maa – match d

mac address

要为主用设备和备用设备指定虚拟 MAC 地址，请在故障转移组配置模式下使用 **macaddress** 命令。要恢复默认虚拟 MAC 地址，请使用此 **no**命令的形式。

mac address*phy_if*[*active_mac*][*standby_mac*]
no mac address*phy_if*[*active_mac*][*standby_mac*]

Syntax Description

phy_if	设置MAC地址的接口的物理名称。
active_mac	主用设备的虚拟 MAC 地址。MAC 地址必须以 h.h.h 格式输入，其中 h 是 16 位十六进制数。
standby_mac	备用设备的虚拟 MAC 地址。MAC 地址必须以 h.h.h 格式输入，其中 h 是 16 位十六进制数。

Command Default

默认值如下：

- 主用设备默认 MAC 地址：00a0.c9*physical_port_number* 。*failover_group_id* 01。
- 备用设备默认 MAC 地址：00a0.c9*physical_port_number* 。*failover_group_id* 02.

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
故障转移组配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果没有为故障转移组定义虚拟 MAC 地址，则会使用默认值。

如果您在同一网络上有多个主用/主用故障转移对，则分配给一对接口的默认虚拟 MAC 地址可能与分配给其他对接口的默认虚拟MAC地址相同。虚拟MAC地址确定。为避免网络中出现重复的MAC地址，请确保为每个物理接口分配一个虚拟的主用和备用 MAC 地址。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

CR_Examples

以下部分示例显示了故障转移组的一种可能配置：

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failovermacaddress	为物理接口指定虚拟 MAC 地址。

mac-address

要手动为接口或子接口分配私有MAC地址，请在**mac-address**接口配置模式下使用该命令。在多情景模式下，此命令可以在每个情景中为接口分配不同的 MAC 地址。对于集群中的单个接口，您可以分配 MAC 地址集群池。要将 MAC 地址恢复为默认值，请使用此命令的 **no**形式。

mac-address {*mac_address* [**standby***mac_address* | **site-id***number* [**site-ipip_address**]] | **cluster-pool***pool_name*}
no
mac-address {*mac_address* [**standby***mac_address* | **site-id***number* [**site-ipip_address**]] | **cluster-pool***pool_name*}

Syntax Description

cluster-pool*pool_name*	对于单个接口模式下的集群（请参阅**clusterinterface-mode**命令），或对于任何集群接口模式下的管理接口，设置要用于每个集群成员上给定接口的MAC地址池。使用 **mac-addresspool**命令定义地址池。
mac_address	以 H.H.H 格式设置此接口的 MAC 地址，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。如果使用故障转移，则此 MAC 地址为主用 MAC 地址。 注释 因为自动生成的**mac-addressauto**地址（命令）以A2开头，所以如果您还想使用自动生成，则不能以 A2 开头手动 MAC 地址。
site-id编号	（可选；仅限路由模式）对于站点间集群，为每个站点配置站点特定的MAC地址。
site-ip*ip_address*	（可选；仅限路由模式）对于站点间集群，为每个站点配置一个站点特定的 IP 地址。该 IP 地址必须与全局 IP 地址位于同一子网。
standby*mac_address*	（可选）设置故障转移的备用 MAC 地址。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

Command Default

默认 MAC 地址是烧录的物理接口 MAC 地址。子接口将继承物理接口 MAC 地址。有些命令会设置物理接口 MAC 地址（包括单情景模式下的此命令），因此继承的地址取决于该配置。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(5)/8.2(2)	与 **mac-addressauto** 命令一起使用时，使用 A2 来启动 MAC 地址会受到限制。
9.0(1)	添加 **cluster-pool**关键字是为了支持集群。
9.5(1)	已添加关 **site-id** 键字。
9.6(1)	已添加关 **site-ip** 键字。

使用指南

在多情景模式下，如果在情景之间共享接口，则可以将唯一 MAC 地址分配给每个情景的接口。借助此功能，ASA 可轻松地将数据包分类到适当的情景中。可使用没有唯一 MAC 地址的共享接口，但受到一些限制。有关详细信息，请参阅 CLI 配置指南。

您可以使用此命令手动分配每个 MAC 地址，也可以使用该命令自动为上下文中的 **mac-addressauto** 共享接口生成 MAC 地址。如果自动生成MAC地址，则可以使用该 **mac-address**命令覆盖生成的地址。

对于单情景模式，或者多情景模式下不共享的接口，您可能想要给子接口分配唯一 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

对于集群，必须为跨网络 EtherChannel 配置全局 MAC 地址。如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的主设备。在多上下文模式下，如果在上下文之间共享一个接口，则应启用 MAC 地址的自动生成。请注意，您必须为非共享接口手动配置 MAC 地址。

对于路由模式下的站点间集群，请在主设备上为每个站点配置一个站点特定的 MAC 地址和 IP 地址，然后在每台设备上使用 **site-id** 命令将其分配给站点。

CR_Examples

以下示例为 GigabitEthernet 0/1.1 配置 MAC 地址：

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
ciscoasa/contextA(config-if)# no shutdown
```

以下示例为跨区以太网通道端口通道 1 配置站点特定的 MAC 地址：

```
ciscoasa(config-if)# interface port-channel 1
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.7.7.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.7.7.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.7.7.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.7.7.4
```

Related Commands

命令	说明
failovermacaddress	主用/备用故障转移的物理接口的主用和备用 MAC 地址。
macaddress	主用/主用故障转移的物理接口的主用和备用 MAC 地址。
mac-addressauto	在多情景模式下自动为共享接口生成MAC地址（主用和备用）。
mode	将安全上下文模式设置为多重或单一。
showinterface	显示接口特征，包括 MAC 地址。

mac-address auto

要自动将专用 MAC 地址分配给每个共享情景接口，请在全局配置模式下使用 **mac-addressauto**命令。要禁用自动 MAC 地址，请使用此命 **no**令的形式。

mac-addressauto [**prefix***prefix*]
no mac-address auto

Syntax Description

prefix前缀	（可选）将用户定义的前缀设置为 MAC 地址的一部分。前 缀 是0~65535之间的十进制值。如果未输入前缀，ASA 将生成默认前缀。 将此前缀转换为 4 位十六进制号码。该前缀可确保每个 ASA 使用唯一的 MAC 地址（使用不同的前缀值），因此，例如，您可以在一个网段上拥有多个 ASA。

Command Default

默认情况下会禁用自动MAC地址生成，但ASASM除外，其默认情况下会启用。如果已启用，ASA 根据接口 (ASA 5500-X) 或背板 (ASASM) 中 MAC 地址的最后两个字节自动生成前缀。如果需要，您也可以自定义该前缀。

如果禁用 MAC 地址生成，请参阅以下默认 MAC 地址：

- 对于 ASA 5500-X 系列设备 - 物理接口使用固化 MAC 地址，并且该物理接口的所有子接口都使用同一固化 MAC 地址。
- 对于 ASASM - 所有 VLAN 接口都使用派生自背板 MAC 地址的同一 MAC 地址。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(5)/8.2(2)	添加了 **prefix** 关键字。MAC 地址格式已更改为使用前缀、使用固定起始值 (A2)，并且对故障转移对中的主单元和辅助单元 MAC 地址使用不同的方案。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。
8.5(1)	现在，自动生成仅对 ASASM 默认启用 (**mac-addressauto**)。

版本	修改
8.6(1)	ASA 现在将自动 MAC 地址生成配置转换为使用默认前缀。ASA 根据接口 (ASA 5500) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。传统的 MAC 地址生成方法不再可用。 注释 为了保持故障转移对无中断升级，如果已启用故障转移，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。

使用指南

为了允许上下文共享接口，我们建议您为每个共享上下文接口分配唯一的 MAC 地址。MAC 地址用于在情景中对数据包进行分类。如果共享某个接口，但在每个情景中没有该接口的唯一MAC地址，则使用目标 IP 地址对数据包进行分类。目的地址与情景 NAT 配置相匹配，与 MAC 地址方法相比，此方法有一些限制。有关对数据包进行分类的信息，请参阅 CLI 配置指南。

在出现生成的MAC 地址与网络中的另一个专用MAC 地址冲突这种极少发生的情况下，您可以在情景中为接口手动设置 MAC 地址。请参阅手 **mac-address**动设置MAC地址的命令。

与手动 MAC 地址的交互

如果您手动分配MAC 地址，并且同时启用自动生成，则会使用手动分配的MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。

由于自动生成的地址以 A2 开头，因此如果您还想使用自动生成，则不能以 A2 开头手动 MAC 地址。

故障转移 MAC 地址

为了能用于故障切换，ASA会为每个接口生成主用和备用MAC地址。如果主用设备进行故障切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。请参阅 <xref> 部分以了解更多信息。

有关使用添加 **prefix** 关键字之前的 **mac-addressauto** 命令的旧版升级故障转移，请参阅<xref>部分的详细信息。

使用前缀的 MAC 地址格式

ASA 使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中 *xx.yy* 是用户定义的前缀或基于接口 (ASA 5500) 或背板 (ASASM) MAC 地址的最后两个字节自动生成的前缀， *zz.zzzz* 是 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

举例来说，如果您设置前缀 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，前缀会被反转 (*xxyy*) 以匹配 ASA 本机形式：

A2**4D.00***zz.zzz.xz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzz.xz*

不带前缀的 MAC 地址格式（传统方法）

如果您使用故障转移并且已升级到 8.6 或更高版本，则可以使用此方法；在这种情况下，您必须手动启用前缀方法。

如果没有前缀，则 MAC 地址使用以下格式生成：

- 主用设备 MAC 地址：12_插槽.*port _subid* 。*contextid* 的值 。
- 备用设备 MAC 地址：02_插槽 。*port _subid* 。*contextid* 的值 。

对于没有接口插槽的平台，插槽始终为 0。 端口 是接口端口。 *subid* 是子接口的内部 ID，不可见。*contextid* 是情景的内部 ID，可使用 **showcontextdetail**命令查看。例如，ID 为 1 的情景中的接口 GigabitEthernet 0/1.200 具有以下生成的 MAC 地址，其中子接口 200 的内部 ID 为 31：

- 主用号码：1200.0131.0001
- 备用：0200.0131.0001

此MAC地址生成方法不允许在重新加载之间使用永久MAC地址，不允许在同一网段上有多个ASA（因为不能保证 MAC 地址唯一），并且不会防止与手动分配的 MAC 地址重叠。我们建议在生成 MAC 地址时使用前缀来避免这些问题。

当生成 MAC 地址时

当你在上下文 **nameif**中为接口配置命令时，新的 MAC 地址会立即生成。如果在配置上下文接口后启用此命令，则输入该命令后会立即为所有接口生成 MAC 地址。如果使用该命 **nomac-addressauto**令，每个接口的 MAC 地址将恢复为默认 MAC 地址。例如，GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。

使用其他方法设置 MAC 地址

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

在系统配置中查看 MAC 地址

要从系统执行空间查看分配的 MAC 地址，请输入 **showrunning-configallcontext**命令。

需要该 **all**选项才能查看分配的 MAC 地址。虽然此命令仅在全局配置模式下可由用户配置，但该命令在 **mac-addressauto** 每个上下文的配置中与分配的MAC地址一起显示为只读条目。仅使用上下文中的命令 **nameif**配置的已分配接口才会分配 MAC 地址。

注释 如果您手动向接口分配MAC地址，但也启用了自动生成，则自动生成的地址会继续显示在配置中，即使正在使用的是手动MAC地址也如此。如果随后删除手动MAC地址，则会使用所显示的自动生成的地址。

查看上下文中的 MAC 地址

要查看上下文中每个接口使用的 MAC 地址，请输入 **showinterface|include(Interface)|(MAC)** 命令。

注释 该命令显 **showinterface**示正在使用的 MAC 地址；如果您手动分配 MAC 地址并启用自动生成，那么您只能从系统配置中查看未使用的自动生成的地址。

CR_Examples

以下示例启用自动 MAC 地址生成，前缀为 78：

