Descripción general de MPF

Una configuración de Modular Policy Framework (MPF) define un conjunto de reglas para aplicar funciones de firewall, como inspección de tráfico y QoS, al tráfico que atraviesa el ASA. MPF permite la clasificación granular de flujos de tráfico, para aplicar diferentes políticas avanzadas a diferentes flujos. MPF se usa con módulos de hardware para redirigir el tráfico de ASA a los módulos que usan Cisco MPF. MPF se puede usar para la inspección avanzada de la capa de aplicación del tráfico clasificando en las capas 5 a 7. Las funciones de limitación de velocidad y QoS también se pueden implementar utilizando MPF.

Como se describe en la figura, Cisco MPF utiliza estos tres objetos de configuración para definir políticas jerárquicas modulares, orientadas a objetos.

Si bien la sintaxis de MPF es similar a la sintaxis de ISR IOS Cisco Modo QoS CLI (MQC) o la sintaxis de Cisco Common Classification Policy Language (C3PL), los parámetros configurables difieren. La plataforma ASA proporciona acciones más configurables en comparación con un ISR para Cisco IOS ZPF. El ASA admite inspecciones de Capa 5 a Capa 7 utilizando un conjunto más rico de criterios para parámetros específicos de la aplicación. Por ejemplo, la función ASA MPF se puede usar para hacer coincidir las direcciones URL de HTTP y los métodos de solicitud, evitar que los usuarios naveguen a sitios específicos durante momentos específicos o incluso evitar que los usuarios descarguen música (MP3) y archivos de video a través de HTTP / FTP o HTTPS / SFTP .

Hay cuatro pasos para configurar MPF en un ASA:

Paso 1. (Opcional) Configure las ACL extendidas para identificar el tráfico granular al que se puede hacer referencia específicamente en el mapa de clase. Por ejemplo, las ACL se pueden usar para hacer coincidir el tráfico TCP, el tráfico UDP, el tráfico HTTP o todo el tráfico a un servidor específico.

Paso 2. Configure el mapa de clase para identificar el tráfico.

Paso 3. Configure un mapa de políticas para aplicar acciones a esos mapas de clase.

Paso 4. Configure una política de servicio para adjuntar el mapa de políticas a una interfaz.

Configurando mapas de clase

Los mapas de clase están configurados para identificar el tráfico de Capa 3/4. Para crear un mapa de clase e ingresar al modo de configuración de mapa de clase, use el comando del modo de configuración global *nombre de* **clase de mapa de** *clase* . Los nombres "clase-predeterminado" y cualquier nombre que comience con "_internal" o "_default" están reservados. El nombre del mapa de clase debe ser único y puede tener hasta 40 caracteres de longitud. El nombre también debe ser descriptivo.

Nota : se utiliza una variación del comando de **mapa de clase** para el tráfico de administración que está destinado al ASA. En este caso, use el comando **class-map type management** *class-name-name* .

Cuando se encuentra en el modo de configuración de mapa de clase, se debe configurar una descripción que explique el propósito del mapa de llamadas mediante el comando **description** .

A continuación, el tráfico que debe coincidir debe identificarse utilizando la **coincidencia con cualquiera** (coincide con todo el tráfico) o **la lista de** *acceso de la* **lista de** *acceso*coincidente para que coincida con el tráfico especificado por una lista de acceso extendida.

Nota : a menos que se especifique lo contrario, solo incluya un comando de **coincidencia** en el mapa de clase.

El ejemplo en la figura proporciona una configuración de mapa de clase de ejemplo.

El ASA también define automáticamente un mapa de clase de Capa 3/4 predeterminado identificado en la configuración por **class-map inspect_default** . En este mapa de clase se identifica la **coincidencia con el tráfico de inspección predeterminado** que coincide con los puertos predeterminados para todas las inspecciones. Cuando se usa en un mapa de políticas, este mapa de clase garantiza que se aplique la inspección correcta a cada paquete, en función del puerto de destino del tráfico. Por ejemplo, cuando el tráfico UDP para el puerto 69 llega al ASA, el ASA aplica la inspección TFTP. Solo en este caso, se pueden configurar múltiples inspecciones para el mismo mapa de clase. Normalmente, el ASA no usa el número de puerto para determinar qué inspección aplicar. Esto proporciona flexibilidad para aplicar inspecciones a puertos no estándar.

