

## CS581 (Computer & Network Security)

### Lab-03

---

#### **Group No.: 05**

Group Members:

- 01. Rajnish Kumar (CIN: 304470392)
- 02. Jay Purohit (CIN: 304455065)
- 03. Rupal Jaiswal (CIN: 304442169)
- 04. Gaurav Prajapati (CIN: 304470132)

## Firewall

Place one computer on the outside interface and a server on inside interface of a Cisco firewall. Configure the firewall to block outside users from initiating any connection to the inside server except through TCP port 445. Turn on logging and submit copy of firewall config file and output of “show logging” as evidence that firewall is blocking all conversations initiated from outside except for file share. You may need to create a network share on the server and mount the shared folder from the client computer

<http://web.calstatela.edu/faculty/egean/cs581/cisco-asa5505-firewall/>

---

We are really sorry for this lab. We had some firewall router issues and we don't know **how flash memory has been erased from firewall router** and due to this problem, we were unable to perform this lab. I also asked professor regarding this issue and finally on Tuesday i.e. 11/17/2018, the firewall router issue been resolved and we did lab on same day when that issue was resolved. I will also submit the proof regarding our firewall problem and how it's been resolved so please don't consider this lab as delay.

---

We, Group No. 5, performed this lab in below steps:

Step 1: Firewall Router Setup [in further labs, if it happens then this step will be very useful]

Step 2: Inside Server Network Configuration

Step 3: Creation of Network Objects

Step 4: Interfaces Configuration

Step 5: Static Routes Configuration

Step 6: Configuration of NAT Rules

Step 7: Configuration of Access Rules

Step 8: Creating a network share and mounting the shared folder

Step 9: Logging screenshots

Step 10: Some Misc. Screenshots

---

## Step 1: Firewall Router Setup

---

We did following steps to set up firewall router:

1. We connected the serial wire of firewall to our laptop.
2. Downloaded the putty software and connected the firewall router on COM3 from the laptop
3. Download Solarwind TFTP Server software.
4. Download asa831-k8.bin and asdm-743.bin
5. Copied asa831-k8.bin and asdm-743.bin to C:/TFTP-Root folder
6. Network Setting: IPV4 Configuration: IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1
7. Firewall appeared first on putty as rommon mode
8. Below command was fired on rommon mode:  
rommon> ADDRESS=192.168.1.10  
rommon> SERVER=192.168.1.1  
rommon> GATEWAY=192.168.1.1  
rommon> PORT=Ethernet0/0

and then

- ```
rommon> tftp
```
9. Now, we are in ciscoasa> mode
  10. Following configuration has been done on ciscoasm mode:

```
ciscoasa> en
ciscoasa# config t
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# no switchport access vlan 2
ciscoasa(config-if)# interface Ethernet0/0
ciscoasa(config-if)# switchport access vlan 1
ciscoasa(config-if)# exit
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)# exit
ciscoasa# copy tftp flash
    => IP: 192.168.1.1
    => Source: asa831-k8.bin
    => Destination: asa831-k8.bin
```

```

ciscoasa# copy tftp flash
⇒ IP: 192.168.1.1
⇒ Source: asdm-743.bin
⇒ Destination: asdm-743.bin
ciscoasa# config t
ciscoasa(config)# boot system disk0://asa831-k8.bin
ciscoasa(config)# asdm image disk0://asdm-743.bin
ciscoasa(config)# write memory
ciscoasa(config)# show running-config boot system

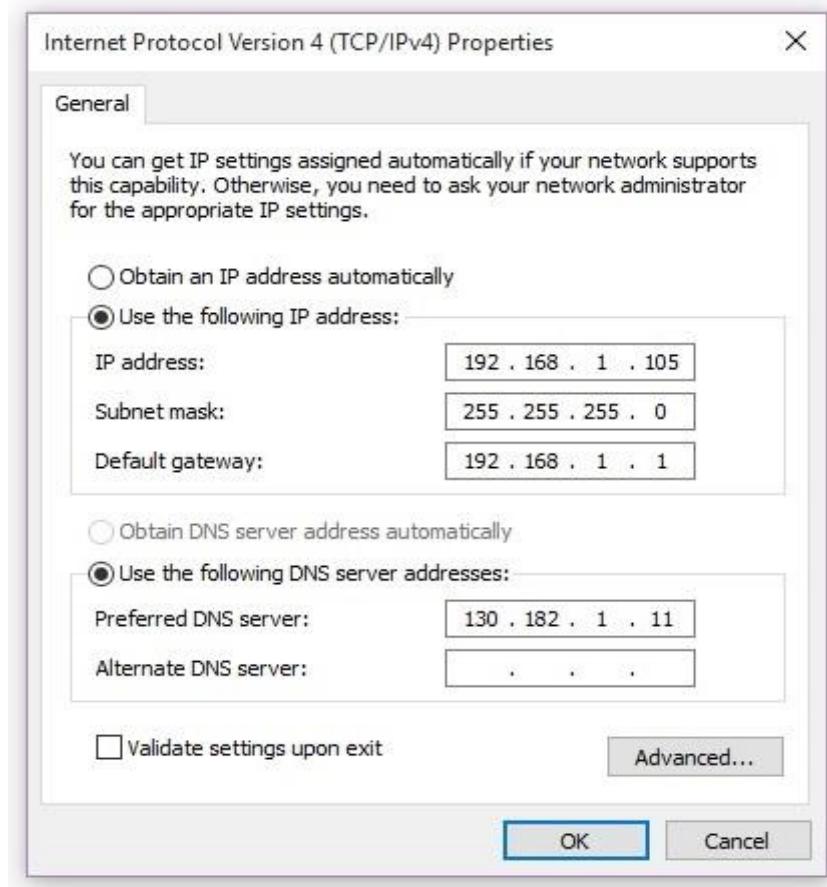
```

11. reload
12. show version

⇒ Hence, setup of firewall router done and asa-831-k8.bin and asdm-743.bin has been saved in firewall's flash memory.

## Step 2: Inside Server Network Configuration

Following screenshot shows the inside server network configuration and steps performed:



 There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

 [Click here to close this webpage.](#)

 [Continue to this website \(not recommended\).](#)

 [More information](#)

# Cisco ASDM 7.4(3)

Cisco ASDM 7.4(3) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

## Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

[Install ASDM Launcher](#)

## Run Cisco ASDM as a Java Web Start application

Java Web Start is required to run ASDM, but it is not installed on this computer.

[Install Java Web Start](#)

Copyright © 2006-2015 Cisco Systems, Inc. All rights reserved.

