Port to Application Mapping

This feature module describes the Port to Application Mapping (PAM) feature. It includes information on the benefits of the feature, supported platforms, configuration tasks, and so forth.

This document includes the following sections:

Feature Overview

Port to Application Mapping (PAM) allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

Using the port information, PAM establishes a table of default port-to-application mapping information at the firewall. The information in the PAM table enables Context-based Access Control (CBAC) supported services to run on non-standard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

PAM also supports host or subnet specific port mapping, which allows you to apply PAM to a single host or subnet using standard access control lists (ACLs). Host or subnet specific port mapping is done using standard ACLs.

How PAM Works

PAM comes standard with the Cisco IOS Firewall feature set software. PAM generates a table of information that identifies specific applications with specific TCP or UDP port information. The PAM table is populated with system-defined mapping information when the firewall router first

starts up. As you customize the mapping information, the PAM table is modified with the new mapping information. This information serves as the default port mapping for traffic passing through the firewall.

PAM works with CBAC to identify the applications associated with various port numbers, including services running on non-standard ports, as it inspect traffic passing through the firewall. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application.

Entries in the PAM table provide three types of mapping information:

- System-defined
- User-defined
- Host-specific

System-defined Port Mapping

PAM creates a table, or database, of system-defined mapping entries using the well-known or registered port mapping information set up during the system start-up. The system-defined entries comprise all the services supported by CBAC, which requires the system-defined mapping information to function properly. The system-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

Note You can override the system-defined entries for specific hosts using the PAM host-specific option. Refer to the "Host-specific Port Mapping" section on page 3.

Table 1 lists the default system-defined services and applications in the PAM table.

Table 1 System-defined Port Mapping

Application Name	Well-known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
http	80	Hypertext Transfer Protocol
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
smtp	25	Simple Mail Transfer Protocol
sqlnet	1521	SQL-NET

Table 1 System-defined Port Mapping (continued)

Application Name	Well-known or Registered Port Number	Protocol Description
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

User-defined Port Mapping

Network services or applications that use non-standard ports require user-defined entries in the PAM table. For example, your network might run HTTP services on the non-standard port 8000 instead of on the system-defined default port (port 80). In this case, you can use PAM to map port 8000 with HTTP services. If HTTP services run on other ports, use PAM to create additional port mapping entries. After you define a port mapping, you can overwrite that entry at a later time by simply mapping that specific port with a different application.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

User-defined port mapping information can also specify a range of ports for an application by establishing a separate entry in the PAM table for each port number in the range.

User-defined entries are saved with the default mapping information when you save the router configuration.

Host-specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet.

With host-specific port mapping, you can use the same port number for different services on different hosts. This means that you can map port 8000 with HTTP services for one host, while mapping port 8000 with Telnet services for another host.

Host-specific port mapping also allows you to apply PAM to a specific subnet when that subnet runs a service that uses a port number that is different from the port number defined in the default mapping information. For example, hosts on subnet 192.168.21.0 might run HTTP services on non-standard port 8000, while other traffic through the firewall uses the default port for HTTP services, which is port 80.

Host-specific port mapping allows you to override a system-defined entry in the PAM table. For example, if CBAC finds an entry in the PAM table that maps port 25 (the system-defined port for SMTP) with HTTP for a specific host, CBAC identifies port 25 as HTTP protocol traffic on that host.

Note If the host-specific port mapping information is the same as an existing system-defined or user-defined default entries, host-specific port changes have no effect.

PAM and CBAC

CBAC uses the information in the PAM table to identify a service or application from traffic flowing through the firewall. With PAM, CBAC can associate non-standard port numbers with specific protocols. For example, if you use PAM to map port 8000 with HTTP services, CBAC can determine that traffic using port 8000 is an HTTP application.

When to Use PAM

Here are a few examples of when you might want to use PAM:

- Use PAM to apply a non-standard port numbers for a service or application.
- Use PAM when a specific host or subnet uses a port number for an application that is different than the default port number established in the PAM table.
- Use PAM when different hosts use the same port number for different applications.

Benefits

- Flexible, per-application port mapping allows CBAC-supported applications to be run on nonstandard ports.
- Network administrators can customize access control for specific applications and services to meet the distinct needs of their networks.

Supported Platforms

- Cisco 800 series
- Cisco uBR900 series
- Cisco 1600 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 7200 series

Supported Standards, MIBs, and RFCs

MIBs

No new or modified MIBs are supported by this feature.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

Standards

No new or modified standards are supported by this feature.

