Using and Configuring PIX/ASA Object Groups

Document ID: 25700

Introduction

This document discusses object groups, a feature introduced in PIX code version 6.2. Object grouping allows objects such as IP hosts or networks, protocols, ports, and Internet Control Message Protocol (ICMP) types to be collected into object groups. Once configured, an object group can then be used with the standard **conduit** or **access–list** PIX commands in order to reference all objects within that group. This reduces the configuration size.

Note: You cannot rename the object groups. You need to delete them and apply them again with the changes.

Note: Once the access–list is created with object groups, it must be applied to the interface with the **access–group** command.

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 PIX Software Release 6.2(2) and later
- Cisco 515 PIX Firewall (any PIX model works with these configurations)
- Cisco ASA with Software release 7.0 and later

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.

Related Products

The information in this document is also applicable to the Cisco 5500 Series Adaptive Security Appliance (ASA) that runs software version 7.0 and later.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Use Object Groups

When you use an object group within a command, you must use the keyword **object−group** before the group name, as shown in this example.

```
access-list 100 permit object-group protocols object-group
   remotes object-group locals object-group services
```

In this example, protocols, remotes, locals, and services are previously defined object group names. Object groups can also be nested, where you can include one object group as a subset of another object group.

The command set is shown in this output.

```
object-group grp_id

object-group description description_text

group-object object_grp_name


object-group icmp-type grp_id

icmp-object icmp_type


object-group network grp_id

network-object host host_addr

network-object net_addr netmask

object-group protocol grp_id

protocol-object protocol


object-group service grp_id {tcp|udp|tcp-udp}

port-object eq service

port-object range begin_service end_service
```

Configure Object Groups

ICMP−Type Configuration

The ICMP−type object group is used in order to specify specific ICMP types for use only with ICMP access control lists (ACLs) and conduits. A full list of ICMP types is located in the PIX command reference for the

object–group command.

```
(config)#object-group icmp-type icmp-allowed
(config-icmp-type)#icmp-object echo
(config-icmp-type)#icmp-object time-exceeded
(config-icmp-type)#exit

(config)#access-list 100 permit icmp any any object-group icmp-allowed
```

Network Configuration

Use the network object group in order to specify host IP addresses or subnet ranges that you want to define in an ACL or conduit. Host IP addresses are prefixed with the keyword **host**, and can be either an IP address or a hostname already defined with the **name** command. You can use this object group as either the source or destination in the associated ACL/conduit.

```
(config)#names
(config)#name 10.1.1.10 myFTPserver

(config)#object-group network ftp_servers

(config-network)#network-object host 10.1.1.14
(config-network)#network-object host myFTPserver

(config-network)#network-object 10.1.1.32 255.255.255.224
(config-network)#exit

(config)#access-list 101 permit ip any object-group ftp_servers
```

If this list consists only of FTP servers, this specific example applies.

```
(config)#access-list 101 permit tcp any object-group ftp_servers eq ftp
```

Protocol Configuration

Use the protocol object group in order to specify a protocol(s) that you want to define in an ACL or conduit. You can use this object group as the protocol type only in the associated ACL or conduit. Note that the allowed protocols for this object group are only the standard PIX protocol names allowed in an **access–list** or **conduit** command, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Generic Routing Encapsulation (GRE), Enhanced Interior Gateway Routing Protocol (EIGRP), Encapsulating Security Payload (ESP), Authentication Header (AH), and so on. Protocols that sit on top of TCP or UDP cannot be specified with a protocol object group. Instead, these protocols use an object group, as shown in this example.

```
(config)#object-group protocol proto_grp_1

(config-protocol)#protocol-object udp
(config-protocol)#protocol-object tcp
(config-protocol)#protocol-object esp
(config-protocol)#exit

(config)#access-list 102 permit object-group proto_grp_1 any any
```

