ASA 5505 – Standard Cisco Firewall

No default password on firewall

Creating hostname on ASA5505 firewall

```
ciscoasa(config)#hostname ABCFood-ASAFirewall
ABCFood-ASAFirewall(config)#
```

Domain name

```
ABCFood-ASAFirewall(config)#domain-name abcfood.co.nz
```

Enable a firewall password

```
ABCFood-ASAFirewall(config)#enable password Admin1
```

Assigning VLANS for DMZ | Inside and Outside Networks

DMZ	Inside Network	Outside network
Semi trsted network where our webservice resided which will be accessesingble for external clients and contractors 192.168.2.0/24 VLAN 3 DMZ	It is not recommended for external cliensts or contractors to access ABC Food internal network which is the most trusted and secured network. 192.168.1.0/24 VLAN 1 INSIDE	Outside network this is a untrusted network why its untrusted because its connected to the main internet connection from the ISP and we cannot control the Internet therefore it is untrusted netwrok. VLAN 2 209.165.200.224/29 OUTSIDE

Security measures on ASA

Inside network has been configured to VLAN 1 and named as inside and security level has been assigned to 100 the highest level of security

VLAN1

```
ABCFood-ASAFirewall(config)#interface vlan 1
ABCFood-ASAFirewall(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
```

```
ABCFood-ASAFirewall(config-if)#ip add 192.168.1.1 255.255.255.0 (inside gateway ip address)
```

```
ABCFood-ASAFirewall(config-if)#security-level 100
```

VLAN 2

Because its slant/29 the subnet mask will be 255.255.255.248

```
ABCFood-ASAFirewall(config)#int vlan 2
ABCFood-ASAFirewall(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ABCFood-ASAFirewall(config-if)#ip add 209.165.200.226 255.255.255.248 (External gateway ip address)
```

```
ABCFood-ASAFirewall(config-if)#security-level 0
```

Please Note:

A stateful firewall should let traffic from highest trusted zone 100 to go out to least trusted zone 0 and shouldn't let least trusted traffic 0 to enter to the most trusted network 100.

However the stateful firewall should let the traffic from the most trusted client to go out and come back to the same client. Ex: PC-B should be able to go out to the internet from internal network through the firewall and return back.

```
ABCFood-ASAFirewall(config-if)#show switch vlan

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    inside                      up       Et0/1, Et0/2, Et0/3, Et0/4

                                        Et0/5, Et0/6, Et0/7

2    outside                      up       Et0/0

ABCFood-ASAFirewall(config-if)#
```

IP Addressed assigned to the firwall so far

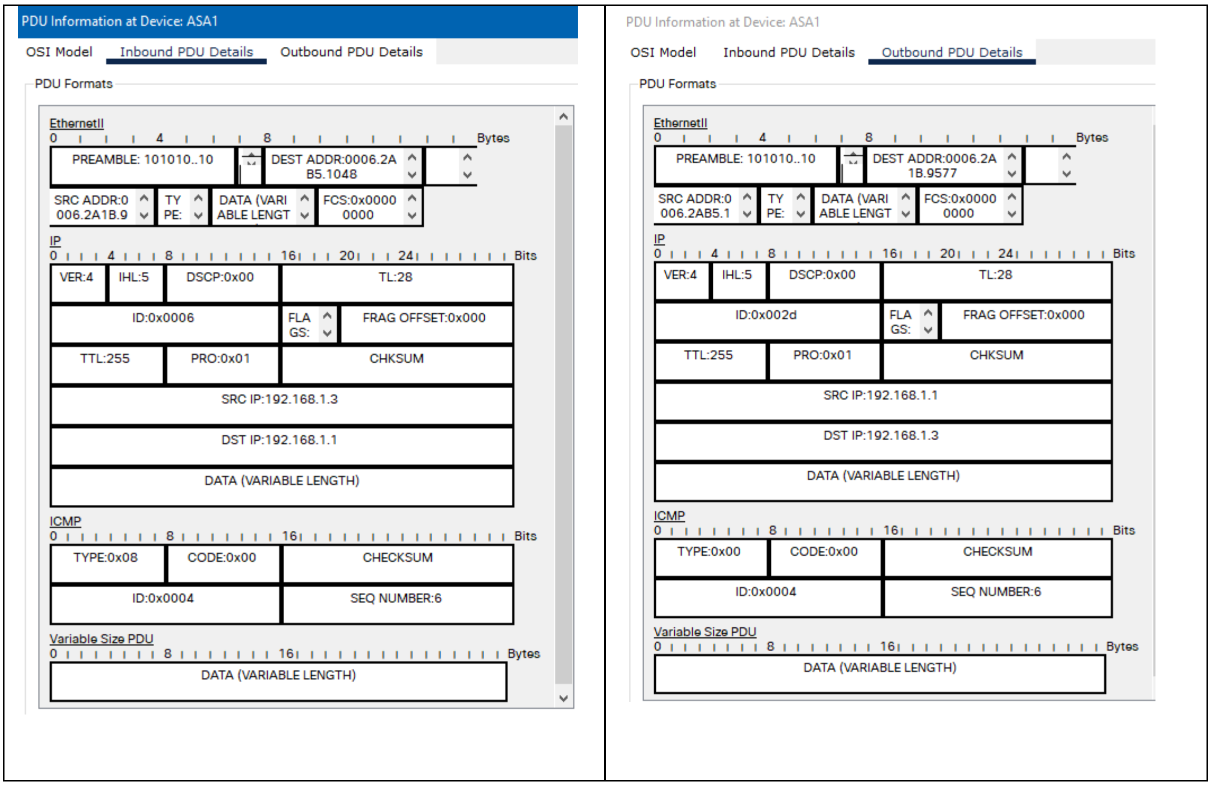
```
ABCFood-ASAFirewall(config-if)#show int ip brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 unassigned YES unset up up
Ethernet0/1 unassigned YES unset up up
Ethernet0/2 unassigned YES unset up up
Ethernet0/3 unassigned YES unset down down
Ethernet0/4 unassigned YES unset down down
Ethernet0/5 unassigned YES unset down down
Ethernet0/6 unassigned YES unset down down
Ethernet0/7 unassigned YES unset down down
Vlan1 192.168.1.1 YES manual up up
```

```
Vlan2 209.165.200.226 YES manual up up
ABCFood-ASAFirewall(config-if)#
```

Ping from client (internal network) laptop to the firewall gateway

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

OSI Layer - Inbound and outbound traffic flow from internal client to ASA Firewall



EthernetII
PREAMBLE: 101010..10
DEST ADDR:0006.2A B5.1048
SRC ADDR:0 006.2A1B.9
TY PE:
DATA (VARI ABLE LENGT
FCS:0x0000 0000