```
ciscoasa(config)# mac-address auto prefix 78
```

该命令的以下输出显示了分配给 Management0/0 接口的 **showrunning-configallcontextadmin** 主 MAC 地址和备用 MAC 地址：

```
ciscoasa# show running-config all context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

该命令的以下输出显 **showrunning-configallcontext**示了所有上下文接口的所有 MAC 地址（主 MAC 地址和备用 MAC 地址）。请注意，由于 GigabitEthernet0/0 和 GigabitEthernet0/1 主接口未在上下文中使用命 **nameif**令进行配置，因此没有为它们生成 MAC 地址。

```
ciscoasa# show running-config all context
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!
context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!
context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
```

```
  config-url disk0:/CTX2.cfg
!
```

Related Commands

命令	说明
failovermacaddress	主用/备用故障转移的物理接口的主用和备用 MAC 地址。
macaddress	主用/主用故障转移的物理接口的主用和备用 MAC 地址。
mac-address	为物理接口或子接口手动设置 MAC 地址（主用和备用）。在多情景模式下，您可以为同一接口在每个情景中设置不同的 MAC 地址。
mode	将安全上下文模式设置为多重或单一。
showinterface	显示接口特征，包括 MAC 地址。

mac-address pool

要添加 MAC 地址池以用于 ASA 集群中的单个接口，请在全局配置模式下使用 **mac-addresspool** 命令。要删除未使用的池，请使用此命 **no**令的形式。

mac-address pool*namestart_mac_address - end_mac_address*
no mac-address pool*name* [*start_mac_address - end_mac_address*]

Syntax Description

name	为池命名，长度最大为 63 个字符。
start_mac_address -end_mac_address	指定第一个 MAC 地址和最后一个 MAC 地址。请注意在短划线 (-) 两侧添加一个空格。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

您可以在接口配置模式下的 **mac-addresscluster-pool**命令中使用该池。为接口手动配置 MAC 地址并不常见，但如果您有特殊需求，则此池用于为每个接口分配唯一的 MAC 地址。

CR_Examples

以下示例添加具有 8 个 MAC 地址的 MAC 地址池，并将其分配给千兆以太网 0/0 接口：

```
ciscoasa(config)# mac-address pool pool1 000C.F142.4CD1 - 000C.F142.4CD7
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-ifc)# mac-address cluster-pool pool1
```

Related Commands

命令	说明
interface	配置接口。
mac-address	为接口配置 MAC 地址。

mac-address-table aging-time

要设置 MAC 地址表条目的超时，请在 **mac-address-tableaging-time** 全局配置模式下使用 命令。要恢复默认值5分钟，请使用此命 **no**令的形式。

mac-address-tableaging-time*timeout_value*
no mac-address-table aging-time

Syntax Description

timeout_value	MAC 地址条目超时之前在 MAC 地址表中停留的时间，该值介于 5 到 720 分钟（12 小时）之间。默认值为 5 分钟。

Command Default

默认超时是 5 分钟。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.7(1)	使用集成路由和桥接时，现在可以在路由模式下配置此命令。

使用指南

没有使用指南。

CR_Examples

以下示例将 MAC 地址超时设置为 10 分钟：

```
ciscoasa(config)# mac-address-timeout aging time 10
```

Related Commands

命令	说明
arp-inspection	启用 ARP 检测，即将 ARP 数据包与静态 ARP 条目进行比较。
firewalltransparent	将防火墙模式设置为透明。
mac-address-tablestatic	将静态 MAC 地址条目添加到 MAC 地址表。
mac-learn	禁用 MAC 地址学习。

命令	说明
showmac-address-table	显示 MAC 地址表，包括动态和静态条目。

mac-address-table static

要将静态条目添加到 MAC 地址表，请在全局配置模式下使用 **mac-address-tablestatic** 命令。要删除静态条目，请使用此命 **no**令的形式。通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。如有必要，可以将静态 MAC 地址添加到 MAC 地址表中。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果具有与静态条目相同 MAC 地址的客户端尝试将流量发送到与静态条目不匹配的接口，则 ASA 会丢弃该流量并生成系统消息。

mac-address-table static*interface_namemac_address*
no mac-address-table static*interface_namemac_address*

Syntax Description

interface_name	源桥组成员接口。
mac_address	您希望添加至此表的 MAC 地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.7(1)	使用集成路由和桥接时，现在可以在路由模式下配置此命令。

CR_Examples

以下示例将一个静态 MAC 地址条目添加到 MAC 地址表：

```
ciscoasa(config)# mac-address-table static inside 0010.7cbe.6101
```

Related Commands

命令	说明
arp	添加一个静态 ARP 条目。
firewalltransparent	将防火墙模式设置为透明。
mac-address-tableaging-time	设置动态 MAC 地址条目的超时。

命令	说明
mac-learn	禁用 MAC 地址学习。
showmac-address-table	显示 MAC 地址表条目。

mac-learn disable

要禁用接口的 MAC 地址获悉，请在全局配置模式下使用 **mac-learn**命令。要重新启用 MAC 地址学习，请使用此命 **no**令的形式。默认情况下，每个接口都会自动获悉进入流量的 MAC 地址，ASA 会将相应的条目添加至 MAC 地址表。您可以根据需要禁用 MAC 地址获悉。

mac-learn*interface_name***disable**
no mac-learn*interface_name***disable**

Syntax Description

interface_name	要在其上禁用MAC学习的桥接组成员接口。
disable	禁用 MAC 学习。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.7(1)	使用集成路由和桥接时，现在可以在路由模式下配置此命令。

CR_Examples

以下示例在外部接口上禁用 MAC 获悉：

```
ciscoasa(config)# mac-learn outside disable
```

Related Commands

命令	说明
clearconfiguremac-learn	将 **mac-learn**配置设置为默认值。
firewalltransparent	将防火墙模式设置为透明。
mac-address-tablestatic	将静态MAC地址条目添加到MAC地址表。
showmac-address-table	显示 MAC 地址表，包括动态和静态条目。

