Support Community Expert Series Webcast:

Troubleshooting Adaptive Security Appliances (ASA), Private Internet Exchange (PIX), and Firewall Service Modules (FWSM)

Kureli Sankar

1/15/13

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency Issue
- Translation problem - multiple devices are in the path
- Firewall does not build any connection through the box
- IPS - Global Correlation signature update problem
- Using the main interface for sending data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

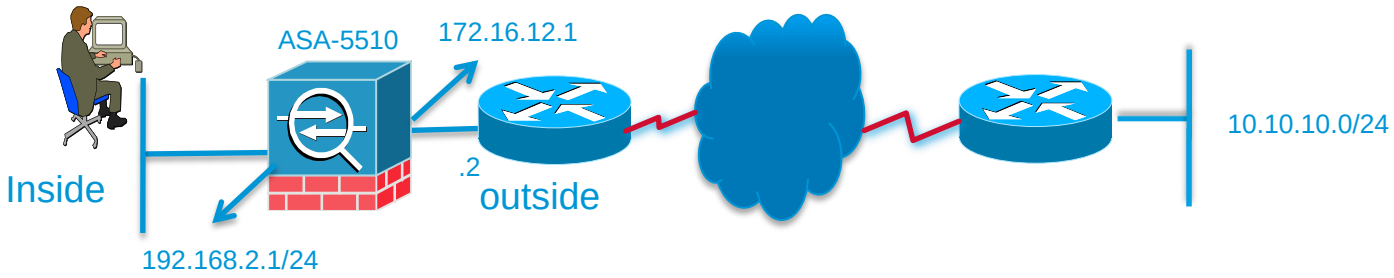
What is NAT

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network.

Why do we configure NAT? Why not no nat for all communication?

If we have plenty of addresses available that are routable we could do that. Routable IPv4 address space is limited so we need to use NAT/PAT to be able to route traffic out to the internet.
Another reason is that the destination network may not be able route the address unless it belongs to their network scheme.

Nat 0 with ACL or Nat exemption



Pre 8.3 Syntax

ASA(config)#access-list no-nat permit ip 192.168.2.0 255.255.255.0 10.10.10.0 255.255.255.0
ASA(config)#nat (inside) 0 access-list no-nat

8.3 + Syntax

ASA(config)# object network obj_source-net
ASA(config-network-object)# subnet 192.168.2.0 255.255.255.0
ASA(config)# object network obj_destination-net
ASA(config-network-object)# subnet 10.10.10.0 255.255.255.0
ASA-5505(config)# nat (inside,outside) source static obj_source-net obj_source-net
destination static obj_destination-net
obj_destination-net

Nat 0 with ACL or Nat exemption

- nat (inside,outside) source static obj_source-net obj_source-net
  destination static obj_destination-net obj_destination-net

Why do we repeat the address or object twice?

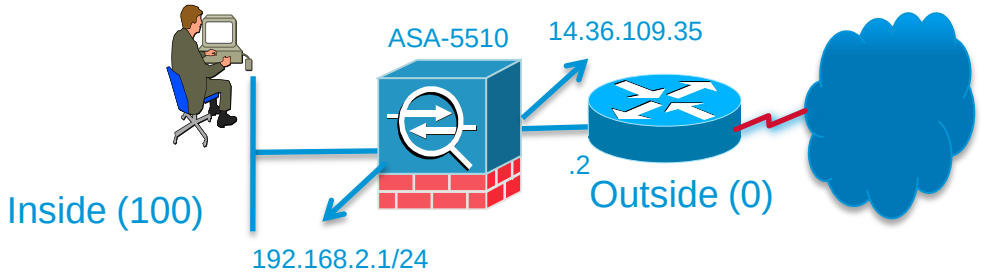
What is the object referring the source address on the inside?
It is obj_source-net

What is the object referring the source address on the outside?
It is obj_source-net

What is the object referring the destination address on the inside?
It is obj_destination-net

What is the destination address on the outside?
It is obj_destination-net

Dynamic PAT



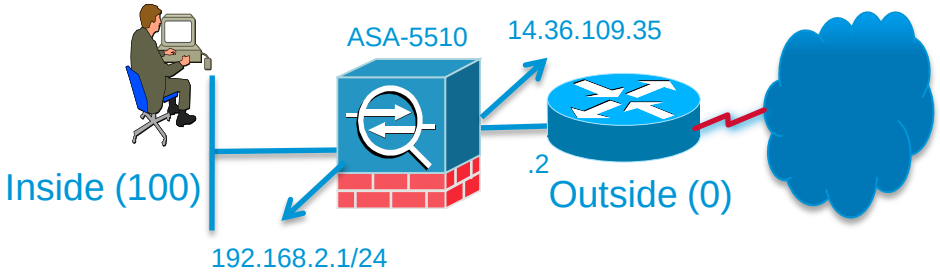
Pre 8.3 Syntax

ASA(config)#nat (inside) **1** 192.168.2.0 255.255.255.0
ASA(config)#global (outside) **1** interface

8.3 + Syntax

ASA(config)# object network obj_192.168.2.0
ASA(config-network-object)# subnet 192.168.2.0 255.255.255.0
ASA(config-network-object)# nat (inside,outside) dynamic interface

Dynamic NAT



Configure dynamic NAT such that when 192.168.2.0/24 go out to the internet they will all look like 14.36.110.0/24

Pre 8.3 Syntax

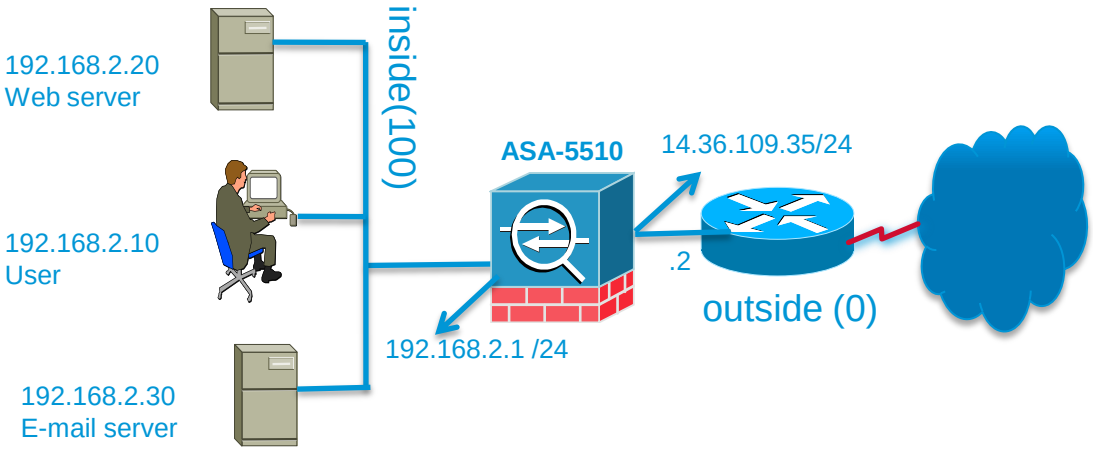
```
ASA(config)#nat (inside) 1 192.168.2.0 255.255.255.0
ASA(config)#global (outside) 1 14.36.110.0 255.255.255.0
```

8.3 + Syntax

```
ASA (config)# object network obj-14.36.110.0
ASA(config-network-object)# subnet 14.36.110.0 255.255.255.0

ASA (config)# object network obj-192.168.2.0
ASA(config-network-object)# subnet 192.168.2.0 255.255.255.0
ASA(config-network-object)# nat (inside,outside) dynamic obj-14.36.110.0
```

Static (1-1) NAT



Configure static 1-1 NAT for inbound traffic from low to high security.