Configuration Tasks

See the following sections for PAM configuration tasks. Each task in the list indicates if it is optional or required:

- Configuring Standard ACLs (optional)
- Configuring PAM (required)
- Verifying PAM (optional)

Configuring Standard ACLs

If you require PAM for a specific host or subnet, use the **access-list** (standard) command in global configuration mode to define an ACL:

Command	Purpose
`Router(config)# access-list` *access-list-number* `permit` *source* `[`*source-wildcard*`]`	(Optional) Create a standard ACL that defines the specific host or subnet for host-specific PAM. For complete information on access-list command, refer to the Cisco IOS release 12.0 *Network Protocols Command Reference, Part 1*.

Configuring PAM

To configure PAM, use the **ip port-map** command in global configuration mode:

Command	Purpose
`Router(config)# ip port-map` *appl_name* `port` *port_num* `[list` *acl_num*`]`	Establish a port mapping entry using the TCP or UDP port number and the application name. (Optional) Use the list option to associate this port mapping to the specific hosts in the ACL. (PAM uses standard access lists only.) If an access list is included, the hosts defined in that ACL have the application *appl_name* running on port *port_num*.

Verifying PAM

To verify the port mapping information, enter the **show ip port-map** command in privileged EXEC mode and review the entries:

```
router# show ip port-map
```

This command displays all entries in the PAM table, including the system-defined entries.

Monitoring and Maintaining PAM

This section describes commands used to monitor and maintain the PAM.

Command	Purpose
`router # show ip port-map [appl_name | port port_num]`	Displays the port mapping information, including the system-defined entries. Include the application name to display a list of entries by application. Include the port number to display the entries by port.
`Router(config)# no ip port-map [appl_name | port port_num]`	Use the **no** form of the **ip port-map** command to delete user-defined port mapping information. This command has no effect on the system-defined port mapping information.

Configuration Examples

This section provides the following PAM configuration examples:

- Mapping an Application to a Non-standard Port
- Mapping an Application with a Port Range
- Invalid Port Mapping Entry
- Mapping an Application to a Port for a Specific Host
- Mapping an Application to a Port for a Subnet
- Overriding a System-defined Port Mapping
- Mapping Different Applications to the Same Port

Mapping an Application to a Non-standard Port

In this example, non-standard port 8000 is established as the user-defined default port mapping for HTTP services:

```
ip port-map http port 8000
```

Mapping an Application with a Port Range

The following PAM entries establish a range of non-standard ports for HTTP services:

```
ip port-map http 8001
ip port-map http 8002
ip port-map http 8003
ip port-map http 8004
```

Invalid Port Mapping Entry

This example is not valid because it tries to establish port 21, which is the system-defined default port for FTP, as the user-defined port for HTTP services:

```
ip port-map http port 21
```

Mapping an Application to a Port for a Specific Host

In this example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services:

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

Mapping an Application to a Port for a Subnet

In this example, a specific subnet runs HTTP services on port 8080. ACL 50 identifies the subnet, while port 8080 is mapped with HTTP services:

```
access-list 50 permit 192.168.92.0
ip port-map http 8080 list 50
```

Overriding a System-defined Port Mapping

In this example, a specific host runs HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.33), while port 25 is mapped with HTTP services:

```
access-list 15 permit 192.168.33.33
ip port-map http port 25 list 15
```

Mapping Different Applications to the Same Port

In this example, the same port number is required by different services running on different hosts. Port 8000 is required for HTTP services for host 192.168.3.4, while port 8000 is also required for FTP services for host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, while the PAM entries maps the ports with the services for each ACL:

```
access-list 10 permit 192.168.3.4
access-list 20 permit 192.168.5.6
ip port-map http port 8000 list 10
ip port-map http ftp 8000 list 20
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **ip port-map**
- **show ip port-map**

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

command **|** {**begin | include | exclude**} *regular-expression*

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression "PeakRate" appears:

show atm vc | begin PeakRate

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

ip port-map

To establish Port to Application Mapping (PAM), use the **ip port-map** configuration command. Use the **no** form of this command to delete user-defined PAM entries.

ip port-map *appl_name* **port** *port_num* **[list** *acl_num***]**

[no] ip port-map *appl_name* **port** *port_num* **[list** *acl_num***]**

Syntax Description

appl_name	Specifies the name of the application with which to apply the port mapping.
port	Indicates that a port number maps to the application.
port_num	Identifies a port number in the range 1 to 65535.
list	Indicates that the port mapping information applies to a specific host or subnet.
acl_num	Identifies the standard access control list (ACL) number used with PAM.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **ip port-map** command associates TCP or UDP port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is one of three types:

- System-defined
- User-defined
- Host-specific

System-defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall CBAC feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

Table 2 list the default system-defined services and applications in the PAM table.

Table 2 System-defined Port Mapping

Application Name	Well-known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
http	80	Hypertext Transfer Protocol
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
smtp	25	Simple Mail Transfer Protocol
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override the system-defined entries for a specific host or subnet using the **list** option in the **ip port-map** command.

User-defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ip port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ip port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ip port-map** command to associate another service or application with the specific port.

Host-specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** option for the **ip port-map** command to specify an ACL for a host or subnet that uses PAM.

Note If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

This section provides examples for adding and removing user-defined PAM configuration entries at the firewall.

In this example, non-standard port 8000 is established as the user-defined default port for HTTP services:

