# ASA 8.X and later: Add or Modify an Access List through the ASDM GUI Configuration Example

### Contents

Introduction **Prerequisites** Requirements **Components Used Conventions Background Information** Configure **Network Diagram** Add a New Access List Create a Standard Access List Create a Global Access Rule Edit an Existing Access List **Delete an Access List** Export the Access Rule Export the Access List Information Verify **Troubleshoot Related Information** 

### **Introduction**

This document explains how to use Cisco Adaptive Security Device Manager (ASDM) in order to work with access control lists. This includes the creation of a new access list, how to edit an existing access list and other functionalities with the access lists.

### **Prerequisites**

### **Requirements**

There are no specific requirements for this document.

#### **Components Used**

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance (ASA) with version 8.2.X
- Cisco Adaptive Security Device Manager (ASDM) with version 6.3.X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### **Conventions**

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

### **Background Information**

Access lists are primarily used to control the traffic flow through the firewall. You can allow or deny specific types of traffic with access lists. Every access list contains a number of access list entries (ACEs) that control the traffic flow from a specific source to a specific destination. Normally, this access list is bound to an interface to notify the direction of the flow into which it should look. Access lists are mainly categorized into two broad types.

- 1. Inbound access lists
- 2. Outbound access lists

Inbound access lists apply to the traffic that enters that interface, and outbound access lists apply to the traffic that exits the interface. The inbound/outbound notation refers to the direction of the traffic in terms of that interface but not to the movement of traffic between higher and lower security interfaces.

For TCP and UDP connections, you do not need an access list to allow returning traffic because the security appliance allows all returning traffic for established bidirectional connections. For connectionless protocols such as ICMP, the security appliance establishes unidirectional sessions, so you either need access lists to apply access lists to the source and destination interfaces in order to allow ICMP in both directions, or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as bidirectional connections.

From the ASDM version 6.3.X, there are two types of access lists that you can configure.

- 1. Interface access rules
- 2. Global access rules

Note: Access rule refers to an individual access list entry (ACE).

Interface access rules are bound to any interface at the time of their creation. Without binding them to an interface, you can not create them. This differs from the Command Line example. With CLI, you first create the access list with the **access list** command, and then bind this access list to an interface with the **access-group** command. ASDM 6.3 and later, the access list is created and bound to an interface as a single task. This applies to the traffic flowing through that specific interface only.

Global access rules are not bound to any interface. They can be configured through the ACL Manager tab in the ASDM and are applied to the global ingress traffic. They are implemented when there is a match based on the source, the destination, and the protocol type. These rules are not replicated on each interface, so they save memory space.

When both these rules are to be implemented, interface access rules normally takes the precedence over the global access rules.

## **Configure**

In this section, you are presented with the information to configure the features described in this document.

### **Network Diagram**

This document uses this network setup:



### Add a New Access List

Complete these steps in order to create a new access list with ASDM:

1. Choose Configuration > Firewall > Access Rules, and click the Add Access Rule



button.

 Choose the interface to which this access list has to bound, along with the action to be performed on the traffic i.e., permit/deny. Then click the **Details** button in order to select the source

network.

| 🖆 Add Acc    | ess Rule       | <b>S</b> |
|--------------|----------------|----------|
| Interface: ( | inside 🕥       |          |
| Action: 💿    | Permit O Deny  |          |
| Source:      | any 🕞          |          |
| Destination  | any 🕘          |          |
| Service:     | ip 🕢           |          |
| Description: |                |          |
| 🕑 Enable L   | ogging         |          |
| Logging      | Level: Default |          |
| More Opt     | ions           | (*)      |
|              | OK Cancel Help | Note     |

: Here is a brief explanation of the different fields that are shown in this window:Interface—Determines the interface to which this access list is bound.Action—Determines the action type of the new rule. Two options are available. Permit allows all matching traffic and Deny blocks all matching traffic.Source—This field specifies the source of the traffic. This can be anything among a Single IP address, a network, an interface IP address of the firewall or a network object group. These can be selected with the Details button.Destination—This field specifies the source of the traffic. These can be selected with the Details button.Destination—This field specifies the source of the traffic. This can be anything among a Single IP address, a network, an interface IP address of the firewall or a network, an interface IP address of the firewall or a network, an interface IP address of the firewall or a network an interface IP address of the firewall or a network, an interface IP address of the firewall or a network an interface IP address of the firewall or a network and the traffic. This can be anything among a Single IP address, a network, an interface IP address of the firewall or a network object group. These can be selected with the Details button.Service—This field determines the protocol or service of the traffic to which this access list is applied. You can also define a service-group that contains a set of different protocols.

 After you click the **Details** button, a new window that contains the existing Network Objects is displayed. Select the **inside-network**, and click **OK**.

| Manager             | - 1       | ID Address     | Notes a de      | Decointian  | Object NAT As |
|---------------------|-----------|----------------|-----------------|-------------|---------------|
| IVenic<br>IPv4 Mehy | work Obie | IF Address     | IVEUIIdSK       | Description | COJECT NAT A  |
| an 🖓 an             | N         | 0.0.0.0        | 0.0.0.0         |             |               |
| n De                | ide-n     | 172.16.11.0    | 255.255.255.0   |             |               |
| - will ma           | anage     | 10.77.241.64   | 255.255.255.192 |             |               |
| - 🙀 ou              | tside     | 209.165.200.0  | 255.255.255.224 |             |               |
| - 📇 20              | .1.1.10   | 20.1.1.10      | 255.255.255.255 |             |               |
| - 🔳 17              | 2.16      | 172.16.11.1    | 255.255.255.255 |             |               |
| - 🖪 17              | 2.16      | 172.16.11.10   | 255.255.255.255 |             |               |
| - 🔳 17              | 2.16      | 172.16.12.2    | 255.255.255.255 |             |               |
|                     | 9.16      | 209.165.200.10 | 255.255.255.255 |             |               |
| L 20                | 9.16      | 209.165.200.10 | 255.255.255.255 |             |               |
| - 📇 20              | 9.16.,,   | 209.165.200.10 | 255.255.255.255 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |
|                     |           |                |                 |             |               |

4. You are returned to the **Add Access Rule** window. Type **any** in the Destination field. and click **OK** in order to complete the configuration of the access

| Interface:   | inside 💌          |  |
|--------------|-------------------|--|
| Action: 💿    | Permit O Deny     |  |
| Source: (    | inside-network/24 |  |
| Destination  | bny -             |  |
| Service:     | ф                 |  |
| Description: |                   |  |
| 🕑 Enable L   | ogging            |  |
| Logging      | Level: Default 💌  |  |
| More Opt     | ions              |  |