命令	说明
showrunning-configmac-learn	显示 **mac-learn** 配置。

mac-learn 泛洪

要启用针对非 IPv4/IPv6 数据包的未知 MAC 地址泛洪，请在全局配置模式下使用 **mac-learn flood**命令。要禁用 MAC 地址泛洪，请使用此命 **no**令的形式。

mac-learn flood
no mac-learn flood

Command Default

已禁用泛洪。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.7(1)	添加了此命令。

CR_Examples

以下示例启用 MAC 泛洪：

```
ciscoasa(config)# mac-learn flood
```

Related Commands

命令	说明
clearconfiguremac-learn	将 **mac-learn**配置设置为默认值。
mac-address-tablestatic	将静态 MAC 地址条目添加到 MAC 地址表。
showmac-address-table	显示 MAC 地址表，包括动态和静态条目。
showrunning-configmac-learn	显示 **mac-learn** 配置。

mac-list

如要指定用于使 MAC 地址豁免身份验证和/或授权的 MAC 地址列表，请在全局配置模式下使用 **mac-list** 命令。要删除 MAC 列表条目，请使用此命 **no**令的形式。

mac-list*id* { **deny** | **permit** } *macmacmask*
no mac-list*id* { **deny** | **permit** } *macmacmask*

Syntax Description

deny	如果在 **aaamac-exempt** 命令中指定流量，则表示匹配此 MAC 地址的流量不匹配 MAC 列表，并且应同时接受身份验证和授权。如果使用 MAC 地址掩码（例如，ffff.ffff.0000）允许一系列 MAC 地址，并且要强制该范围内的一个 MAC 地址进行身份验证和授权，您可能需要在 MAC 列表中添加拒绝条目。
ID	指定十六进制 MAC 访问列表号。要将一组 MAC 地址分组，请根据需要多次使用相同的 ID 值输入 **mac-list** 命令。条目的顺序很重要，因为数据包使用它匹配的第一个条目，而不是最佳匹配场景。如果有一个 permit 条目，但想要拒绝 permit 条目允许的地址，请务必在 permit 条目之前输入 deny 条目。
mac	指定 12 位十六进制形式的源 MAC 地址；即 nnnn.nnnn.nnnn
macmask	指定应该用于匹配的 MAC 地址部分。例如，ffff.ffff.ffff 与 MAC 地址完全匹配。 ffff.ffff.0000 仅匹配前 8 位数。
permit	表示匹配此 MAC 地址的流量与 MAC 列表匹配，并且在 **aaamac-exempt** 命令中指定该流量时可免除身份验证和授权。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

要启用 MAC 地址豁免执行身份验证和授权，请使用 **aaamac-exempt** 命令。您仅可以添加 **aaamac-exempt** 命令的一个实例，因此请确保您的 MAC 列表包括要豁免的所有 MAC 地址。您可以创建多个 MAC 列表，但一次只能使用一个。

CR_Examples

以下示例绕过单个 MAC 地址的身份验证：

```
ciscoasa(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# aaa mac-exempt match abc
```

以下条目绕过硬件 ID 为 0003.E3 的所有思科 IP 电话的身份验证：

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

以下示例绕过对除 00a0.c95d.02b2 之外的一组 MAC 地址的身份验证。将 deny 语句输入 permit 语句之前，因为 00a0.c95d.02b2 也匹配 permit 语句，如果它放在最前面，则永远不会匹配 deny 语句。

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

Related Commands

命令	说明
aaaauthentication	启用用户身份验证。
aaaauthorization	启用用户授权服务。
aaamac-exempt	豁免 MAC 地址列表的身份验证和授权。
clearconfiguremac-list	删除先前由 **mac-list** 命令指定的 MAC 地址列表。
showrunning-configmac-list	显示先前在 **mac-list** 命令中指定的 MAC 地址列表。

mail-relay

要配置本地域名，请在参数配置模式下使用 **mail-relay**命令。要禁用此功能，请使用此**no** 命令的形式。

mail-relaydomain_nameaction { **drop-connection** | **log** }
no mail-relaydomain_nameaction { **drop-connection** | **log** }

Syntax Description

domain_name	域名。
drop-connection	关闭连接。
log	生成系统日志消息。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
参数配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例显示如何为特定域配置邮件中继：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mail-relay mail action drop-connection
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。

命令	说明
showrunning-configpolicy-map	显示所有当前的策略映射配置。

management-access

要允许在使用 VPN 时对进入 ASA 的接口以外的接口进行管理访问，请在 **management-access**全局配置模式下使用该命令。要禁用管理访问，请使用此命 **no**令的形式。

management-access管理接口
no management-access管理接口

Syntax Description

管理接口	指定从另一个接口进入 ASA 时想要访问的管理接口的名称。可以指定物理或虚拟接口。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。
9.9.(2)	现在，可以指定虚拟接口。
9.14(1)	SNMP 不再受支持。
9.17(1)	如果您使用 CiscoSSH 堆栈（命 **ssh stack ciscossh**令），则 SSH 不支持此功能。

使用指南

此命令允许您连接到除使用完整隧道 IPsec VPN 或 SSL VPN 客户端（AnyConnect 2.x 客户端、SVC 1.x）时或跨站点间 IPsec 进入 ASA 的接口以外的接口。隧道。您可以使用 Telnet、SSH、Ping 或 ASDM 连接至 ASA 接口。您还可以使用管理访问接口作为通过 VPN 隧道发送的系统日志消息的源接口。

只能定义一个管理访问接口。

在 9.5(1) 及更高版本中，由于使用单独的管理和数据路由表进行路由考虑，VPN 终止接口和管理访问接口需要是同一类型：两者都需要是仅管理接口或常规数据接口。因此，请勿在仅管理接口上配置管理访问，除非在极少数情况下 VPN 终端接口会仅用于管理。

如果您使用 CiscoSSH 堆栈（命 **ssh stack ciscossh**令），则 SSH 不支持此功能。

9.14(1) 及更高版本的 SNMP 不支持此功能。 对于 VPN 上的 SNMP，我们建议在 9.18(2) 及更高版本中的环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。

在管理访问接口网络和 VPN 网络之间使用身份 NAT（VPN 流量的常见 NAT 配置）时，必须指定 **natroute-lookup** 命令。如果没有路由查找，ASA 就会将流量从命令中指定的 **nat**接口发送出去，而不管路由表的内容是什么。例如，配置 **management-accessinside**，以便在外部输入的 VPN 用户可以管理内部接口。如果identity **nat**命令指定 **(inside,outside)**，则您不希望ASA将管理流量发送到内部网络；它将永远不会返回内部接口IP地址。路由查询选项允许 ASA 将流量直接发送到内部接口 IP 地址，而不是流入内部网络。对于从VPN客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。

CR_Examples

以下示例显示如何将名为 inside 的防火墙接口配置为管理访问接口：

```
ciscoasa(config)# management-access inside
```

Related Commands

命令	说明
clearconfiguremanagement-access	为 ASA 的管理访问删除内部接口的配置。
showmanagement-access	显示为管理访问配置的内部接口的名称。

management-only

要将接口设置为仅接受管理流量，请在 **management-only** 接口配置模式下使用该命令。要允许通过流量，请使用此命令的 **no** 形式。

management-only [**individual**]
no management-only [**individual**]

Syntax Description

individual	对于 Firepower 9300 ASA 安全模块集群，您必须在跨区接口模式下为管理接口指定 **individual** 关键字。

Command Default

管理 是否 适用接口（如果适用） 默认情况下将设置为管理专用模式。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.0(1)	运行配置中此命令的位置已移至接口部分的顶部，以支持ASA集群，其中对管理接口有特殊豁免。
9.4(1.152)	添加了 **individual** 关键字。

使用指南

大多数型号包含一个名为 管理 *n* /*n* 的专用管理接口，用于支持流向 ASA 的流量。但是，您可以使用该 **management-only** 命令将任何接口配置为仅管理接口。

注释 对于除 ASA 5585-X 之外的所有型号，您无法禁用管理接口的仅管理模式默认情况下，此命令始终处于启用状态。EXTENSI

在透明防火墙模式下，除了允许的最大数量的直通流量接口，您还可以将管理接口（物理接口、子接口[如果所用的型号支持]或由管理接口组成的 EtherChannel 接口[如果有多个管理接口]）用作单独的管理接口。您不能将任何其他接口类型用作管理接口。

如果您的模型不包含管理接口，则必须从数据接口管理透明防火墙。

在多情景模式下，您无法跨情景共享任何接口，包括管理接口。要为每个情景提供管理，您可以创建管理接口的子接口，然后向每个情景分配管理子接口。请注意，除 ASA 5585-X 外，管理接口不允许子接口，因此对于每个上下文管理，您必须连接到数据接口。

管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

CR_Examples

以下示例禁用管理接口上的仅管理模式：

```
ciscoasa(config)# interface management0/0
ciscoasa(config-if)# no management-only
```

以下示例在子接口上启用仅管理模式：

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# management-only
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。

map-domain

要配置映射地址和端口 (MAP) 域，请在全局配置模式下使用 **map-domain** 命令。使用此 **no**命令的形式删除MAP域。

map-domain*name*
no map-domain*name*

Syntax Description

name MAP域的名称，是最多48个字符的字母数字字符串。该名称还可以包含以下特殊字符：句点(.)、斜线 (/) 和冒号 (:)。

Command Default

无默认值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.13(1)	引入了此命令。

使用指南

映射地址和端口（映射）主要是在服务提供商（SP）网络中使用的一项功能。服务提供商可以运行 IPv6 网络、映射域，同时支持 IPv4 用户，以及与公共互联网上的 IPv4 站点通信的需要。映射在 RFC7597、RFC7598 和 RFC7599 中定义。