Pre 8.3 Syntax

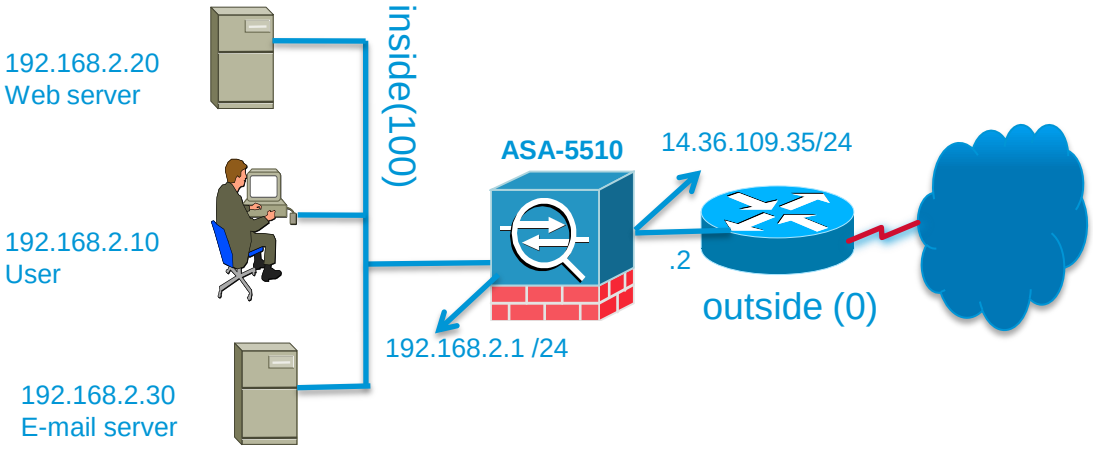
```
ASA(config)#static (inside,outside) 14.36.109.30 192.168.2.30
ASA(config)#static (inside,outside) 14.36.109.20 192.168.2.20
```

8.3 + Syntax

```
ASA(config)# object network obj-192.168.2.20
ASA(config-network-object)# host 192.168.2.20
ASA(config-network-object)# nat (inside,outside) static 14.36.109.20

ASA(config)# object network obj-192.168.2.30
ASA(config-network-object)# host 192.168.2.30
ASA(config-network-object)# nat (inside,outside) static 14.36.109.30
```

Static PAT



Configure static PAT for inbound traffic from low to high security.

Pre 8.3 Syntax

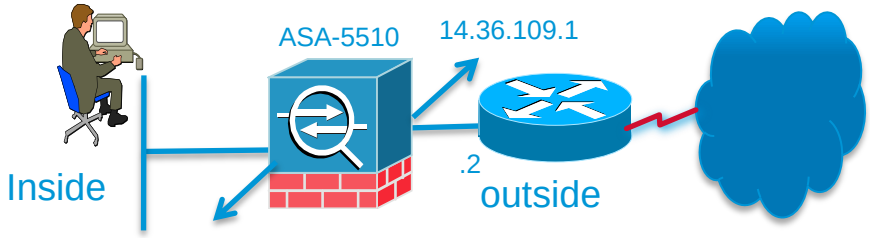
```
ASA(config)#static (inside,outside) tcp 14.36.109.36 25 192.168.2.30 25
ASA(config)#static (inside,outside) tcp interface 80 192.168.2.20 80
```

8.3 + Syntax

```
ASA(config)# object network obj-192.168.2.30
ASA(config-network-object)# host 192.168.2.30
ASA(config-network-object)# nat (inside,outside) static 14.36.109.36 service tcp 25 25

ASA(config)# object network obj-192.168.2.20
ASA(config-network-object)# host 192.168.2.20
ASA(config-network-object)# nat (inside,outside) static interface service tcp 80 80
```

Twice NAT



If user 192.168.2.2 goes out to Google 72.14.204.105 then make the user looks Like 14.36.109.2 and when Google responds back to us make Google look like 192.168.2.105

```
ASA(config)# object network obj-192.168.2.2
ASA(config-network-object)# host 192.168.2.2
ASA(config)# object network obj-192.168.2.2-mapped
ASA(config-network-object)# host 14.36.109.2

ASA(config)# object network obj-google
ASA(config-network-object)# host 72.14.204.105
ASA(config)# object network obj-google-mapped
ASA(config-network-object)# host 192.168.2.105

ASA(config)# nat (inside,outside) source static obj-192.168.2.2 obj-192.168.2.2-mapped
                                                destination static obj-google-mapped obj-
google
```

NAT Order of Operations

Pre 8.3 NAT order of operation:

http://tools.cisco.com/squish/2cc91

8.3+ NAT order of operation:
http://tools.cisco.com/squish/2A000

Useful 8.3+ NAT links

All you need to know about 8.3 upgrade:
https://supportforums.cisco.com/docs/DOC-12690

Before and after NAT config samples:
https://supportforums.cisco.com/docs/DOC-9129

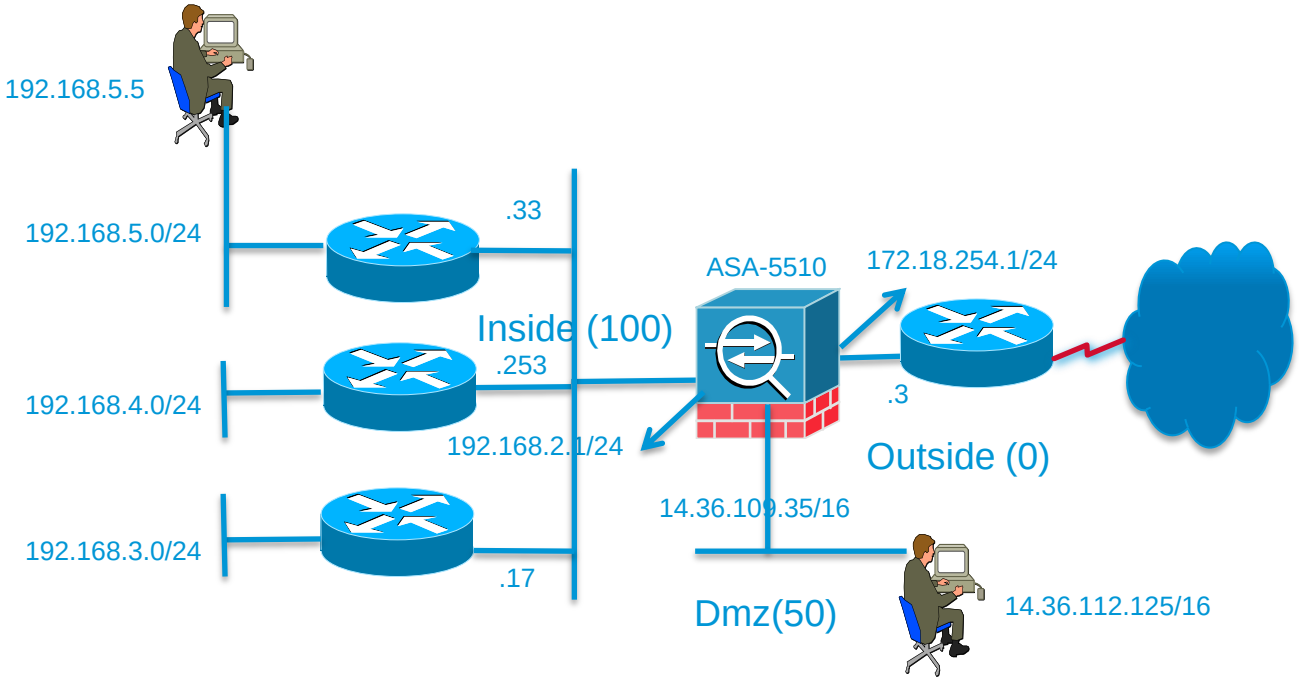
ASA 8.3 Asymmetric NAT rules matched for forward and reverse flows: https://supportforums.cisco.com/docs/DOC-12569