```
ip port-map http port 8000
```

The following PAM entries establish a range of non-standard ports for HTTP services:

```
ip port-map http 8001
ip port-map http 8002
ip port-map http 8003
ip port-map http 8004
```

In this example the command fails because it tries to map port 21, which is the system-defined default port for FTP, with HTTP:

```
ip port-map http port 21
```

In this example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services:

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, port 21, which is normally reserved for FTP services, is mapped to the RealAudio application for the hosts in list 10. In this configuration, hosts in list 10 do not recognize FTP activity on port 21:

```
ip port-map realaudio port 21 list 10
```

In the following example, the **ip port-map** command fails and generates an error message:

```
ip port-map netshow port 21
Command fail: the port 21 has already been defined for ftp by the system.
              No change can be made to the system defined port mappings.
```

The **no** form of this command deletes user-defined entries from the PAM table. It has no effect on the system-defined port mappings. This command deletes the host-specific port mapping of FTP:

```
no ip port-map ftp port 1022 list 10
```

In this example, the command fails because it tries to delete the system-defined default port for HTTP:

```
no ip port-map http port 80
```

In this example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services:

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In this example, a specific subnet runs HTTP services on port 8080. ACL 50 identifies the subnet, while the PAM entry maps port 8080 with HTTP services:

```
access-list 50 permit 192.168.92.0
ip port-map http 8080 list 50
```

In this example, a specific host runs HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.43), while port 25 is mapped with HTTP services:

```
access-list 15 permit 192.168.33.43
ip port-map http port 25 list 15
```

In this example, the same port number is required by different services running on different hosts. Port 8000 is required for HTTP services by host 192.168.3.4, while port 8000 is required for Telnet services by host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, while PAM maps the ports with the services for each ACL:

```
access-list 10 permit 192.168.3.4
access-list 20 permit 192.168.5.6
ip port-map http port 8000 list 10
ip port-map http ftp 8000 list 20
```

Related Commands

Command	Description
show ip port-map	Displays the Port to Application Mapping information.

show ip port-map

To display the Port to Application Mapping (PAM) information, use the **show ip port-map** privileged EXEC command.

show ip port-map [*appl_name* | **port** *port_num*]

Syntax Description

appl_name	Specifies the name of the application to which to apply the port mapping.
port *port_num*	Specifies the alternative port number that maps to the application.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to display the port mapping information at the firewall, including the system-defined and user-defined information. Include the application name to display the list of entries by application. Include the port number to display the entries by port.

Examples

Show the port mapping information, including system-defined mapping information:

```
show ip port-map
Default mapping: vdolive          port 7000               system defined
Default mapping: sunrpc           port 111                system defined
Default mapping: netshow          port 1755               system defined
Default mapping: cuseeme          port 7648               system defined
Default mapping: tftp             port 69                 system defined
Default mapping: real-audio-video port 7070               system defined
Default mapping: streamworks      port 1558               system defined
Default mapping: ftp              port 21                 system defined
Default mapping: h323             port 1720               system defined
Default mapping: smtp             port 25                 system defined
Default mapping: http             port 80                 system defined
Default mapping: msrpc            port 135                system defined
Default mapping: exec             port 512                system defined
Default mapping: login            port 513                system defined
Default mapping: sql-net          port 1521               system defined
Default mapping: tftp             port 70                 user defined
Host specific:   ftp              port 1000   in list 10  user defined
Host specific:   netshow          port 70     in list 10  user defined
Host specific:   smtp             port 70     in list 50  user defined
```

Show the port mapping information for FTP services:

```
sh ip port-map ftp
Default mapping: ftp              port 21                 system defined
Host specific:   ftp              port 1000   in list 10  user defined
```

Show the ports associated with the NetShow application, including both the default and host-specific port mapping information:

```
sh ip port-map  netshow
Default mapping: netshow          port 1755               system defined
Host specific:   netshow          port 21     in list 10  user defined
```

Show the applications associated with port 69, including both the default and host-specific port mapping information:

```
sh ip port-map port 69
Default mapping: tftp             port 69                 user defined
Host specific:   netshow          port 69     in list 50  user defined
Host specific:   smtp             port 69     in list 10  user defined
```

Related Commands

Command	Description
ip port-map	Enables Port to Application Mapping (PAM).