## Step 3: Creation of Network Objects

- All Network Objects

The screenshot shows the Cisco ASDM 7.4 interface for ASA, specifically the 'Network Objects/Groups' configuration page under the 'Firewall' section. The left sidebar lists various firewall configurations, with 'Network Objects/Groups' selected. The main pane displays a table of network objects, categorized by type (IPv4 and IPv6). The table includes columns for Name, IP Address, Netmask, Description, and Object NAT Address.

| Name            | IP Address    | Netmask       | Description | Object NAT Address |
|-----------------|---------------|---------------|-------------|--------------------|
| any             |               |               |             |                    |
| inside-network  | 192.168.1.0   | 255.255.255.0 |             |                    |
| outside-network | 10.86.44.0    | 255.255.255.0 |             |                    |
| 10.86.44.156    | 10.86.44.156  |               |             |                    |
| G5_Inside       | 192.168.1.105 |               |             |                    |
| G5_Outside      | 10.86.44.151  |               |             |                    |
| obj_any         | 0.0.0.0       | 0.0.0.0       |             | outside (P)        |
| any             |               |               |             |                    |

At the bottom of the interface, there are 'Apply' and 'Reset' buttons, and a status bar showing the user is 'admin' with session ID '15'. The Windows taskbar at the bottom includes icons for File Explorer, Google Chrome, and Internet Explorer, along with the date and time (11/17/2015 5:46:16 PM UTC).

- Network Object Configuration of 10.86.44.156 (will used for file sharing)

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help Type topic to search Go

Home Configuration Monitoring Save Refresh Back Forward Help

**Firewall**

Configuration > Firewall > Objects > Network Objects/Groups

Add Edit Delete Where Used Not Used

Filter: Filter|Clear

| Name            | IP Address    | Netmask       | Description | Object NAT Address |
|-----------------|---------------|---------------|-------------|--------------------|
| any             |               |               |             |                    |
| inside-network  | 192.168.1.0   | 255.255.255.0 |             |                    |
| outside-network | 10.86.44.0    | 255.255.255.0 |             |                    |
| 10.86.44.156    | 10.86.44.156  |               |             |                    |
| G5_Inside       | 192.168.1.105 |               |             |                    |
| G5_Outside      | 10.86.44.151  |               |             |                    |
| obj_any         | 0.0.0.0       | 0.0.0.0       |             | outside (P)        |
| any             |               |               |             |                    |

**Edit Network Object**

Name: 10.86.44.156

Type: Host

IP Version:  IPv4  IPv6

IP Address: 10.86.44.156

Description:

NAT

OK Cancel Help

Apply Reset

<admin> 15 11/17/15 5:47:06 PM UTC

Search the web and Windows

Windows Taskbar icons: File Explorer, Google Chrome, Microsoft Edge, Internet Explorer, FileZilla, and others.

- Network Object Configuration of G5\_Inside (Laptop is working as Inside server)

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Type topic to search Go

Home Configuration Monitoring Save Refresh Back Forward Help

**Firewall**

Configuration > Firewall > Objects > Network Objects/Groups

Add Edit Delete Where Used Not Used

Filter: Filter Clear

| Name             | IP Address           | Netmask       | Description | Object NAT Address |
|------------------|----------------------|---------------|-------------|--------------------|
| any              |                      |               |             |                    |
| inside-network   | 192.168.1.0          | 255.255.255.0 |             |                    |
| outside-network  | 10.86.44.0           | 255.255.255.0 |             |                    |
| 10.86.44.156     | 10.86.44.156         |               |             |                    |
| <b>G5_Inside</b> | <b>192.168.1.105</b> |               |             |                    |
| G5_Outside       | 10.86.44.151         |               |             |                    |
| obj_any          | 0.0.0.0              | 0.0.0.0       |             | outside (P)        |
| any              |                      |               |             |                    |

**Edit Network Object**

Name: G5\_Inside

Type: Host

IP Version:  IPv4  IPv6

IP Address: 192.168.1.105

Description:

NAT

OK Cancel Help

Apply Reset

Device List

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Objects
- Network Objects/Groups**
- Service Objects/Groups
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Search the web and Windows

11/17/15 5:47:46 PM UTC

5:46 PM 11/17/2015

- Network Object Configuration of G5\_Outside (Desktop is working as outside)

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Type topic to search Go

Cisco

**Firewall**

Device List

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Firewall > Objects > Network Objects/Groups

Add Edit Delete Where Used Not Used Filter Clear

Filter:

| Name            | IP Address    | Netmask       | Description | Object NAT Address |
|-----------------|---------------|---------------|-------------|--------------------|
| any             |               |               |             |                    |
| inside-network  | 192.168.1.0   | 255.255.255.0 |             |                    |
| outside-network | 10.86.44.0    | 255.255.255.0 |             |                    |
| 10.86.44.156    | 10.86.44.156  |               |             |                    |
| G5_Inside       | 192.168.1.105 |               |             |                    |
| G5_Outside      | 10.86.44.151  |               |             | outside (P)        |
| obj_any         | 0.0.0.0       | 0.0.0.0       |             |                    |

**Edit Network Object**

Name: G5\_Outside

Type: Host

IP Version:  IPv4  IPv6

IP Address: 10.86.44.151

Description:

NAT

OK Cancel Help

Apply Reset

11/17/15 5:48:06 PM UTC

Windows Search the web and Windows

11/17/2015 5:47 PM

## Step 4: Interfaces Configuration

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help Type topic to search Go

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interfaces

Device List

Startup Wizard

Interfaces

Routing

Static Routes

Route Maps

IPv4 Prefix Rules

OSPF

RIP

EIGRP

Multicast

Proxy ARP

Device Name/Password

System Time

Interfaces Switch Ports

| Name    | Switch Ports                    | Enabled | Security Level | IP Address   | Subnet Mask Prefix Length | Restrict Traffic flow | VLAN  | Management Only | MTU   | Active MAC Address |
|---------|---------------------------------|---------|----------------|--------------|---------------------------|-----------------------|-------|-----------------|-------|--------------------|
| inside  | Ethernet0/1, Ethernet0/2, Et... | Yes     | 100            | 192.168.1.1  | 255.255.255.0             |                       | vlan1 | No              | 1,500 |                    |
| outside | Ethernet0/0                     | Yes     | 0              | 10.86.44.151 | 255.255.255.0             |                       | vlan2 | No              | 1,500 |                    |

Add Edit Delete

Device Setup Firewall Remote Access VPN Site-to-Site VPN Device Management

Enable traffic between two or more interfaces which are configured with same security levels  
 Enable traffic between two or more hosts connected to the same interface

Apply Reset

<admin> 15 6:13 PM 11/17/2015

Search the web and Windows

6:13 PM 11/17/2015

## Step 5: Static Routes Configuration

The screenshot shows the Cisco ASDM 7.4 interface for ASA. The title bar reads "Cisco ASDM 7.4 for ASA - 192.168.1.1". The menu bar includes File, View, Tools, Wizards, Window, Help, and a search bar "Type topic to search Go". The top navigation bar has links for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. The main window title is "Configuration > Device Setup > Routing > Static Routes". On the left, a tree view shows "Device List" with nodes like Startup Wizard, Interfaces, Routing, Static Routes (selected), Route Maps, OSPF, RIP, EIGRP, Multicast, Proxy ARP, Device Name/Password, and System Time. Below the tree is a sidebar with icons for Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management. The main content area displays a table titled "Specify static routes." with the following data:

| Interface | IP Address | Netmask/<br>Prefix Length | Gateway IP   | Metric/<br>Distance | Options |
|-----------|------------|---------------------------|--------------|---------------------|---------|
| outside   | 0.0.0.0    | 0.0.0.0                   | 10.86.44.151 | 1                   | None    |

Buttons on the right side of the table include Add, Edit, and Delete. At the bottom of the main window are Apply and Reset buttons. The status bar at the bottom shows "11/17/15 6:15:16 PM UTC" and other system information.