#### Add an access rule before an existing one:

Complete these steps in order to add an access rule just before an already existing access rule:

1. Select the existing access list entry, and click **Insert** from the **Add** drop-down



2. Choose the Source and Destination, and click the **Details** button of the Service field to

|                      | 🖆 Insert A               | ccess Rule                |
|----------------------|--------------------------|---------------------------|
|                      | Interface:<br>Action: () | inside 💌<br>Permit 🔿 Deny |
|                      | Source:                  | 172.16.2.10               |
|                      | Destination              | any 🔄                     |
|                      | Service:                 | P                         |
|                      | Description:             |                           |
|                      | 🕑 Enable L               | ogging                    |
|                      | Logging l                | Level: Default            |
|                      | More Opt                 | ions                      |
|                      |                          | OK Cancel H               |
| choose the Protocol. |                          |                           |

3. Choose HTTP the protocol, and click **OK**.

| filter:         |          |                   |                   |           |             | Filte |
|-----------------|----------|-------------------|-------------------|-----------|-------------|-------|
| Name            | Protocol | Source Ports      | Destination Ports | ICMP Type | Description |       |
| 100 h323        | tcp      | default (1-65535) | 1720              |           |             |       |
| - 100 hostname  | tcp      | default (1-65535) | 101               |           |             |       |
| TOP http        | tep      | default (1-65535) | 80                |           |             |       |
| https           | tcp      | default (1-65535) | 443               |           |             |       |
| · ret ident     | tcp      | default (1-65535) | 113               |           |             |       |
| 🐨 imap4         | tcp      | default (1-65535) | 143               |           |             |       |
| - TOP Inc       | tcp      | default (1-65535) | 194               |           |             |       |
| 👷 kerberos      | tcp      | default (1-65535) | 750               |           |             |       |
| - 👥 klogin      | tcp      | default (1-65535) | 543               |           |             |       |
| kshell          | tcp      | default (1-65535) | 544               |           |             |       |
| 🐨 Idap          | tcp      | default (1-65535) | 389               |           |             |       |
| - 🚾 Idaps       | tcp      | default (1-65535) | 636               |           |             |       |
| 100 login       | tcp      | default (1-65535) | 513               |           |             |       |
| 100 lotusnotes  | tcp      | default (1-65535) | 1352              |           |             |       |
| ng lpd          | tcp      | default (1-65535) | 515               |           |             |       |
| netbios-ssr     | tcp      | default (1-65535) | 139               |           |             |       |
| nfs             | tcp      | default (1-65535) | 2049              |           |             |       |
| te nntp         | tcp      | default (1-65535) | 119               |           |             |       |
| - te pcanywh    | tcp      | default (1-65535) | 5631              |           |             |       |
| ner pim-auto-re | top      | default (1-65535) | 496               |           |             |       |
| elected Service | erere.   |                   | 2020              |           |             |       |

4. You are returned to the Insert Access Rule window. The Service field is filled with **tcp/http** as the selected protocol. Click **OK** in order to complete the configuration of the new access list

| Interface:   | inside 💌        |   |
|--------------|-----------------|---|
| Action: 💿    | Permit 🔿 Deny   |   |
| Source:      | 172.16.2.10     | G |
| Destination  | any             |   |
| Service:     | tcp/http        | C |
| Description: |                 |   |
| Enable L     | ogging          |   |
| Logging      | evel: Default 💌 |   |
| More Opt     | ions            |   |

You can now observe the new access rule shown just before the already existing entry for the Inside-Network.

| #            | Enabled        | Source                  | Destination        | Service          | Action   | Hits | Logging        |
|--------------|----------------|-------------------------|--------------------|------------------|----------|------|----------------|
| <b>5</b> -   | MZ (2 implicit | incoming rules)         |                    |                  |          |      | dina industria |
| 1            |                | any                     | Any less secure ne | <u>⊐e&gt;</u> ip | 🖌 Permit |      |                |
| 2            |                | 🧼 any                   | 🏟 any              | <u>∎</u> ip      | 🕲 Deny   |      |                |
| "Şəl ir      | nside (3 incom | ing rules)              |                    |                  |          |      |                |
| 1            | <b>2</b>       | <b>3</b> 172.16.2.10    | 🟟 any              | ttp http         | 🖌 Permit |      |                |
| 2            |                | 📑 inside-network/24     | any                |                  | 🖌 Permit |      |                |
| 3            |                | 🏟 any                   | <li>any</li>       | IP-ip            | 🕲 Deny   |      |                |
| "Şəl n       | hanage (2 imp  | licit incoming rules)   |                    |                  |          |      |                |
| 1            |                | <ul> <li>any</li> </ul> | Any less secure ne | 11 ip            | 🖌 Permit |      |                |
| 2            |                | <ul> <li>any</li> </ul> | any                |                  | O Deny   |      |                |
| - <b>P</b> o | utside (4 inco | ming rules)             |                    |                  |          |      |                |
| 1            | ~              | 🧔 any                   | A 192.168.5.3      | smtp             | 🖌 Permit | 0    | )              |
| 2            | 4              | 🏟 any                   | A 192.168.5.5      | ter https        | 🖌 Permit | 0    | i -            |
| 3            | 4              | 🏟 any                   | 3 192.168.5.4      | 100 domain       | 🖌 Permit | 0    | 1              |
| 4            |                | <ul> <li>any</li> </ul> | 🌖 any              | IP IP            | 🔞 Deny   |      |                |

**Note:** The order of the access rules is very important. While processing each packet to filter, the ASA examines if the packet matches any of the access rule criterion in a sequential order and if a match happens, it implements the action of that access rule. When an access rule is matched, it does not proceed to further access rules and verify them again.

#### Add an Access Rule after an existing one:

Complete these steps in order to create an access rule just after an already existing access rule.

1. Select the access rule after which you need to have a new access rule, and choose Insert

| l | onfie | <b>u</b> ra | at | ion > Firewall > Ac | ces | s Ru | les | 1 |
|---|-------|-------------|----|---------------------|-----|------|-----|---|
|   | ÷.    | dd          | +  | 🕑 Edit 📋 Delete     | +   | ÷    | X   |   |
|   | 4     | Ac          | b  | Access Rule         |     |      |     |   |
|   |       | In          | se | rta.                | s   | )    |     |   |
|   | Ŧ     | Ins         | se | rt After            |     |      |     |   |
|   | 1 5   | 1           | Τ  | 🤍 any               |     |      |     | 1 |

After from the Add drop-down menu.