IP
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x0006
FLA GS:
FRAG OFFSET:0x000
TTL:255
PRO:0x01
CHKSUM
SRC IP:192.168.1.3
DST IP:192.168.1.1
DATA (VARIABLE LENGTH)

ICMP
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x0004
SEQ NUMBER:6

Variable Size PDU
DATA (VARIABLE LENGTH)

EthernetII
PREAMBLE: 101010..10
DEST ADDR:0006.2A 1B.9577
SRC ADDR:0 006.2AB5.1
TY PE:
DATA (VARI ABLE LENGT
FCS:0x0000 0000

IP
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x002d
FLA GS:
FRAG OFFSET:0x000
TTL:255
PRO:0x01
CHKSUM
SRC IP:192.168.1.1
DST IP:192.168.1.3
DATA (VARIABLE LENGTH)

ICMP
TYPE:0x00
CODE:0x00
CHECKSUM
ID:0x0004
SEQ NUMBER:6

Variable Size PDU
DATA (VARIABLE LENGTH)

Creating static route from Firwall to go out to the external router

Showing exiting route on the Firewall

```
ABCFood-ASAFirewall(config-if)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
209.165.200.0/29 is subnetted, 2 subnets
C 209.165.200.0 255.255.255.248 is directly connected, outside, Vlan2
C 209.165.200.224 255.255.255.248 is directly connected, outside, Vlan2
ABCFood-ASAFirewall(config-if)#
```

Creating static route to the first external router

Creating route from any ip address from any subnet mask to send traffic to External (ISP) ip address 209.165.200.225

```
ABCFood-ASAFirewall(config-if)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

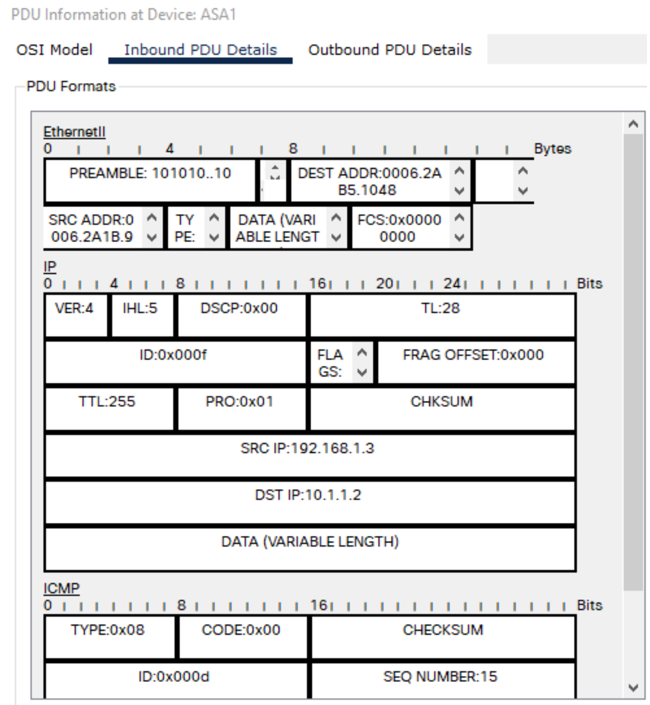
```
ABCFood-ASAFirewall(config)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C 192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
209.165.200.0/29 is subnetted, 2 subnets
C 209.165.200.0 255.255.255.248 is directly connected, outside, Vlan2
C 209.165.200.224 255.255.255.248 is directly connected, outside, Vlan2
S* 0.0.0.0/0 [1/0] via 209.165.200.225
```

Network Address translation (NAT)

Ip addresses of internal network from any ip 192.168.1.0 with subnet 255.255.255.0 will be translated to a public ip address while exiting the firewall to access the public internet

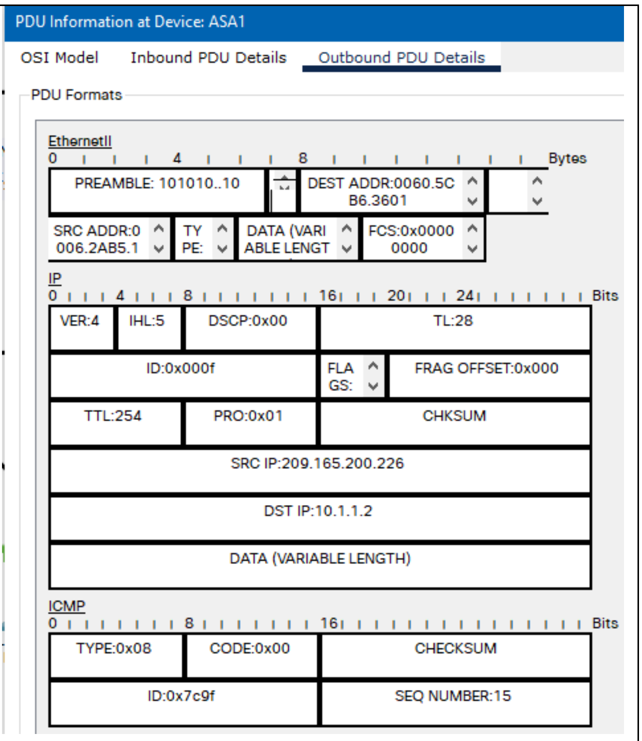
```
ABCFood-ASAFirewall(config)#object network
% Incomplete command.
ABCFood-ASAFirewall(config)#object network inside-net
ABCFood-ASAFirewall(config-network-object)#subnet 192.168.1.0 255.255.255.0
ABCFood-ASAFirewall(config-network-object)#nat (inside,outside) dynamic interface
ABCFood-ASAFirewall(config-network-object)#end
```

As you can see on the Figure below ICMP traffic from 192.168.1.3 from the ASA Firewall while exiting on the OSI layer it translates the IP address in to a public ip address to 209.165.200.226



PREAMBLE: 101010..10
DEST ADDR:0006.2AB5.1048
SRC ADDR:0006.2A1B.9
TYPE:
DATA (VARIABLE LENGT
FCS:0x00000000
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x000f
FLAGS:
FRAG OFFSET:0x000
TTL:255
PRO:0x01
CHKSUM
SRC IP:192.168.1.3
DST IP:10.1.1.2
DATA (VARIABLE LENGTH)
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x000d
SEQ NUMBER:15

Inbound SRC IP: 192.168.1.3



PREAMBLE: 101010..10
DEST ADDR:0060.5CB6.3601
SRC ADDR:0006.2AB5.1
TYPE:
DATA (VARIABLE LENGT
FCS:0x00000000
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x000f
FLAGS:
FRAG OFFSET:0x000
TTL:254
PRO:0x01
CHKSUM
SRC IP:209.165.200.226
DST IP:10.1.1.2
DATA (VARIABLE LENGTH)
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x7c9f
SEQ NUMBER:15

Outbound SRC IP: 209.165.200.226