Service Configuration

Use the service object group in order to specify specific or ranges of TCP and/or UDP ports that you want to define in an ACL or conduit. You can use this object group as either the source port(s) or destination port(s) in the associated ACL/conduit, as shown in this example.

```
(config)#object-group service allowed_prots tcp
(config-service)#port-object eq ftp
(config-service)#port-object range 2020 2021
(config-service)#exit

(config)#object-group service high_ports tcp-udp
(config-service)#port-object range 1024 65535
(config-service)#exit

(config)#access-list 103 permit tcp any object-group
        high_ports any object-group allowed_prots
```

Note: Enhanced service object–groups were introduced with the release of software version 8.0. Enhanced service object–groups enable the ASA/PIX to combine IP protocols together in the same service group, which eliminates the need for protocol and icmp–type specific object groups. The protocol type must not be specified in order to configure an enhanced service object–group.

```
(config)#object-group service RTPUsers
(config-service)#service-object icmp echo-reply
(config-service)#service-object icmp echo
(config-service)#service-object tcp http
(config-service)#service-object tcp https
(config-service)#service-object tcp http
(config-service)#service-object tcp pptp
(config-service)#service-object udp domain
(config-service)#service-object udp isakmp
(config-service)#service-object esp
(config-service)#service-object gre
(config-service)#exit
(config)#access-list acl_inside permit object-group RTPUsers 192.168.50.0
255.255.255.0 any
(config)#show access-list acl_inside
access-list acl_inside line 1 extended permit object-group RTPUsers
192.168.50.0 255.255.255.0 any
access-list acl_inside line 1 extended permit icmp
192.168.50.0 255.255.255.0 any echo-reply (hitcnt=0)
access-list acl_inside line 1 extended permit icmp
192.168.50.0 255.255.255.0 any echo (hitcnt=0)
access-list acl_inside line 1 extended permit tcp
192.168.50.0 255.255.255.0 any eq www (hitcnt=0)
access-list acl_inside line 1 extended permit tcp
192.168.50.0 255.255.255.0 any eq https (hitcnt=0)
access-list acl_inside line 1 extended permit udp
192.168.50.0 255.255.255.0 any eq domain (hitcnt=0)
access-list acl_inside line 1 extended permit esp
192.168.50.0 255.255.255.0 any (hitcnt=0)
access-list acl_inside line 1 extended permit gre
192.168.50.0 255.255.255.0 any (hitcnt=0)
access-list acl_inside line 1 extended permit udp
192.168.50.0 255.255.255.0 any eq isakmp (hitcnt=0)
access-list acl_inside line 1 extended permit tcp
192.168.50.0 255.255.255.0 any eq pptp (hitcnt=0)
```

Object–Group Nesting Configuration

Only object groups of the same type can be nested within another. For example, you cannot nest a protocol–type object group within a network–type object–group.

In order to nest a group within a group, issue the **group–object** subcommand. In this example, you can use the `all_hosts` group in an ACL or conduit in order to specify all four hosts. Or, you can use either `host_grp_1` or `host_grp_2` in order to specify only the two hosts within each group.

```
(config)#object-group network host_grp_1

(config-network)#network-object host 10.1.1.10
(config-network)#network-object host 10.1.1.14
(config-network)#exit

(config)#object-group network host_grp_2

(config-network)#network-object host 172.16.10.1
(config-network)#network-object host 172.16.10.2
(config-network)#exit


(config)#object-group network all_hosts

(config-network)#group-object host_grp_1

(config-network)#group-object host_grp_2

(config-network)#exit
```

Verify

This section provides information you can use in order to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show running−config object−group** Shows the currently defined ACLs.
- **show access−list** *<acl>* Shows the ACL and the associated hit counter for each line. This command shows the expanded ACL entries for each object group defined.
- **clear object−group [***grp_type***]** When entered without a parameter, the **clear object−group** command removes all defined object groups that are not used in a command. The use of the *grp_type* parameter removes all defined object groups that are not used in a command for that group type only.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Documentation for PIX Firewall**
- **Cisco Secure PIX Firewall Command References**
- **Cisco PIX 500 Series Security Appliances Support**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**

Updated: Feb 02, 2006   Document ID: 25700