2. Specify the Interface, Action, Source, Destination and Service fields, and click **OK** to complete the configuration this access

| Interface: ( | inside 💌       |  |
|--------------|----------------|--|
| Action:      | Permit O Deny  |  |
| Source:      | 172.16.3.20    |  |
| Destination  | 192.168.10.5   |  |
| Service;     | ip             |  |
| Description: |                |  |
| 🗹 Enable L   | ogging         |  |
| Logging      | Level: Default |  |
| More Oot     | ions           |  |

You can view that the newly configured access rule sits just after the already configured one.

| Add    | • 🗹 Edit       | Î Delete 🕈 🎸 🐰 🖟    | 🖻 💼 - 🔍 Find 🔛 Diag | ram 調 Export | 🝷 😚 Clear Hits | Show |
|--------|----------------|---------------------|---------------------|--------------|----------------|------|
| ŧ      | Enabled        | Source              | Destination         | Service      | Action         | Hits |
| 540    | MZ (2 implicit | incoming rules)     |                     |              |                |      |
| 1      |                | 🦚 any               | Any less secure ne  | IP ip        | 🖌 Permit       |      |
| 2      |                | 🧼 any               | 🏟 any               | 🗶 ip         | 🕴 Deny         |      |
| .şəl i | nside (4 incom | ing rules)          |                     |              |                |      |
| 1      | ~              | 3 172.16.2.10       | any                 | 100 http     | 🖌 Permit       | 0    |
| 2      | 4              | 🛃 inside-network/24 | 🥥 any               | 2P/ip        | 🛷 Permit       | (    |
| 3      |                | 172.16.3.20         | . 192.168.10.5      | IP ip        | 🖌 Permit       |      |
| 4      |                | any                 | <li>any</li>        | .se∕ip       | 🔞 Deny         |      |

#### **Create a Standard Access List**

Complete these steps in order to create a standard access list with the ASDM GUI.

1. Choose Configuration > Firewall > Advanced > Standard ACL > Add, and click Add



2. Give a number in the range allowed for the standard access list, and click

| 🜃 Add ACI | Ľ.   |         |   |
|-----------|------|---------|---|
| ACL Name: | 100  |         |   |
| ОК        | Canc | el Help | ì |
| K.        |      | el Help |   |

3. Right-click the access list, and choose Add ACE in order to add an access rule to this



access list.

ACL

4. Select the **Action**, and specify the **Source address**. If required, specify the **Description** also. Click **OK** in order to complete the configuration of the access

| ACCION:   | Permit Deny |
|-----------|-------------|
| ddress:   | 172.16.1.11 |
|           |             |
| escriptio | n:          |
|           |             |
|           |             |

#### Create a Global Access Rule

Complete these steps in order to create an extended access list that contains global access rules.

1. Choose Configuration > Firewall > Advanced > ACL Manager > Add, and click Add ACL

| <b>4</b> / | vdd 🔹 🗹 Edit 📋 D | elete 🗲 🗲 🐰 🗏   | 6 - 国 |
|------------|------------------|-----------------|-------|
| +          | Add ACL          | le              | De    |
| ÷          | Add IPv6 ACL     |                 |       |
| ÷          | Add ACE          | 2.16.2.10       | ٩     |
| -          | Incert           | -Internal-Hosts |       |
| 1          | Incert After     | 2.16.2.5        |       |

button.

| 🖆 Add ACL     |        |      | × |
|---------------|--------|------|---|
| ACL Name: 111 |        |      | ] |
| ОК            | Cancel | Help |   |
|               |        |      |   |

- 2. Specify a name for the access list, and click OK.
- 3. Right-click the access list, and choose Add ACE in order to add an access rule to this

| 4 | Add ACL             |
|---|---------------------|
|   | Add IPv6 ACL        |
| ÷ | Add ACE             |
| B | Rename ACL          |
|   | Rule Table Settings |

access list.

4. Complete the Action, Source, Destination, and Service fields, and click **OK** in order to complete the configuration of the global access

|              | 10.14.14.000   |
|--------------|----------------|
| Source:      | 10.14.16.200   |
| Destination  | 192.168.200.10 |
| Service:     | udp/domain     |
| Description: |                |
| 🕑 Enable L   | ogging         |
|              | evel: Default  |
| Logging      |                |

You can now view the global access rule, as shown.

| ** |                  |                       |             |          |
|----|------------------|-----------------------|-------------|----------|
|    | In 14 16 200     | I 192 168 200 10      | ure, domain | 2 Dermit |
|    | <br>10.14.10.200 | <u>192.100.200.10</u> | Goundani    | • Fernic |

#### **Edit an Existing Access List**

This section discusses how to edit an existing access.

#### Edit the Protocol field to create a service group:

Complete these steps in order to create a new service-group.

1. Right-click the access rule that needs to be modified, and choose **Edit** in order to modify that specific access

| #      | Enabled        | Source                | Destin       | ation  | 6            | Service   |         | Action   | Hit |
|--------|----------------|-----------------------|--------------|--------|--------------|-----------|---------|----------|-----|
| 🗐 🦊 D  | MZ (2 implicit | incoming rules)       |              |        |              |           |         |          |     |
| 1      |                | 🎱 any                 | 🎱 Arr        | y less | secure ne    | 🕑 ip      |         | 🧳 Permit |     |
| 2      |                | 🦚 any                 | 🌍 ang        | 1      |              | ₽ lp      |         | 🕴 Deny   |     |
| 🗄 🦊 ir | side (4 incom  | ing rules)            |              |        |              |           |         |          |     |
| 1      | <b>V</b>       | 172.16.2.10           | 📢 an         |        |              | D. Ja     | -       | Permit   |     |
| 2      | ~              | 🚜 inside-network/24   | 🎱 ang        | ~      | Add Access   | Rule      |         | P Permit |     |
| 3      | 1              | <b>172.16.3.20</b>    | <b>I</b> 19  | *      | Insert       |           |         | P Permit |     |
| 4      |                | 🥥 any                 | 🌍 ang        | 季      | Insert After |           |         | Deny     |     |
| n 🍋 🗄  | nanage (2 imp  | licit incoming rules) |              | a      | Edit         |           |         | 1        |     |
| 1      |                | 🎱 any                 | Any          | -      | Delete       |           |         | Permit   |     |
| 2      |                | 🥥 any                 | 🌍 ang        |        |              |           | 829.378 | Deny     |     |
| ė 🦊 o  | utside (4 inco | ming rules)           |              | P      | Cut          |           | Ctrl+X  |          |     |
| 1      | 4              | 🏟 any                 | 르 192        | -      | Copy         |           | Ctrl+C  | P Permit |     |
| 2      | ~              | 🧼 any                 | <b>3</b> 19  | 100    | Paste        |           | CtdeX   | P Permit |     |
| 3      | ~              | 🎱 any                 | <b>B</b> 193 | 1      | Paste After  | ŝ.        |         | P Permit |     |
| 4      |                | 🧼 any                 | 🌍 ang        | 4      | Clear Hit Co | usł       |         | Deny     |     |
|        |                |                       |              |        | cied nic co  | Giller    |         |          |     |
|        |                |                       |              |        | Show Log     |           |         |          |     |
|        |                |                       |              | 44     | Packet Trac  | e         |         | 0        |     |
|        |                |                       |              |        | Export       |           | •       |          |     |
|        |                |                       |              |        | Rule Table 9 | ettings . |         |          |     |