```
ABCFood-ASAFirewall#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
translate_hits = 2, untranslate_hits = 2
```

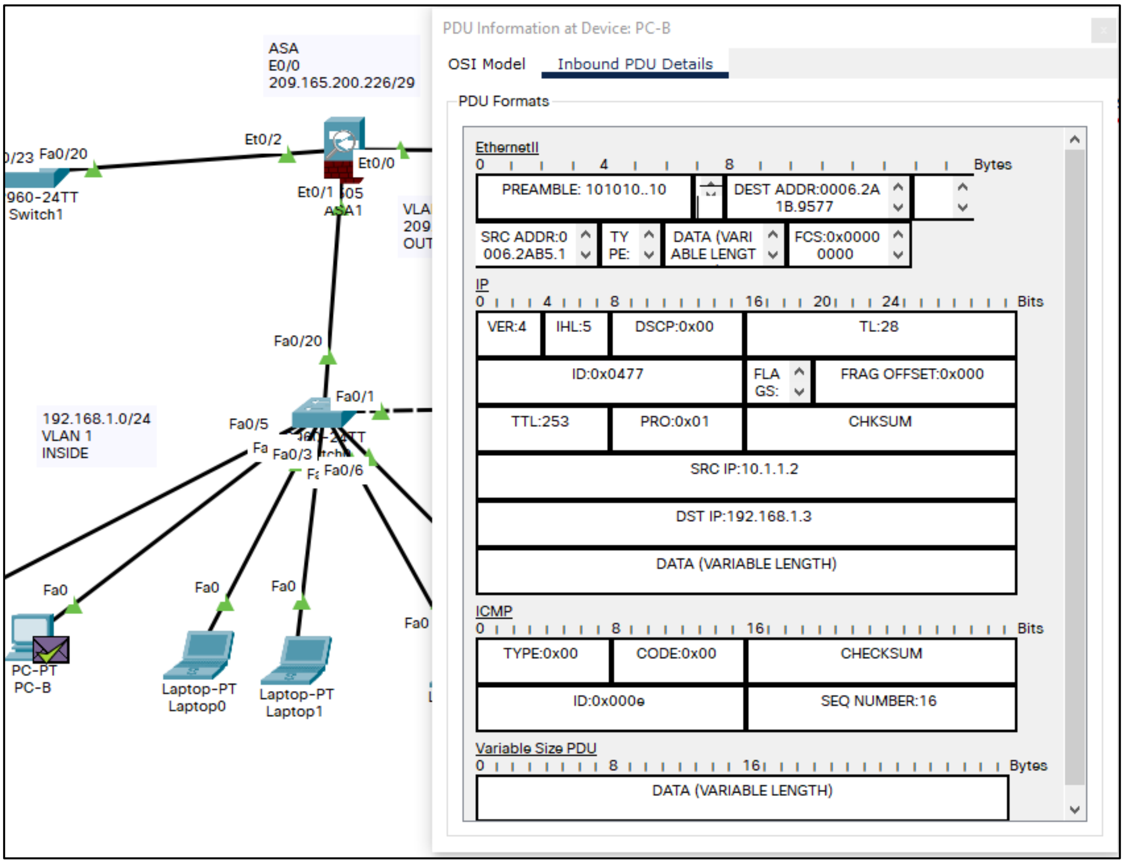
Creating a policy framework for ICMP traffic to flow back in to the original destination

Class map, policy map, service policy

- Class map basically uses to identify an ip address of a traffic
- Policy map identifies the action to take based on the traffic
- Service policy is to actually to implement the service policy