Para mostrar información sobre la configuración del mapa de clase, use el comando **show running-config class-map** .

Para eliminar todos los mapas de clase, use el comando **clear configure class-map** en el modo de configuración global.

Los mapas de políticas se utilizan para vincular los mapas de clase con acciones. Utilice el comando del modo de configuración global **policy-map** *policy-map-name* para aplicar acciones al tráfico de Capa 3 y 4. El nombre del mapa de políticas debe ser único y tener hasta 40 caracteres de longitud. El nombre también debe ser descriptivo.

En el modo de configuración del mapa de políticas, config-pmap, use los siguientes comandos:

- **descripción** - Añadir texto de descripción.
- **class** *class-map-name* : identifica un mapa de clase específico en el que realizar acciones.

El número máximo de mapas de políticas es 64. Puede haber múltiples mapas de clase de Capa 3/4 en un mapa de políticas, y se pueden asignar múltiples acciones de uno o más tipos de características a cada mapa de clases.

Nota : La configuración incluye un mapa de políticas de Capa 3/4 predeterminado que ASA usa en la política global predeterminada. Se llama **global_policy** y realiza una inspección en el tráfico de inspección predeterminado. Sólo puede haber una política global. Por lo tanto, para modificar la política global, edítelo o reemplácelo.

Estos son los tres comandos más comunes disponibles en el modo de configuración del mapa de políticas:

- **establecer conexión** : establece los valores de conexión.
- **inspeccionar** : proporciona servidores de inspección de protocolo.
- **policía** - Establece límites de velocidad para el tráfico en esta clase.

Las acciones se aplican al tráfico de forma bidireccional o unidireccional según la función.

Para mostrar información sobre la configuración del mapa de políticas, use el comando **show running-config policy-map** .

Use el comando **clear configure policy-map** en el modo de configuración global para eliminar todos los mapas de políticas.

Configurar la política de servicio

Para activar un mapa de políticas globalmente en todas las interfaces o en una interfaz específica, use el comando del modo de configuración global de la **política de servicio**para habilitar un conjunto de políticas en una interfaz:

política de servicio política *nombre-mapa* [**global** | **interfaz** *intf*]

El ejemplo en la Figura 1 configura el mapa de políticas y su política de servicio asociada.

Utilice el verificador de sintaxis en la Figura 2 para implementar el marco de políticas modular.

Política predeterminada de ASA

La configuración predeterminada de ASA incluye una política global que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica la inspección al tráfico global. De lo contrario, la política de servicio puede aplicarse a una interfaz o globalmente. El resultado de la figura muestra la configuración de la política de servicio predeterminada.

Las políticas de servicio de interfaz tienen prioridad sobre la política de servicio global para una característica determinada. Por ejemplo, si hay una política global con inspecciones y una política de interfaz con inspecciones, entonces solo se aplican las inspecciones de política de interfaz a esa interfaz.

Para modificar la política global, un administrador debe editar la política predeterminada o deshabilitar la política predeterminada y aplicar una nueva política.

Para mostrar información sobre la configuración de la política de servicio, use el comando de **servicio de la política** o el comando **show running-config service-policy** .

Use el comando **clear configure service-policy**en el modo de configuración global para eliminar todas las políticas de servicio. El comando **clear service-policy** borra las estadísticas de la política de servicio.

Overview of MPF

A Modular Policy Framework (MPF) configuration defines a set of rules for applying firewall features, such as traffic inspection and QoS, to the traffic that traverses the ASA. MPF allows granular classification of traffic flows, to apply different advanced policies to different flows. MPF is used with hardware modules to redirect traffic granularly from the ASA to the modules that use Cisco MPF. MPF can be used for advanced Application Layer inspection of traffic by classifying at Layers 5 through 7. Rate limiting and QoS features can also be implemented using MPF.