2. Click the **Details** button in order to modify the protocol associated with this access

| Action: ()   | inside<br>Permit O Deny |
|--------------|-------------------------|
| Source:      | 172.16.2.10             |
| Destination  | any                     |
| Service:     | tcp/http                |
| Description: |                         |
| Enable I     | ogging                  |
| El cuerto e  |                         |
| Logging      | Level: Default 💌        |

3. You can select any protocol other than HTTP if required. If there is only a single protocol to be selected, then there is no need to create the service group. It is useful to create a service group when there is a requirement to identify numerous non-adjacent protocols to be matched by this access rule. Choose Add > TCP service group in order to create a new TCP service group. Note: In the same way, you can also create a new UDP service group or

| 44  | vdd 🔹 🎬 Edit                               | Delete     |      | here Used      |        |
|-----|--|------------|------|----------------|--------|
| IP) | Service Group.                             | 00.        |      |                |        |
| 10  | TCP Service Gr                             | oup        |      | rce Ports      | Destin |
| ue) | UDP Service Group<br>TCP-UDP Service Group |            |      | lt (1-65535)   | 80     |
| 10  |  |            |      | lt (1-65535)   | 443    |
| Kat | ICMP Group                                 | ICMP Group |      |                | 113    |
|     | Destand Group                              |            |      | ilt (1-65535)  | 143    |
| R   | Protocol Group                             | 1000       |      | ilt (1-65535)  | 194    |
|     | terberos                                   | tcp        | defa | ult (1-65535)  | 750    |
|     | 👿 klogin                                   | tcp        | defa | ault (1-65535) | 543    |
|     | teshell                                    | tcp        | defa | ult (1-65535)  | 544    |

ICMP group and etc.

4. Specify a name for this service group, select the protocol on the left side menu, and click Add in order to move them to the Members in Group menu on the right side. Numerous protocols can be added as members of a service group based on the requirement. The protocols are added one by one. After all the members are added, click OK.

| up Name:<br>crintion: | Allow-Ports            |    |           |                   |  |
|-----------------------|------------------------|----|-----------|-------------------|--|
| Existing S            | iervice/Service Group: |    |           | Members in Group: |  |
| Name                  |                        | l. | 1         | Name              |  |
| - 10                  | lotusnotes             | ~  |           | ttp               |  |
| 10                    | p lpd                  |    | 1         | 100/ https        |  |
| 10                    | netbios-ssn            |    |           | то рор3           |  |
| TO                    | nfs                    |    |           | 😰 smtp            |  |
| 10                    | nntp                   |    |           | 1                 |  |
| 10                    | pcanywhere-data        |    |           |                   |  |
| TO                    | pim-auto-rp            |    |           |                   |  |
| TO                    | pop2                   |    | Carrier   | 6                 |  |
| TO                    | pptp                   |    | Add >>    |                   |  |
| 10                    | 🛿 rsh                  |    | << Remove |                   |  |
| - 19                  | 👂 rtsp                 |    |           |                   |  |
| 10                    | 🕼 sip                  |    |           |                   |  |
| TO                    | > sqinet               |    |           |                   |  |
| <u>10</u>             | 🦻 ssh                  |    |           |                   |  |
| 10                    | sunrpc                 |    |           |                   |  |
| 10                    | tacacs                 | -  |           |                   |  |
| 10                    | ▶ talk                 | ~  |           |                   |  |
| Create ne             | ew member:             |    | ~ .       |                   |  |
| Port/Ran              | 1e:                    |    |           |                   |  |

 The newly created service group can be viewed under the tab TCP service groups. Click OK button to return to the Edit Access Rule window.

| ilter:             |                 |              |                   |           |             |
|--------------------|-----------------|--------------|-------------------|-----------|-------------|
| Name               | Protocol        | Source Ports | Destination Ports | ICMP Type | Description |
|                    | acha, icmp      |              |                   | 3         |             |
| an 🔒               | an              |              |                   |           |             |
| eigrp              | eigrp           |              |                   |           |             |
| - da esp           | esp             |              |                   |           |             |
| - 🕹 gre            | gre             |              |                   |           |             |
| icmp               | icmp            |              |                   |           |             |
| - imp              | 5 icmpo         |              |                   |           |             |
| - igmp             | igmp            |              |                   |           |             |
| - State            | igrp            |              |                   |           |             |
| P.                 | ip loinin       |              |                   |           |             |
| - ipinip           | i iprap         |              |                   |           |             |
| L conf             | nos             |              |                   |           | _           |
| ospr               | ospr            |              |                   |           |             |
| pcp.               | pep             |              |                   |           |             |
| pim and a pim      | pin             |              |                   |           |             |
| sip here           | sop             |              |                   |           |             |
|                    | uda             |              |                   |           |             |
| TCP Service        | Groups          |              |                   |           |             |
| + TCP Service      | -Ports tro      | (i)          |                   |           | Ĥ.          |
| Contraction of the |                 |              |                   |           |             |
| elected Service    | 0 <sup>21</sup> |              |                   |           |             |

6. You can see that the Service field is populated with the newly created service group. Click

| 🚰 Edit Acc               | ess Rule                |
|--------------------------|-------------------------|
| Interface:<br>Action: () | inside<br>Permit O Deny |
| Source:                  | 172.16.2.10             |
| Destination              | any                     |
| Service:                 | Allow-Ports             |
| Description:             |                         |
| 🗹 Enable L               | ogging                  |
| Logging I                | Level: Default          |
| More Opt                 | ions                    |
|                          | OK Cancel Hel           |

OK in order to complete the edit.