```
ABCFood-ASAFirewall(config)#class-map inspection_default
ABCFood-ASAFirewall(config-cmap)#match default-inspection-traffic
ABCFood-ASAFirewall(config-cmap)#exit
ABCFood-ASAFirewall(config)#policy-map global_policy
ABCFood-ASAFirewall(config-pmap)#class inspection_default
ABCFood-ASAFirewall(config-pmap-c)#inspect icmp
ABCFood-ASAFirewall(config-pmap-c)#exit
ABCFood-ASAFirewall(config)#
ABCFood-ASAFirewall(config)#service-policy global_policy global
ABCFood-ASAFirewall(config)#
```

As you now can see on the figure below traffic from the PC-B 192.168.1.3 has passed through the firewall and gone to the public facing router 10.1.1.2 then returned back from the router through the firewall to the destination.



PDU Information at Device: PC-B

PDU Formats

EthernetII

PREAMBLE: 101010..10 | DEST ADDR:0006.2A1B.9577 | SRC ADDR:0006.2AB5.1 | TYPE: | DATA (VARIABLE LENGT | FCS:0x00000000

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:28
ID:0x0477 | FLAGS: | FRAG OFFSET:0x000
TTL:253 | PRO:0x01 | CHKSUM
SRC IP:10.1.1.2
DST IP:192.168.1.3
DATA (VARIABLE LENGTH)

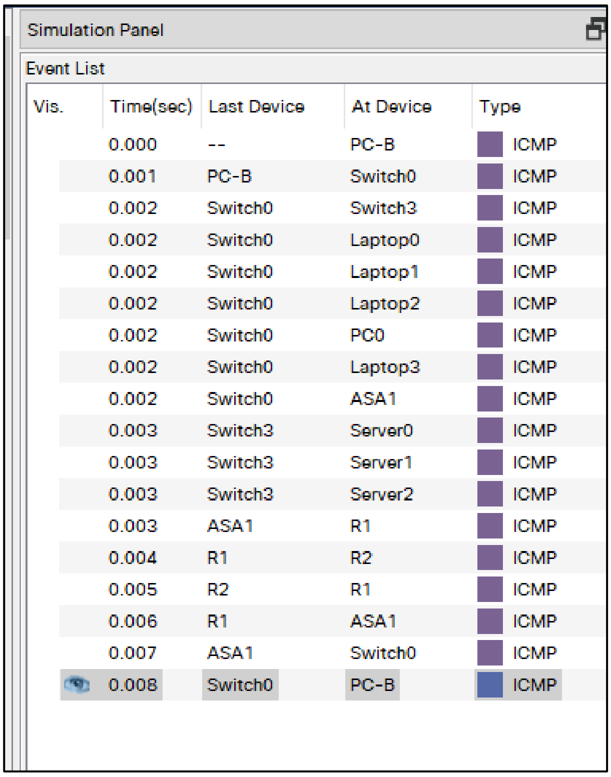
ICMP

TYPE:0x00 | CODE:0x00 | CHECKSUM
ID:0x000e | SEQ NUMBER:16

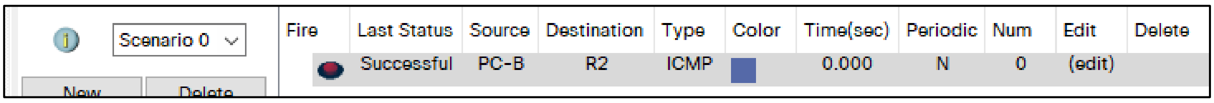
Variable Size PDU

DATA (VARIABLE LENGTH)

Successsful ICMP traffic flow



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC-B	■ ICMP
	0.001	PC-B	Switch0	■ ICMP
	0.002	Switch0	Switch3	■ ICMP
	0.002	Switch0	Laptop0	■ ICMP
	0.002	Switch0	Laptop1	■ ICMP
	0.002	Switch0	Laptop2	■ ICMP
	0.002	Switch0	PC0	■ ICMP
	0.002	Switch0	Laptop3	■ ICMP
	0.002	Switch0	ASA1	■ ICMP
	0.003	Switch3	Server0	■ ICMP
	0.003	Switch3	Server1	■ ICMP
	0.003	Switch3	Server2	■ ICMP
	0.003	ASA1	R1	■ ICMP
	0.004	R1	R2	■ ICMP
	0.005	R2	R1	■ ICMP
	0.006	R1	ASA1	■ ICMP
	0.007	ASA1	Switch0	■ ICMP
👁	0.008	Switch0	PC-B	■ ICMP



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC-B	R2	ICMP	■	0.000	N	0	(edit)	

ABCFood-ASAFirewall(config)#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
translate_hits = 3, untranslate_hits = 3

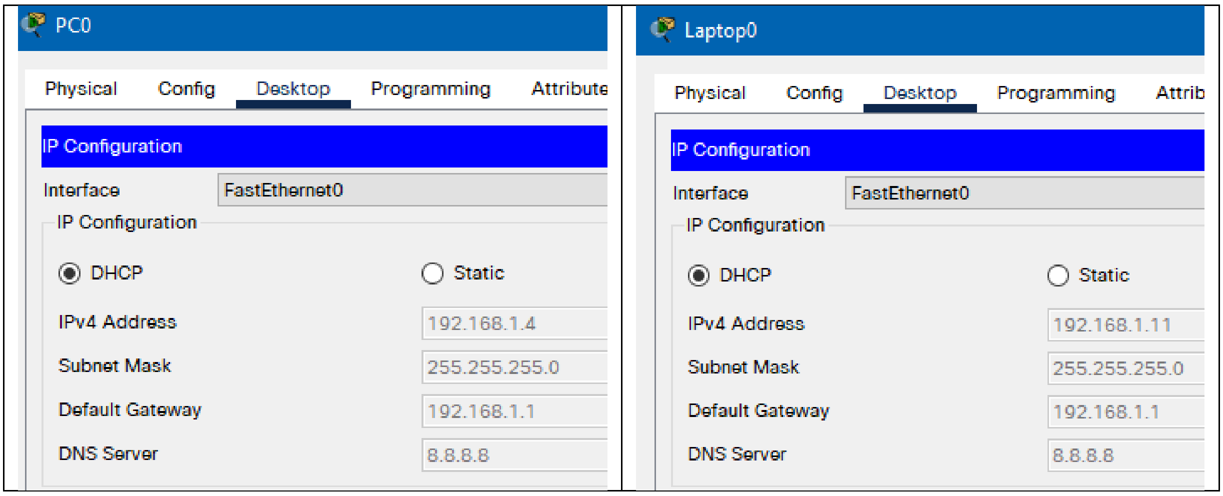
Configuring DHCP, AAA and SSH

setting up a DHCP Server

ABCFood-ASAFirewall(config)#dhcpd
ABCFood-ASAFirewall(config)#dhcpd add 192.168.1.4-192.168.1.28 inside

ABCFood-ASAFirewall(config)#dhcpd add 192.168.1.4-192.168.1.28 inside
ABCFood-ASAFirewall(config)#
ABCFood-ASAFirewall(config)#dhcpd dns 8.8.8.8 interface inside (Assigning Google’s DNS)
ABCFood-ASAFirewall(config)#dhcpd enable inside

Figure below indicates dynamic ip address assigned from the DHCP server to inside network clints



PC0 – IP Configuration

Interface: FastEthernet0

IP Configuration: ● DHCP ○ Static

IPv4 Address: 192.168.1.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 8.8.8.8

Laptop0 – IP Configuration

Interface: FastEthernet0

IP Configuration: ● DHCP ○ Static

IPv4 Address: 192.168.1.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 8.8.8.8

lets imagine if external or an Internal IT administrator is managing the ASA Firewall server of ABC Food limited

First create a user with password

```
ABCFood-ASAFirewall(config)#username ABCAdmin1 password Admin1
```

we should create a SSH secure protocol channel with AAA

- Authentication
- Authorisation
- Accounting

```
ABCFood-ASAFirewall(config)#aaa auth
ABCFood-ASAFirewall(config)#aaa authentication ?

configure mode commands/options:
ssh SSH
telnet Telnet
ABCFood-ASAFirewall(config)#aaa authentication
```

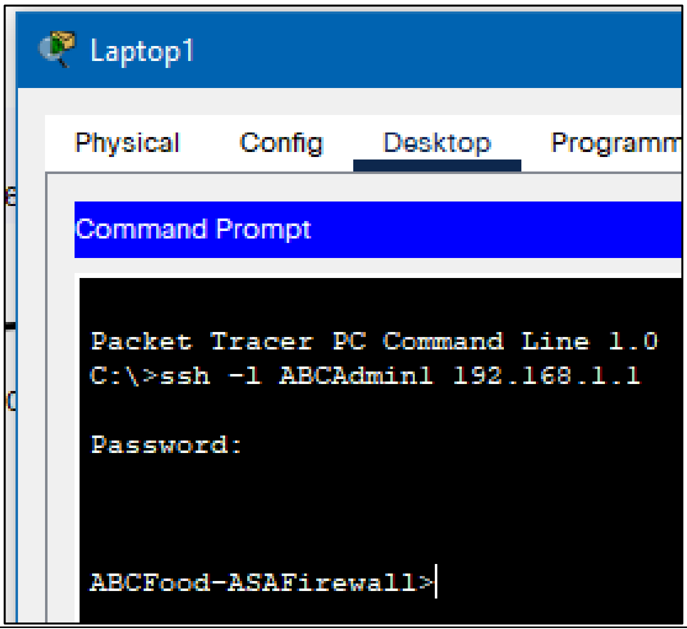
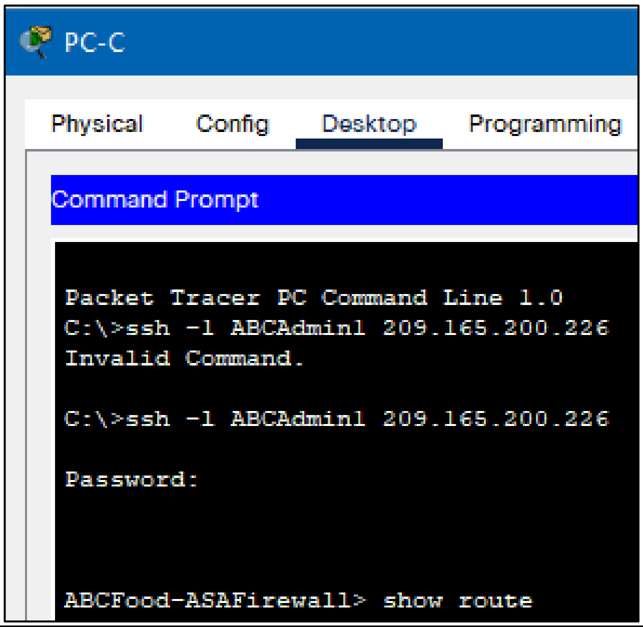
Setting up an encryption methodology to secure credentials with RSA algorithm