## Step 6: Configuration of NAT Rules

- outside (up: please check the screenshot as selected and in bottom, diagram is also shown)

Screenshot of Cisco ASDM 7.4 for ASA - 192.168.1.1 showing the configuration of NAT Rules.

The interface shows the Firewall > NAT Rules configuration screen. The left sidebar lists various firewall configurations like Access Rules, NAT Rules, Service Policy Rules, etc. The main pane displays two NAT rules:

| #                             | Source Intf | Dest Intf | Source  | Destination | Service | Source            | Destination | Service       | Option        |
|-------------------------------|-------------|-----------|---------|-------------|---------|-------------------|-------------|---------------|---------------|
| 1                             | outside     | outside   | any     | G5_Inside   | any     | - Original - (\$) | G5_Outside  | - Original -  |               |
|                               | outside     | outside   | any     | G5_Outside  | any     | G5_Inside (\$)    | any         | - Original -- | - Original -- |
| "Network Object" NAT (Rule 2) |             |           |         |             |         |                   |             |               |               |
| 2                             | inside      | outside   | obj_any | any         | any     | any               | outside (P) | - Original -- | - Original -- |

The right pane shows the Address and Services tabs. The Addresses tab lists network objects including IPv4 and IPv6 objects. The Services tab lists various service definitions.

Below the configuration pane, a network diagram illustrates the ASA's connection to the outside world. It shows an external interface labeled "any" connected to the ASA's "outside" interface, which is then connected to another "outside" interface labeled "G5\_Outside" with the IP address "10.86.44.151". A "Static" connection is shown between the ASA's "outside" interface and the external "outside" interface.

At the bottom, there are "Apply" and "Reset" buttons, and a status bar showing the user is "admin" with session ID "15". The system date and time are also displayed at the bottom right.

- outside (down: please check the screenshot as selected and in bottom, diagram is also shown)

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help Type topic to search Go

Home Configuration Monitoring Save Refresh Back Forward Help

**Firewall**

Device List

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Objects
  - Network Objects/Groups
  - Service Objects/Groups
  - Class Maps
  - Inspect Maps
  - Regular Expressions
  - TCP Maps
  - Time Ranges
- Unified Communications
- Advanced

**Configuration > Firewall > NAT Rules**

Add Edit Delete Find Diagram Packet Trace

| Match Criteria: Original Packet |             |           |            |             | Action: Translated Packet |                    |                |                |        |
|---------------------------------|-------------|-----------|------------|-------------|---------------------------|--------------------|----------------|----------------|--------|
| #                               | Source Intf | Dest Intf | Source     | Destination | Service                   | Source             | Destination    | Service        | Option |
| 1                               | outside     | outside   | any        | G5_Inside   | any                       | -- Original - (\$) | G5_Outside     | -- Original -- |        |
|                                 | outside     | outside   | G5_Outside | any         | any                       | G5_Inside (\$)     | -- Original -- | -- Original -- |        |
| Network Object* NAT (Rule 2)    |             |           |            |             |                           |                    |                |                |        |
| 2                               | inside      | outside   | obj_any    | any         | any                       | outside (?)        | -- Original -- | -- Original -- |        |

Filter: Filter/Clear

Name

- IPv4 Network Objects
  - any
  - inside-network/24
  - outside-network/24
  - 10.86.44.156
  - G5\_Inside
  - G5\_Outside
  - obj\_any
- IPv6 Network Objects
  - any

The diagram shows a central blue circle representing the ASA firewall. It has two horizontal connections labeled "outside" at both ends. The left connection is labeled "G5\_Outside" and "10.86.44.151". The right connection is labeled "G5\_Inside". A yellow double-headed arrow labeled "Static" connects the two "outside" ports. The "G5\_Inside" port is connected to a blue oval representing the "inside" network.

Apply Reset

<admin> 15 11/17/15 6:06:26 PM UTC 6:05 PM 11/17/2015

Search the web and Windows

## Step 7: Configuration of Access Rules

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

**Firewall**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Objects
  - Network Objects/Groups
  - Service Objects/Groups
  - Class Maps
  - Inspect Maps
  - Regular Expressions
  - TCP Maps
  - Time Ranges
- Unified Communications
- Advanced

Configuration > Firewall > Access Rules

Add Edit Delete Up Down Find Diagram Export Clear Hits Show Log Packet Trace

| #                          | Enabled                             | Source Criteria:                            | Destination Criteria:                         | Service                                  | Action                                     | Hits | Logging | Time | Description   |
|----------------------------|-------------------------------------|---------------------------------------------|-----------------------------------------------|------------------------------------------|--------------------------------------------|------|---------|------|---------------|
| inside (1 incoming rule)   |                                     |                                             |                                               |                                          |                                            |      |         |      |               |
| 1                          | <input checked="" type="checkbox"/> | <input checked="" type="radio"/> any        | <input checked="" type="radio"/> G5_Inside    | <input checked="" type="radio"/> TCP     | <input checked="" type="checkbox"/> Deny   | 0    |         |      |               |
| outside (2 incoming rules) |                                     |                                             |                                               |                                          |                                            |      |         |      |               |
| 1                          | <input checked="" type="checkbox"/> | <input checked="" type="radio"/> any        | <input checked="" type="radio"/> 10.86.44.156 | <input checked="" type="radio"/> TCP 445 | <input checked="" type="checkbox"/> Permit | 10   |         |      |               |
| 2                          | <input checked="" type="checkbox"/> | <input checked="" type="radio"/> G5_Outside | <input checked="" type="radio"/> G5_Inside    | <input checked="" type="radio"/> TCP 445 | <input checked="" type="checkbox"/> Permit | 21   |         |      |               |
| Global (1 implicit rule)   |                                     |                                             |                                               |                                          |                                            |      |         |      |               |
| 1                          |                                     | <input checked="" type="radio"/> any        | <input checked="" type="radio"/> any          | <input checked="" type="radio"/> IP      | <input checked="" type="checkbox"/> Deny   |      |         |      | Implicit rule |

Access Rule Type  IPv4 and IPv6  IPv4 Only  IPv6 Only

Diagram showing the flow of traffic from 'any' source through the 'inside' interface to 'G5\_Inside' (192.168.1.105) via TCP port 445. The action is 'Deny'.

