Setup:

ASA5510 has 3 Ethernet cables connected to a Cisco 2950 Switch.
E0/0 is connected to an outside router but is not relevant to this story.

E0/1 – Has the Users vlan 202 and the Servers vlan 50
E0/2 – Has many vlans (one for each of our Lab desks) (Vlan 102 to vlan106)
E0/3 – has just the one vlan 210 for management.

The switch provides the layer 2 vLANS only, and does not route.

The ASA does all the routing.

Here are the ASA outputs using the following commands:

terminal pager 0
sh clock
sh run
sh int ip brief
sh ip address
sh ver
sh route

```
ciscoasa# sh run
: Saved
:
: Serial Number: JMX1049K21L
: Hardware:   ASA5510-K8, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.0(4)42
!
hostname ciscoasa
enable password xxxxxxxxxxxxxxx encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd xxxxxxxxxxxxxxxxxx  encrypted
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif Outside-Internet
 security-level 100
 ip address 122.56.33.108 255.255.255.248
!
interface Ethernet0/1
 no nameif
 security-level 100
 no ip address
!
interface Ethernet0/1.50
 vlan 50
 nameif Servers
 security-level 100
 ip address 192.168.50.1 255.255.255.0
!
interface Ethernet0/1.202
 vlan 202
 nameif Users
```

```
 security-level 100
 ip address 192.168.202.1 255.255.255.0
!
interface Ethernet0/2
 no nameif
 security-level 100
 no ip address
!
interface Ethernet0/2.102
 vlan 102
 nameif Pod2
 security-level 100
 ip address 192.168.102.1 255.255.255.0
!
interface Ethernet0/2.103
 vlan 103
 nameif Pod3
 security-level 100
 ip address 192.168.103.1 255.255.255.0
!
interface Ethernet0/2.104
 vlan 104
 nameif Pod4
 security-level 100
 ip address 192.168.104.1 255.255.255.0
!
interface Ethernet0/2.105
 vlan 105
 nameif Pod14
 security-level 100
 ip address 192.168.105.1 255.255.255.0
!
interface Ethernet0/2.107
 vlan 107
 nameif Pod1-Jeff
 security-level 100
 ip address 192.168.107.1 255.255.255.0
!
interface Ethernet0/2.110
 vlan 110
 nameif Pod10
 security-level 100
 ip address 192.168.110.1 255.255.255.0
!
interface Ethernet0/2.115
 vlan 115
 nameif Pod15
 security-level 100
 ip address 192.168.115.1 255.255.255.0
!
interface Ethernet0/2.116
 vlan 116
 nameif Pod16
 security-level 100
 ip address 192.168.116.1 255.255.255.0
!
interface Ethernet0/2.118
 vlan 118
 nameif Pod18
 security-level 100
 ip address 192.168.118.1 255.255.255.0
!
interface Ethernet0/2.119
 vlan 119
 nameif Pod19
 security-level 100
 ip address 192.168.119.1 255.255.255.0
!
interface Ethernet0/2.120
 vlan 120
 nameif Pod20
```

```
 security-level 100
 ip address 192.168.120.1 255.255.255.0
!
interface Ethernet0/2.121
 vlan 121
 nameif Pod21
 security-level 100
 ip address 192.168.121.1 255.255.255.0
!
interface Ethernet0/2.122
 vlan 122
 nameif Pod22
 security-level 100
 ip address 192.168.122.1 255.255.255.0
!
interface Ethernet0/3
 no nameif
 security-level 100
 no ip address
!
interface Ethernet0/3.210
 vlan 210
 nameif ManageInternal
 security-level 100
 ip address 192.168.210.2 255.255.255.0
!
interface Management0/0
 management-only
 no nameif
 security-level 100
 no ip address
!
boot system disk0:/asa904-42-k8.bin
ftp mode passive
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
object-group service DM_INLINE_SERVICE_1
 service-object tcp-udp
 service-object ip
 service-object icmp
 service-object icmp echo
 service-object icmp echo-reply
object-group service DM_INLINE_SERVICE_2
 service-object tcp-udp
 service-object ip
 service-object icmp echo
 service-object icmp echo-reply
 service-object icmp
access-list ManageInternal_access_in extended permit object-group TCPUDP any4 any4
access-list ManageInternal_access_in extended permit ip any4 any4 log
access-list ManageInternal_access_in extended permit icmp any4 any4 object-group DM_INLINE_ICMP_1
access-list ManageInternal_access_in extended permit icmp any4 any4
access-list Servers_access_in extended permit object-group DM_INLINE_SERVICE_1 any4 any4
access-list Servers_access_in extended deny ip any any
access-list Users_access_in extended permit object-group DM_INLINE_SERVICE_2 any4 any4
access-list Users_access_in extended deny ip any4 any4
pager lines 24
logging enable
logging asdm informational
mtu Outside-Internet 1500
mtu Servers 1500
mtu Users 1500
mtu Pod2 1500
mtu Pod3 1500
mtu Pod4 1500
mtu Pod14 1500
mtu Pod1-Jeff 1500
```

```
mtu Pod10 1500
mtu Pod15 1500
mtu Pod16 1500
mtu Pod18 1500
mtu Pod19 1500
mtu Pod20 1500
mtu Pod21 1500
mtu Pod22 1500
mtu ManageInternal 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo Servers