7. Hover your mouse over that specific service group in order to view all the associated protocols.

| <b>#</b> | Enabled        | Source                  | Destination                             | Service     | Э         | Action          | Hits |
|----------|----------------|-------------------------|---|-------------|-----------|-----------------|------|
| S 🥦 DM   | AZ (2 implicit | incoming rules)         | 1 C C C C C C C C C C C C C C C C C C C |             |           |                 |      |
| 1        |                | 🧼 any                   | Any less secure ne                      | <u>⊫</u> ip |           | 🖌 Permit        |      |
| 2        |                | 🧼 any                   | 🍅 any                                   | JE- ip      |           | 🕴 Deny          |      |
| ins 🥵    | ide (4 incom   | ing rules)              |   |             |           |                 |      |
| 1        | 2              | A 172.16.2.10           | 🄄 eny                                   | 🔞 Allo      | w-Ports   | 🖌 Permit        | 12,  |
| 2        | ~              | 🙀 inside-network/24     | iany                                    | JE ip       |           | 🖌 Permit        | ો    |
| 3:       | 4              | <b>I</b> 172.16.3.20    | 192.168.10.5                            | 1P ip       | TCP Grou  | p: Allow-Ports  |      |
| 4        |                | any                     | <ul> <li>any</li> </ul>                 | <u>ж</u> ір | TCP: http | (80)<br>c (443) |      |
| 🔊 🥬 ma   | anage (2 imp   | licit incoming rules)   |   |             | TCP: pop  | 3 (110)         |      |
| 1        |                | <ul> <li>any</li> </ul> | Any less secure ne                      | <u>₽</u> p  | TCP: smtp | o (25)          |      |
| 2        |                | anv.                    | anv 🙆                                   | IP ID       |           | C Denv          | )    |

Edit the Source/Destination fields to create a Network object group:

Object groups are used to simplify the creation and maintenance of access lists. When you group like objects together, you can use the object group in a single ACE instead of having to enter an ACE for each object separately. Before you create the object group, you need to create the objects. In ASDM terminology, object is called network object and object group is called network object group.

Complete these steps:

1. Choose Configuration > Firewall > Objects > Network Objects/Groups > Add, and click Network Object in order to create a new network

| <b>1</b> | Network Object       |     |             |            |
|----------|----------------------|-----|-------------|------------|
|          | Network Object Group |     | ddress      | Netmask    |
| -IP      | v4 Network Objects   |     |             |            |
|          | 🍈 🍅 any              | 0.0 | .0.0        | 0.0.0      |
|          | 📑 DMZ-network        | 172 | 2.16.1.0    | 255.255.25 |
|          | 📑 inside-network     | 172 | .16.11.0    | 255.255.25 |
|          | 📷 manage-network     | 10. | 77.241.64   | 255.255.25 |
|          | 对 outside-network    | 209 | 0.165.200.0 | 255.255.25 |
|          | 172 16 1 9           | 172 | 1613        | 255 255 25 |

object.

2. Fill in the Name, IP Address and Netmask fields, and click

| Name (optional): | Internal-10     |  |
|------------------|-----------------|--|
| IP Address:      | 172.16.11.10    |  |
| Netmask:         | 255.255.255.255 |  |
| Description:     |                 |  |

OK.

3. The newly created network object can be seen in the list of the objects. Click

| ilter:                 |  |                     |
|------------------------|--|---------------------|
| Name                   | 🔺 1 IP Address   | Netmask             |
| - IPv4 Network Objects | in the second se | and a second second |
| 🕂 🥥 ariy               | 0.0.0  | 0.0.0.0             |
| DMZ-network            | 172.16.1.0   | 255.255.255.0       |
| 💀 🚮 inside-network     | 172.16.11.0  | 255.255.255.0       |
| - 🖪 Internal-10        | 172.16.11.10   | 255.255.255.255     |
| - 🖪 Internal-12        | 172.16.11.12   | 255.255.255.255     |
| - 🔠 Internal-15        | 172.16.11.15   | 255.255.255.255     |
| - 🔠 Internal-24        | 172.16.11.24   | 255.255.255.255     |
| - 🔳 Internal-26        | 172.16.11.26   | 255.255.255.255     |
| 🔳 Internal-32          | 172.16.11.32   | 255.255.255.255     |
| 📑 manage-network       | 10.77.241.64   | 255.255.255.192     |

4. Choose Configuration > Firewall > Objects > Network Objects/Groups > Add, and click Network Object Group in order to create a new network object



5. The available list of all network objects can be found on the left pane of the window. Select individual network objects, and click the **Add** button in order to make them members of the newly created network object group. Group Name must be specified in the field allocated for it.

| Citran I.        |                    |                 |         |           |  |              |                   |
|------------------|--------------------|-----------------|---------|-----------|--|--------------|-------------------|
| Existing Network | Objects/Groups:    |                 |         |           | Members in Group:  |              |                   |
| Name             | A 1 IP Address     | Netmask         | Descrip |           | Name   | IP Address   | NetmaskPrefix Ler |
| E IPv4 Network   | Objects            |                 | ^       | 14        | Internal-10  | 172.16.11.10 | 255.255.255.255   |
| any              | 0.0.0.0            | 0.0.0           |         |           |  |              |                   |
| DMZ-n            | etw 172.16.1.0     | 255.255.255.0   |         |           |  |              |                   |
| - 💑 nside-       | net 172.16.11.0    | 255.255.255.0   |         |           |  |              |                   |
| 📠 Intern         | al-12 172.16.11.12 | 255.255.255.255 | 1.11    |           |  |              |                   |
| - 🗷 Intern       | al-15 172.16.11.15 | 255.255.255.255 |         |           |  |              |                   |
| - 🛎 Intern       | al-24 172.16.11.24 | 255.255.255.255 |         |           |  |              |                   |
| - 📇 Intern       | al-26 172.16.11.26 | 255.255.255.255 |         |           |  |              |                   |
| 🔳 Intern         | al-32 172.16.11.32 | 255.255.255.255 |         |           |  |              |                   |
| 🛃 manag          | e-n 10.77.241.64   | 255.255.255.192 |         |           |  |              |                   |
| 📑 outsid         | e-ne 209.165.200.0 | 255.255.255.192 |         | Add >>    | 1  |              |                   |
| - 🗷 172.16       | 5.1.3 172.16.1.3   | 255.255.255.255 |         | 4         |  |              |                   |
| ₹ 172.16         | 6.1.4 172.16.1.4   | 255.255.255.255 |         | << Rebove |  |              |                   |
| ₫ 172.16         | 5.1.5 172.16.1.5   | 255.255.255.255 |         |           |  |              |                   |
| - 📇 172.1d       | 5.2.10 172.16.2.10 | 255.255.255.255 |         |           |  |              |                   |
| - 3 192.14       | 68.5.3 192.168.5.3 | 255.255.255.255 |         |           |  |              |                   |
| e = 100 10       |                    |                 | >       |           |  |              |                   |
| Country Dates    | ask Object manhair |                 | 10001   |           |  |              |                   |
| Create How Netwo | ork object member: |                 |         |           |  |              |                   |
| Name: (optional) |                    |                 |         |           |  |              |                   |
| Type:            | Network.           |                 | ~       |           |  |              |                   |
| IP Address:      |                    |                 |         |           |  |              |                   |
| Netmask:         | 255.255.255.0      |                 | ~       |           |  |              |                   |
| Descriptions.    |                    |                 |         |           | in the second se |              |                   |