```
ABCFood-ASAFirewall(config)#crypto key generate rsa mod
ABCFood-ASAFirewall(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
```

Do you really want to replace them? [yes/no]: no (because there's encryption enabled already therefore not creating a new keypair)
ERROR: Failed to create new RSA keys named <Default-RSA-Key>

Defining who can access the gateway of the Firewall server

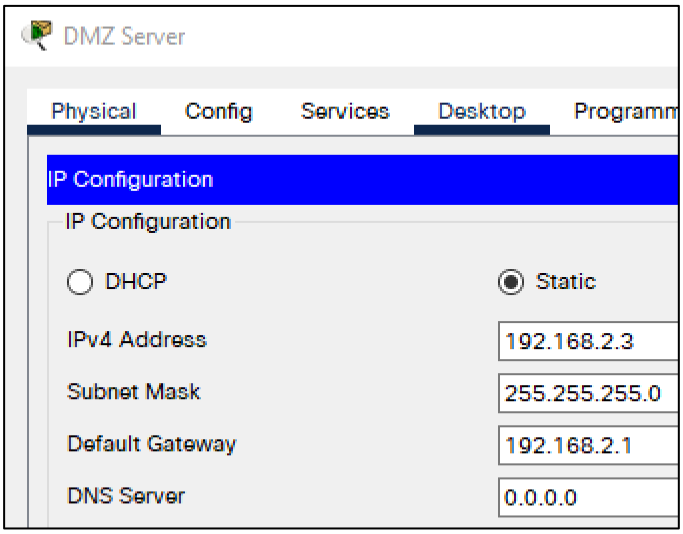
If you want to specify one particular IP address only to access the server	Let say if an external contractor wants to securely access the Firewall External contractor IP 172.16.3.3
ABCFood-ASAFirewall(config)#ssh 192.168.1.3 255.255.255.255 inside	ABCFood-ASAFirewall(config)#ssh 172.16.3.3 255.255.255.255 outside
And if you want to configure multiple administrators with various IP addresses to access Firewall Gateway Figure below indicates Laptop1 can now securely access the Firewall	From the external contractor PC

 Laptop1
Physical
Config
Desktop
Programm
Command Prompt
`Packet Tracer PC Command Line 1.0`
`C:\>ssh -l ABCAdmin1 192.168.1.1`
 	
`Password:`
 	
`ABCFood-ASAFirewall>`
	 PC-C
	Physical
	Config
	Desktop
	Programming
	Command Prompt
	`Packet Tracer PC Command Line 1.0`
	`C:\>ssh -1 ABCAdmin1 209.165.200.226`
	`Invalid Command.`
	
	`C:\>ssh -l ABCAdmin1 209.165.200.226`
	
	`Password:`
	
	`ABCFood-ASAFirewall> show route`

Configuring DMZ, Static NAT and ACL's

Configuring DMZ to access traffic from an external ip address through a Firwall

DMZ IP Address



IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.2.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

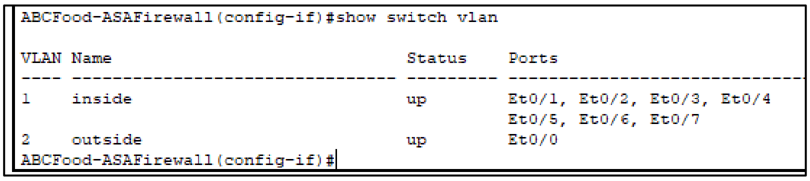
Currently external PC wont be able to ping the DMZ that's because Rotuer 3 (R3) don't have a routing table

```
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 172.16.3.1: Destination host unreachable.
Reply from 172.16.3.1: Destination host unreachable.
Ping statistics for 192.168.2.3:
Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\>
```

Setting up a VLAN to external traffic to securely pass through the Firewall to DMZ

Current VLANs on ASA Firewall

```
ABCFood-ASAFirewall(config-if)#show switch vlan

VLAN Name Status Ports

--- ------------------------------- --------- -------------------------------

1 inside up Et0/1, Et0/2, Et0/3, Et0/4

Et0/5, Et0/6, Et0/7

2 outside up Et0/0

ABCFood-ASAFirewall(config-if)#
```



```
ABCFood-ASAFirewall(config-if)#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
ABCFood-ASAFirewall(config-if)#
```

```
ABCFood-ASAFirewall(config-if)#interface vlan 3
ABCFood-ASAFirewall(config-if)#ip add 192.168.2.1 255.255.255.0
ABCFood-ASAFirewall(config-if)#no forward interface vlan 1
ABCFood-ASAFirewall(config-if)#
ABCFood-ASAFirewall(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
```

```
ABCFood-ASAFirewall(config-if)#security-level 70
```

```
ABCFood-ASAFirewall(config-if)#show switch vlan

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    inside                        up        Et0/1, Et0/2, Et0/3, Et0/4

                                          Et0/5, Et0/6, Et0/7

2    outside                        up        Et0/0

3    dmz                           down (Down because interface hasn't been configured e0/2 yet)
```

Configuring interface from ASA Firewall to the DMZ

```
ABCFood-ASAFirewall(config-if)#int e0/2
ABCFood-ASAFirewall(config-if)#swit
ABCFood-ASAFirewall(config-if)#switchport access vlan 3
```

```
ABCFood-ASAFirewall(config-if)#show switch vlan


VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    inside                        up        Et0/1, Et0/3, Et0/4, Et0/5