icmp permit any echo-reply Servers
icmp permit any echo Users
icmp permit any echo-reply Users
icmp permit any echo ManageInternal
icmp permit any echo-reply ManageInternal
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group Servers_access_in in interface Servers
access-group Users_access_in in interface Users
access-group ManageInternal_access_in in interface ManageInternal
route Outside-Internet 0.0.0.0 0.0.0.0 122.56.33.110 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 ManageInternal
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 ManageInternal
ssh timeout 60
console timeout 0
vpn-addr-assign local reuse-delay 20
no threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password xxxxxxxxxxxxxxxx encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
```

```
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:0a6252208bea6c2de982747806ae0c10
: end
ciscoasa# sh int ip brief
Interface              IP-Address      OK? Method Status            Protocol
Ethernet0/0            122.56.33.108   YES CONFIG down              down
Ethernet0/1            unassigned      YES unset  up                up
Ethernet0/1.50         192.168.50.1    YES CONFIG up                up
Ethernet0/1.202        192.168.202.1   YES CONFIG up                up
Ethernet0/2            unassigned      YES unset  up                up
Ethernet0/2.102        192.168.102.1   YES CONFIG up                up
Ethernet0/2.103        192.168.103.1   YES CONFIG up                up
Ethernet0/2.104        192.168.104.1   YES CONFIG up                up
Ethernet0/2.105        192.168.105.1   YES CONFIG up                up
Ethernet0/2.107        192.168.107.1   YES CONFIG up                up
Ethernet0/2.110        192.168.110.1   YES CONFIG up                up
Ethernet0/2.115        192.168.115.1   YES CONFIG up                up
Ethernet0/2.116        192.168.116.1   YES CONFIG up                up
Ethernet0/2.118        192.168.118.1   YES CONFIG up                up
Ethernet0/2.119        192.168.119.1   YES CONFIG up                up
Ethernet0/2.120        192.168.120.1   YES CONFIG up                up
Ethernet0/2.121        192.168.121.1   YES CONFIG up                up
Ethernet0/2.122        192.168.122.1   YES CONFIG up                up
Ethernet0/3            unassigned      YES unset  up                up
Ethernet0/3.210        192.168.210.2   YES CONFIG up                up
Management0/0          unassigned      YES unset  down              down
ciscoasa# sh ip address
System IP Addresses:
Interface              Name            IP address      Subnet mask     Method
Ethernet0/0            Outside-Internet      122.56.33.108   255.255.255.248 CONFIG
Ethernet0/1.50         Servers         192.168.50.1    255.255.255.0   CONFIG
Ethernet0/1.202        Users           192.168.202.1   255.255.255.0   CONFIG
Ethernet0/2.102        Pod2            192.168.102.1   255.255.255.0   CONFIG
Ethernet0/2.103        Pod3            192.168.103.1   255.255.255.0   CONFIG
Ethernet0/2.104        Pod4            192.168.104.1   255.255.255.0   CONFIG
Ethernet0/2.105        Pod14           192.168.105.1   255.255.255.0   CONFIG
Ethernet0/2.107        Pod1-Jeff       192.168.107.1   255.255.255.0   CONFIG
Ethernet0/2.110        Pod10           192.168.110.1   255.255.255.0   CONFIG
Ethernet0/2.115        Pod15           192.168.115.1   255.255.255.0   CONFIG
Ethernet0/2.116        Pod16           192.168.116.1   255.255.255.0   CONFIG
Ethernet0/2.118        Pod18           192.168.118.1   255.255.255.0   CONFIG
Ethernet0/2.119        Pod19           192.168.119.1   255.255.255.0   CONFIG
Ethernet0/2.120        Pod20           192.168.120.1   255.255.255.0   CONFIG
Ethernet0/2.121        Pod21           192.168.121.1   255.255.255.0   CONFIG
Ethernet0/2.122        Pod22           192.168.122.1   255.255.255.0   CONFIG
Ethernet0/3.210        ManageInternal        192.168.210.2   255.255.255.0   CONFIG
Current IP Addresses:
Interface              Name            IP address      Subnet mask     Method
Ethernet0/0            Outside-Internet      122.56.33.108   255.255.255.248 CONFIG
Ethernet0/1.50         Servers         192.168.50.1    255.255.255.0   CONFIG
Ethernet0/1.202        Users           192.168.202.1   255.255.255.0   CONFIG
Ethernet0/2.102        Pod2            192.168.102.1   255.255.255.0   CONFIG
Ethernet0/2.103        Pod3            192.168.103.1   255.255.255.0   CONFIG
Ethernet0/2.104        Pod4            192.168.104.1   255.255.255.0   CONFIG