对于 MAP 域内的服务提供商来说，MAP 相对于 NAT46 的优势在于，用 IPv6 地址替换用户的 IPv4 地址（在 SP 网络边缘再返回到 IPv4）是无状态的。与 NAT46 相比，这提高了 SP 网络的效率。

有两种 MAP 技术：MAP 转换 (MAP-T) 和 MAP 封装 (MAP-E)。ASA 支持 MAP-T；不支持 MAP-E。

要配置 MAP-T，您需要创建一个或多个域。在客户边缘 (CE) 和边界中继 (BR) 设备上配置 MAP-T 时，请确保将参与每个域的每台设备使用相同的参数。

您最多可以配置 25 个 MAP-T 域。在多情景模式下，您最多可以在每个情景中配置 25 个域。

CR_Examples

以下示例创建一个名为 1 的 MAP-T 域，并为该域配置转换规则。

```
ciscoasa(config)# map-domain 1
```

```
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

命令	说明
basic-mapping-rule	配置 MAP 域的基本映射规则。
default-mapping-rule	配置 MAP 域的默认映射规则。
ipv4-prefix	为 MAP 域中的基本映射规则配置 IPv4 前缀。
ipv6-prefix	为 MAP 域中的基本映射规则配置 IPv6 前缀。
map-domain	配置映射地址和端口 (MAP) 域。
share-ratio	在 MAP 域中配置基本映射规则中的端口数。
showmap-domain	显示有关映射地址和端口 (MAP) 域的信息。
start-port	配置 MAP 域中基本映射规则的起始端口。

map-name

要将用户定义的属性名称映射到思科属性名称，请在 ldap-attribute-map 配置模式下使用 **map-name** 命令。

要删除此映射，请使用此命 **no**令的形式。

map-name*user-attribute-name Cisco-attribute-name*
nomap-name*user-attribute-name Cisco-attribute-name*

Syntax Description

user-attribute-name	指定要映射到思科属性的用户定义属性的名称。
Cisco-attribute-name	指定映射至用户定义名称的思科属性名称。

Command Default

默认情况下，不存在名称映射。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
ldap-attribute-map 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

通过 **map-name** 命令，您可以将自己的属性名称映射到思科 属性名称。然后，可以将生成的属性映射绑定到 LDAP 服务器。通常的步骤包括：

1. 在全局配置模式下使用 **ldapattribute-map** 命令来创建未填充的属性映射。此命令将进入 ldap-attribute-map 配置模式。
2. 在 ldap-attribute-map 配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 aaa-server 主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。请注意此命令中“ldap”后面的连字符。

注释 要正确使用属性映射功能，您需要了解 Cisco LDAP 属性名称和值以及用户定义的属性名称和值。

CR_Examples

以下示例命令将用户定义的属性名称 Hours 映射到 LDAP 属性映射 myldapmap 中的思科属性名称 cVPN3000-Access-Hours：

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
ciscoasa(config-ldap-attribute-map)#
```

在 ldap-attribute-map 配置模式下，您可以输入“？”显示思科 LDAP 属性名称的完整列表：

```
ciscoasa(config-ldap-attribute-map)# map-name <name>
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
 :
 :
  cVPN3000-X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

Related Commands

命令	说明
ldapattribute-map(globalconfigurationmode)	创建并命名 LDAP 属性映射，以将用户定义的属性名称映射到思科 LDAP 属性名称。
ldap-attribute-map(aaa-serverhostmode)	将 LDAP 属性映射绑定到 LDAP 服务器。
map-value	将用户定义的属性值映射到思科属性。
show running-config ldap attribute-map	显示特定运行 LDAP 属性映射或所有运行属性映射。
clearconfigureldapattribute-map	删除所有 LDAP 属性映射。

mapping-service (已弃用)

要为 Cisco Intercompany Media Engine 代理配置映射服务，请使用 UC-IME 配置模式下的 **mapping-service**命令。要从代理中删除映射服务，请使用此命令的 **no**形式。

mapping-servicelistening-interface接口 [**listening-port**端口] **uc-ime-interface**接口
nomapping-servicelistening-interface接口 [**listening-port**端口] **uc-ime-interface**接口

Syntax Description

interface	指定要用于侦听接口或 uc-ime 接口的接口的名称。
listening-interface	配置 ASA 用来侦听映射请求的接口。
listening-port	（可选）配置映射服务的侦听端口。
port	（可选）指定 ASA 侦听映射请求的 TCP 端口号。端口号必须为 1024 或更高版本，以避免与设备上的其他服务（例如 Telnet 或 SSH）冲突。默认情况下，端口号为 TCP 8060。
uc-ime-interface	配置连接到远程 Cisco UCM 的接口。

Command Default

默认情况下，思科公司间媒体引擎代理的路径外部署的映射服务侦听 TCP 端口 8060。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
UC-IME 配置	• 是	—	• 是	—	—

Command History

版本	修改
8.3(1)	添加了此命令。
9.4(1)	此命令与所**uc-ime**有模式命令一起已被弃用。

使用指南

对于 ASA 上思科公司间媒体引擎代理的路径外部署， 会将映射服务添加到代理配置。要配置映射服务，必须指定侦听映射请求的外部接口（远程企业端）以及连接到远程思科 UCM 的接口。

注释 您只能为 Cisco Intercompany Media Engine 代理配置一个映射服务器。

为路径外部署配置思科公司间媒体引擎代理时，您需要配置映射服务。

在关闭路径部署中，入站和出站思科公司间媒体引擎呼叫将通过启用了思科公司间媒体引擎代理的自适应安全设备。自适应安全设备位于 DMZ 中，并配置为主要支持思科公司间媒体引擎。正常的面向互联网的流量不会流经此 ASA。

对于所有入站呼叫，信令将定向至 ASA，因为有目的思科 UCM 是使用 ASA 上的全局 IP 地址进行配置的。对于出站呼叫，被叫方可以是互联网上的任何IP地址；因此，ASA配置了映射服务，以便在 ASA 上为互联网上被叫方的每个全局 IP 地址动态提供内部 IP 地址。

思科 UCM 将所有出站呼叫直接发送到自适应安全设备上的映射内部 IP 地址，而不是被叫方在互联网上的全局 IP 地址。然后，ASA 将呼叫转发至被叫方的全局 IP 地址。

CR_Examples

以下示例显示...：

```
ciscoasa
(config)# uc-ime offpath_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
ciscoasa(config-uc-ime)# mapping-service listening-interface inside listening-port 8060
uc-ime-interface outside
```

Related Commands

命令	说明
showrunning-configuc-ime	显示思科公司间媒体引擎代理的运行中配置。
showuc-ime	显示有关回退通知、映射服务会话和信令会话的统计数据或详细信息。
uc-ime	在 ASA 上创建 Cisco Intercompany Media Engine 代理实例。

map-value

要将用户定义的值映射到思科 LDAP 值，请在 ldap-attribute-map 配置模式下使用 **map-value**命令。要删除映射中的条目，请使用此命令的 **no** 形式。

map-value*user-attribute-name user-value-string Cisco-value-string*
nomap-value*user-attribute-name user-value-string Cisco-value-string*

Syntax Description

思科值字符串	为思科属性指定思科值字符串。
user-attribute-name	指定要映射到思科属性名称的用户定义属性名称。
用户值字符串	指定要映射到思科属性值的用户定义值字符串。

Command Default

默认情况下，没有映射到思科属性的用户定义值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
ldap-attribute-map 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

通过 **map-value** 命令，您可以将自己的属性值映射到思科属性名称和值。然后，可以将生成的属性映射绑定到 LDAP 服务器。通常的步骤包括：

1. 在全局配置模式下使用 **ldapattribute-map** 命令来创建未填充的属性映射。此命令将进入 ldap-attribute-map 配置模式。
2. 在 ldap-attribute-map 配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 aaa-server 主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。请注意此命令中“ldap”后面的连字符。

注释 要正确使用属性映射功能，您需要了解 Cisco LDAP 属性名称和值以及用户定义的属性名称和值。

CR_Examples

以下示例在 ldap-attribute-map 配置模式下输入，将用户属性 Hours 的用户定义值设置为名为 workDay 的用户定义时间策略和思科定义的名为 Daytime 的时间策略：

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-value Hours workDay Daytime
ciscoasa(config-ldap-attribute-map)#
```

Related Commands

命令	说明
ldapattribute-map(globalconfigurationmode)	创建并命名 LDAP 属性映射，以将用户定义的属性名称映射到思科 LDAP 属性名称。
ldap-attribute-map(aaa-serverhostmode)	将 LDAP 属性映射绑定到 LDAP 服务器。
map-name	将用户定义的 LDAP 属性名称与思科 LDAP 属性名称映射。
show running-config ldap attribute-map	显示特定运行 LDAP 属性映射或所有运行属性映射。
clearconfigureldapattribute-map	删除所有 LDAP 映射。

mask

使用模块化策略框架时，通过在匹配或类配置模式下使用 **match** 命令掩蔽与 **mask**命令或类映射匹配的数据包部分。此掩码操作在用于应用流量的检测策略映射（使用 **policy-maptypeinspect**命令）中可用；但是，并非所有应用都允许此操作。例如，您可以使用 **mask** 命令进行 DNS 应用检测，以便在允许流量通过 ASA 之前掩蔽报头标志。要禁用此操作，请使用此命令的 no 形式。

mask [**log**]
nomask [**log**]