                                          Et0/6, Et0/7

2    outside                        up        Et0/0

3    dmz                           up        Et0/2
```

Assigning a static public ip address on Firewall to map it to pass traffic to DMZ

Currently ISP public ip address range is 209.165.200.224/29

209.168.200.225 has been assigned to Router 1

209.168.200.226 has been assigned to the Firewall as external gateway ip

209.168.200.227 is available which will be assigned to webserver

```
ABCFood-ASAFirewall(config-if)#object network dmz-server
ABCFood-ASAFirewall(config-network-object)#host 192.168.2.3
ABCFood-ASAFirewall(config-network-object)#nat (? (will tell what options are available)

network-object mode commands/options:
any Global address space
inside Name of interface Vlan1
outside Name of interface Vlan2
dmz Name of interface Vlan3
ABCFood-ASAFirewall(config-network-object)#nat (
```

```
ABCFood-ASAFirewall(config-network-object)#nat (dmz, outside) static 209.165.200.227
ABCFood-ASAFirewall(config-network-object)#exit
```

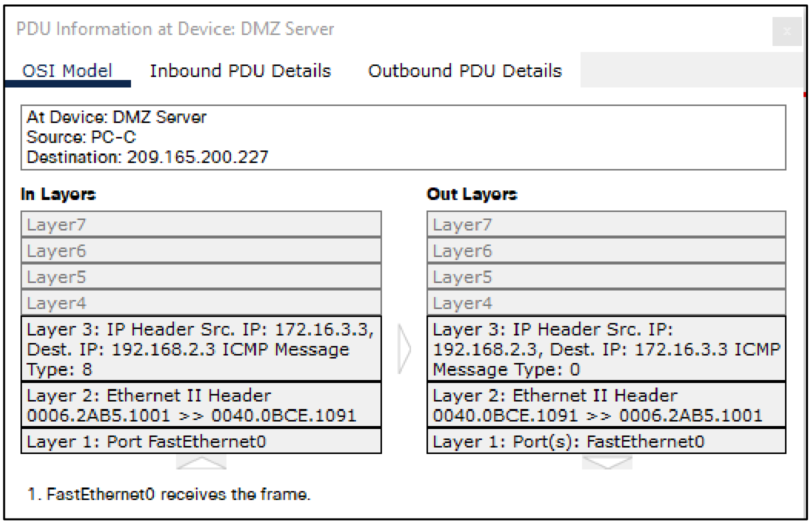
External PC still wont be able to pass through the firewall because no ACLs been created

```
ABCFood-ASAFirewall(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
```

Allowing also allow TCP traffic on port 80

```
ABCFood-ASAFirewall(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
```