ASA 8.3 NAT video:
https://supportforums.cisco.com/videos/1014

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- Firewall does not build any connection through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

Case Study: 1 L-2 adjacency



Problem: Source (14.36.112.125) on the dmz was unable to reach 192.168.5.5

Relevant ASA config:

```
object network obj_192.168.5.5
 nat (inside,DMZ) static 14.36.109.7

route inside 192.168.5.0 255.255.255.0 192.168.2.33
```

Diagnosis

- Dmz captures show icmp packets arriving. They don't leave the inside interface

We sent 10,000 pings with timeout 0 from the host on the Dmz.

```
ASA#cap capdmz int Dmz match ip host 14.36.109.7 any
ASA#cap capin int inside match ip ho 192.168.5.5 any
```

```
ASA#sh cap
capture capdmz type raw-data interface Dmz [Buffer Full - 524208 bytes]
  match ip host 14.36.109.7 any
capture capin type raw-data interface inside [Capturing - 0 bytes]
  match ip host 192.168.5.5 any
```

Diagnosis

- asp drop output and captures do not show any clue

```
ASA# sh asp drop

Frame drop:
  Reverse-path verify failed (rpf-violated)                23
  Flow is denied by configured rule (acl-drop)             85
  First TCP packet not SYN (tcp-not-syn)                    4
  TCP RST/FIN out of order (tcp-rstfin-ooo)                 6
  Slowpath security checks failed (sp-security-failed)      5
  FP L2 rule drop (l2_acl)                                 84

 Last clearing: 11:43:30 EST Jan 5 2013 by cisco

 Flow drop:
 Last clearing: 11:43:30 EST Jan 5 2013 by cisco
```

Diagnosis

- Syslogs do not show any clue either. The ICMP connection is built as expected.

  ASA# sh logg | i 14.36.109.7

  Jan 05 2013 11:43:32 14.36.109.35 : %ASA-6-302020: Built inbound ICMP connection for faddr 14.36.1.206/11 gaddr 14.36.109.7/0 laddr 192.168.5.5/0

  Jan 05 2013 11:43:36 14.36.109.35 : %ASA-6-302021: Teardown ICMP connection for faddr 14.36.1.206/11 gaddr 14.36.109.7/0 laddr 192.168.5.5/0

Solution

- What could it be besides Route, Translation and Permission?
- What needs to happen in order for these ICMP request packets to leave the inside interface and head towards the host?

The ASA has to have an arp entry for the router's IP address. Let us check that.

```
route inside 192.168.5.0 255.255.255.0 192.168.2.33
```

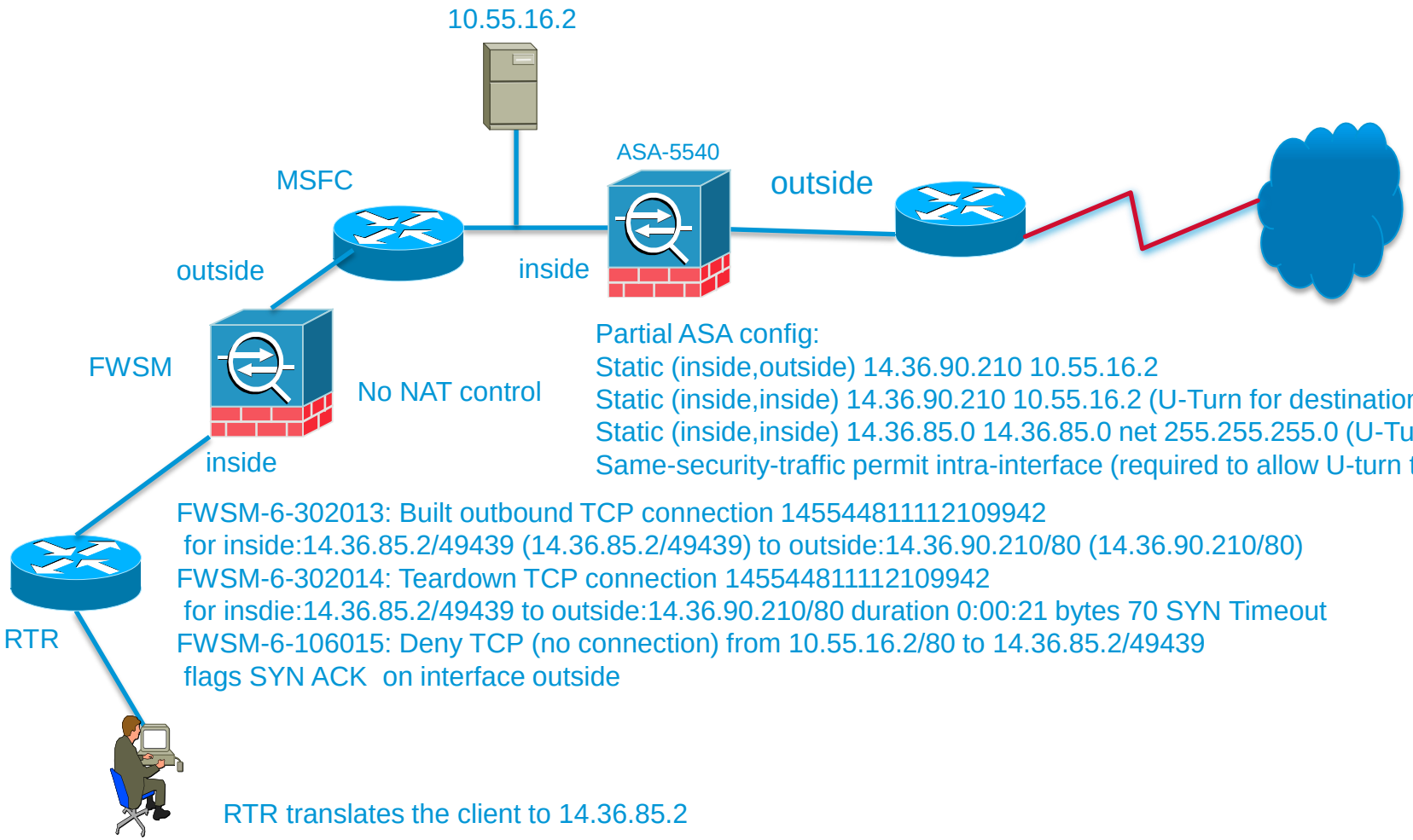
```
ASA# sh arp | i inside
        inside 192.168.2.17 0012.d949.0bf8
        inside 192.168.2.253 5057.a884.1e34
        inside 192.168.2.2 0013.d4b7.d062 891
```

No arp entry for the router in question 192.168.2.33.