6. Click **OK** after you add all the members in to group.

|            | Netroeniden       | osts          |                 |             |   |  |                                  |        |
|------------|-------------------|---------------|-----------------|-------------|---|--|----------------------------------|--------|
| scription  | в <u>-</u>        |               |                 |             |   |  |                                  |        |
| ) Existing | g Network Objects | /Groups:      |                 |             |   | Members in Group:  |                                  |        |
| Name       |                   | IP Address    | Netmask         | Description |   | Name   | IP Address                       | Netma  |
| E-IPv      | 4 Network Object  | s             |                 |             |   | - 📇 Internal-10  | 172.16.11.10                     | 255.25 |
| 1          | any               | 0.0.0.0       | 0.0.0.0         |             |   | - 📇 Internal-12  | 172.16.11.12                     | 255.25 |
| 10         | DMZ-netw          | 172.16.1.0    | 255.255.255.0   |             |   | - 📇 Internal-15  | 172.16.11.15                     | 255.25 |
|            | 💑 inside-net      | 172.16.11.0   | 255.255.255.0   |             |   | 🗏 Internal-24  | 172.16.11.24                     | 255.25 |
| -          | 💑 manage-n        | 10.77.241.64  | 255.255.255.192 |             |   | 🛛 😹 Internal-26  | 172.16.11.26                     | 255.29 |
| -          | outside-ne        | 209.165.200.0 | 255.255.255.192 |             |   | 🖺 Internal-32  | 172.16.11.32                     | 255.25 |
| 1          | 3 172.16.1.3      | 172-16-1.3    | 255.255.255.255 |             |   |  |                                  |        |
|            | 3 172.16.1.4      | 172.16.1.4    | 255.255.255.255 |             |   |  |                                  |        |
| -          | 3 172.16.1.5      | 172.16.1.5    | 255.255.255.255 |             |   |  |                                  |        |
|            | 3 172.16.2.10     | 172.16.2.10   | 255.255.255.255 |             |   | 1  |                                  |        |
| F          | 8 192.168.5.3     | 192.168.5.3   | 255.255.255.255 |             | - Add SS - S  |  |                                  |        |
| -          | 3 192.168.5.4     | 192.168.5.4   | 255.255.255.255 |             |   |  |                                  |        |
| - L.       | 3 192.168.5.5     | 192.168.5.5   | 255.255.255.255 |             | << Remove   |  |                                  |        |
|            |                   |               |                 |             |   | 5d.  |                                  |        |
|            |                   |               | ( CK            | Cancel      | — 🖳 192   | .168.5.4<br>2.168.5.5  | 192.168.5.4<br>192.168.5.5       |        |
|            |                   |               | (W)             | Cancel      | - 🗐 192   | 2.168.5.4<br>2.168.5.5<br>ork Objects  | 192.168.5.4<br>192.168.5.5       |        |
| 1          |                   |               | OK I            | Cancel      | - 🖳 192<br>- 🖳 192<br>- IPv6 Netwo                                      | .168.5.4<br>2.168.5.5<br>ork Objects   | 192.168.5.4<br>192.168.5.5       |        |
| 1          |                   |               | ( CK            | Cancel      | ныр<br>- 🖳 192<br>- 🖳 192<br>- IPv6 Netwo<br>- 🍲 any                    | 2.168.5.4<br>2.168.5.5<br>ork Objects  | 192.168.5.4<br>192.168.5.5       |        |
| 1          |                   |               | <u>(</u>        | Cancel      | - 🖳 192<br>- 🖳 192<br>- IPv6 Netwo<br>- 🐼 any<br>IPv4 Netwo             | 2.168.5.4<br>2.168.5.5<br>ork Objects<br>ork Object Groups                   | 192.168.5.4<br>192.168.5.5<br>11 |        |
|            |                   |               | CK              | Cancel      | Help<br>- I 192<br>IPv6 Netwo<br>IPv6 Netwo<br>IPv4 Netwo<br>IPv4 Netwo | 2.168.5.4<br>2.168.5.5<br>ork Objects<br>ork Object Groups<br>Internal-Hosts | 192.168.5.4<br>192.168.5.5       |        |

You can now view the network object group.

7. In order to modify any source/destination field of an existing access list with a network group object, right-click the specific access rule, and choose

| #   | Enabled  | Source      |               | Destination     |     | Service     |
|-----|--|-------------|---------------|-----------------|-----|-------------|
| e 🔊 | DMZ (2 implicit  | incoming ru | ules)         |                 | -   |             |
| 1   |  | 🌍 any       |               | Any less secure | ne  | 🥑 ip        |
| 2   |  | 🏟 any       |               | any             |     | <u>⊫</u> ∳p |
| à 🔊 | inside (3 incom  | ing rules)  |               |                 |     |             |
| 1   | Image: A start and a start | 🖪 172.      | 16.2.10       | any             |     | Allow       |
| 2   |  | 10          | Add Access 8  | 2 Jac           |     | 💌 ip        |
| 3   |  | Q 4         | AUG ACCOST    | NOCH .          |     | <u>в</u> р  |
| 🛱 🦊 | manage (2 imp  | licit inc 🔮 | Insert        |                 |     |             |
| 1   |  | 🏟 a 🏺       | Insert After. | 29              | ie; | ip 🤨        |
| 2   |  | 0           | Edit          |                 |     | 1 ip        |
| 🗄 🔊 | outside (4 inco  | ming ru     | Delete        |                 |     |             |
| 1   | <b>v</b>   | 🔷 a 🐫       |               |                 | -   | res smtp    |
| 2   | 4  | 🔷 a 💑       | Cut           | Ctrl+X          |     | to https    |
|     |  | A B         | Conv          | Chrl+C          |     | size does a |