Apply Reset Advanced...

Addresses Services Time Ranges

Addresses

Add Edit Delete Where Used Not Used

Filter: Filter Clear

Name

IPv4 Network Objects

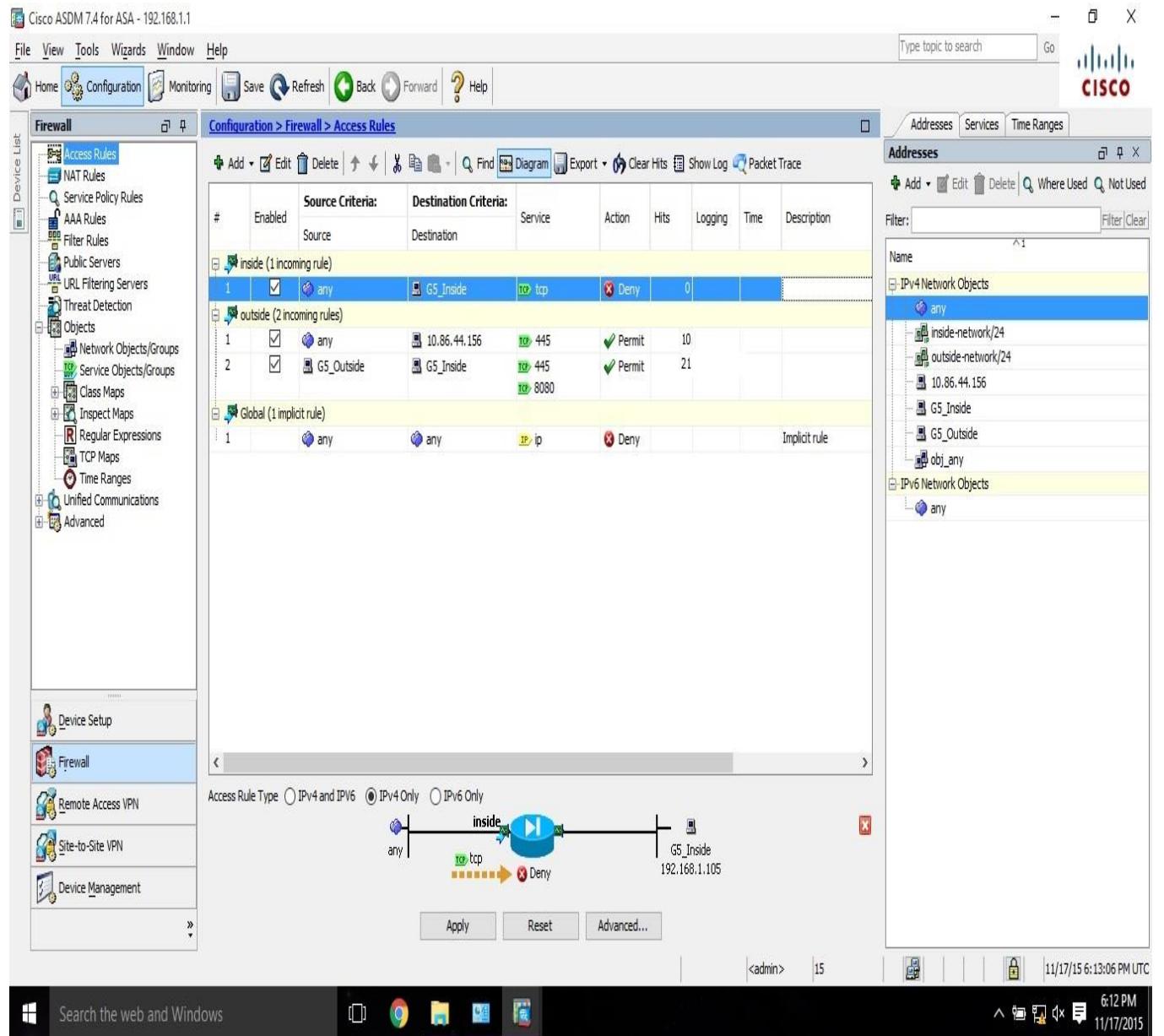
- any
  - inside-network/24
  - outside-network/24
  - 10.86.44.156
  - G5\_Inside
  - G5\_Outside
  - obj\_any

IPv6 Network Objects

- any

<admin> 15 11/17/15 6:13:06 PM UTC 6:12 PM 11/17/2015

Search the web and Windows



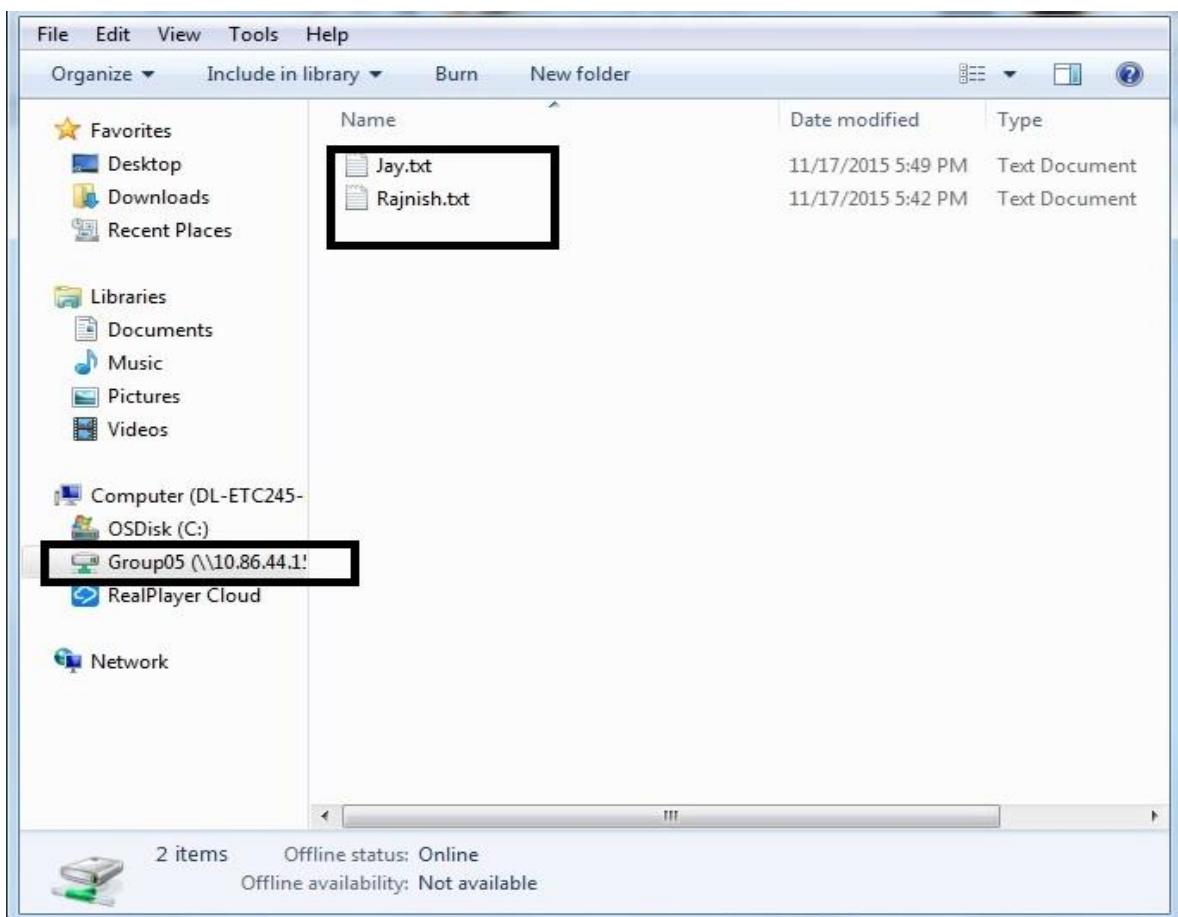
## Step 8: Creating a network share and mounting the shared folder