Syntax Description

log	记录匹配。系统日志消息数取决于应用。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
匹配和类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

检查策略图由一个或多个 **match**和 **class**命令组成。检查策略图可用的确切命令取决于应用程序。在输入 **match** 或 **class** 命令标识应用流量后（ **class** 命令是指现有的 **class-maptypeinspect**命令，该命令转而包含 **match** 命令），可以输入 **mask**命令来掩蔽匹配的部分数据包使用 **match** 命令或 **class** 命令。

在第 3/4 层策略映射（简称 **policy-map** 命令）中使用 **inspect** 命令启用应用检测时，您可以启用包含此操作的检测策略映射，例如，输入 **inspectdnsdns_policy_map** 命令，其中 dns_policy_map 是检测策略映射的名称。

CR_Examples

以下示例在允许流量通过 ASA 之前掩蔽 DNS 报头中的 RD 和 RA 标志的示例：

```
ciscoasa(config-cmap)# policy-map type inspect dns dns-map1
ciscoasa(config-pmap-c)# match header-flag RD
ciscoasa(config-pmap-c)# mask log
ciscoasa(config-pmap-c)# match header-flag RA
ciscoasa(config-pmap-c)# mask log
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-maptypeinspect	定义特殊的应用检查操作。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

mask-banner

要模糊服务器横幅，请在参数配置模式下使用 **mask-banner**命令。要禁用此功能，请使用此**no** 命令的形式。

mask-banner
no mask-banner

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
参数配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例显示如何屏蔽服务器横幅：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

mask-syst-reply

要对客户端隐藏 FTP 服务器响应，请在 FTP 映射配置模式下使用 **mask-syst-reply** 命令。通过使用 **ftp-map** 命令可以进入该模式。要删除配置，请使用此命令的 no 形式。

mask-syst-reply
no mask-syst-reply

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下会启用此命令。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
FTP 映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

与严格 FTP 检测配合使用 mask-syst-reply 命令可保护 FTP 服务器系统免受客户端侵害。启用此命令后，服务器对 **syst** 命令的应答将替换为一串 X。

CR_Examples

以下示例导致 ASA 将 FTP 服务器对 syst 命令的应答替换为 X：

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# mask-syst-reply
ciscoasa(config-ftp-map)#
```

命令	说明
class-map	定义要应用的安全操作的流量类。
ftp-map	定义 FTP 映射并启用 FTP 映射配置模式。
inspectftp	应用特定的FTP映射来用于应用程序检查。
policy-map	将类映射与特定的安全操作相关联。
request-commanddeny	指定要禁止的 FTP 命令。

match access-list

当使用模块化策略框架时，通过在类映射配置模式下使用 **matchaccess-list** 命令，使用访问列表来标识要应用操作的流量。要删除该 **matchaccess-list** 命令，请使用此命 **no**令的形式。

match access-list*access_list_name*
no match access-list*access_list_name*

Syntax Description

access_list_name	指定用作匹配条件的访问列表的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

配置模块化策略框架包括四项任务：

1. 标识要使用**class-map** 命令应用操作的第 3 层和第 4 层流量。

输入 **class-map** 命令后，您可以输入 **matchaccess-list**命令来标识流量。或者，您也可以输入其他类型的 **match** 命令，例如**matchport** 命令。类映射中只能包含一个 **matchaccess-list**命令，且不能将其与其他类型的 **match** 命令组合使用。例外情况是，如果您定义 **matchdefault-inspection-traffic**命令匹配 ASA 可检测的所有应用使用的默认 TCP 和 UDP 端口，则可以使用 **matchaccess-list**命令缩小要匹配的流量。由于该命令指定了要匹配的端口，因此 **matchdefault-inspection-traffic** 访问列表中的任何端口都将被忽略。

1. （仅限应用检测）使用 **policy-maptypeinspect** 命令定义应用检测流量的特殊操作。
2. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。
3. 使用 **service-policy** 命令在接口上激活这些操作。

CR_Examples

以下示例创建与三个访问列表匹配的三个第 3/4 层类映射：

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp
ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp
ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match any

使用模块化策略框架时，请在类映射配置模式下使用 **matchany** 命令匹配要应用操作的所有流量。要删除该 **matchany** 命令，请使用此命 **no**令的形式。

match any
no match any

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

配置模块化策略框架包括四项任务：

1. 标识要使用**class-map** 命令应用操作的第 3 层和第 4 层流量。

输入 **class-map** 命令后，您可以输入 **matchany**命令来标识所有流量。或者，您也可以输入其他类型的 **match** 命令，例如**matchport** 命令。您不能将**matchany** 命令与其他类型的 **match** 命令结合使用。

1. （仅限应用检测）使用 **policy-maptypeinspect** 命令定义应用检测流量的特殊操作。
2. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。
3. 使用 **service-policy** 命令在接口上激活这些操作。

CR_Examples

此示例显示如何使用类映射和 **matchany** 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchany
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchaccess-list	根据访问列表匹配流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match apn

如要配置 GTP 消息中的无线接入点名称匹配条件，请在策略映射配置模式下使用 **matchapn** 命令。要删除匹配条件，请使用此 **no**命令的形式。

match [**not**] **apnregex** {*regex_name* | **class***regex_class_name*}
no match [**not**] **apnregex** [*regex_name* | **class***regex_class_name*]

Syntax Description

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

可以在 GTP 策略映射中配置此命令。

CR_Examples

以下示例显示如何为 GTP 检测策略映射中的无线接入点名称配置匹配条件：

```
ciscoasa(config-pmap)# match apn class gtp_regex_apn
```

Related Commands

命令	说明
inspectgtp	配置 GTP 流量检测。

match application-id

要配置 Diameter 消息的 Diameter 应用标识符的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchapplication-id** 命令。要删除匹配条件，请使用此 **no**命令的形式。

match [**not**] **application-id***app_id* [*app_id_2*]
no match [**not**] **application-id***app_id* [*app_id_2*]

Syntax Description

app_id	Diameter 应用程序名称或编号 (0-4294967295)。如果要匹配某个连续编号的应用范围，可以再添加一个 ID。您可以按应用名称或编号来定义范围，该范围将适用于第一个 ID 和第二个 ID 之间的所有编号。

Command Default

Diameter 检测允许所有应用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南

可以在 Diameter 检测类映射或策略映射中配置此命令。使用它可根据 Diameter 应用 ID 过滤流量。然后，可以丢弃数据包、连接或记录匹配的流量。

这些应用会注册到 IANA。以下是支持的核心应用，但您可以对其他应用进行过滤。有关应用名称的列表，请参阅 CLI 帮助。

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0)。这是基础 Diameter 协议。

IETF 在 http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml 上列出了已注册的应用程序、命令代码和属性值对，但 Diameter 检查并不支持所有列出的项目。有关它们的技术规范，请参阅 3GPP 网站。

CR_Examples

以下示例显示如何为 3gpp-s6a 和 3gpp-s13 应用 ID 配置匹配条件。

```
ciscoasa(config)# class-map type inspect diameter match-any log_app
ciscoasa(config-cmap)# match application-id 3gpp-s6a
ciscoasa(config-cmap)# match application-id 3gpp-s13
```

Related Commands

命令	说明
class-maptypeinspect	创建检查类别图。
inspectdiameter	启用 Diameter 检测。
policy-maptypeinspect	创建检查策略映射。

match as-path

要匹配 BGP 自治系统路径访问列表，请在路由映射配置模式下使用 match as-path 命令。要删除路径列表条目，请使用此命令的 no 形式。

matchas-path路径列表编号
nomatchas-path路径列表编号

Syntax Description

路径列表编号	自治系统路径访问列表编号。

Command Default

未定义任何路径列表。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由图配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

match as-path 和 set weight 命令设置的值会覆盖全局值。例如，使用 match as-path 和 set weight route-map 配置命令分配的权重会覆盖使用 neighbor weight 命令分配的权重。

路由映射可包含多个部分。不匹配至少一个与 route-map 命令相关的 match 子句的任何路由将被忽略；也就是说，系统将不为出站路由映射通告路由，也不会为入站路由映射接受路由。如果仅修改某些数据，则必须指定显式匹配项来配置第二个 route-map 部分。它可以接受多个 path-list-name。

CR_Examples

以下示例设置自治系统路径，以匹配 BGP 自治系统路径访问列表 as-path-acl：

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

Related Commands

命令	说明
set-weight	指定路由表的BGP权重。

命令	说明
neighbor-weight	为邻居连接分配权重。

match avp

要为 Diameter 消息中的 Diameter 属性值对 (AVP) 配置匹配条件，请在类映射或策略映射配置模式下使用 **matchavp** 命令。要删除匹配条件，请使用此 **no**命令的形式。