8. The Edit Access Rule window appears. Click on the Details button of the Source field in

| Interface:<br>Action: • | inside<br>Permit O Deny  |
|-------------------------|--|
| Source:                 | inside-network/24  |
| Destination             | any  |
| Service:                | ب<br>ب   |
| Description:            |  |
| Enable Lo               | ogging   |
| Logging L               | evel: Default  |
| More Opti               | ions and a second s |
|                         |  |

9. Select the All-Internal-Hosts network object group, and click OK

| Filter:    |                      |             |             | Fb             |
|------------|----------------------|-------------|-------------|----------------|
| Name       | - 1 IP Address       | Netmask     | Description | Object NAT Add |
| I La       | 172.16 172.16.1.3    | 255.255.255 |             |                |
|            | 172.16 172.16.1.4    | 255.255.255 |             |                |
|            | 172.16 172.16.1.5    | 255.255.255 |             |                |
|            | 172.16 172.16.2.10   | 255.255.255 |             |                |
| - 8        | 192.16 192.168.5.3   | 255.255.255 |             |                |
| - 3        | 192.16 192.168.5.4   | 255.255.255 |             |                |
|            | 192.16 192.168.5.5   | 255.255.255 |             |                |
| B IPv4 Ne  | twork Object Groups  |             |             |                |
| = 46       | All-Inte             | - 50 - 5    |             |                |
|            | S Inte 172.16.11.10  | 255.255.255 | N           |                |
|            | S Inte 172.16.11.12  | 255,255,255 |             |                |
|            | S Inte 172.16.11.15  | 255.255.255 |             |                |
|            | Inte 172.16.11.24    | 255.255.255 |             |                |
|            | Inte 172.16.11.26    | 255.255.255 |             |                |
|            | Inte 172.16.11.32    | 255.255.255 |             |                |
| ∃-Interfac | Des                  |             |             |                |
| - 23       | DMZ                  |             |             |                |
| - 00       | inside               |             |             |                |
|            | manage               |             |             |                |
| - 1251     | outside              |             |             |                |
|            |                      |             |             | С              |
| 🔂 Edi      | t Access Rule        |             |             |                |
| 2.2.6      | 1.14                 |             |             |                |
| Action     | Ce: Inside           |             |             |                |
| ACCON      | Perilic Oberly       |             | -           |                |
| Source     | : All-Internal-Hosts | ,           | -           |                |
| Destin     | ation any            |             |             |                |
| Service    | e: ip                |             |             |                |
|            |                      |             | Server.     |                |
| Descrip    | otion:               |             |             |                |
| E En       | able Logging         |             |             |                |
|            | aning Laugh Default  | -           |             |                |
| LOG        | gging Level: Derauk  |             |             |                |
| 1.000      | Ontions              |             |             |                |
| More       | c opcions            |             |             |                |
| More       | coptions             |             |             |                |
| More       | - options            |             | Cancel      |                |

11. Hover your mouse over the Source field of the access rule in order to view the members of

|            | Configur | ation > Fire   | wall > Access Ru      | kes<br>X 🗈 🏬 - Q Find 🖭 Dia    | igram 🎧 Export 👻 | 😚 Clear Hits |
|------------|----------|----------------|-----------------------|--------------------------------|------------------|--------------|
|            | #        | Enabled        | Source                | Destination                    | Service          | Action       |
|            | e 🔊 o    | MZ (2 implicit | incoming rules)       |                                |                  |              |
|            | 1        |                | 🥥 any                 | Any less secure ne             | . <u></u> ip     | 🖌 Permit     |
|            | 2        |                | 🧼 any                 | <ul> <li>any</li> </ul>        |                  | 🕴 Deny       |
|            | 🖨 🔊 ir   | nside (3 incom | ing rules)            |                                |                  |              |
|            | 1        | <b>V</b>       | 3 172.16.2.10         | iany                           | Allow-Ports      | 🖌 Permit     |
|            | 2        |                | Al-Internal-H         | osts \land any                 | IP (p            | 🖌 Permit     |
|            | 3        |                | 🍅 any                 | Internal-10 env                | æ ip             | 🕴 Deny       |
|            | 🖨 🥵 n    | anage (2 imp   | licit incoming rules) | Internal-12                    |                  |              |
|            | 1        |                | <li>any</li>          | Internal-15 Any less secure ne | . <u>IP</u> ip   | 🖌 Permit     |
|            | 2        |                | 🌍 any                 | Internal-26 any                | 1E> ip           | 🕲 Deny       |
|            | E        | utside (4 inco | ming rules)           | Internal-32                    |                  |              |
| the group. | 11       |                | any                   | <b>I</b> 192 168 5 3           | ter smin         | A Permit     |

#### Edit the Source Port:

Complete these steps in order to modify the source port of an access rule.

1. In order to modify the source port of an existing access rule, right-click it, and choose **Edit**. The Edit Access Rule window appears.

| £        | Enabled       | Source                | Destination        | Service     | Action        | Hits  | Logging |
|----------|---------------|-----------------------|--------------------|-------------|---------------|-------|---------|
| M DMZ    | (2 implicit i | incoming rules)       |                    |             |               |       |         |
| L        |               | any                   | Any less secure ne | 11 ip       | Permit        |       |         |
| 2        |               | any any               | i any              | IP ip       | 3 Deny        |       |         |
| 5 insid  | le (4 incomi  | ng rules)             | - 60 - 14<br>-     |             | 10.00         |       |         |
| 1.       | ~             | 3 172.16.2.10         | i any              | Allow-Ports | 🖌 Permit      | 0     |         |
| 2        | V             | Al-Internal-Hosts     | iany any           | II- Ip      | 🖌 Permit      | 0     |         |
| 3 -      | - <u>-</u>    | 172.16.2.5            | 200.10.10.10       | 🕩 ip        | Permit 🖉      | 0     | 1. E    |
| 4        | 🕵 Edit        | Access Rule           |                    |             |               |       | 1       |
| 1        | Interfac      | e: incide             |                    |             |               |       |         |
| 2        | Ashien        | O Durant O Duran      |                    |             |               |       |         |
| 🔊 outs   | Action:       | • Permit O Deny       |                    |             |               |       |         |
| Ω        | Source:       | 172.16,2.5            |                    | 9           |               |       |         |
| 2        | Destinat      | tion 200.10.10.10     |                    | -           |               |       |         |
| 3        | Concerned in  |                       |                    |             |               |       |         |
| 4        | Service:      | tcp                   |                    |             |               |       |         |
|          | Descript      | ion                   |                    |             |               |       |         |
|          | - Design      | and to                |                    |             |               |       |         |
|          |               | ble Loading           |                    |             |               |       |         |
|          | [V] cild      | tie Logging           |                    |             |               |       |         |
|          | Logo          | ping Level: Default   | ~                  |             |               |       |         |
|          | More          | Ontions               |                    |             |               |       | 6       |
|          | E les         | while Out             |                    |             |               |       | 6       |
|          | M.C.          | able Kule             |                    |             |               |       |         |
|          | Traffic       | Direction: 🛞 In 🔅     | out                |             |               |       |         |
|          | Source        | e Service: tcp/ftp    |                    | (TCP of     | r UDP service | only) |         |
|          | 1.000         |                       | 10                 |             |               | 8876  |         |
| ess Rule | 10031         | g Interval: [300] sec | -000s              |             |               |       |         |
|          | Time F        | Range: 🗹              |                    |             |               |       |         |