```
ABCFood-ASAFirewall(config)#access-group OUTSIDE-DMZ in interface outside
```

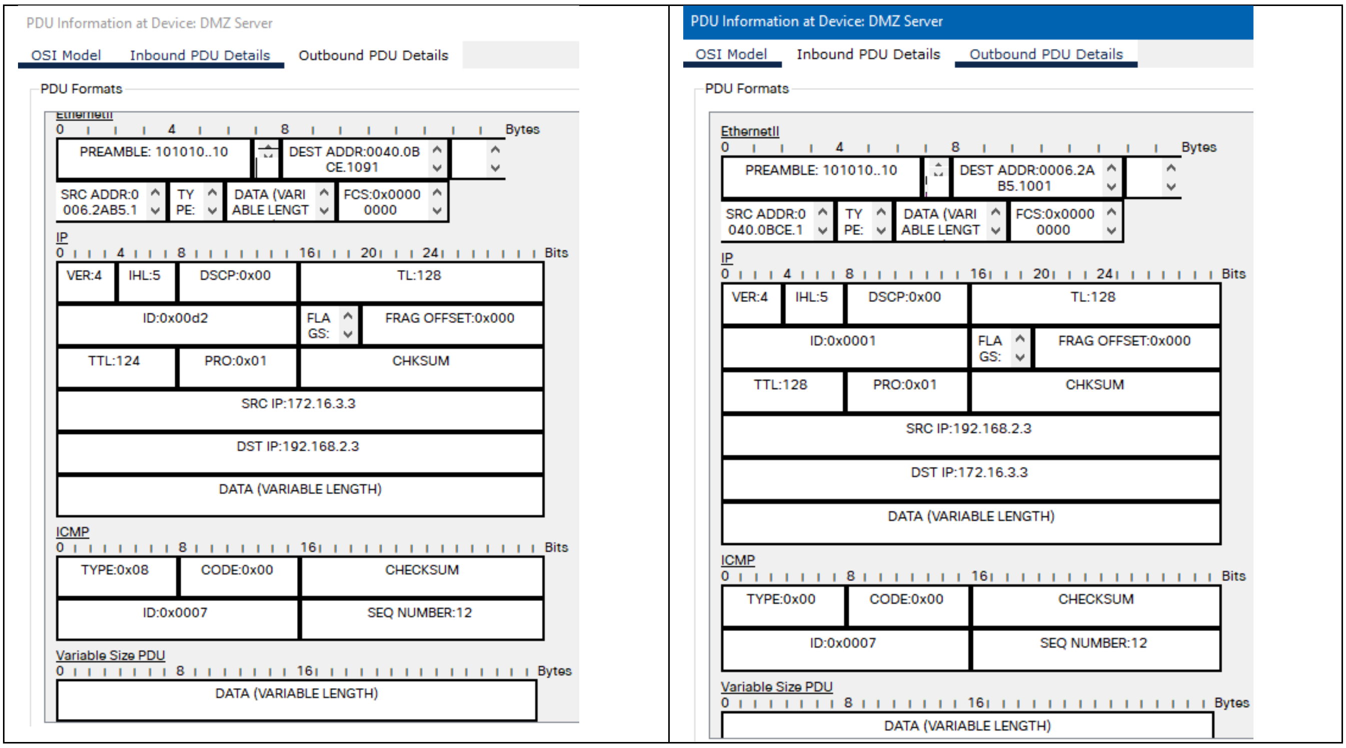


At Device: DMZ Server
Source: PC-C
Destination: 209.165.200.227

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 172.16.3.3, Dest. IP: 192.168.2.3 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 192.168.2.3, Dest. IP: 172.16.3.3 ICMP Message Type: 0
Layer 2: Ethernet II Header 0006.2AB5.1001 >> 0040.0BCE.1091	Layer 2: Ethernet II Header 0040.0BCE.1091 >> 0006.2AB5.1001
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Successful ICMP traffic flowing from External PC to DMZ



Inbound PDU Details

Ethernet
PREAMBLE: 101010..10
DEST ADDR:0040.0BCE.1091
SRC ADDR:0006.2AB5.1
TYPE:
DATA (VARIABLE LENGT
FCS:0x00000000

IP
VER:4
IHL:5
DSCP:0x00
TL:128
ID:0x00d2
FLAGS:
FRAG OFFSET:0x000
TTL:124
PRO:0x01
CHKSUM
SRC IP:172.16.3.3
DST IP:192.168.2.3
DATA (VARIABLE LENGTH)

ICMP
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x0007
SEQ NUMBER:12

Variable Size PDU
DATA (VARIABLE LENGTH)

Outbound PDU Details

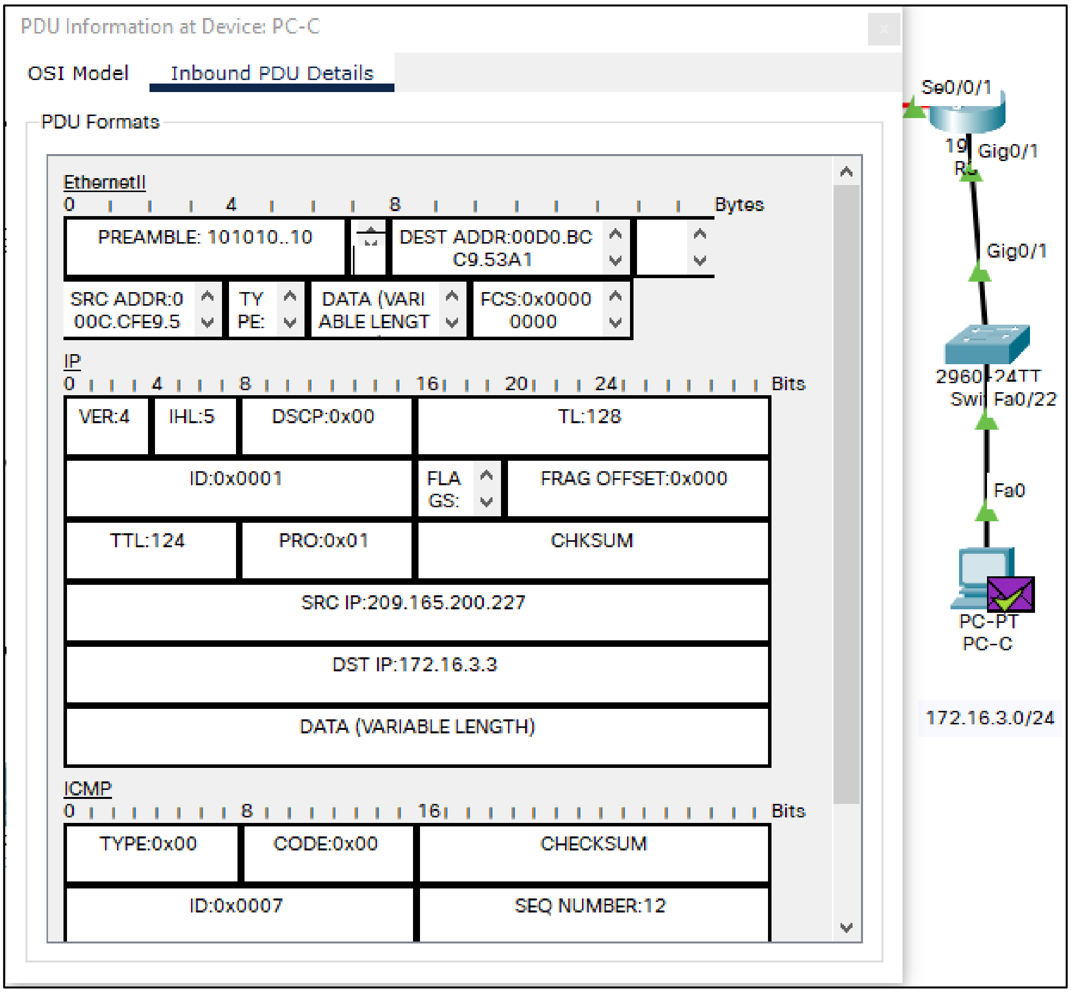
EthernetII
PREAMBLE: 101010..10
DEST ADDR:0006.2AB5.1001
SRC ADDR:0040.0BCE.1
TYPE:
DATA (VARIABLE LENGT
FCS:0x00000000

IP
VER:4
IHL:5
DSCP:0x00
TL:128
ID:0x0001
FLAGS:
FRAG OFFSET:0x000
TTL:128
PRO:0x01
CHKSUM
SRC IP:192.168.2.3
DST IP:172.16.3.3
DATA (VARIABLE LENGTH)

ICMP
TYPE:0x00
CODE:0x00
CHECKSUM
ID:0x0007
SEQ NUMBER:12

Variable Size PDU
DATA (VARIABLE LENGTH)

DMZ traffic through the Static NAT ip address 209.165.200.227 to the External PC 172.16.3.3



PDU Information at Device: PC-C

OSI Model | Inbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | DEST ADDR:00D0.BC C9.53A1

SRC ADDR:0 00C.CFE9.5 | TY PE: | DATA (VARI ABLE LENGT | FCS:0x0000 0000

IP

0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0001 | FLA GS: | FRAG OFFSET:0x000

TTL:124 | PRO:0x01 | CHKSUM

SRC IP:209.165.200.227

DST IP:172.16.3.3

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

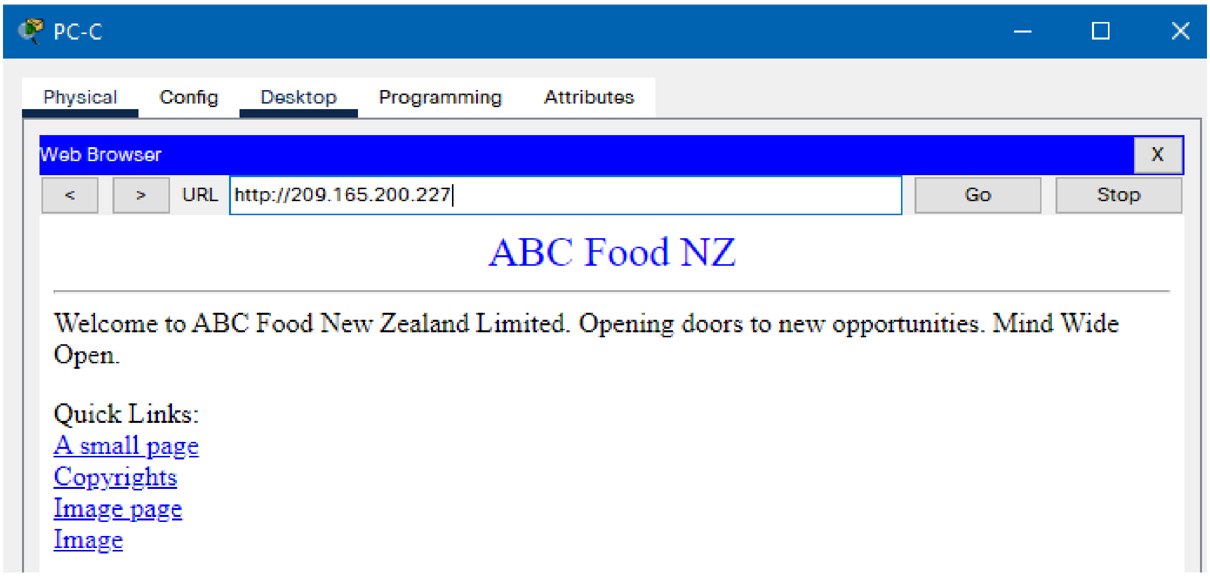
TYPE:0x00 | CODE:0x00 | CHECKSUM

ID:0x0007 | SEQ NUMBER:12

Ping from External PC-C to the Static public IP to pass traffic through to DMZ