As described in the figure, Cisco MPF uses these three configuration objects to define modular, object-oriented, hierarchical policies.

Although the MPF syntax is similar to the ISR IOS Cisco Modular QoS CLI (MQC) syntax or the Cisco Common Classification Policy Language (C3PL) syntax, the configurable parameters differ. The ASA platform provides more configurable actions as compared to an ISR for Cisco IOS ZPF. The ASA supports Layer 5 to Layer 7 inspections using a richer set of criteria for application-specific parameters. For instance, the ASA MPF feature can be used to match HTTP URLs and request methods, prevent users from surfing to specific sites during specific times, or even prevent users from downloading music (MP3) and video files via HTTP/FTP or HTTPS/SFTP.

There are four steps to configure MPF on an ASA:

Step 1. (Optional) Configure extended ACLs to identify granular traffic that can be specifically referenced in the class map. For example, ACLs can be used to match TCP traffic, UDP traffic, HTTP traffic, or all traffic to a specific server.

Step 2. Configure the class map to identify traffic.

Step 3. Configure a policy map to apply actions to those class maps.

Step 4. Configure a service policy to attach the policy map to an interface.

Configuring Class Maps

Class maps are configured to identify Layer 3/4 traffic. To create a class map and enter class-map configuration mode, use the **class-map** *class-map-name* global configuration mode command. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. The class map name must be unique and can be up to 40 characters in length. The name should also be descriptive.

Note: A variation of the **class-map** command is used for management traffic that is destined to the ASA. In this case, use the **class-map type management** *class-map-name* command.

When in class-map configuration mode, a description explaining the purpose of the call map should be configured using the **description** command.

Next, traffic to match should be identified using the **match any** (matches all traffic) or **match access-list** *access-list-name* to match traffic specified by an extended access list.

Note: Unless otherwise specified, only include one **match** command in the class map.

The example in the figure provides a sample class map configuration.

The ASA also automatically defines a default Layer 3/4 class map identified in the configuration by **class-map inspection_default**. Identified in this class map is the **match default-inspection-traffic** which matches the default ports for all inspections. When used in a policy map, this class map ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For example, when UDP traffic for port 69

reaches the ASA, the ASA applies the TFTP inspection. In this case only, multiple inspections can be configured for the same class map. Normally, the ASA does not use the port number to determine which inspection to apply. This provides flexibility to apply inspections to non-standard ports.

To display information about the class map configuration, use the **show running-config class-map** command.

To remove all class maps, use the **clear configure class-map** command in global configuration mode.

Define and Activate a Policy

Policy maps are used to bind class maps with actions. Use the **policy-map** *policy-map-name* global configuration mode command, to apply actions to the Layer 3 and 4 traffic. The policy map name must be unique and up to 40 characters in length. The name should also be descriptive.

In policy-map configuration mode, config-pmap, use the following commands:

- **description** - Add description text.
- **class** *class-map-name* - Identify a specific class map on which to perform actions.

The maximum number of policy maps is 64. There can be multiple Layer 3/4 class maps in one policy map, and multiple actions can be assigned from one or more feature types to each class map.

Note: The configuration includes a default Layer 3/4 policy map that the ASA uses in the default global policy. It is called **global_policy** and performs an inspection on the default inspection traffic. There can only be one global policy. Therefore, to alter the global policy, either edit it or replace it.

These are the three most common commands available in policy map configuration mode:

- **set connection** - Sets connection values.
- **inspect** - Provides protocol inspection servers.
- **police** - Sets rate limits for traffic in this class.

Actions are applied to traffic bidirectionally or unidirectionally depending on the feature.

To display information about the policy map configuration, use the **show running-config policy-map** command.

Use the **clear configure policy-map** command in global configuration mode, to remove all policy maps.

Configure the Service Policy

To activate a policy map globally on all interfaces or on a targeted interface, use the**service-policy** global configuration mode command to enable a set of policies on an interface:

service-policy *policy-map-name* [**global** | **interface** *intf*]

The example in Figure 1 configures the policy map and its associated service policy.