要仅按属性匹配 AVP，请使用以下命令：

match [**not**] **avp***code* [*code-2*] [**vendor-id***id_number*]
no match [**not**] **avp***code* [*code-2*] [**vendor-id***id_number*]

要基于属性的值匹配 AVP，请使用以下命令：

match [**not**] **avp***code* [**vendor-id***id_number*] *value*
no match [**not**] **avp***code* [**vendor-id***id_number*] *value*

Syntax Description

code	属性值对的名称或编号（1-4294967295）。对于第一个代码，您可以指定自定义 AVP 的名称或已在 RFC 或 3GPP 技术规范中注册且受该软件直接支持的某个 AVP 的名称。如果要匹配 AVP 的范围，请仅按编号指定第二个代码。如果要按值匹配 AVP，则无法指定第二个代码。有关 AVP 名称的列表，请参阅 CLI 帮助。
value	AVP 的值部分。只有 AVP 的数据类型受支持，才能配置此项目。例如，可以为具有地址数据类型的 AVP 指定 IP 地址。有关如何配置此参数的详细信息，请参阅下面的“使用”部分。
vendor-id*id_number*	（可选。）也要一并匹配的供应商的 ID 编号，范围为 0-4294967295。例如，3GPP 供应商 ID 为 10415，IETF 为 0。

Command Default

Diameter 检测允许所有 AVP。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南

可以在 Diameter 检测类映射或策略映射中配置此命令。可用于根据 Diameter AVP 过滤流量。然后，可以丢弃数据包、连接或记录匹配的流量。

使用 CLI 帮助获取 AVP 名称列表。IETF 在 上有一个注册应用程序、命令代码和属性值对的列表 https://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml ，尽管 Diameter 检查并不支持所有列出的项目。有关它们的技术规范，请参阅 3GPP 网站。

如果您正在配置值匹配，以下是支持的数据类型的值选项的具体语法：

- Diameter Identity、Diameter URI、Octet String - 使用正则表达式或正则表达式类对象匹配这些数据类型。

{**regex***regex_name* | **class***regex_class*}

- Address - 指定要匹配的 IPv4 或 IPv6 地址。例如，10.100.10.10 或 2001:DB8::0DB8:800:200C:417A。
- Time - 指定开始和结束日期及时间。两者均为必填项目。时间采用 24 小时格式。

date*yearmonthday***time***hh*:*mm*:*ss***date***yearmonthday***time***hh*:*mm*:*ss*

例如：

date2015feb5time12:00:00date2015mar9time12:00:00

- Numeric - 指定编号的范围：

range*number_1number_2*

有效的编号范围取决于数据类型：

- Integer32：-2147483647 到 2147483647
- Integer64：-9223372036854775807 到 9223372036854775807
- Unsigned32：0 到 4294967295
- Unsigned64：0 到 18446744073709551615
- Float32：小数点表示方式，精度为 8 位数
- Float64：小数点表示方式，精度为 16 位数

CR_Examples

以下示例显示如何为 host-ip-address AVP on Capability Exchange 请求/应答命令消息上显示的特定 IP 地址配置匹配条件。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

Related Commands

命令	说明
class-maptypeinspect	创建检查类别图。
diameter	创建自定义属性-值对。
inspectdiameter	启用 Diameter 检测。
policy-maptypeinspect	创建检查策略映射。

match body

要配置 ESMTP 消息正文消息的长度或行长度的匹配条件，请在类映射或策略映射配置模式下使用 **matchbody** 命令。要删除已配置的部分，请使用**no**此命令的形式。

match [**not**] **body** [**length** | **linelength**] **gt**字节
no match [**not**] **body** [**length** | **linelength**] **gt**字节

Syntax Description

length	指定 ESMTP 正文消息的长度。
线长	指定 ESMTP 正文消息的行长度。
bytes	指定要匹配的数量（以字节为单位）。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例显示如何在 ESMTP 检查策略映射中配置正文行长度的匹配条件：

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)#**matchbodylinelengthgt1000**

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match called-party

要配置 H.323 被叫方的匹配条件，请在策略映射配置模式下使用 **matchcalled-party** 命令。要禁用此功能，请使用此**no**命令的形式。

match [**not**] **called-party** [**regex***regex*]
no match [**not**] **match** [**not**] **called-party** [**regex***regex*]

Syntax Description

regex regex	指定匹配正则表达式。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例展示如何在 H.323 检测类映射中为被叫配置匹配条件：

```
ciscoasa(config-cmap)# match called-party regex caller1
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match calling-party

要配置H.323主叫方的匹配条件，请在策略映射配置模式下使用**matchcalling-party**命令。要禁用此功能，请使用此**no**命令的形式。

match [**not**] **calling-party** [**regex***regex*]
nomatch [**not**] **match** [**not**] **calling-party** [**regex***regex*]

Syntax Description

regex regex	指定匹配正则表达式。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例显示如何在 H.323 检测类映射中为主叫方配置匹配条件：

```
ciscoasa(config-cmap)# match calling-party regex caller1
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match certificate

要配置证书匹配规则，请在 crypto ca trustpoint 配置模式下使用 **matchcertificate** 命令。要从配置中删除规则，请使用此命 **no**令的形式。

matchcertificate*map-name* [**overrideocsp** [**trustpoint***trustpoint-name*] *seq-num***url***URL* | **override cdp***seq-num***url***URL*]
nomatchcertificate*map-name* [**overrideocsp** [*seq-num***url***URL*] | **overridecdp** [*seq-num***url***URL*]]

Syntax Description

map-name	指定与此规则匹配的证书映射的名称。在配置匹配规则之前，必须配置证书映射。最大长度为 65 个字符。
覆盖 OCSP	指定该规则旨在覆盖证书中的 OCSP URL。
seq-num	设置此匹配规则的优先级。有效范围是 1 至 10000。ASA 首先评估具有最小序列号的匹配规则，然后评估序列号较大的匹配规则，直到找到匹配项。
信任点	（可选）指定使用信任点来验证 OCSP 响应方证书。
trustpoint-name	（可选）标识要与覆盖一起使用的信任点，以验证响应方证书。
url	指定访问 URL 获取 OCSP 吊销状态。
URL	标识用于访问 OCSP 吊销状态的 URL。
覆盖 cdp	指定规则的目的是覆盖证书中的 CRL URL。
seq-num	设置列表中每个 URL 的等级。指定 1 到 5 之间的值。ASA 首先尝试最低等级 (1) 的 URL。
url	指定访问 URL 获取 CRL 吊销状态。
URL	用于访问 CRL 吊销状态的 URL。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
crypto ca trustpoint 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。
9.13(1)	添加了用于配置 cdp 覆盖的调配。
9.15(1)	在此版本之前，静态 CDP 可以唯一地映射到正在验证的链中的每个证书。但是，每个证书仅支持一个此类映射。 在此版本中，match certificate cdp override 命令接受同一映射名称的多个实例。

使用指南

在 PKI 证书验证过程中，ASA 将通过使用 CRL 检查或在线证书状态协议 (OCSP) 来检查证书吊销状态以维护安全性。通过 CRL 检查，ASA 可以检索、解析和缓存 CRL，从而提供已撤销证书的完整列表。OCSP 提供了一种更具可扩展性的检查撤销状态的方法，因为 OCSP 将证书状态本地化在验证机构上，并查询特定证书的状态。

证书匹配规则允许您配置 OCSP URL 覆盖，即指定要检查撤销状态的 URL，而不是远程用户证书 AIA 字段中的 URL。通过匹配规则，您还可以配置用于验证 OCSP 响应方证书的信任点，这可以让 ASA 验证来自任何 CA 的响应方证书，包括自签名证书和客户端证书验证路径外部的证书。

与 OCSP 类似，您可以使用 **matchcertificate** 命令来配置 CDP URL 覆盖。此命令支持通过证书映射识别静态 CDP URL。对于需要 CRL 验证的每个证书，根据证书中的 CDP 扩展和此配置中映射的任何 URL 检索 CRL。在 [**config-ca-crl**子模式下，可以使用 **policy** 命令用于从证书或静态 CDP 中排除 CDP。

您现在可以将多个静态 CDP 配置到单个映射。要删除单个实例，请在命令的 **no** 形式中指定 URL 和序号。确保指定的URL和序列号与您配置的值相同。如果您未提及任何特定信息，则映射的所有条目都将被删除。具有或删除映射的多个实例的调配不适用于 OCSP。

配置 OCSP 时，请注意以下要求：

- 可在一个信任点配置中配置多个匹配规则，但每个 crypto CA 证书映射只能有一个匹配规则。但是，您可以配置多个加密 CA 证书映射，并将其与同一信任点关联。
- 在配置匹配规则之前，必须配置证书映射。
- 要配置信任点以验证自签名 OCSP 响应者证书，您需要将自签名响应者证书作为受信任的 CA 证书导入到其自己的信任点。然后，您在**matchcertificate**客户端证书验证信任点中配置命令，以使用包含自签名 OCSP 响应者证书的信任点来验证响应者证书。这同样适用于验证客户端证书验证路径之外的响应者证书。
- 如果同一 CA 颁发客户端证书和响应方证书，则信任点可以同时验证这两个证书。但是，如果不同的 CA 颁发客户端证书和响应方证书，则需要配置两个信任点，每个证书一个信任点。
- OCSP 服务器（响应者）证书通常会签署 OCSP 响应收到响应后，ASA 会尝试验证响应方证书。CA 通常会将其 OCSP 响应方证书的生命周期设置为相对较短的时间段，以将被破坏的几率降到最低。CA 通常还会在响应方证书中包含 ocsp-no-check 扩展，指示此证书不需要处于吊销状态正在检查。但如果此扩展不存在，ASA 会尝试使用信任点中指定的相同方法检查其撤销状态。如果响应者证书无法验证，则撤销检查失败。为了避免这种可能性，请在 **revocation-checknone** 配置响应方证书验证信任点时使用该命令，并在 **revocation-checkocsp**配置客户端证书时使用该命令。