```
C:\>ping 209.165.200.227

Pinging 209.165.200.227 with 32 bytes of data:

Reply from 209.165.200.227: bytes=32 time=22ms TTL=124
Reply from 209.165.200.227: bytes=32 time=20ms TTL=124
Reply from 209.165.200.227: bytes=32 time=11ms TTL=124
Reply from 209.165.200.227: bytes=32 time=14ms TTL=124

Ping statistics for 209.165.200.227:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 22ms, Average = 16ms

C:\>
```

Confirming TCP traffic to the Webserver 209.165.200.227



http://209.165.200.227

ABC Food NZ

Welcome to ABC Food New Zealand Limited. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Key Things to remember:

It wouldn't make any sense or cause a security threat for any traffic generating from DMZ to enter internal network to access Finance or other internal network.

Internal network administrator will be able to access the DMZ/ Firewall Server via SSH secure channel

External contractor or Network Admin will be able to access the Firewall via SSH Secure channel

Anyone in internal network will be able to access the external PC-C 172.16.3.3

Creating VLAN between Departments

Naming of VLANs for Clients

```
Switch>en
Switch#conf t

Switch(config)#vlan 10
Switch(config-vlan)#name Ops
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Finance
Switch(config-vlan)#exit
```

```
Switch#show mac address-table

          Mac Address Table
-------------------------------------------


Vlan    Mac Address       Type        Ports
----    -----------       --------    -----


   1    0006.2ab5.1048    DYNAMIC     Fa0/20
   1    0090.210d.65d9    DYNAMIC     Fa0/1
   1    00e0.8f28.51de    DYNAMIC     Fa0/7
   1    00e0.b046.ea01    DYNAMIC     Fa0/1
  10    0006.2a1b.9577    DYNAMIC     Fa0/21
  10    0007.ece5.3215    DYNAMIC     Fa0/5
  20    0001.96b8.4367    DYNAMIC     Fa0/4
  20    000c.cf22.c18c    DYNAMIC     Fa0/3
  30    00d0.972b.7456    DYNAMIC     Fa0/2
  30    00d0.bc2d.e472    DYNAMIC     Fa0/6
```

Assigning Operations team to VLAN 10 (Timeline 1:44)

PC 1	PC 2
Switch(config)#int fa0/5 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit	Switch(config)#int fa0/2 1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit

Assigning Management team to VLAN 20

Laptop 1	Laptop 2
Switch(config)#int fa0/4 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit	Switch(config)#int fa0/3 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit

Assigning Finance team to VLAN 30

Laptop 3	Laptop 4
Switch(config)#int fa0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit	Switch(config)#int fa0/6 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Assigning Servers to VLANS (Ops)

Switch(config)#int fa0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit	

Assigning VLANs For Servers

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#vlan 10
Switch(config-vlan)#name Operations
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Finance
Switch(config-vlan)#exit
```

Assigning VLANS Servers

Server 1 - Operations	**Server 2 - Management**	**Server 3 - Finance**
Switch(config)#int fa0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit	Switch(config)#int fa0/3 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit	Switch(config)#int fa0/4 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

```
Switch(config)#
Switch(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch(config)#
```

Ping fails between two switches
Switch to Switch communication >> Best practice to set up a VLAN trunk

Enabling VLAN Trunk On switch 1

```
Switch(config)#
Switch(config)#int fa0/8
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

Switch(config-if)#switchport nonegotiate
```

Enabling VLAN Trunk On switch 2 (Servers are connected to)

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport nonegotiate
Switch(config-if)#
```

Ping from Client to Server on VLAN 10 (Operations)

From 1.11 (VLAN 10) to Server 1.18 (VLAN 10)	From 1.11 (VLAN 10) to Server 1.19 (VLAN 20)
Packet Tracer PC Command Line 1.0 C:\>ping 192.168.1.18 Pinging 192.168.1.18 with 32 bytes of data: Reply from 192.168.1.18: bytes=32 time=9ms TTL=128 Reply from 192.168.1.18: bytes=32 time<1ms TTL=128 Reply from 192.168.1.18: bytes=32 time<1ms TTL=128 Reply from 192.168.1.18: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.1.18: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 9ms, Average = 2ms	C:\>ping 192.168.1.19 Pinging 192.168.1.19 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.19: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>

1.12 (VLAN 20) to 1.19 (VLAN 20)	1.12 (VLAN 20) to 1.20 ((VLAN 30))
C:\>ping 192.168.1.19 Pinging 192.168.1.19 with 32 bytes of data: Reply from 192.168.1.19: bytes=32 time=9ms TTL=128 Reply from 192.168.1.19: bytes=32 time<1ms TTL=128	C:\>ping 192.168.1.20 Pinging 192.168.1.20 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out.

Reply from 192.168.1.19: bytes=32 time<1ms TTL=128 Reply from 192.168.1.19: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.1.19: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 9ms, Average = 2ms	Ping statistics for 192.168.1.20: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

1.14 (VLAN 30) to 1.20 (VLAN 30)	**1.14 (VLAN 30) to 1.18 (VLAN 10)**
C:\>ping 192.168.1.20 Pinging 192.168.1.20 with 32 bytes of data: Reply from 192.168.1.20: bytes=32 time<1ms TTL=128 Reply from 192.168.1.20: bytes=32 time<1ms TTL=128 Reply from 192.168.1.20: bytes=32 time<1ms TTL=128 Reply from 192.168.1.20: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.1.20: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms	 C:\>ping 192.168.1.18 Pinging 192.168.1.18 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.18: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>

Reference:

https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/routconf.html

https://w7cloud.com/packet-tracer-cisco-commands-list-cli-basic/

https://www.netwrix.com/cisco_commands_cheat_sheet.html

Saleh Al-Moghrabi - YouTube

Greg South - YouTube