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections build through the box
- IPS - Global Correlation signature update problem
- Using the main interface for sending data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

Case Study: 2 Translation problem



Partial ASA config:
Static (inside,outside) 14.36.90.210 10.55.16.2
Static (inside,inside) 14.36.90.210 10.55.16.2 (U-Turn for destination)
Static (inside,inside) 14.36.85.0 14.36.85.0 net 255.255.255.0 (U-Turn for source)
Same-security-traffic permit intra-interface (required to allow U-turn traffic)

FWSM-6-302013: Built outbound TCP connection 145544811112109942
for inside:14.36.85.2/49439 (14.36.85.2/49439) to outside:14.36.90.210/80 (14.36.90.210/80)
FWSM-6-302014: Teardown TCP connection 145544811112109942
for insdie:14.36.85.2/49439 to outside:14.36.90.210/80 duration 0:00:21 bytes 70 SYN Timeout
FWSM-6-106015: Deny TCP (no connection) from 10.55.16.2/80 to 14.36.85.2/49439
flags SYN ACK on interface outside

Problem: 172.2.201.2 is trying to reach http://xyz.cisco.com which resolves to 14.36.90.210 and the page doesn't load.

28

Solution

Removed the lines below:

static (inside,outside) 14.36.90.210 10.55.16.2
static (inside,inside) 14.36.90.210 10.55.16.2
static (inside,inside) 14.36.85.0 14.36.85.0 net 255.255.255.0
same-security-traffic permit intra-interface

Replaced the first line from above with the dns keyword:

static (inside,outside) 14.36.90.210 10.55.16.2 **dns**

Learn about DNS doctoring here:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00807968d1.shtml

Question

If the DNS request does not go through the ASA, how could we solve the problem?

Solution

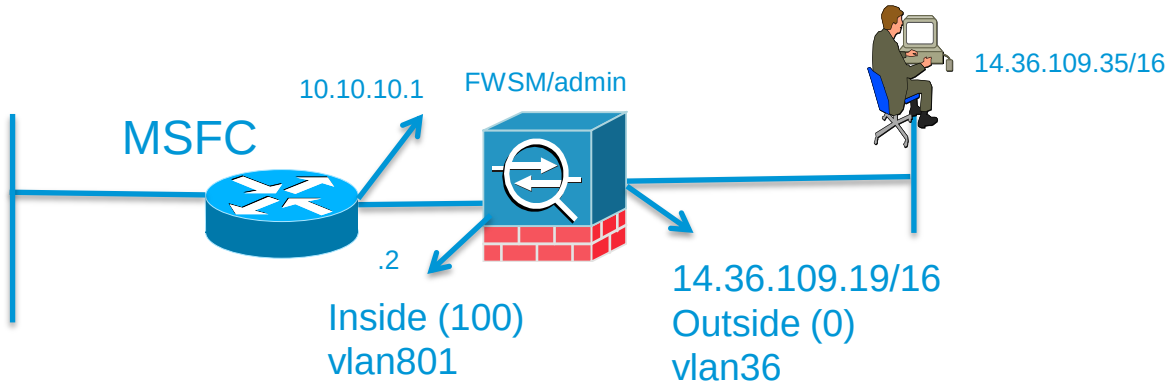
If the DNS name resolution traffic does not traverse the ASA, then we could configure D-NAT on the FWSM so, the initial SYN out of the FWSM will be sent to the 10.55.16.2 address and not the 14.36.90.210 address.

On the FWSM configure:
static (outside,inside) 14.36.90.210 10.55.16.2

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections built through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New Feature

Case Study: 3 No new connections built



Problem: No connections are built through the FWSM. Unable to ping from the SVI (Switch Virtual Interface) to the directly connected host on the outside.

Source IP: 10.10.10.1 / Source VLAN - 801
Destination IP: 14.36.109.35 / Destination VLAN - 36

Diagnosis

- Verified basic Route, Translation and Permission. MSFC had a route configured for the 14.36.109.0/24 network via the admin context inside interface address 10.10.10.2

```
SW-6509#sh run | i ip route
ip route 14.36.109.0 255.255.255.0 10.10.10.2
```

- sh logg | i 10.10.10.2 shows no output at all
- Configured an access-list and captures on the ingress and egress interface. We see packets ingress but not egress.

```
access-list tac extended permit ip host 10.10.10.1 host 14.36.109.35
access-list tac extended permit ip host 14.36.109.35 host 10.10.10.1

cap capin interface inside access-list tac
cap capout interface outside access-list tac

fwsm/admin/pri/act# sh cap
capture capin type raw-data access-list tac interface inside[Capturing - 168 bytes]
capture capout type raw-data access-list tac interface outside[Capturing - 0 bytes]
fwsm/admin/pri/act# sh cap capin
2 packets seen, 2 packets captured
  1: 00:07:32.1528865544 802.1Q vlan#801 P0 10.10.10.1 > 14.36.109.35: icmp: echo request
  2: 00:07:34.1528867534 802.1Q vlan#801 P0 10.10.10.1 > 14.36.109.35: icmp: echo request
```

Diagnosis

- Though configured, there are no existing x-lates on the box and no new ones are getting built either.

```
fwsm/admin/pri/act# sh run nat
nat (inside) 10 0.0.0.0 0.0.0.0
fwsm/admin/pri/act# sh run global
global (outside) 10 14.36.201.1-14.36.201.10 netmask 255.255.255.0

fwsm/admin/pri/act# sh xlate
0 in use, 1 most used
```

- The unit has already been reloaded.
- Issue “clear np all stats” and then send 10,000 pings from the source to the destination with a timeout of “0” and watch which counter increments in the “sh np all stats | e : 0” You will notice “Deny Conns (Conn State): 10300” increment.

What could it be? FWSM receives the packets and simply does not process them. Denies to build connections. WHY?