Ethernet0/2.105        Pod14           192.168.105.1   255.255.255.0   CONFIG
Ethernet0/2.107        Pod1-Jeff       192.168.107.1   255.255.255.0   CONFIG
Ethernet0/2.110        Pod10           192.168.110.1   255.255.255.0   CONFIG
Ethernet0/2.115        Pod15           192.168.115.1   255.255.255.0   CONFIG
Ethernet0/2.116        Pod16           192.168.116.1   255.255.255.0   CONFIG
Ethernet0/2.118        Pod18           192.168.118.1   255.255.255.0   CONFIG
Ethernet0/2.119        Pod19           192.168.119.1   255.255.255.0   CONFIG
```

```
Ethernet0/2.120     Pod20           192.168.120.1   255.255.255.0   CONFIG
Ethernet0/2.121     Pod21           192.168.121.1   255.255.255.0   CONFIG
Ethernet0/2.122     Pod22           192.168.122.1   255.255.255.0   CONFIG
Ethernet0/3.210     ManageInternal      192.168.210.2   255.255.255.0   CONFIG
ciscoasa# sh ver


Cisco Adaptive Security Appliance Software Version 9.0(4)42
Device Manager Version 5.2(4)

Compiled on Fri 09-Sep-16 14:51 by builders
System image file is "disk0:/asa904-42-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 52 mins 25 secs

Hardware:   ASA5510-K8, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz,
Internal ATA Compact Flash, 256MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55xx on-board accelerator (revision 0x0)
                Boot microcode      : CN1000-MC-BOOT-2.00
                SSL/IKE microcode   : CNLite-MC-SSLm-PLUS-2.03
                IPSec microcode     : CNlite-MC-IPSECm-MAIN-2.08
                Number of accelerators: 1

 0: Ext: Ethernet0/0        : address is 0019.2f8f.210e, irq 9
 1: Ext: Ethernet0/1        : address is 0019.2f8f.210f, irq 9
 2: Ext: Ethernet0/2        : address is 0019.2f8f.2110, irq 9
 3: Ext: Ethernet0/3        : address is 0019.2f8f.2111, irq 9
 4: Ext: Management0/0      : address is 0019.2f8f.2112, irq 11
 5: Int: Not used           : irq 11
 6: Int: Not used           : irq 5

Licensed features for this platform:
Maximum Physical Interfaces     : Unlimited     perpetual
Maximum VLANs                   : 100           perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active  perpetual
Encryption-DES                  : Enabled       perpetual
Encryption-3DES-AES             : Enabled       perpetual
Security Contexts               : 2             perpetual
GTP/GPRS                        : Disabled      perpetual
AnyConnect Premium Peers        : 2             perpetual
AnyConnect Essentials           : Disabled      perpetual
Other VPN Peers                 : 250           perpetual
Total VPN Peers                 : 250           perpetual
Shared License                  : Disabled      perpetual
AnyConnect for Mobile           : Disabled      perpetual
AnyConnect for Cisco VPN Phone  : Disabled      perpetual
Advanced Endpoint Assessment    : Disabled      perpetual
UC Phone Proxy Sessions         : 2             perpetual
Total UC Proxy Sessions         : 2             perpetual
Botnet Traffic Filter           : Disabled      perpetual
Intercompany Media Engine       : Disabled      perpetual
Cluster                         : Disabled      perpetual

This platform has an ASA 5510 Security Plus license.

Serial Number: JMX1049K21L
Running Permanent Activation Key: 0x5e0a0774 0xa8506e82 0x64b12da8 0xa3187408 0x011be298
Configuration register is 0x1
Configuration last modified by enable_15 at 15:23:29.089 UTC Wed Oct 30 2019
ciscoasa# sh 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    192.168.122.0 255.255.255.0 is directly connected, Pod22
C    192.168.107.0 255.255.255.0 is directly connected, Pod1-Jeff
C    192.168.104.0 255.255.255.0 is directly connected, Pod4
C    192.168.121.0 255.255.255.0 is directly connected, Pod21
C    192.168.120.0 255.255.255.0 is directly connected, Pod20
C    192.168.105.0 255.255.255.0 is directly connected, Pod14
C    192.168.210.0 255.255.255.0 is directly connected, ManageInternal
C    192.168.110.0 255.255.255.0 is directly connected, Pod10
C    192.168.115.0 255.255.255.0 is directly connected, Pod15
C    192.168.202.0 255.255.255.0 is directly connected, Users
C    192.168.102.0 255.255.255.0 is directly connected, Pod2
C    192.168.119.0 255.255.255.0 is directly connected, Pod19
C    192.168.50.0 255.255.255.0 is directly connected, Servers
C    192.168.118.0 255.255.255.0 is directly connected, Pod18
C    192.168.103.0 255.255.255.0 is directly connected, Pod3
C    192.168.116.0 255.255.255.0 is directly connected, Pod16
ciscoasa#
```