Use the Syntax Checker in Figure 2 to implement modular policy framework.

ASA Default Policy

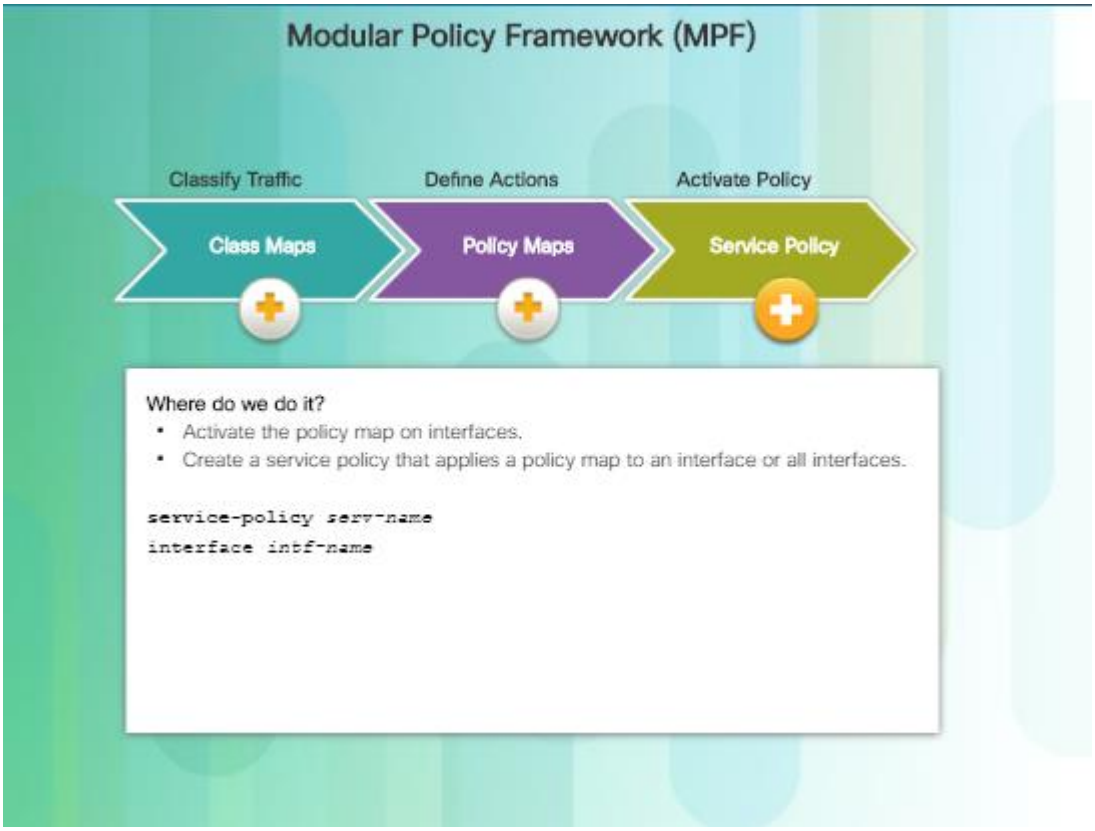
The ASA default configuration includes a global policy that matches all default application inspection traffic and applies inspection to the traffic globally. Otherwise, the service policy can be applied to an interface or globally. The output in the figure displays the default service policy configuration.

Interface service policies take precedence over the global service policy for a given feature. For example, if there is a global policy with inspections, and an interface policy with inspections, then only the interface policy inspections are applied to that interface.

To alter the global policy, an administrator needs to either edit the default policy or disable the default policy and apply a new policy.