- 如果 ASA 未找到匹配项，它将使用 **ocspurl** 命令中指定的 URL。如果尚未配置 **ocspurl** 命令，ASA 将使用远程用户证书的 AIA 字段。如果证书没有 AIA 扩展，则吊销状态检查失败。

CR_Examples

以下示例显示如何为名为 newtrust 的信任点创建证书匹配规则。该规则有一个名为 mymap 的映射、序列号为 4、一个名为 mytrust 的信任点，并且指定了 URL 10.22.184.22。

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
 url 10.22.184.22
ciscoasa(config-ca-trustpoint)#
```

以下示例显示如何配置加密 CA 证书映射，然后配置匹配证书规则，以识别包含 CA 证书的信任点以验证响应方证书。如果 newtrust 信任点中识别的 CA 未颁发 OCSP 响应方证书，则需要此证书。

1. 配置标识映射规则应用到的客户端证书的证书映射。在本示例中，证书映射的名称是 mymap，序列号是 1。subject-name 的 CN 属性等于 mycert 的任何客户端证书都与 mymap 条目匹配。

```
ciscoasa(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)#
```

2. 配置包含用于验证 OCSP 响应方证书的 CA 证书的信任点。对于自签名证书，这是自签名证书本身，已导入且受本地信任。此外，您还可以通过外部 CA 注册获取用于此目的的证书。当系统提示您进行操作时，粘贴 CA 证书。

```
ciscoasa(config-ca-cert-map)# exit
ciscoasa(config)# crypto ca trustpoint mytrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word “quit” on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit

INFO: Certificate has the following attributes:
Fingerprint: 7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

3. 配置原始信任点 newtrust，使用 OCSP 作为吊销检查方法。然后，设置一个包含在步骤 2 中配置的证书映射 mymap 和自签名信任点 mytrust 的匹配规则。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate newtrust
```

```
Enter the base 64 encoded CA certificate.
End with the word “quit” on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint: 9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# revocation-check ocsp
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust
 4 url 10.22.184.22
```

使用newtrust信任点进行客户端证书身份验证的任何连接都会检查客户端证书，以确定客户端证书是否与 mymap 证书映射中指定的属性规则匹配。如果是，ASA 将访问 10.22.184.22 的 OCSP 响应方获取证书撤销状态，然后使用 mytrust 信任点验证响应方证书。

注释 newtrust 信任点配置为通过 OCSP 为客户端证书执行吊销检查。但是，会为默认吊销检查方法（无）配置 mytrust 信任点。因此，不会对 OCSP 响应方证书执行吊销检查。

以下示例显示使用 CDP 配置匹配证书规则。该规则有一个名为 test 的映射名称，1、2 和 3 分别为序号和静态 URL。为证书选择 CDP 时，ASA 会为与名为 *test*的证书映射匹配的任何证书选择 3 个 CDP。如果 ASA 确定在验证证书时需要 CRL，将按给定顺序尝试 URL，直到成功检索到 CRL 为止。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 1 url http://1.1.1.1
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 2 url http://1.1.1.2
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 3 url http://1.1.1.3
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
crypto ca certificate map	创建加密 CA 证书映射。在全局配置模式下使用此命令。
cryptocatrustpoint	进入加密ca信任点配置模式。在全局配置模式下使用此命令。
ocspdisable-nonce	禁用 OCSP 请求的 nonce 扩展。
ocspurl	指定要用于检查与信任点关联的所有证书的 OCSP 服务器。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

匹配证书允许过期证书（已弃用）

要允许管理员豁免对某些证书进行过期检查，请在 ca-trustpool 配置模式下使用 **matchcertificateallowexpired-certificate**命令。要禁用某些证书的豁免，请使用此命令的 **no** 形式。

match certificate<map>allow expired-certificate
no match certificate<map>allow expired-certificate

Syntax Description

allow	允许接受过期的证书。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
CA-trustpool 配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。
9.13(1)	此命令行已删除。

使用指南

trustpool match 命令利用证书映射对象为全局信任池策略配置证书特定的例外情况或覆盖。匹配规则是相对于正在验证的证书编写的。

Related Commands

命令	说明
matchcertificateskiprevocationcheck	豁免某些证书执行吊销检查。

match certificate skip revocation-check

要允许管理员免于对某些证书执行吊销检查，请在 ca-trustpool 配置模式下使用 **matchcertificateskiprevocation-check**命令。要禁用吊销检查豁免，请使用此命令的 **no** 形式。

matchcertificatemapskiprevocation-check
nomatchcertificatemapskiprevocation-check

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
CA-trustpool 配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

trustpool match 命令利用证书映射对象为全局信任池策略配置证书特定的例外情况或覆盖。匹配规则是相对于正在验证的证书编写的。

CR_Examples

以下示例显示跳过对使用者 DN 公用名称为“mycompany123”的证书的有效性检查。

```
crypto ca certificate map mycompany 1subject-name attr cn eq mycompany123crypto ca trustpool
 policymatch certificate mycompany skip revocation-check
```

Related Commands

命令	说明
matchcertificateallowexpired-certificate	豁免对某些证书进行到期检查。

match cmd

要在 ESMTP 命令谓词上配置匹配条件，请在策略映射配置模式下使用 **matchcmd** 命令。要禁用此功能，请使用此**no**命令的形式。

match [**not**] **cmd** [**verb***verb* | **linelengthgt***bytes* | **RCPTcountgt***recipients_number*]
no match [**not**] **cmd** [**verb***verb* | **linelengthgt***bytes* | **RCPTcountgt***recipients_number*]

Syntax Description

动词 动词	指定 ESMTP 命令谓词。
行长度 *gt* 字节	指定线的长度。
RCPT count gtrecipients_number	指定收件人邮件地址的数量。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例显示如何在 ESMTP 检测策略映射中为 ESMTP 事务中交换的谓词（方法）NOOP 配置匹配条件：

```
ciscoasa(config-pmap)# match cmd verb NOOP
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match command-code

要为 Diameter 消息的 Diameter 命令代码配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchcommand-code** 命令。要删除匹配条件，请使用此 **no**命令的形式。

match [**not**] **command-code***code* [*code_2*]
no match [**not**] **command-code***code* [*code_2*]

Syntax Description

code Diameter 命令代码名称或编号（0-4294967295）。如果要匹配某个连续编号的命令代码范围，可以再添加一个代码。您可以按命令代码名称或编号来定义范围，该范围将适用于第一个代码和第二个代码之间的所有编号。请参阅 CLI 帮助以获取命令代码名称列表。EXTEN

Command Default

Diameter 检测允许所有命令代码。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南

可以在 Diameter 检测类映射或策略映射中配置此命令。使用它可根据 Diameter 命令代码过滤流量。然后，可以丢弃数据包、连接或记录匹配的流量。

IETF 在http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml 上列出了已注册的应用程序、命令代码和属性值对，但 Diameter 检查并不支持所有列出的项目。有关它们的技术规范，请参阅 3GPP 网站。

CR_Examples

以下示例显示如何为 host-ip-address AVP on Capability Exchange 请求/应答命令消息上显示的特定 IP 地址配置匹配条件。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip

ciscoasa(config-cmap)# match command-code cer-cea

ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

Related Commands

命令	说明
class-maptypeinspect	创建检查类别图。
inspectdiameter	启用 Diameter 检测。
policy-maptypeinspect	创建检查策略映射。

match community

要匹配边界网关协议 (BGP) 社区，请在路由映射配置模式下使用 match community 命令。要从配置文件中删除 match community 命令并将系统恢复到软件删除 BGP 社区列表条目的默认状态，请使用此命令的 no 形式。

match community { *standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**] }
no match community { *standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**] }

Syntax Description

标准列表编号	指定从 1 到 99 的标准社区列表编号，用于标识一个或多个允许或拒绝社区组。
扩展列表编号	指定从 100 到 500 的扩展社区列表编号，用于标识一个或多个允许或拒绝社区组
community-list-name	社区列表名称。
精确的	（可选）表示需要完全匹配。所有社区以及仅指定社区必须存在。

Command Default

没有与路由映射匹配的社区列表。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由图配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

路由映射可包含多个部分。任何与 route-map 命令相关的至少一个 match 命令不匹配的路由将被忽略；也就是说，系统将不为出站路由映射通告路由，也不会为入站路由映射接受路由。如果仅修改某些数据，则必须指定显式匹配项来配置第二个 route-map 部分。