Test results:

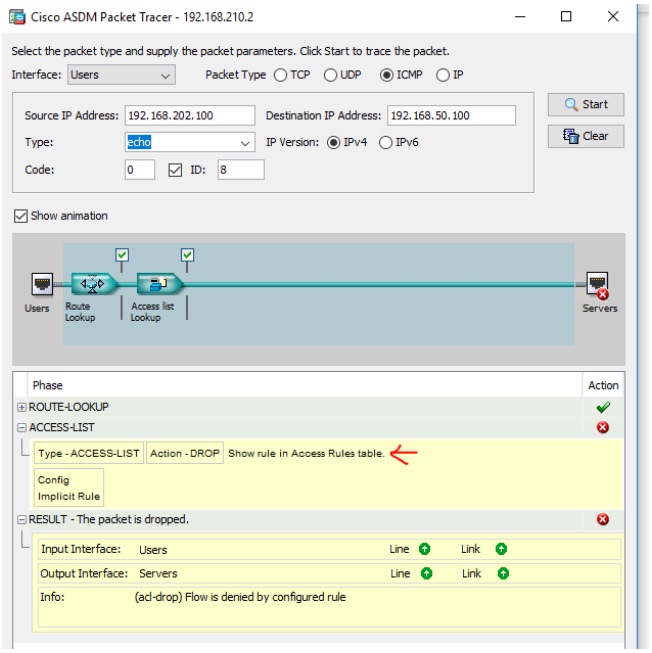
I've concentrated on ping testing:
From a device (192.168.210.100-ManageInternal VLAN) to another device (192.168.50.100-ServersVlan)
From a device (192.168.202.100-ManageInternal VLAN) to another device (192.168.50.100-ServersVlan)

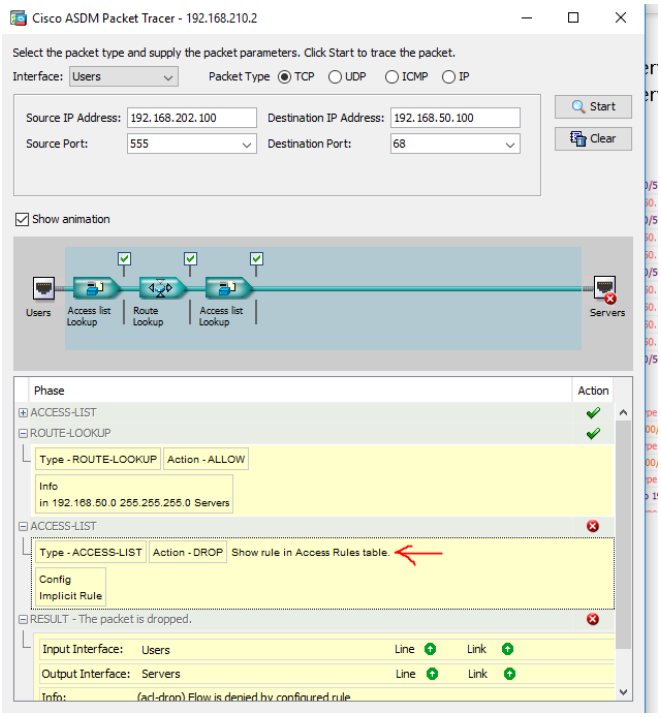
I have also tried telnetting on ports 68 and 23 just to identify the rules in question.