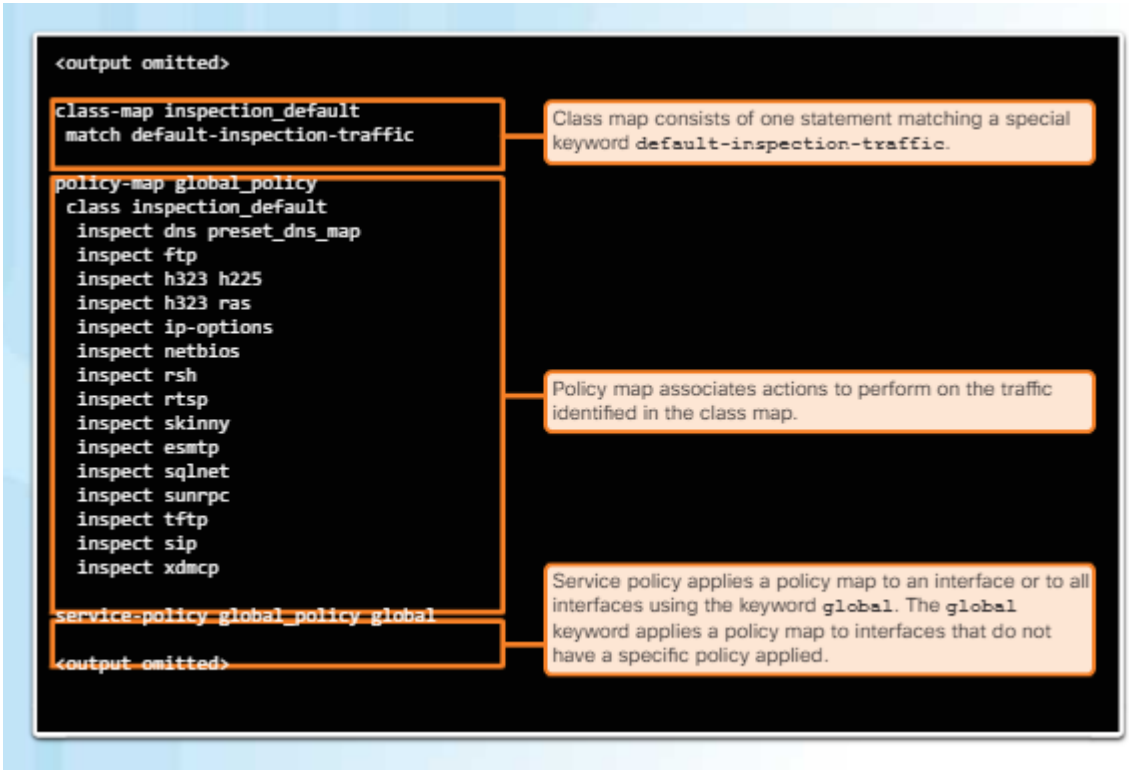
To display information about the service policy configuration, use the **show service-policy** or the **show running-config service-policy** command.

Use the **clear configure service-policy** command in global configuration mode to remove all service policies. The **clear service-policy** command clears the service policy statistics.



```
CCNAS-ASA(config)# access-list UDP permit udp any any
CCNAS-ASA(config)# access-list TCP permit tcp any any
CCNAS-ASA(config)# access-list SERVER permit ip any host 10.1.1.1
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-TCP
CCNAS-ASA(config-cmap)# description "This class-map matches all TCP traffic"
CCNAS-ASA(config-cmap)# match access-list TCP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-UDP
CCNAS-ASA(config-cmap)# description "This class-map matches all UDP traffic"
CCNAS-ASA(config-cmap)# match access-list UDP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-HTTP
CCNAS-ASA(config-cmap)# description "This class-map matches all HTTP traffic"
CCNAS-ASA(config-cmap)# match port TCP eq http
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map TO-SERVER
CCNAS-ASA(config-cmap)# description "Class map matches traffic  10.1.1.1"
CCNAS-ASA(config-cmap)# match access-list SERVER
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
```

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```


<output omitted>
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
service-policy global_policy global
<output omitted>
Class map consists of one statement matching a special keyword default-inspection-traffic.
Policy map associates actions to perform on the traffic identified in the class map.
Service policy applies a policy map to an interface or to all interfaces using the keyword global. The global keyword applies a policy map to interfaces that do not have a specific policy applied.