2. Click the **More Options** drop-down button in order to modify the Source Service field, and click **OK**.You can view the modified access rule, as

|   |   | The The Tole To    | 🥪 any        | Alow-Ports | V Permit | 0 |
|---|---|--------------------|--------------|------------|----------|---|
| 2 | ~ | All-Internal-Hosts | 🎱 any        | IP ip      | 🖌 Permit | 0 |
| 3 |   | 172.16.2.5         | 200.10.10.10 | tcp        | 🥩 Permit | 0 |
| 4 |   | 🏈 any              | 🏟 any        | 🗶 ip       | 🕴 Deny   |   |

#### **Delete an Access List**

Complete these steps in order to delete an access list:

1. Before you delete an existing access list, you need to delete the access list entries (the access rules). It is not possible to delete the access list unless you first delete all of the

access rules.Right-click the access rule to be deleted, and choose **Delete**.

| 1 | ~        | 🏈 an | iy       | 📑 192                  | 2.168.5.3 | 📧 smtp    | V Pi |
|---|----------|------|----------|------------------------|-----------|-----------|------|
| 2 | <b>Z</b> | 🧐 ar | л        | Add Assess Duly        |           | TCP https | V P  |
| 3 |          | 🌍 ar |          | Add Access Rule        |           | 🚾 domain  | V Pi |
| 4 | 4        |      | <u>中</u> | Insert<br>Insert After |           | IP/ ip    | 😮 D  |
|   |          | 1    | đ        | Edit                   |           |           |      |
|   |          |      | Î        | Delete                 |           |           |      |
|   |          |      | ж        | Cut                    | Ctrl+X    |           |      |

2. Complete the same Delete operation on all the existing access rules, and then select the access list and choose **Delete** in order to delete it.

#### **Export the Access Rule**

ASDM access rules bind the access list with the respective interface while ACL Manager tracks all extended access lists. The access rules that are created with the ACL Manager do not bind to any interface. These access lists are generally used for the purpose of NAT-Exempt, VPN-Filter and similar other functions where there is no association with the interface. ACL Manager contains all the entries that you have in the **Configuration > Firewall > Access Rules** section. In addition, **ACL Manager** does also contain the global access rules that are not associated to any interface. ASDM is organized in such a way that you can export an access rule from any access list to another one with ease.

For example, if you need an access rule that is already a part of a global access rule to be associated with an interface, you do not need to configure that again. Instead, you can perform a **Cut & Paste** operation to achieve this.

1. Right-click the specified access rule, and choose

| No    | Address                     |         | Action  | हे जाहे  | Description |  |  |  |
|-------|-----------------------------|---------|---|----------|-------------|--|--|--|
| E 100 | (Meleonologica              |         | 11100000                                      | 9 - A 18 |             |  |  |  |
| 1     | Ⅰ 172.16.1.11 Ⅰ 172.16.1.14 | 4 4 4 4 | Add ACL<br>Add ACE<br>Insert<br>Insert After. |          |             |  |  |  |
|       |                             |         | Edit<br>Delete                                |          |             |  |  |  |
|       |                             | Ba      | Сору  | Сору     |             |  |  |  |
|       |                             |         | Paste   |          | Ctrl+¥      |  |  |  |
|       |                             | 100     | Tanata Afran                                  |          |             |  |  |  |

#### Cut.

2. Select the required access list into which you need to insert this access rule. You can use **Paste** in the tool bar to insert the access rule.

#### **Export the Access List Information**

You can export the access list information to another file. Two formats are supported to export this information.

- 1. Comma Separated Value (CSV) format
- 2. HTML format

Right click any of the access rules, and choose **Export** in order to send the access list information to a file.



Here is the access list information shown in HTML format.

| # Enable  | ed Source              | Destination              | Service     | Action | Hits | Logging | Time | Description   |
|-----------|------------------------|--------------------------|-------------|--------|------|---------|------|---|
| DMZ (2    | incoming rules)        |                          |             |        |      |         |      |   |
| 1 True    | 172.16.1.10            | any                      | ip          | Permit |      | Default |      |   |
| 2         | any                    | any                      | ip          | Deny   |      | Default |      | Implicit rule   |
| inside (3 | incoming rules)        |                          |             |        |      |         |      |   |
| 1 True    | 172.16.2.10            | any                      | Allow-Ports | Permit | 0    | Default |      |   |
| 2 True    | All-Internal-Hosts     | any                      | ip          | Permit | 0    | Default |      |   |
| 3         | any                    | any                      | ip          | Deny   |      | Default |      | Implicit rule   |
| manage (  | 2 implicit incoming ru | ıles)                    |             |        |      |         |      |   |
| 1         | any                    | Any less secure networks | ip          | Permit |      | Default |      | Implicit rule: Permit all traffic to less secure networks |
| 2         | any                    | any                      | ip          | Deny   |      | Default |      | Implicit rule   |
| outside ( | 4 incoming rules)      |                          |             |        |      |         |      |   |
| 1 True    | any                    | 192.168.5.3              | tcp/smtp    | Permit | 0    | Default |      |   |
| 2 True    | any                    | 192.168.5.5              | tcp/https   | Permit | 0    | Default |      |   |
| 3 True    | any                    | 192.168.5.4              | tcp/domain  | Permit | 0    | Default |      |   |
| 4         | any                    | any                      | ip          | Deny   |      | Default |      | Implicit rule   |

## **Verify**

There is currently no verification procedure available for this configuration.

## **Troubleshoot**

There is currently no specific troubleshooting information available for this configuration.

## **Related Information**

- ASDM Configuration Examples and TechNotes
- ASA Configuration Examples and Technotes
- <u>Technical Support & Documentation Cisco Systems</u>