Oct 30 2019	15:30:00	110002	192.168.202.100	53507			Failed to locate egress interface for UDP from Users: 192.168.202.100/53507 to 192.168.1.254/53
Oct 30 2019	15:29:51	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:49	110002	192.168.202.100	54257			Failed to locate egress interface for UDP from Users: 192.168.202.100/54257 to 192.168.1.254/53
Oct 30 2019	15:29:46	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:41	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:37	110002	192.168.202.100	56760			Failed to locate egress interface for UDP from Users: 192.168.202.100/56760 to 192.168.1.254/53
Oct 30 2019	15:29:36	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:31	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:26	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:21	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:29:16	110002	192.168.202.100	56666			Failed to locate egress interface for UDP from Users: 192.168.202.100/56666 to 192.168.1.254/53

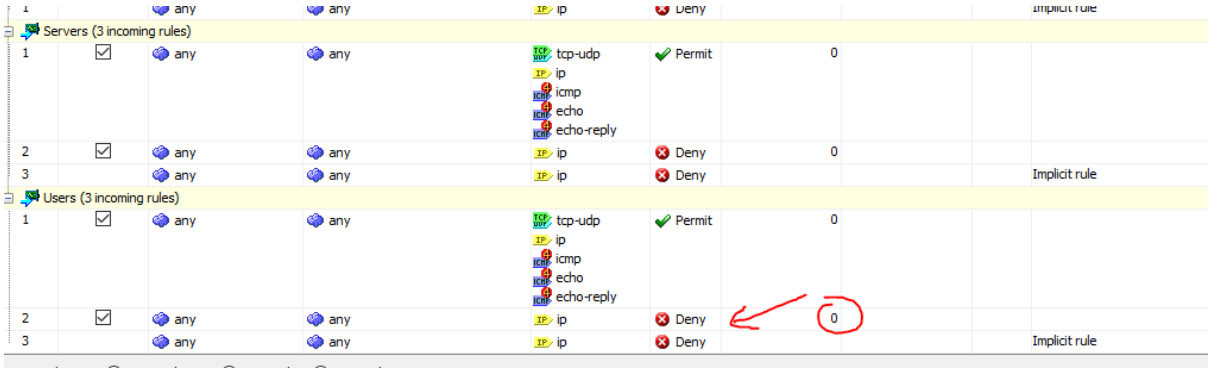
Oct 30 2019	15:06:56	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:06:54	106001	192.168.202.100	49159	192.168.50.100	68	Inbound TCP connection denied from 192.168.202.100/49159 to 192.168.50.100/68 flags SYN on interface Users
Oct 30 2019	15:06:51	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:06:51	106001	192.168.202.100	49159	192.168.50.100	68	Inbound TCP connection denied from 192.168.202.100/49159 to 192.168.50.100/68 flags SYN on interface Users
Oct 30 2019	15:06:46	106014	192.168.202.100		192.168.50.100		Deny inbound icmp src Users: 192.168.202.100 dst Servers: 192.168.50.100 (type 8, code 0)
Oct 30 2019	15:06:41	110002	192.168.202.100	56811			Failed to locate egress interface for UDP from Users: 192.168.202.100/56811 to 192.168.1.254/53

When a do a packet trace:





In both cases the packet tracer blames the following deny rule:
But you can see that I have allowed all ping and tcp/udp so why does it deny???:
I also find it odd that the hit count does not rise??:



From the two test devices 192.168.202.100/24 and 192.168.50.100/24, I can ping their respective default gateways 192.168.202.1/24 and 192.168.50.1/24 which happen to be the interfaces on the ASA: See the successful output from packet tracer: