

CHAPTER 11

Firewall Configuration

Setting Policies Using RF Director

Aliases

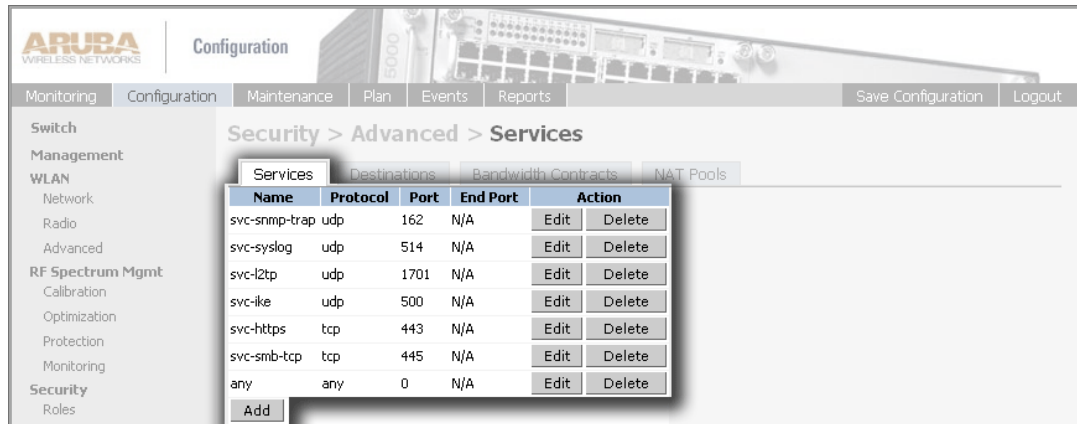
Aliases are a convenient way to associate a human understandable name with a specific object. AirOS enables administrators to assign easily understandable names to network ports (services) and specific IP Addresses or groups of IP Addresses

Defining Service Aliases

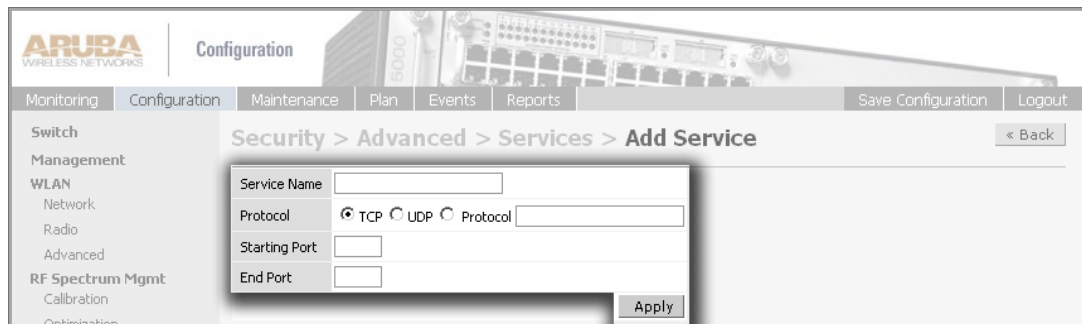
Service aliases apply to protocol/port numbers. Service aliases may be configured in RF Director.

Normally only one alias need be defined for a particular service, however some services use more than one protocol. In the case where a service uses multiple protocols, a separate alias must be defined for each protocol.

Navigate to the Configuration > Security > Advanced > Services page.



Add a new Service Alias. Click the Add button. The Add Service page will appear.



The options and parameters available for configuration on the Add Service page are:

- Service Name A plane language name that identifies the alias.

NOTE—Default service aliases begin with *svc-* followed by the name of the protocol.

- Protocol Specify the protocol, either by using the radio buttons or by entering the protocol number (0 - 255).

- Starting Port Sets the lower port number of a protocol port range.

- End Port Sets the upper port number of a protocol port range.

NOTE—If the service uses a single port, enter the starting port number here also.

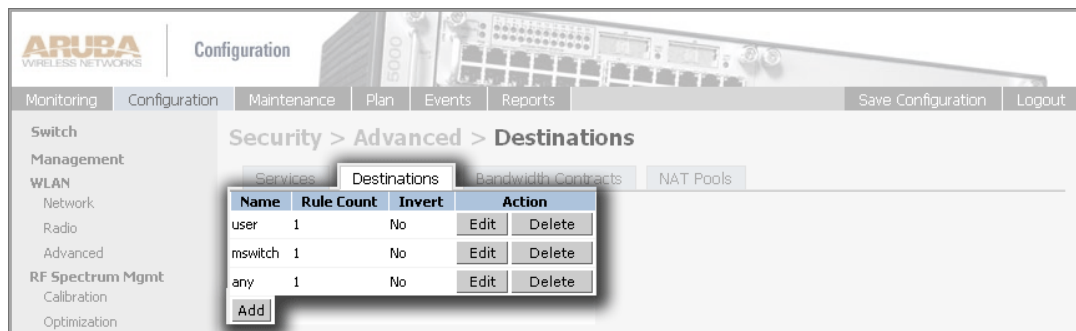
- 1 Enter a name in the Service Name text field.
- 2 Check the appropriate Protocol radio button.
- 3 Enter the Starting Port.
- 4 Enter the End Port (If this service uses only a single port, enter the starting port number here).
- 5 Click Apply and Save Configuration

Defining Source and Destination Aliases

Source and destination aliases may be configured in RF Director.

Source and destination aliases apply to specific IP addresses or groups of IP addresses. The alias is a convenient method to identify these addresses in easily readable way. They are used with traffic policies to specify the source or destination of a packet.

Navigate to the Configuration > Security > Advanced > Destinations page.

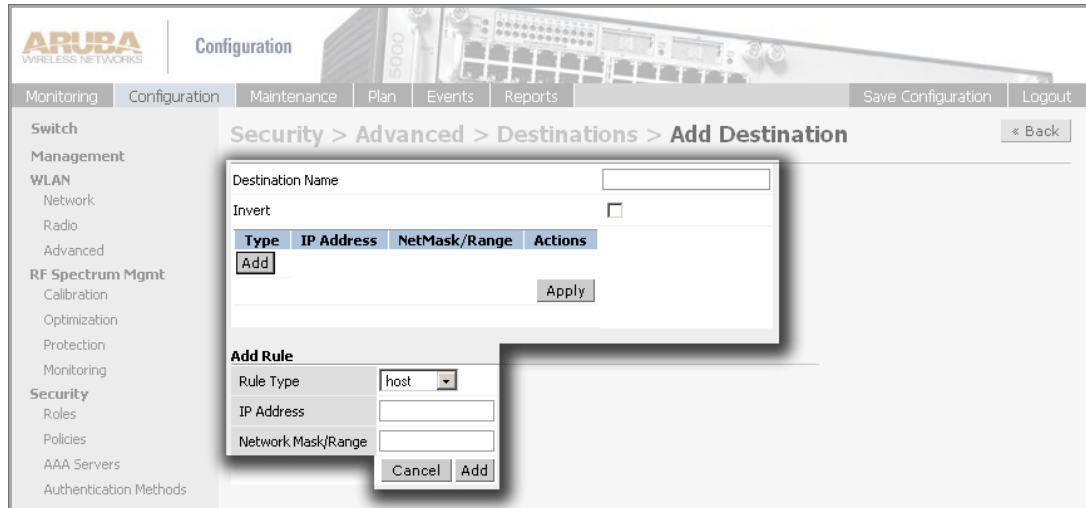


You may add, delete, or modify source and destination aliases on this page.

Aruba provides 3 pre-defined aliases which should not be altered or deleted.

- User
When applied to an authenticated user the alias is replaced by an IP Address assigned to that user.
- Mswitch
Represents the IP Address, loopback address, or VLAN 1 address of the switch upon which the policy is running.
- Any
Represents any IP Address

Add a new alias by clicking the Add button, the Add Destinations page appears.



- 1 Click the Add button to expand the page and expose the Add Rule section, near the bottom.
- 2 Enter a name for the new destination in the Destination Name text box.
- 3 Select a rule type using the Rule Type pull-down menu.

The choices for rule types are:

- Host Use this selection to specify a single address. Do not enter anything in the Network Mask/Range field.
 - Network Use this selection when specifying an IP subnet. It comprises a
 - Range Use this selection when specifying a sequential range of IP Addresses. When specifying a range enter the upper address in the Network Mask/Range field.
- The maximum number of addresses is 16 when specifying a range.

- 4 Enter an IP Address in the IP Address field.
- 5 Enter a netmask or upper address of an IP range in the Network Mask/Range field.

NOTE—If you wish to specify a range with more than 16 addresses, select the Network Rule Type then enter network number and subnet mask in the IP Address and Network Mask fields.

- 6 Click Add, then click Apply and Save Configuration.

Firewall Policies

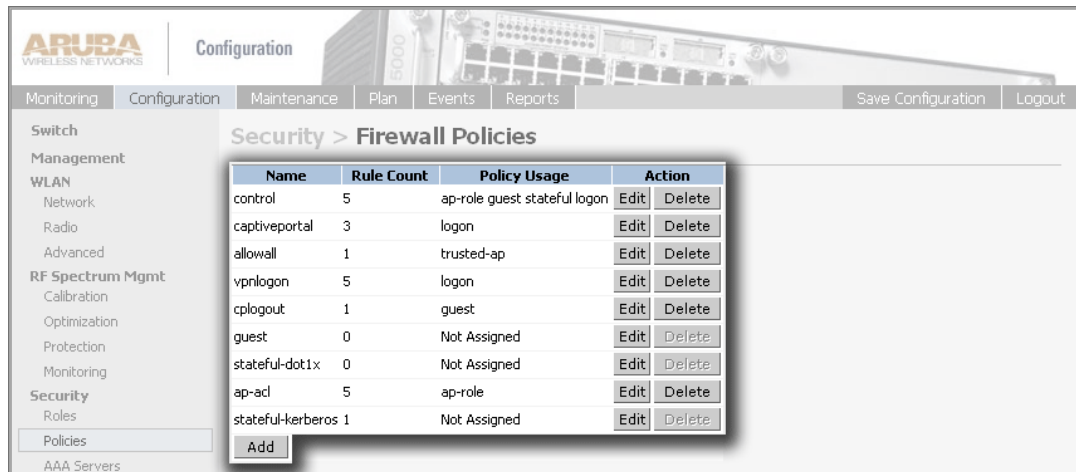
Aruba AirOS firewall policies are stateful and bi-directional. Stateful policies mean that when a packet matches a rule, they must match exactly, the policy will create a session entry so that the session may continue in both directions.

Firewall policies consist of a set of rules that are applied in a specific order against network traffic presented at the firewall. The rule at the top of the list is applied first.

Rules are organized in top-down lists where the first rule applied to the traffic is at the top of the list. Traffic is tested against each rule in order until a match is found. When a match occurs the rule is applied and no other testing occurs.

Policies can be applied to physical ports or to user roles.

Navigate to the Configuration > Security > Policies page.



Name	Rule Count	Policy Usage	Action
control	5	ap-role guest stateful logon	Edit Delete
captiveportal	3	logon	Edit Delete
allowall	1	trusted-ap	Edit Delete
vpnlogon	5	logon	Edit Delete
cplogout	1	guest	Edit Delete
guest	0	Not Assigned	Edit Delete
stateful-dot1x	0	Not Assigned	Edit Delete
ap-acl	5	ap-role	Edit Delete
stateful-kerberos	1	Not Assigned	Edit Delete

From the Firewall Policies page you may Edit, Delete, or Add policies.

Rules in Firewall Policies.

Rules in firewall policies are applied to traffic that presents itself to the switch. Rules examine the source address, destination address, and the kind of information (service) the packet contains.

The Source and Destination elements of a rule have the same 5 options. Those options are:

- any This option will test true for traffic from any source or to any destination.
- user This option will test true only for traffic to or from a known user.
- host This option will test true only for traffic to or from a specific IP Address.
- network This option will test true only for traffic to or from a network specified by a network address and subnet mask
- alias This option will test true only for traffic to or from the address or addresses defined in a specified alias, see [“Defining Source and Destination Aliases”](#) on page 191.

The Service element of a rule has 5 options. Those options are:

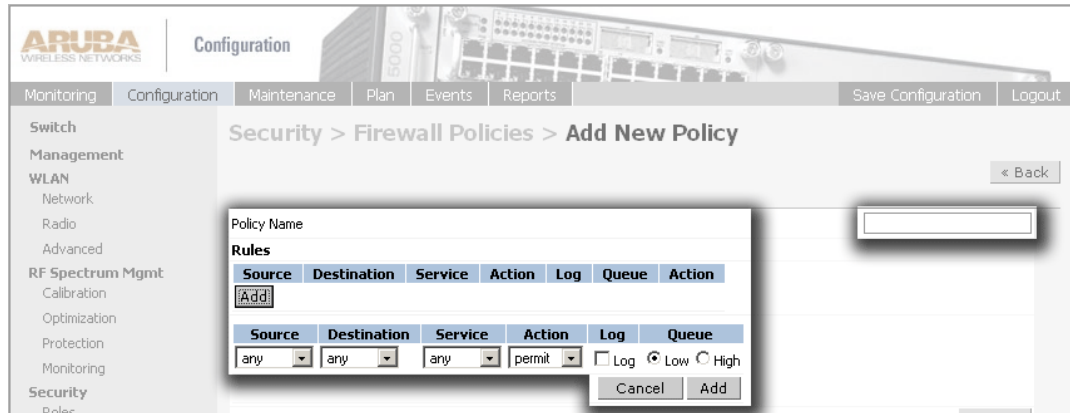
- any This option will test true for any type of traffic.
- tcp This option will test true for only tcp traffic.
- udp This option will test true for only udp traffic..
- service This option will test true for only traffic to or from a specified service alias.
- protocol This option will test true for only traffic with a specified protocol number.

The Action element of a rule has 5 options. Those options are:

- Permit Forward the packet without modification.
- Deny Drop the packet with no notification.
- src-nat Change the source IP address of the packet and forward it. If no source NAT pool is specified the IP address of the Aruba switch will be substituted for the original source address.

- dst-net Change the destination IP address of the packed and to the switch IP address and forward it.
- redirect

Add a policy by clicking on the Add button, the Add New Policy page appears.



The Add New Policy page is where you name your new policy and define rules for that policy.

- 1 Enter a meaningful name in the Policy Name field at the right hand side of the page.
- 2 Select a traffic source from the Source pull-down menu.
- 3 Select a traffic destination from the Destination pull-down menu.
- 4 Select an action from the Action pull-down menu.
- 5 Select Log in you wish each packet matching this rule to be recorded in the system logfile.
- 6 Set a queue priority, high or low by selecting the cooresponding Queue radio button.
Queue priority sets the priority of outbound wireless traffic.
- 7 Click Add.
- 8 When you are done adding rules, click Apply and Save Configuration.

Applying Policies to Physical Ports

Policies may be applied to either physical ports or user roles.

Navigate to the Configuration > Switch > Port page.

The screenshot shows the Aruba Configuration interface for the 'Switch > Port' page. The 'Port Selection Options' section includes radio buttons for 'Administrative State', 'Operational State', 'Port Mode', 'VLAN Association', and 'Trusted'. The 'Port Selection' section displays a grid of port checkboxes, with port 1 selected. The 'Configure Selected Ports' section is highlighted with a red zigzag line and contains the following options:

- Enable Port:
- Enable 802.3af Power Over Ethernet:
- Enable Cisco Power Over Ethernet(Enabling this option will disable 802.3af Power Over Ethernet):
- Make Port Trusted:
- Port Mode: Access Trunk
- Enter VLAN(s):
- Firewall Policy:
- Enable MUX:

An 'Apply' button is located at the bottom right of the 'Configure Selected Ports' section.

Select the port to which you wish to apply a policy, then use the pull-down menu to select a policy to apply.

Click Apply and Save Configuration.

Defining Roles Using RF Director

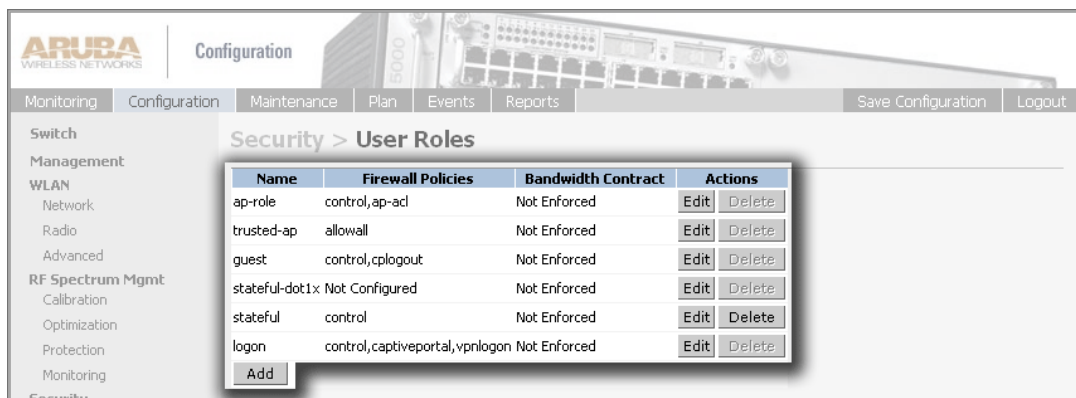
Role Design

A role is assigned to a user when they connect to the network, and possibly again after they are authenticated.

Roles determine what network resources the user may access. Roles may be very broad-based, allowing access to many resources or they may be very narrow in scope, allowing access to very limited resources. Sometimes, a role is used to grant a particular user, or group of users, access to a specific resource that other users are not.

Configuring Roles

Navigate to the Configuration > Security > Roles page to view roles.



Name	Firewall Policies	Bandwidth Contract	Actions
ap-role	control,ap-acl	Not Enforced	Edit Delete
trusted-ap	allowall	Not Enforced	Edit Delete
guest	control,cplogout	Not Enforced	Edit Delete
stateful-dot1x	Not Configured	Not Enforced	Edit Delete
stateful	control	Not Enforced	Edit Delete
logon	control,captiveportal,vpnlogon	Not Enforced	Edit Delete

Add

Click the Add button to begin adding a new role to the list. The Add Role page will appear.

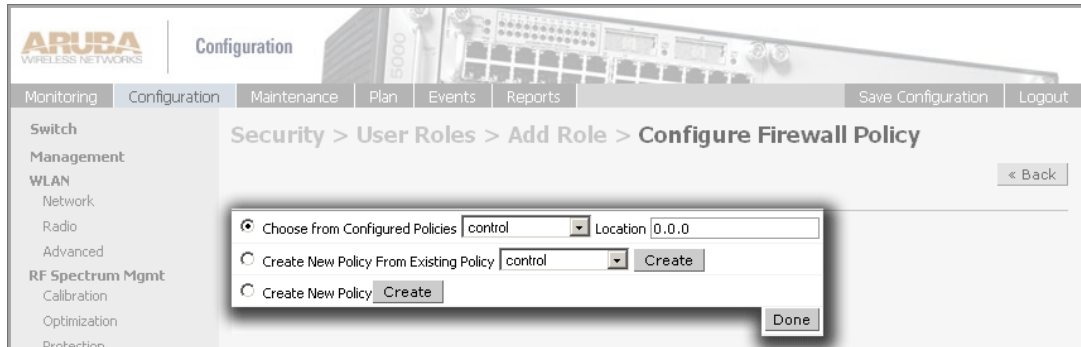
The screenshot shows the Aruba Configuration web interface. The breadcrumb path is **Security > User Roles > Add Role**. A navigation bar at the top includes **Monitoring**, **Configuration**, **Maintenance**, **Plan**, **Events**, **Reports**, **Save Configuration**, and **Logout**. A left sidebar lists various configuration categories: **Switch Management**, **WLAN** (Network, Radio, Advanced), **RF Spectrum Mgmt** (Calibration, Optimization, Protection, Monitoring), **Security** (Roles, Policies, AAA Servers, Authentication Methods, VPN Settings, Advanced), and **WLAN Intrusion Detection** (Rogue AP, Denial of Service, Man-In-the-Middle, Signatures, Policies). The main content area is titled **Add Role** and contains the following configuration sections:

- Role Name:**
- Firewall Policies:** A table with columns **Name**, **Rule Count**, **Location**, and **Action**. An **Add** button is located below the table.
- Re-authentication Interval:** Disabled **Change** (0 disables re-authentication. A positive value enables authentication)
- Role VLAN ID:** Not Assigned **Change**
- Bandwidth Contract:** Not Enforced **Change**
- VPN Dialer:** Not Assigned **Change**
- L2TP Pool:** Not Assigned **Change**
- PPTP Pool:** Not Assigned **Change**

At the bottom of the form, there is a **Commands** section with a **View Commands** link and an **Apply** button.

Adding Firewall Policies

Add firewall policies, begin by clicking the Add button under the Firewall Policies header on the page. The Configure Firewall Policy page then appears.



You may choose one of three options on this page:

- Specify an existing policy.
- Create a new policy using an existing policy as a model.
- Create a new policy from scratch.

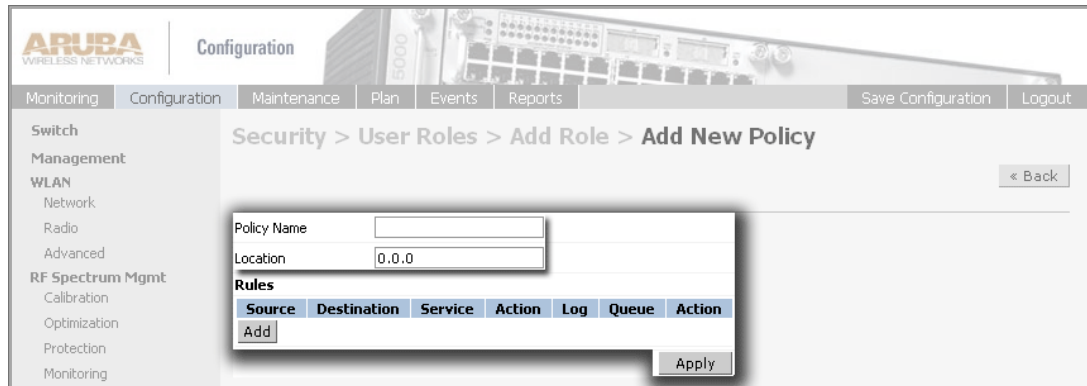
Specify an existing policy.

- 1 Select the Choose from Configured Policies radio box.
- 2 Specify a particular AP (if you wish to apply this policy only when using the specified AP) by entering the its location in the Location text box.
- 3 Click Done.

Create a New Policy From an Existing Policy

- 1 Select the Create New Policy From Existing Policy radio button.

- 2 Click the **Creat** button. The **Add New Policy** page appears.



- 3 Create a new policy in exactly the same way you would in **“Firewall Policies”** on [page 193](#).

Create a New Policy from Scratch

- 1 Select the **Create New Policy** radio button.
- 2 Click **Create**. The **Add New Policy** page appears.
- 3 Create a new policy in exactly the same way you would in **“Firewall Policies”** on [page 193](#).

Configuring Other Policy Options

In addition to creating new policies for a role, you may add or adjust 6 additional options.

- **Re-authentication Interval** By default a user will remain authenticated until the login session is terminated. Use this option to force periodic re-authentication.
- **Role VLAN ID** When a VLAN is specified for this option, the user will be mapped to that VLAN.
NOTE—This option only applies if authentication is done at Layer 2.
- **Bandwidth Contract** This option applies a bandwidth contract to the role.
- **VPN Dialer** Use this option to assign a specific VPN dialer to a user role. For more information about configuring VPN dialers, see [“VPN Configuration”](#) on page 207.
- **L2TP Pool** Use this option to specify the address pool from which a VPN user will be assigned an IP address when the user negotiates an L2TP/IPSEC session. For more information see [“VPN Configuration”](#) on page 207.
- **PPTP Pool** Use this option to specify the address pool from which a VPN user will be assigned an IP address when that user negotiates a PPTP session. For more information see [“VPN Configuration”](#) on page 207.

Setting Policies Using the CLI

This portion of the chapter describes the process of configuring firewall (traffic) policies using the Command Line Interface. The processes described here mirror the processes in the first part of the chapter which describes firewall configuration using RF Director, a web-based graphical user interface.

Defining Service Aliases

Define a service alias using the `net service <name> {ProtocolNum | TCP <startAddr> <endAddr> | UDP <startAddr> <endAddr>}` command from the CLI.

You may define a service alias by giving it a name, then choosing to specify one of three options:

- **UDP** Use this option to specify UDP as the service. Specify a port for the service by including a single value after the UDP specifier or a range of ports by including two values representing *startAddr* and *endAddr*. The valid range for ports is 0-65535.
- **TCP** Use this option to specify TCP as the service. Specify a port for the service by including a single value after the UDP specifier or a range of ports by including two values representing *startAddr* and *endAddr*. The valid range for ports is 0-65535.
- **Protocol Number** Use this option to specify the service by its protocol number. No port or port range may be specified when using this option.

Define the service alias.

```
(Aruba) (config) #net service svc-foo-udp udp 7066 7165
(Aruba) (config) #net service svc-foo-tcp tcp 10555
(Aruba) (config) #net service svc-foo-chaos 16
```

The current service alias configurations may be viewed using the `show netservice` command from the CLI.

```
(Aruba) (config) #show netservice

Services
-----
Name          Protocol  Ports
-----
svc-snmp-trap  udp      162
svc-syslog     udp      514
svc-l2tp       udp      1701
svc-ike        udp      500
svc-https      tcp      443
svc-smb-tcp    tcp      445
svc-dhcp       udp      67 68
.
.
.
```

Defining Source and Destination Aliases

Define a source/destination alias and enter the config-dest mode using the `netdestination <name>` command from the CLI.

After entering the config-dest mode you may specify one of 3 types of destinations for your alias:

- **host** Use this command to specify a specific host IP address for the alias.
- **network** Use this command to specify a network or sub-net as a source or destination. Specify a network number followed by a subnet mask.
- **range** Use this command to specify a range of valid IP addresses. Specify the lower address followed by the higher.

- 1 Enter the config-dest mode and define the name for the alias

```
(Aruba) (config) #netdestination dest-foo-any
```

- 2 Configure the alias as host with an IP address of 192.196.10.200.

```
(Aruba) (config-dest) #host 192.196.10.200
```

Firewall Policies

Firewall policies are configured using the `ip access-list session <name>` command from the CLI.

- 1 Enter the `config-sess-aclname` mode.

```
(Aruba) (config) #ip access-list session foo-acl
(Aruba) (config-sess-foo-acl)#
```

- 2 Enter rules in the order you wish them to be applied.

```
(Aruba) (config-sess-foo-acl)# user alias Int_net svc-dhcp permit
(Aruba) (config-sess-foo-acl)# user alias Int_net svc-dns permit
(Aruba) (config-sess-foo-acl)# user any svc-http permit
(Aruba) (config-sess-foo-acl)# user any svc-https permit
(Aruba) (config-sess-foo-acl)# user any svc-ike permit
(Aruba) (config-sess-foo-acl)# user any any deny
```

If you wish to change the position of a rule in the list, use the `position` option to move the rule to a specific line.

```
(Aruba) (config-sess-foo-acl)# user any svc-ike permit position 3
```

Use the `show access-list <aclName>` command from the CLI to view a specific firewall policy.

Use the `show access-list brief` command to see a listing of the current ACLs

```
(Aruba) (config) #show access-list brief

Access list table
-----
Name          Type      Use Count  Roles
-----
control       session   4          logon ap-role stateful guest
captiveportal session   1          logon
allowall      session   1          trusted-ap
vpnlogon      session   1          logon
cplogout      session   1          guest
guest         session   0
stateful-dot1x session   0
ap-acl        session   1          ap-role
stateful-kerberos session   0
```


Applying Policies to Physical Ports

Add a policy to a specific port from the CLI using the `interface fastethernet` mode commands.

- 1 Enter the `config-if` mode.

```
(Aruba) (config) #interface fastethernet 1/22
(Aruba) (config-if)#
```

- 2 Assign a policy to a the port used when entering the `config-if` mode.

```
(Aruba) (config-if)#ip access-group guest session
```

Defining Roles Using the CLI

Configuring Roles

Roles are configured in the CLI using the `config-role` mode commands.

Define a user role and enter the `config-role` mode.

```
(Aruba) (config) #user-role foo-user
(Aruba) (config-role) #
```

Begin to enter the role parameters.

```
(Aruba) (config-role) #dialer default-dialer
(Aruba) (config-role) #pool pptp-pool-1
```

Defining Access Control Lists in the CLI

ACL are applied to physical interfaces using the `ip access-group` command in the CLI.

```
(Aruba) (config) #ip access-list standard foo-1
(Aruba) (config-std-foo-1)#
```

Standard ACLs

Create standard ACLs using the `standard` option of the `access-list` command.

```
(Aruba) (config-std-foo-1)# permit 192.168.10.0 255.255.255
(Aruba) (config-std-foo-1)# permit host 192.168.20.15
(Aruba) (config-std-foo-1)# deny any
```

Extended ACLs

Create extended ACLs using the `extended` option of the `access-list` command.

```
(Aruba) (config) #ip access-list extended foo-ext-1
(Aruba) (config-ext-foo-ext-1)# permit tcp any host 1.1.1.1 range
67 69
(Aruba) (config-ext-foo-ext-1)#permit icmp 1.1.1.0 0.0.0.255 any
echo-reply
```

MAC ACLs

Create MAC ACLs using the `mac` option of the `access-list` command.

```
(Aruba) (config) #ip access-list mac foo-mac-1
(Aruba) (config-mac-foo-mac-1)# permit host 00:01:01:03:04:05
(Aruba) (config-mac-foo-mac-1)# permit 00:0a:ff:02:ad:01
ff:ff:ff:00:00:00
```

Ethertype ACLs

Create Ethertype ACLs using the `eth` option of the `access-list` command.

```
(Aruba) (config) #ip access-list eth foo-eth-1  
(Aruba) (config-eth-foo-eth-1)# permit 2048
```