---

Steps:

- ⇒ telnet 10.86.44.156 445 from outside machine first
- ⇒ if it is logging then do the below navigations:
  - Server side
    - Create a folder “Group05”
    - Right click on “Group05”
    - Properties
    - Select “Sharing” tab
    - Click “Share”
    - Give the permission as “Everyone”
    - Click “Done” -> Close
  - Client side:
    - Open My Computer
    - Add a Network Location
    - Path: \\10.86.44.156\Group05

Below is the screenshot of mounted folder as named: **Group05**



## Step 9: Logging screenshots

Real-Time Log Viewer - 192.168.1.1

File Tools Window Help

Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help

Filter By: Filter Build Filter Show All Find:

| Severity | Date        | Time     | Syslog ID | Source IP     | Source Port | Destination IP | Destination Port | Description                                                                                                                         |
|----------|-------------|----------|-----------|---------------|-------------|----------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 6        | Nov 17 2015 | 17:36:02 | 725002    | 192.168.1.105 | 18205       |                |                  | Device completed SSL handshake with client inside:192.168.1.105/18205                                                               |
| 6        | Nov 17 2015 | 17:36:02 | 725001    | 192.168.1.105 | 18205       |                |                  | Starting SSL handshake with client inside:192.168.1.105/18205 for TLSv1 session.                                                    |
| 6        | Nov 17 2015 | 17:36:02 | 302013    | 192.168.1.105 | 18205       | 192.168.1.1    | 443              | Built inbound TCP connection 652 for inside:192.168.1.105/18205 (192.168.1.105/18205) to identity:192.168.1.1/443 (192.168.1.1/443) |
| 6        | Nov 17 2015 | 17:35:55 | 302010    |               |             |                |                  | 2 in use, 13 most used                                                                                                              |
| 4        | Nov 17 2015 | 17:35:50 | 106023    | 192.168.1.105 | 55059       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/55059 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:46 | 106023    | 192.168.1.105 | 55059       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/55059 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:44 | 106023    | 192.168.1.105 | 55059       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/55059 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:43 | 106023    | 192.168.1.105 | 55059       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/55059 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:42 | 106023    | 192.168.1.105 | 55059       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/55059 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:36 | 106023    | 192.168.1.105 | 60635       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/60635 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:32 | 106023    | 192.168.1.105 | 60635       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/60635 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:30 | 106023    | 192.168.1.105 | 60635       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/60635 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:29 | 106023    | 192.168.1.105 | 60635       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/60635 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 4        | Nov 17 2015 | 17:35:28 | 106023    | 192.168.1.105 | 60635       | 130.182.1.11   | 53               | Deny udp src inside:192.168.1.105/60635 dst outside:130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 6        | Nov 17 2015 | 17:35:21 | 725007    | 192.168.1.105 | 18204       |                |                  | SSL session with client inside:192.168.1.105/18204 terminated.                                                                      |
| 6        | Nov 17 2015 | 17:35:21 | 106015    | 192.168.1.105 | 18204       | 192.168.1.1    | 443              | Deny TCP (no connection) from 192.168.1.105/18204 to 192.168.1.1/443 flags FIN ACK on interface inside                              |
| 6        | Nov 17 2015 | 17:35:21 | 302014    | 192.168.1.105 | 18204       | 192.168.1.1    | 443              | Teardown TCP connection 651 for inside:192.168.1.105/18204 to identity:192.168.1.1/443 duration 0:00:00 bytes 1097 TCP Reset-0      |
| 5        | Nov 17 2015 | 17:35:21 | 111007    |               |             |                |                  | Begin configuration: 192.168.1.105 reading from http [POST]                                                                         |
| 6        | Nov 17 2015 | 17:35:21 | 605005    | 192.168.1.105 | 18204       | 192.168.1.1    | https            | Login permitted from 192.168.1.105/18204 to inside:192.168.1.1/https for user "enable_15"                                           |
| 6        | Nov 17 2015 | 17:35:21 | 725002    | 192.168.1.105 | 18204       |                |                  | Device completed SSL handshake with client inside:192.168.1.105/18204                                                               |
| 6        | Nov 17 2015 | 17:35:21 | 725001    | 192.168.1.105 | 18204       |                |                  | Starting SSL handshake with client inside:192.168.1.105/18204 for TLSv1 session.                                                    |
| 6        | Nov 17 2015 | 17:35:21 | 302013    | 192.168.1.105 | 18204       | 192.168.1.1    | 443              | Built inbound TCP connection 651 for inside:192.168.1.105/18204 (192.168.1.105/18204) to identity:192.168.1.1/443 (192.168.1.1/443) |

Syslog Details

#ASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.

The ASA discarded a TCP packet that has no associated connection in the ASA connection table. The ASA looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the ASA

Explanation Recommended Action Details

Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

Search the web and Windows

6:15 PM  
11/17/2015

Real-Time Log Viewer - 192.168.1.1

**File Tools Window Help**

**Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help**

**Filter By:** Filter Build Filter Show All Find:

| Severity | Date        | Time     | Syslog ID | Source IP     | Source Port | Destination IP | Destination Port | Description                                                                                                                      |
|----------|-------------|----------|-----------|---------------|-------------|----------------|------------------|----------------------------------------------------------------------------------------------------------------------------------|
| !        | Nov 17 2015 | 18:18:05 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Teardown ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                     |
| !        | Nov 17 2015 | 18:18:03 | 302020    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Built inbound ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                |
| !        | Nov 17 2015 | 18:18:00 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Teardown ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                     |
| !        | Nov 17 2015 | 18:17:58 | 302020    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Built inbound ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                |
| !        | Nov 17 2015 | 18:17:55 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Teardown ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                     |
| !        | Nov 17 2015 | 18:17:55 | 405001    |               |             |                |                  | Received ARP request collision from 10.86.44.151/6c62.6d50.51aa on interface outside                                             |
| !        | Nov 17 2015 | 18:17:53 | 302020    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Built inbound ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                |
| !        | Nov 17 2015 | 18:17:51 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Teardown ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                     |
| !        | Nov 17 2015 | 18:17:49 | 302020    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Built inbound ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                |
| !        | Nov 17 2015 | 18:16:50 | 106023    | 192.168.1.105 | 61429       | 130.182.1.11   | 53               | Deny udp src inside: 192.168.1.105/61429 dst outside: 130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]              |
| !        | Nov 17 2015 | 18:16:46 | 106023    | 192.168.1.105 | 61429       | 130.182.1.11   | 53               | Deny udp src inside: 192.168.1.105/61429 dst outside: 130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]              |
| !        | Nov 17 2015 | 18:16:44 | 106023    | 192.168.1.105 | 61429       | 130.182.1.11   | 53               | Deny udp src inside: 192.168.1.105/61429 dst outside: 130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]              |
| !        | Nov 17 2015 | 18:16:44 | 405001    |               |             |                |                  | Received ARP request collision from 10.86.44.151/6c62.6d50.51aa on interface outside                                             |
| !        | Nov 17 2015 | 18:16:43 | 106023    | 192.168.1.105 | 61429       | 130.182.1.11   | 53               | Deny udp src inside: 192.168.1.105/61429 dst outside: 130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]              |
| !        | Nov 17 2015 | 18:16:42 | 106023    | 192.168.1.105 | 61429       | 130.182.1.11   | 53               | Deny udp src inside: 192.168.1.105/61429 dst outside: 130.182.1.11/53 by access-group "inside_access_in" [0x0, 0x0]              |
| !        | Nov 17 2015 | 18:16:00 | 302010    |               |             |                |                  | 2 in use, 13 most used                                                                                                           |
| !        | Nov 17 2015 | 18:15:56 | 725007    | 192.168.1.105 | 18236       |                |                  | SSL session with client inside: 192.168.1.105/18236 terminated.                                                                  |
| !        | Nov 17 2015 | 18:15:56 | 106015    | 192.168.1.105 | 18236       | 192.168.1.1    | 443              | Deny TCP (no connection) from 192.168.1.105/18236 to 192.168.1.1/443 flags FIN ACK on interface inside                           |
| !        | Nov 17 2015 | 18:15:56 | 302014    | 192.168.1.105 | 18236       | 192.168.1.1    | 443              | Teardown TCP connection 683 for inside: 192.168.1.105/18236 to identity: 192.168.1.1/443 duration 0:00:00 bytes 1097 TCP Reset-0 |
| !        | Nov 17 2015 | 18:15:56 | 111007    |               |             |                |                  | Begin configuration: 192.168.1.105 reading from http [POST]                                                                      |
| !        | Nov 17 2015 | 18:15:56 | 605005    | 192.168.1.105 | 18236       | 192.168.1.1    | https            | Login permitted from 192.168.1.105/18236 to inside: 192.168.1.1/https for user "enable_15"                                       |
| !        | Nov 17 2015 | 18:15:56 | 725002    | 192.168.1.105 | 18236       |                |                  | Device completed SSL handshake with client inside: 192.168.1.105/18236                                                           |
| !        | Nov 17 2015 | 18:15:56 | 725001    | 192.168.1.105 | 18236       |                |                  | Starting SSL handshake with client inside: 192.168.1.105/18236 for TLSv1 session                                                 |

**Syslog Details**

ASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.

The ASA discarded a TCP packet that has no associated connection in the ASA connection table. The ASA looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the ASA will drop the packet.

**Explanation Recommended Action Details**

**Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging**

Search the web and Windows

6:17 PM 11/17/2015

Real-Time Log Viewer - 192.168.1.1

**File Tools Window Help**

**Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help**

**Filter By:** Filter Build Filter Show All Find:

| Severity | Date        | Time     | Syslog ID | Source IP     | Source Port | Destination IP | Destination Port | Description                                                                                                                           |
|----------|-------------|----------|-----------|---------------|-------------|----------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| 6        | Nov 17 2015 | 18:20:19 | 106023    | 10.86.44.151  | 60129       | 192.168.1.105  | 53               | Deny udp src inside: 10.86.44.151/60129 dst outside: 192.168.1.105/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 6        | Nov 17 2015 | 18:20:15 | 106023    | 10.86.44.151  | 60129       | 192.168.1.105  | 53               | Deny udp src inside: 10.86.44.151/60129 dst outside: 192.168.1.105/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 6        | Nov 17 2015 | 18:20:13 | 106023    | 10.86.44.151  | 60129       | 192.168.1.105  | 53               | Deny udp src inside: 10.86.44.151/60129 dst outside: 192.168.1.105/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 6        | Nov 17 2015 | 18:20:12 | 106023    | 10.86.44.151  | 60129       | 192.168.1.105  | 53               | Deny udp src inside: 10.86.44.151/60129 dst outside: 192.168.1.105/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 6        | Nov 17 2015 | 18:20:11 | 106023    | 10.86.44.151  | 60129       | 192.168.1.105  | 53               | Deny udp src inside: 10.86.44.151/60129 dst outside: 192.168.1.105/53 by access-group "inside_access_in" [0x0, 0x0]                   |
| 6        | Nov 17 2015 | 18:20:08 | 302021    | 192.168.1.105 | 0           | 192.168.1.1    | 31679            | Tear down ICMP connection for faddr 192.168.1.105/0 gaddr 192.168.1.1/31679 laddr 192.168.1.1/31679                                   |
| 5        | Nov 17 2015 | 18:20:08 | 111010    |               |             |                |                  | User 'enable_15' running 'CLI' from IP 0.0.0.0, executed 'ping 192.168.1.105'                                                         |
| 5        | Nov 17 2015 | 18:20:08 | 111008    |               |             |                |                  | User 'enable_15' executed the 'ping 192.168.1.105' command.                                                                           |
| 6        | Nov 17 2015 | 18:20:08 | 302020    | 192.168.1.1   | 31679       | 192.168.1.105  | 0                | Built outbound ICMP connection for faddr 192.168.1.105/0 gaddr 192.168.1.1/31679 laddr 192.168.1.1/31679                              |
| 6        | Nov 17 2015 | 18:20:02 | 405001    |               |             |                |                  | Received ARP request collision from 10.86.44.151/6c62.6d50.51aa on interface outside                                                  |
| 6        | Nov 17 2015 | 18:19:56 | 725007    | 192.168.1.105 | 18237       |                |                  | SSL session with client inside: 192.168.1.105/18237 terminated.                                                                       |
| 6        | Nov 17 2015 | 18:19:56 | 106015    | 192.168.1.105 | 18237       | 192.168.1.1    | 443              | Deny TCP (no connection) from 192.168.1.105/18237 to 192.168.1.1/443 flags FIN ACK on interface inside                                |
| 6        | Nov 17 2015 | 18:19:56 | 302014    | 192.168.1.105 | 18237       | 192.168.1.1    | 443              | Tear down TCP connection 688 for inside: 192.168.1.105/18237 to identity: 192.168.1.1/443 duration 0:00:00 bytes 1097 TCP Reset-0     |
| 5        | Nov 17 2015 | 18:19:56 | 111007    |               |             |                |                  | Begin configuration: 192.168.1.105 reading from http [POST]                                                                           |
| 6        | Nov 17 2015 | 18:19:56 | 605005    | 192.168.1.105 | 18237       | 192.168.1.1    | https            | Login permitted from 192.168.1.105/18237 to inside: 192.168.1.1/https for user "enable_15"                                            |
| 6        | Nov 17 2015 | 18:19:56 | 725002    | 192.168.1.105 | 18237       |                |                  | Device completed SSL handshake with client inside: 192.168.1.105/18237                                                                |
| 6        | Nov 17 2015 | 18:19:56 | 725001    | 192.168.1.105 | 18237       |                |                  | Starting SSL handshake with client inside: 192.168.1.105/18237 for TLSv1 session.                                                     |
| 6        | Nov 17 2015 | 18:19:56 | 302013    | 192.168.1.105 | 18237       | 192.168.1.1    | 443              | Built inbound TCP connection 688 for inside: 192.168.1.105/18237 (192.168.1.105/18237) to identity: 192.168.1.1/443 (192.168.1.1/443) |
| 6        | Nov 17 2015 | 18:18:05 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Tear down ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                         |
| 6        | Nov 17 2015 | 18:18:03 | 302020    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Built inbound ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                     |
| 6        | Nov 17 2015 | 18:18:00 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Tear down ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                         |
| 6        | Nov 17 2015 | 18:17:58 | 302020    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Built inbound ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                     |
| 6        | Nov 17 2015 | 18:17:55 | 302021    | 192.168.1.105 | 1           | 10.86.44.151   | 0                | Tear down ICMP connection for faddr 192.168.1.105/1 gaddr 10.86.44.151/0 laddr 10.86.44.151/0                                         |