Solution

Pay close attention to the “show log” output below:

```
fwsm/admin/pri/act# sh logg
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Name logging: enabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: level debugging, 7897 messages logged
    Buffer logging: level debugging, 11850 messages logged
    Trap logging: level debugging, facility 20, 76 messages logged
        Logging to inside 10.10.10.3 tcp/9999 disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

TCP logging is configured. It also shows that it is disabled meaning the syslog server is not listening on 9999. It may be reachable via ICMP but it surely is not listening on tcp port 9999.

Solution

So what if the syslog server is not reachable?

If the syslog server is udp (best effort) port 514 based then no problem.
If the syslog server cannot be reached on the tcp port 9999 configured then, no new connections will be built through the firewall.

This rule applies to PIX, ASA as well as FWSM.
To mitigate this issue "**logging permit-hostdown**" command must be added.

Read command reference:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm41/command/reference/l2.html#wp1655679

By default, if you have enabled logging to a syslog server that uses a TCP connection, the FWSM does not allow new network access sessions when the syslog server is unavailable for any reason.

http://tools.cisco.com/Support/BugToolKit/
you can go to the above link login with your CCO ID and then key in this defect ID CSCsm58090

CSCsm58090 details (not resolved yet)

When a FWSM is configured to send Syslogs to a syslog server over the TCP protocol, if that TCP connection fails all traffic through the firewall will be dropped (this is by design). When this condition is encountered, it is very hard to tell that the cause of the traffic failure is due to the TCP syslog server being unreachable. Currently the only way to determine that this is the cause of the traffic failures is to check one of the following:

- Observe the following counter incrementing from the output of 'show np 3 stats'
- Deny Conns (Conn State): 156107
- See that the syslog destination is marked 'disabled' as in the following output of 'show log':

When this situation is encountered, the FWSM should make it very obvious to any user logged into the firewall that new connections are being denied because the TCP syslog server is unreachable. The firewall should send logs to the local buffer indicating this, as well as send a notification to any logged in administrator.

Polling Question 2

Which firewall device(s) do you have installed in your network?

a) Cisco PIX 500 Series Security Appliances

b) Cisco ASA 5500 Series Adaptive Security Appliance

c) Cisco Catalyst 6500 Series Firewall Services Module

d) IOS Firewall

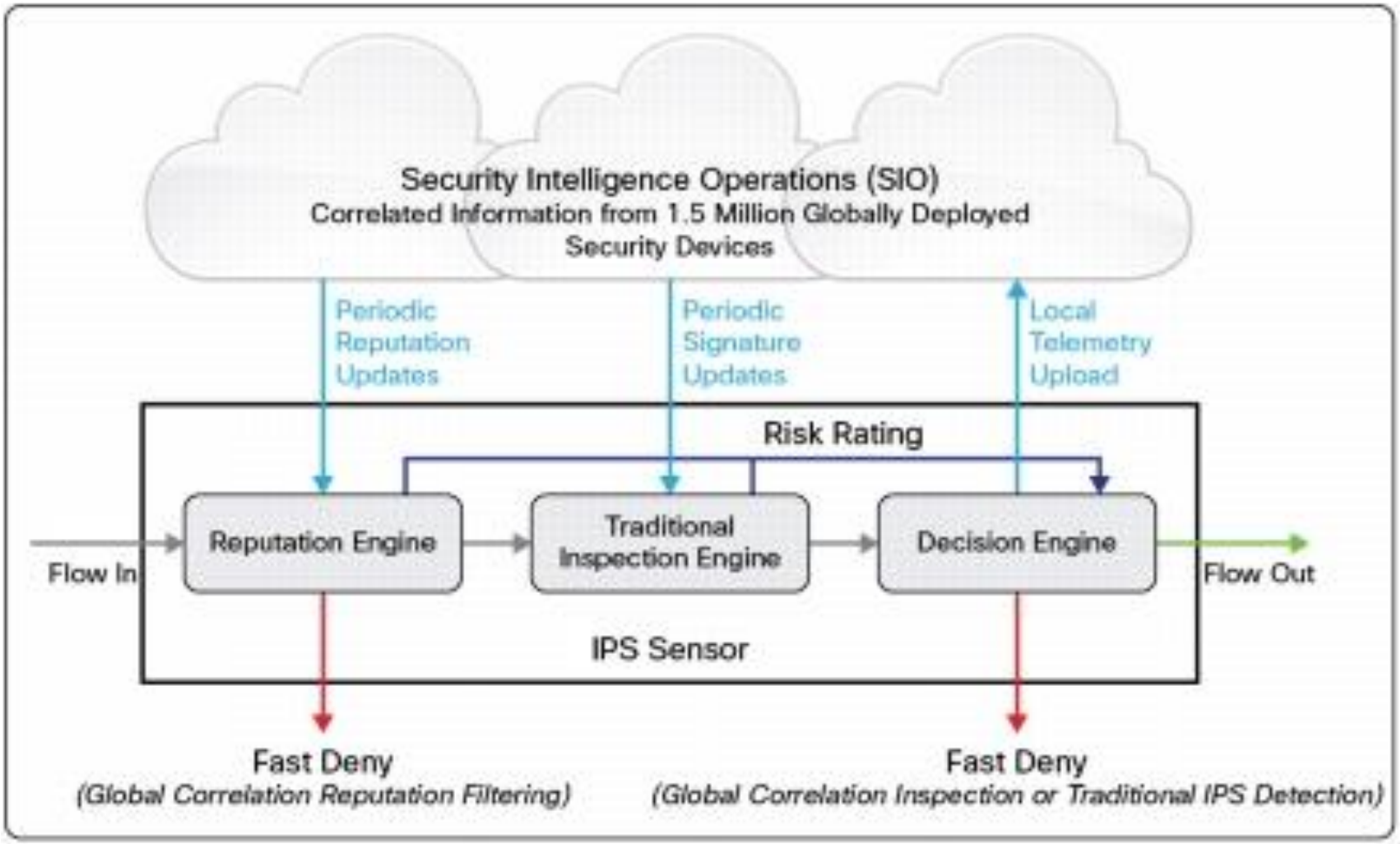
e) A combination of the above

f) Other

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency Issue
- Translation problem - multiple devices are in the path
- Firewall does not build any connection through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

What is Global Correlation?



http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps12156/white_paper_c11-715386.html

Global Correlation on Cisco IPS

Bad traffic denied by a Cisco IPS sensor falls into three categories:

- **Global Correlation Reputation Filtering:** Based on reputation alone. Flow is not passed to the traditional inspection engines.
- **Global Correlation Inspection:** Based on a combination of traditional inspection and network reputation information. The risk rating mechanism combines the two threat signals.
- **Traditional IPS Detection:** Based on traditional inspection techniques, including protocol decoding engines, signature based inspection, and anomaly detection via statistical analysis of network traffic. In this case, network reputation information for the traffic flow is not available or does not have an effect on the flow.

Global Correlation / Signature package is not updated:

Double check the following:

- Make sure firewalls along the path allow ports 443/80 for the sensor's IP address
- Configure DNS server to allow GC features to function
- Valid IPS license to allow GC features to function
- Sensor supports GC features (ie IPS 7.x or higher and not AIP SSC module
- On IPS CLI check: show statistics global-correlation
- Check for GC messages in the show tech under /usr/cids/idsRoot/log/main.log for clues.

Advance Troubleshooting

- Login using a service account.
- Use the command below using your CCO account:

-bash-3.2$ su

-bash-3.2$ curl -v –u CCOuserID http://ccpuserID@72.163.7.60//swc/esd/01/273556262/guest/IPS-sig-S674-req-E4.pkg

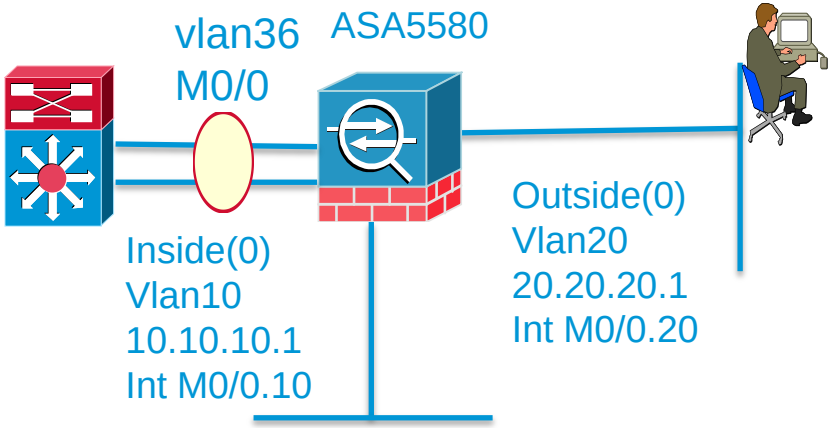
the host password for user ’CCOuserID':********

The output will provide more details as to where the the HTTP request is getting dropped.

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections build through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

Case Study: 4 Main int. not passing data



Relevant switch config:

```
interface GigabitEthernet2/35
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan36
ip address 14.36.119.227 255.255.0.0
!
```

Relevant ASA config:

```
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 14.36.119.226 255.255.0.0
!
interface Management0/0.10
 vlan 10
 nameif Inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Management0/0.20
 vlan 20
 nameif Outside
 security-level 0
 ip address 20.20.20.1 255.255.255.0
```

Problem: Unable to ping 14.36.119.227 from 14.36.119.226 and vice versa

Diagnosis

captures on the mgmt interface shows just the requests being sent out but not replies arriving:

cap capmgmt match icmp host 14.36.119.226 host 14.36.119.227

sh cap capmgmt detail

4 packets captured
1: 16:01:25.910261 5475.d05b.0980 0017.0f17.af80 0x0800 114: 14.36.119.226 > 14.36.119.227: icmp: echo request (ttl 255, id 30161)
2: 16:01:27.909987 5475.d05b.0980 0017.0f17.af80 0x0800 114: 14.36.119.226 > 14.36.119.227: icmp: echo request (ttl 255, id 12956)
3: 16:01:29.909971 5475.d05b.0980 0017.0f17.af80 0x0800 114: 14.36.119.226 > 14.36.119.227: icmp: echo request (ttl 255, id 18027)
4: 16:01:31.909971 5475.d05b.0980 0017.0f17.af80 0x0800 114: 14.36.119.226 > 14.36.119.227: icmp: echo request (ttl 255, id 11750)

This is because the ASA is sending untagged packets and the switch port is expecting tagged packets.

Case Study: 4 Main int. not passing data

http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/intrface.html#wp1044006

If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterfaces to pass traffic, ensure that the physical interface does not pass traffic by leaving out the nameif command. If you want to let the physical interface pass untagged packets, you can configure the nameif command as usual.

Solution:

Add the following command under the interface config on the switch.