**Syslog Details**

**#ASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.**

The ASA discarded a TCP packet that has no associated connection in the ASA connection table. The ASA looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the ASA

**Explanation Recommended Action Details**

**Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging**

Search the web and Windows 6:19 PM 11/17/2015

Real-Time Log Viewer - 192.168.1.1

**File Tools Window Help**

**Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help**

Filter By: Filter Build Filter Show All Find:

| Severity | Date        | Time     | Syslog ID | Source IP     | Source Port | Destination IP | Destination Port | Description                                                                                                                         |
|----------|-------------|----------|-----------|---------------|-------------|----------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 6        | Nov 17 2015 | 18:24:27 | 725007    | 192.168.1.105 | 18248       |                |                  | SSL session with client inside:192.168.1.105/18248 terminated.                                                                      |
| 6        | Nov 17 2015 | 18:24:27 | 106015    | 192.168.1.105 | 18248       | 192.168.1.1    | 443              | Deny TCP (no connection) from 192.168.1.105/18248 to 192.168.1.1/443 flags FIN ACK on interface inside                              |
| 6        | Nov 17 2015 | 18:24:27 | 302014    | 192.168.1.105 | 18248       | 192.168.1.1    | 443              | Tear down TCP connection 700 for inside:192.168.1.105/18248 to identity:192.168.1.1/443 duration 0:00:00 bytes 1097 TCP Reset-0     |
| 5        | Nov 17 2015 | 18:24:27 | 111007    |               |             |                |                  | Begin configuration: 192.168.1.105 reading from http [POST]                                                                         |
| 6        | Nov 17 2015 | 18:24:27 | 605005    | 192.168.1.105 | 18248       | 192.168.1.1    | https            | Login permitted from 192.168.1.105/18248 to inside:192.168.1.1/https for user "enable_15"                                           |
| 6        | Nov 17 2015 | 18:24:26 | 725002    | 192.168.1.105 | 18248       |                |                  | Device completed SSL handshake with client inside:192.168.1.105/18248                                                               |
| 6        | Nov 17 2015 | 18:24:26 | 725001    | 192.168.1.105 | 18248       |                |                  | Starting SSL handshake with client inside:192.168.1.105/18248 for TLSv1 session.                                                    |
| 6        | Nov 17 2015 | 18:24:26 | 302013    | 192.168.1.105 | 18248       | 192.168.1.1    | 443              | Built inbound TCP connection 700 for inside:192.168.1.105/18248 (192.168.1.105/18248) to identity:192.168.1.1/443 (192.168.1.1/443) |
| 4        | Nov 17 2015 | 18:24:26 | 106017    | 10.86.44.156  |             | 10.86.44.156   |                  | Deny IP due to Land Attack from 10.86.44.176 to 10.86.44.176                                                                        |
| 4        | Nov 17 2015 | 18:24:22 | 106017    | 10.86.44.156  |             | 10.86.44.156   |                  | Deny IP due to Land Attack from 10.86.44.176 to 10.86.44.176                                                                        |
| 4        | Nov 17 2015 | 18:24:20 | 106017    | 10.86.44.156  |             | 10.86.44.156   |                  | Deny IP due to Land Attack from 10.86.44.176 to 10.86.44.176                                                                        |
| 4        | Nov 17 2015 | 18:24:19 | 106017    | 10.86.44.156  |             | 10.86.44.156   |                  | Deny IP due to Land Attack from 10.86.44.176 to 10.86.44.176                                                                        |
| 4        | Nov 17 2015 | 18:24:18 | 106017    | 10.86.44.156  |             | 10.86.44.156   |                  | Deny IP due to Land Attack from 10.86.44.176 to 10.86.44.176                                                                        |
| 6        | Nov 17 2015 | 18:23:56 | 725007    | 192.168.1.105 | 18247       |                |                  | SSL session with client inside:192.168.1.105/18247 terminated.                                                                      |
| 6        | Nov 17 2015 | 18:23:56 | 106015    | 192.168.1.105 | 18247       | 192.168.1.1    | 443              | Deny TCP (no connection) from 192.168.1.105/18247 to 192.168.1.1/443 flags FIN ACK on interface inside                              |
| 6        | Nov 17 2015 | 18:23:56 | 302014    | 192.168.1.105 | 18247       | 192.168.1.1    | 443              | Tear down TCP connection 699 for inside:192.168.1.105/18247 to identity:192.168.1.1/443 duration 0:00:00 bytes 1097 TCP Reset-0     |
| 5        | Nov 17 2015 | 18:23:56 | 111007    |               |             |                |                  | Begin configuration: 192.168.1.105 reading from http [POST]                                                                         |
| 6        | Nov 17 2015 | 18:23:56 | 605005    | 192.168.1.105 | 18247       | 192.168.1.1    | https            | Login permitted from 192.168.1.105/18247 to inside:192.168.1.1/https for user "enable_15"                                           |
| 6        | Nov 17 2015 | 18:23:56 | 725002    | 192.168.1.105 | 18247       |                |                  | Device completed SSL handshake with client inside:192.168.1.105/18247                                                               |
| 6        | Nov 17 2015 | 18:23:56 | 725001    | 192.168.1.105 | 18247       |                |                  | Starting SSL handshake with client inside:192.168.1.105/18247 for TLSv1 session.                                                    |
| 6        | Nov 17 2015 | 18:23:56 | 302013    | 192.168.1.105 | 18247       | 192.168.1.1    | 443              | Built inbound TCP connection 699 for inside:192.168.1.105/18247 (192.168.1.105/18247) to identity:192.168.1.1/443 (192.168.1.1/443) |
| 4        | Nov 17 2015 | 18:23:47 | 106023    | 192.168.1.105 |             | 10.86.44.154   |                  | Deny icmp src inside:192.168.1.105 dst outside:10.86.44.154 (type 8, code 0) by access-group "inside_access_in" [0x0, 0x0]          |
| 6        | Nov 17 2015 | 18:23:47 | 802071    | 192.168.1.105 | 1           | in R6 44 151   | 0                | Tear down ICMP connection for faddr 192.168.1.105/1 cardnr 10 R6 44 151/lbaddr 10 R6 44 151/h                                       |