```
interface GigabitEthernet2/35
Switchport
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 36
```

Solution

- Once the “native vlan” command is added under the interface config of the switch, replies are sent by the switch. Notice no vlan tag in the main interface capture but there is vlan tag information on the sub-interface capture.

ASA#sh cap capmgmt detail (capture taken on the main interface)

4 packets captured
1: 16:00:53.234988 0017.0f17.af80 5475.d05b.0980 0x0800 114: 14.36.119.227 > 14.36.119.226: icmp: echo request (ttl 255, id 869)
2: 16:00:53.235171 5475.d05b.0980 0017.0f17.af80 0x0800 114: 14.36.119.226 > 14.36.119.227: icmp: echo reply (ttl 255, id 11426)
3: 16:00:53.236849 0017.0f17.af80 5475.d05b.0980 0x0800 114: 14.36.119.227 > 14.36.119.226: icmp: echo request (ttl 255, id 870)
4: 16:00:53.236956 5475.d05b.0980 0017.0f17.af80 0x0800 114: 14.36.119.226 > 14.36.119.227: icmp: echo reply (ttl 255, id 2829)

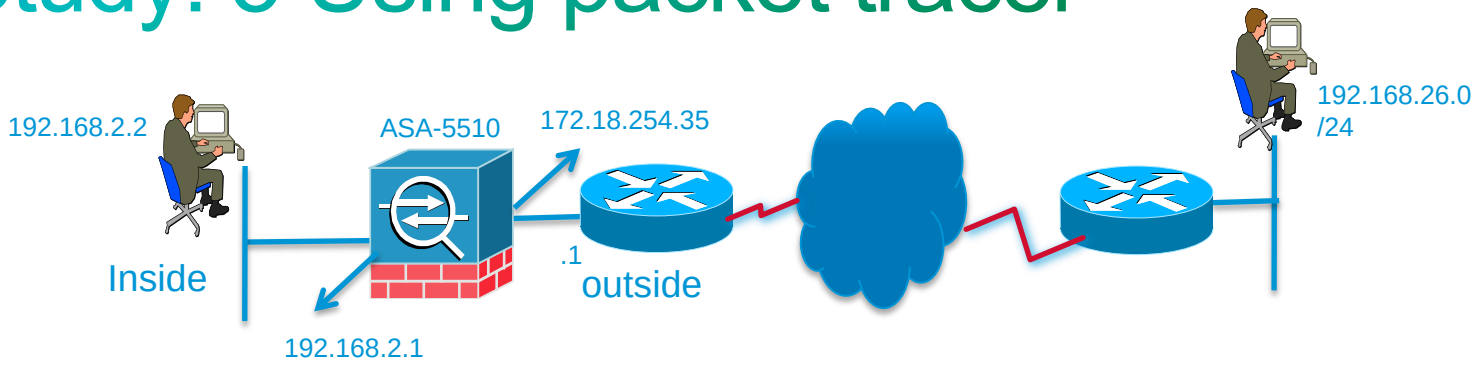
ASA# sh cap capout detail (capture taken on the sub-interface)

2 packets captured
1: 22:24:42.770910 0023.333c.bacf 0a00.0a00.0a00 0x8100 Length: 118
802.1Q vlan#20 P0 20.20.20.1 > 20.20.20.2: icmp: echo request (ttl 255, id 8516)
2: 22:24:44.769918 0023.333c.bacf 0a00.0a00.0a00 0x8100 Length: 118
802.1Q vlan#20 P0 20.20.20.1 > 20.20.20.2: icmp: echo request (ttl 255, id 24012)

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency Issue
- Translation problem - multiple devices are in the path
- Firewall does not build any connection through the box
- IPS Global Correlation problem
- Using the main interface for sending data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

Case Study: 5 Using packet tracer



Relevant ASA config:

```
object network remote_network
 subnet 192.168.26.0 255.255.255.192

object network obj_any
 subnet 0.0.0.0 0.0.0.0

nat (inside,outside) source static obj_any obj_any destination static remote_network remote_network

object network obj_any
 nat (inside,outside) dynamic interface

route outside 192.168.26.0 255.255.255.0 172.18.254.1 1
```

Problem: Packet tracer shows that host 192.168.2.2 will look like the outside Interface address when talking to the remote network 192.168.26.65

Diagnosis

packet-tracer input inside tcp 192.168.2.2 1025 192.168.26.65 23

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.26.0 255.255.255.0 outside

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj_any
 nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.2.2/1025 to 172.18.254.34/1025

Why is this flow using Dynamic PAT?

Solution

- Examine the object remote_network closely as well as the destination IP address in the packet tracer output as well as the route statement. What do you see?

```
object network remote_network
subnet 192.168.26.0 255.255.255.192

route outside 192.168.26.0 255.255.255.0 172.18.254.1 1
```

Destination IP address in packet tracer **192.168.26.65**

Host 192.168.26.65 does not belong in the subnet 192.168.26.0 255.255.255.192

The subnet mask in the remote_network object needs to be changed to match that of the route statement.

```
object network remote_network
subnet 192.168.26.0 255.255.255.0
```

Solution

- Packet tracer output after fixing the mask in the object remote_network

ASA# packet-tracer input inside tcp 192.168.2.2 1025 192.168.26.65 23

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj_any obj_any destination static remote_network remote_network
Additional Information:
NAT divert to egress interface outside
Untranslate 192.168.26.65/23 to 192.168.26.65/23

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj_any obj_any destination static remote_network remote_network
Additional Information:
Static translate 192.168.2.2/1025 to 192.168.2.2/1025

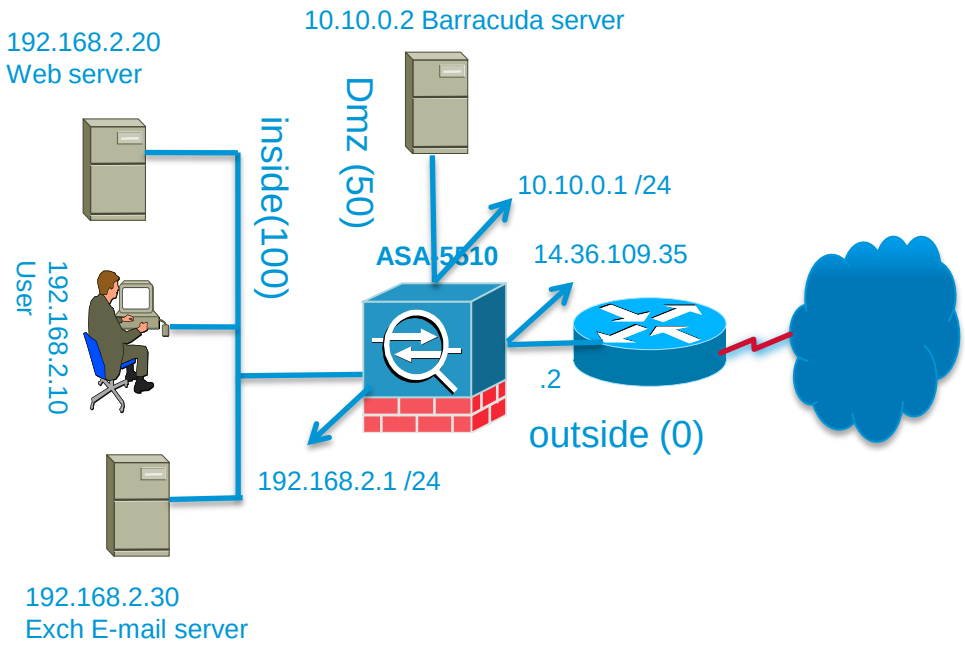
Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections build through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

How to map two different servers to the same IP address

```
nat (inside) 1 192.168.2.0 255.255.255.0
global (outside) 1 interface

static (dmz,outside) tcp 14.36.109.40 25 10.10.0.2 25
```



With the above configuration Barracuda server receives e-mail (sent to the MX record) from the internet, cleans it up and sends it to the exchange server on the inside.

Exchange server sends e-mail out directly.

Now, the problem is Exchange server is not looking like the MX record IP address when sending e-mail out. How do we solve this problem?

How to map two different servers to the same IP address

Solution: Pre 8.3 NAT format

New translation for Exchange server

```
nat (inside) 2 192.168.2.30 255.255.255.255
global (outside) 2 14.36.109.40
```

Existing translation for Barracuda server

```
static (dmz,outside) tcp 14.36.109.40 25 10.10.0.2 25
```

Solution: Post 8.3+ NAT format

```
Object network obj-exchange
 host 192.168.2.30
  nat (inside,outside) dynamic 14.36.109.40

Object network obj-barracuda
 host 10.10.0.2
  nat (dmz,outside) static 14.36.109.40 service tcp 25 25
```

Polling Question 3

Which security topics would you like to see in a future Webcast?

a) More on firewalls

b) Intrusion Detection and Prevention Systems

c) VPN

d) Physical Security

e) AAA

f) Cisco Security Manager (CSM)

g) New Features and Products

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections build through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

Failover pair zero downtime code upgrade

- What platform ASA or FWSM or PIX?
- From what code to what code?
- Does Cisco support zero downtime code upgrade between the two code versions in question?

Question 1: What is the upgrade path from 7.0.7 to 8.2.5?

Check the release note link for ASA 8.2. Simply google "asa release note 8.2" and take the first hit.
http://www.cisco.com/en/US/docs/security/asa/asa82/release/notes/asarn82.html

Read under Upgrading Between Major Releases

To ensure that your configuration updates correctly, you must upgrade to each major release in turn. Therefore, to upgrade from Version 7.0 to Version 8.2, first upgrade from 7.0 to 7.1, then from 7.1 to 7.2, and finally from Version 7.2 to Version 8.2 (8.1 was only available on the ASA 5580).

Failover pair zero downtime code upgrade

Question 2: Does zero downtime apply when upgrading ASA5510 code from 7.0.7 to 8.2.5?

Answer to the previous question answered this question as well.

Let us check the failover pair upgrade guide for ASA:
Simply google “asa manage software configuration guide 8.2”
and take the first hit.

Choose System Administration >> Managing Software and Configuration >> Performing Zero Downtime Upgrades for Failover Pairs.
http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/admin_swconfig.html#wp1053398

Failover pair zero downtime code upgrade

If the code version is 8.2.5(33)

===➔ 8 is the Major release

===➔ 2 is the Minor release

===➔ 5 is the Maintenance release

===➔ 33 is the Interim release

- You can upgrade from any maintenance release to any other maintenance release within a minor release.
- You can upgrade from a minor release to the next minor release. You cannot skip a minor release.
- You can upgrade from the last minor release of the previous version to the next major release.

Failover pair zero downtime code upgrade

Question: 3 Is FWSM 3.2.10 to 4.1(10) supported for zero downtime Upgrade?

If you refer this link:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm41/configuration/guide/swcnfg_f.html#wp1064044

You can upgrade to a newer release from any prior major or minor release without downtime. For example, you can upgrade from 3.2(1) to 4.1 or from 4.0(1) to 4.1 without installing any releases in between.

So, going from 3.2(10) to 4.1(10) without downtime is supported by Cisco.

Check the FWSM release note link for 4.1:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm41/release/notes/fwsmrn41.html

chassis system requirement and make sure the code is compatible to run the new FWSM 4.1 code.

Failover pair zero downtime code upgrade

Question: 4 What is the code upgrade procedure for FWSM code upgrade from 3.2(10) to 4.1(10)?

1. tftp the code to both the units – copy tftp flash:image
2. If multiple context, on the active unit's system context, execute "write mem all”
3. reload the standby unit which will come back as standby and running the new code
4. on the standby execute "failover active", it is now the active unit
5. Reload the unit that is now standby

Upgrade procedure can be found here:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm41/configuration/guide/swcnfg_f.html#wp1064244

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections build through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

Scan Safe web security configuration

http://www.cisco.com/en/US/docs/security/asa/asa90/configuration/guide/protect_cloud_web_security.html

- Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity. Introduced in ASA 9.0(1) code.
- No additional hardware required.
- The ASA can optionally authenticate and identify users with Identity Firewall (IDFW) and AAA rules.
- ASA transparently redirects selected HTTP and HTTPS traffic to the Cloud Web Security proxy servers.

Scan Safe Configuration - steps

- Configure scan safe servers and license

```
scansafe general-options
server primary fqdn proxy193.scansafe.net port 8080
server backup fqdn proxy1363.scansafe.net port 8080
retry-count 5
 license 5F696F3448E40BDA66228A06E1092BCB
```

- Configure access-list to match both http as well as https traffic

```
access-list inside_http extended permit tcp any any eq www
access-list inside_https extended permit tcp any any eq https
```

- Configure class-map for http as well as https and match the access-list configured above

```
class-map inside-http-class
  match access-list inside_http
class-map inside-https-class
  match access-list inside_https
```

Scan Safe Configuration - steps

- Configure L-7 policy-map for both protocols http and https Scansafe inspection

```
policy-map type inspect scansafe http-pmap
parameters
default group httptraffic
http

policy-map type inspect scansafe https-pmap
parameters
default group httpstraffic
https
```

- Configure a new policy-map or use the existing policy-map – usually named global_policy

```
policy-map inside-policy
  class inside-http-class
    inspect scansafe http-pmap fail-close
  class inside-https-class
    inspect scansafe https-pmap fail-close
```

- Finally apply the policy-map via a service-policy