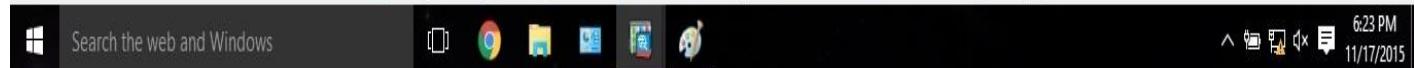
**Syslog Details**

**#ASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.**

The ASA discarded a TCP packet that has no associated connection in the ASA connection table. The ASA looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the ASA

**Explanation Recommended Action Details**

Emergency Alerts Critical Errors Warnings Notifications Informational Debugging



## Step 10: Some Misc. screenshots

---

- Firewall Router's Screenshots:

1. sh version

The screenshot shows a PuTTY terminal window titled "COM1 - PuTTY". The command "ciscoasa# sh version" is entered, followed by the system's version information, hardware details, and a list of network interfaces with their addresses and IRQ settings. It also displays licensed features and their status.

```
ciscoasa# sh version

Cisco Adaptive Security Appliance Software Version 8.3(1)
Device Manager Version 7.4(3)

Compiled on Thu 04-Mar-10 16:56 by builders
System image file is "disk0:/asa831-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 20 hours 42 mins

Hardware:    ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 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-2.06

0: Int: Internal-Data0/0      : address is 881d.fc66.ba64, irq 11
1: Ext: Ethernet0/0          : address is 881d.fc66.ba5c, irq 255
2: Ext: Ethernet0/1          : address is 881d.fc66.ba5d, irq 255
3: Ext: Ethernet0/2          : address is 881d.fc66.ba5e, irq 255
4: Ext: Ethernet0/3          : address is 881d.fc66.ba5f, irq 255
5: Ext: Ethernet0/4          : address is 881d.fc66.ba60, irq 255
6: Ext: Ethernet0/5          : address is 881d.fc66.ba61, irq 255
7: Ext: Ethernet0/6          : address is 881d.fc66.ba62, irq 255
8: Ext: Ethernet0/7          : address is 881d.fc66.ba63, irq 255
9: Int: Internal-Data0/1      : address is 0000.0003.0002, irq 255
10: Int: Not used            : irq 255
11: Int: Not used            : irq 255

Licensed features for this platform:
Maximum Physical Interfaces      : 8           perpetual
VLANs                           : 3           DMZ Restricted
Dual ISPs                        : Disabled     perpetual
VLAN Trunk Ports                : 0           perpetual
Inside Hosts                     : 10          perpetual
Failover                         : Disabled     perpetual
VPN-DES                          : Enabled      perpetual
VPN-3DES-AES                     : Enabled      perpetual
SSL VPN Peers                    : 2           perpetual
Total VPN Peers                  : 10          perpetual
Shared License                   : Disabled     perpetual
AnyConnect for Mobile             : Disabled     perpetual
AnyConnect for Cisco VPN Phone   : Disabled     perpetual
AnyConnect Essentials             : Disabled     perpetual
<--- More --->
```

```
COM1 - PuTTY
AnyConnect Essentials      : 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

This platform has a Base license.

Serial Number: JMX1841407M
Running Permanent Activation Key: 0x6220e26e 0x88a749cb 0x08d3f554 0x8c74ecb4 0x
cd262692
Configuration register is 0x112003
Configuration last modified by enable_15 at 18:15:39.738 UTC Tue Nov 17 2015
ciscoasa#
ciscoasa#
```

## 2. sh interface

```
COM1 - PuTTY
ciscoasa# sh interface
Interface Vlan1 "inside", is down, line protocol is down
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
    MAC address 881d.fc66.ba64, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
    20111 packets input, 1393901 bytes
    29872 packets output, 14922971 bytes
    2832 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
Interface Vlan2 "outside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
    MAC address 881d.fc66.ba64, MTU 1500
    IP address 10.86.44.151, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
    68298 packets input, 34658190 bytes
    9090 packets output, 5081308 bytes
    23360 packets dropped
    1 minute input rate 0 pkts/sec,  421 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 1 pkts/sec,  491 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 1 pkts/sec
Interface Ethernet0/0 "", is up, line protocol is up
  Hardware is 88E6095, BW 100 Mbps, DLY 100 usec
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    Input flow control is unsupported, output flow control is unsupported
    Available but not configured via nameif
    MAC address 881d.fc66.ba5c, MTU not set
<--- More --->
```

```
COM1 - PuTTY

Input flow control is unsupported, output flow control is unsupported
Available but not configured via nameif
MAC address 881d.fc66.ba5c, MTU not set
IP address unassigned
121383 packets input, 40434954 bytes, 0 no buffer
Received 68980 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
52185 switch ingress policy drops
9192 packets output, 5310412 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
0 rate limit drops
0 switch egress policy drops
Interface Ethernet0/1 "", is down, line protocol is down
Hardware is 88E6095, BW 100 Mbps, DLY 100 usec
    Auto-Duplex, Auto-Speed
Input flow control is unsupported, output flow control is unsupported
Available but not configured via nameif
MAC address 881d.fc66.ba5d, MTU not set
IP address unassigned
23319 packets input, 2365045 bytes, 0 no buffer
Received 518 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
0 switch ingress policy drops
30095 packets output, 15517738 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
0 rate limit drops
0 switch egress policy drops
<--- More --->[]
```