```
service-policy inside-policy interface inside
```

Agenda

- Pre and Post 8.3+ NAT
- L-2 Adjacency issue
- Translation problem - multiple devices are in the path
- No x-lates or connections build through the box
- IPS - Global Correlation signature update problem
- Using the main interface for passing data
- Using Packet Tracer to troubleshoot
- How to map two different servers to the same IP address
- Failover pair zero downtime code upgrade
- Scan Safe – New Feature
- ASA CX Context-Aware Security – New (Module) Feature

ASA CX Context-Aware Security

- The CX module on ASA can provide a contextual view of the traffic based on application type, user identity, endpoint device type, destination URLs and reputation. The PRSM (Prime Security Manager) device manager provides a consistent interface to managing single or multiple CX devices. The functionality CX and PRSM provide tools that help customers get visibility into the kind of applications that are going through their network and apply control policies based on contextual information.

- Data sheet can be found here:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-701659.html

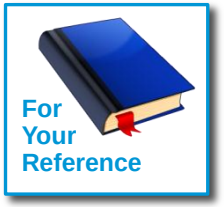
ASA CX Context-Aware Security

Platform Support/Compatibility
The ASA CX SSP-10 and SSP-20 are supported on Cisco ASA 5585-X platforms running Cisco ASA Software Release 8.4.4 and higher.
The solution can be managed using Cisco Prime Security Manager.

For more information, please visit the following links:

- Cisco ASA CX Context-Aware Security: http://www.cisco.com/go/asacx.
- Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa.
- Cisco Prime Security Manager: http://www.cisco.com/go/prsm.
- Cisco Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/
- ps2952/serv_group_home.html.

References



- **Cisco Support Community** – Firewalling Community
  https://supportforums.cisco.com/community/netpro/security/firewall
- **ASA**
  - ASA release notes
    http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html
  - ASA configuration guide
    http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
  - ASA syslog guide
    http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html
- **FWSM**
  - FWSM documentation link
    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html
  - ASA/PIX/FWSM: packet capture using CLI and ASDM
    http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a0080a9edd6.shtml
- **Bug took-kit**
  http://www.cisco.com/pcgi-bin/Support/Bugtool/home.pl

“ I hope everyone enjoyed today’s presentation”

Happy troubleshooting and stay tuned for more in the future.

- Poonguzhali (Kureli) Sankar

Trivia Question (select the correct answer)

What do Cisco's security systems products and the location for the 2013 Super Bowl have in common?

A. In 2008, Cisco pushed Firewall and VPN performance to new heights with new ASAs, announcing these new products the same year New Orleans last hosted the Super Bowl.

B. Cisco expanded its security systems product portfolio by adding to its threat defense and secure connectivity products and services for networked businesses the same year that the Super Bowl was last played in New Orleans.

C. Cisco delivered over 10 new products, software enhancements, and services across its security product portfolio in 2005 announced these new products the same year the Super bowl was last played in New Orleans.

Q & A

Expert responding some of your questions verbally. Use the Q&A panel to continue asking your questions

We Appreciate Your Feedback!

Those who fill out the Evaluation Survey will enter a raffle to win:

$50 Amazon Gift Card

To complete the evaluation, please click on link provided in the chat or in the pop-up once the event is closed.

You can also go to https://www.ciscofeedback.vovici.com/se.ashx?s=6A5348A728809439

Ask The Experts Event (with Kureli)

If you have additional questions, you can ask them to Kureli. She will be answering from January 15th to January 25th.
https://supportforums.cisco.com/thread/2192556

You can watch the video or read the Q&A 5 business days after the event at
https://supportforums.cisco.com/community/netpro/ask-the-expert/webcasts

Next Expert Series Webcast in Spanish

Topic: NX-OS: Routing Considerations with Virtual PortChannel (VPC) Topologies

Tuesday, January 22nd, at

9 a.m. CST (Mexico City)
10 a.m. EST New York
4 p.m. CET Paris

Join Cisco Expert

Virgilio Vargas

During the live event you will learn the basics Virtual PortChannel (VPC) and the differences between NX-OS and Cisco IOS Software

Register for this live Webcast @

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=S&SEMINAR_CODE=S17654&PRIORITY_CODE=cisco

January Expert Series Webcast in Japanese

Topic: FabricPath Refresher: From Fundamental to Virtual Port-Channel Plus (vPC+)

Tuesday January 29, at

10:00 a.m. JST Tokyo

Monday January 28th 5:00 p.m. PST San Francisco

Join Cisco Expert:

Kaoru Yamashita

During the live event you will about FabricPath and Virtual PortChannel Plus (vPC+)

Register at @

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=J&SEMINAR_CODE=S17564&PRIORITY_CODE=cisco

Next Expert Series Webcast in Portuguese

Topic: Cisco Catalyst 6500 Series Switches: Troubleshooting and Best Practices

Tuesday February 5, at

11 a.m. Brasilia City (UTC -2 hours)
8 a.m. New York
1 p.m. Lisbon (UTC)

Join Cisco Expert

Rafael Lima

During this live event you'll learn how to troubleshoot common issues Cisco Catalyst 6500 Switches

Register for this live Webcast @

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=P&SEMINAR_CODE=S17666&PRIORITY_CODE=cisco

Ask the Expert Events – English Current

Topic: Basic Introduction and Troubleshooting on Cisco Nexus 7000 NX-OS Virtual Device Context

Join Cisco Expert: **Vignesh Rajendran**

Learn about troubleshooting on Cisco Nexus 7000 NX-OS Virtual Device Context

---

Topic: Cisco Intrusion Prevention System

Join Cisco Expert: **Robert Albach**
Learn and ask questions about Cisco Intrusion Prevention System (IPS)

Topic: Cisco Prime Network Registrar

Join Cisco Experts: **Jim Brown and Peter Newcomb**
Learn and ask questions about Cisco Prime Network Registrar.

Join the discussions of these Ask The Expert Events at: They **end on January 18th**.
https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts

Ask the Expert Events – English Current

Topic: Configuring and Troubleshooting MPLS Traffic Engineering

Join Cisco Expert: **Saurabh Chopra**
Learn and ask questions about how MPLS Traffic Engineering can help to best utilize your MPLS network.

Topic: FlexVPN and Internet Key Exchange Version 2 (IKEv2)

Join Cisco Expert: **Jay Young-Taylor**

Learn and ask questions about FlexVPN and IKEv2

Events End Friday January 25th
Join the discussion for these Ask The Expert Events at:
https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts

We invite you to actively collaborate in the Cisco Support Community and social media

https://supportforms.cisco.com


http://www.facebook.com/CiscoSupportCommunity


http://twitter.com/#!/cisco_support

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


https://plus.google.com/110418616513822966153?prsrc=3#110418616513822966153/posts


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


https://play.google.com/store/apps/details?id=com.cisco.swtg_android


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

We have communities in other languages

If you speak Spanish, Portuguese, Japanese, Polish or Russian, we invite you to ask your questions and collaborate in your language:

- Spanish → https://supportforums.cisco.com/community/spanish
- Portuguese → https://supportforums.cisco.com/community/portuguese
- Japanese → https://supportforums.cisco.com/community/csc-japan
- Polish → https://supportforums.cisco.com/community/etc/netpro-polska
- Russian → https://supportforums.cisco.com/community/russian

Trivia Answer

What do Cisco's security systems products and the location for the 2013 Super Bowl have in common?

A. In 2008, Cisco pushed Firewall and VPN performance to new heights with new ASAs, announcing these new products the same year New Orleans last hosted the Super Bowl.

B. **Cisco expanded its security systems product portfolio by adding to its threat defense and secure connectivity products and services for networked businesses the same year that the Super Bowl was last played in New Orleans.**

C. Cisco delivered over 10 new products, software enhancements, and services across its security product portfolio in 2005 announced these new products the same year the Super bowl was last played in New Orleans.

Correct Answer b.
Cisco expanded its security systems product portfolio by adding to its threat defense and secure connectivity products and services for networked businesses in 2004 which was the last year that Super bowl was played in New Orleans. New Orleans is once again hosting the Super Bowl this year making it the 10th time that the city has hosted the event.

Thank You for Your Time

Please Take a Moment to Complete the Evaluation

Thank you.