基于社区列表编号的匹配是适用于 BGP 的一种匹配命令类型。

CR_Examples

以下示例显示匹配社区列表 1 的路由的权重设置为 100。社区值为 109 的任何路由的权重都会设置为 100。

```
ciscoasa(config)#  community-list 1 permit 109
```

```
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)#  match community 1
ciscoasa(config-route-map)# set weight 100
```

以下示例显示匹配社区列表 1 的路由的权重设置为 200。只有社区为 109 的任何路由都会将权重设置为 200。

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1 exact
ciscoasa(config-route-map)# set weight 200
```

在以下示例中，与社区列表 LIST_NAME 匹配的路由的权重将设置为 100。只有社区为 101 的任何路由都会将权重设置为 100。

```
ciscoasa(config)#  community-list LIST_NAME permit 101
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community LIST_NAME
ciscoasa(config-route-map)# set weight 100
```

以下示例显示与扩展社区列表 500。具有扩展社区 1 的任何路由都将权重设置为 150。

```
ciscoasa(config)#  community-list 500 permit [0-9]*
ciscoasa(config)# route-map MAP_NAME permit 10
ciscoasa(config-route-map)# match extcommunity 500
ciscoasa(config-route-map)# set weight 150
```

Related Commands

命令	说明
set-weight	指定路由表的 BGP 权重。
community-list	创建或配置 BGP 社区列表。

match default-inspection-traffic

如要为类映射中的 inspect 命令指定默认流量，请在 class-map 配置模式下使用 **matchdefault-inspection-traffic**命令。要删除此规范，请使用此 **no**命令的形式。

matchdefault-inspection-traffic
nomatchdefault-inspection-traffic

Syntax Description

此命令没有任何参数或关键字。

Command Default

有关每个检测的默认流量，请参阅使用指南部分。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.6(2)	为 DNS over TCP 检测添加了 TCP/53，默认情况下未启用该检测。还添加了 M3UA 和 STUN 的默认端口。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 class-map 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的**match**语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用 **matchdefault-inspection-traffic**命令，您可以匹配各个 **inspect** 命令的默认流量。**matchdefault-inspection-traffic**命令可与其他 match 命令结合使用，该命令通常是 **permitip***src-ipdst-ip* 形式的访问列表。

将第二个 **match** 命令与 **matchdefault-inspection-traffic**命令结合使用的规则是使用 **matchdefault-inspection-traffic**命令指定协议和端口信息，使用第二个 **match** 命令指定所有其他信息（例如 IP 地址）。对于 [**match**] 命令，在第二个 **inspect** 命令中指定的任何协议或端口信息都将被忽略。

例如，下例中指定的端口 65535 将被忽略：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchdefault-inspection-traffic
ciscoasa(config-cmap)# match port 65535
```

用于检测的默认流量如下：

InspectionType	ProtocolType	SourcePort	DestinationPort
ctiqbe	tcp	不适用	2748
dcerpc	tcp	不适用	135
diameter	tcp、sctp	不适用	3868
dns	udp, tcp	53	53
ftp	tcp	不适用	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	不适用	1720
h323 ras	udp	不适用	1718-1719
http	tcp	不适用	80
icmp	icmp	不适用	不适用
ils	tcp	不适用	389
im	tcp	不适用	1-65539
ip-options	rsvp	不适用	不适用
ipsec 直通	udp	不适用	500
m3ua	sctp	不适用	2905
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	不适用
radius-accounting	udp	不适用	1646
rpc	udp	111	111
rsh	tcp	不适用	514
rtsp	tcp	不适用	554
sctp	sctp	any	any
SIP	tcp, udp	不适用	5060

skinny	tcp	不适用	2000
smtp	tcp	不适用	25
sqlnet	tcp	不适用	1521
stun	tcp, udp	不适用	3478
tftp	udp	不适用	69
waas	tcp	不适用	1-65535
xdmcp	udp	177	177

CR_Examples

以下示例显示如何使用类映射和 **matchdefault-inspection-traffic**命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchdefault-inspection-traffic
ciscoasa(config-cmap)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
matchany	包括类映射中的所有流量。
showrunning-configclass-map	显示有关类映射配置的信息。

match dns-class

要为DNS资源记录或“问题”部分中的域系统类配置匹配条件，请在类映射或策略映射配置模式下使用 **matchdns-class** 命令。要删除已配置的类，请使用此命 **no**令的形式。

match [**not**] **dns-class** {**eq***c_well_known* | *c_val*} {**range***c_val1 c_val2*}
no match [**not**] **dns-class** {**eq***c_well_known* | *c_val*} {**range***c_val1 c_val2*}

Syntax Description

eq	指定精确匹配项。
c_ware_known	按已知名称 IN 指定 DNS 类。
c_val	在 DNS class 字段中指定任意值 (0-65535)。
range	指定范围。
c_val1 c_val2	指定范围匹配中的值。每个值介于 0 到 65535 之间。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

默认情况下，此命令检查 DNS 消息的所有字段（问题和 RR）并与指定的类匹配。DNS 查询和响应都会被检查。

使用以下两个命令可以将匹配范围缩小到 DNS 查询的问题部分：match not header-flag QR 和 match question。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何为 DNS 检测策略映射中的 DNS 类配置匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-class eq IN
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match dns-type

要为 DNS 类型（包括查询类型和 RR 类型）配置匹配条件，请在类映射或策略映射配置模式下使用 **matchdns-type** 命令。要删除已配置的 DNS 类型，请使用此命 **no**令的形式。

match [**not**] **dns-type** {**eq***t_well_known* | *t_val*} {**range***t_val1 t_val2*}
no match [**not**] **dns-type** {**eq***t_well_known* | *t_val*} {**range***t_val1 t_val2*}

Syntax Description

eq	指定精确匹配项。
良好知悉	按已知名称指定 DNS 类型：A、NS、CNAME、SOA、TSIG、IXFR 或 AXFR。
t_val	在 DNS 类型字段中指定任意值 (0-65535)。
range	指定范围。
t_val1 t_val2	指定范围匹配中的值。每个值介于 0 到 65535 之间。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

默认情况下，此命令检查 DNS 消息的所有部分（问题和 RR）并匹配指定的类型。DNS 查询和响应都会被检查。

使用以下两个命令可以将匹配范围缩小到 DNS 查询的问题部分：match not header-flag QR 和 match question。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何为 DNS 检测策略映射中的 DNS 类型配置匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match domain-name

要为 DNS 消息域名列表配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchdomain-name** 命令。要删除已配置的部分，请使用**no**此命令的形式。

match [**not**] **domain-nameregex***regex_id*
match [**not**] **domain-nameregexclass***class_id*
no match [**not**] **domain-nameregex***regex_id*
no match [**not**] **domain-nameregexclass***class_id*

Syntax Description

regex	指定正则表达式。
regex_id	指定正则表达式ID。
class	指定包含多个正则表达式条目的类映射。
class_id	指定正则表达式类映射ID。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令将 DNS 消息中的域名与预定义列表进行匹配。压缩域名将在匹配之前进行扩展。结合其他 DNS 匹配命令，可以将匹配条件缩小到某个特定字段。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中匹配 DNS 域名：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match domain-name regex
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match dpc

要为 M3UA 数据消息的目的点代码 (DPC) 配置匹配条件，请在策略映射配置模式下使用 **matchdpc** 命令。要删除匹配条件，请使用此 **no**命令的形式。

match [**not**] **dpc***code*
no match [**not**] **dpc***code*

Syntax Description

code	*Zone-Region-sp* 格式的目标点代码。

Command Default

M3UA 检测允许所有目的点代码。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.6(2)	添加了此命令。

使用指南

您可以在 M3UA 检测策略映射中配置此命令。可以根据目标点代码丢弃数据包。点代码采用 区 域-地区 *-sp* 格式，其中每个元素的可能值取决于 SS7 变体。可以在策略映射中的 **ss7variant** 命令中定义变体。

- ITU - 点代码为 14 位，格式为 3-8-3。值范围为 [0-7]-[0-255]-[0-7]。这是默认的 SS7 变量。
- ANSI - 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
- Japan - 点代码为 16 位，格式为 5-4-7。值范围为 [0-31]-[0-15]-[0-127]。
- China - 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。

CR_Examples

以下示例显示如何为 ITU 配置特定目标点代码的匹配条件。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

Related Commands

命令	说明
inspectm3ua	启用 M3UA 检测。
matchopc	匹配 M3UA 始发点代码。
policy-maptypeinspect	创建检查策略映射。
ss7variant	标识要在策略映射中使用的 SS7 变量。

match dscp

要在类映射中标识IETF定义的DSCP值（在IP报头中），请在class-map配置模式下使用**matchdscp**命令。要删除此规范，请使用此 **no**命令的形式。

matchdscp{*values*}
no match dscp{*values*}

Syntax Description

values	在IP报头中指定最多八个不同的IETF定义的DSCP值。范围是0到63。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 class-map 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的**match**语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用**matchdscp** 命令，可以匹配 IP 报头中 IETF 定义的 DSCP 值。

CR_Examples

以下示例显示如何使用类映射和 **matchdscp**命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchdscp af43 cs1 ef
ciscoasa(config-cmap)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
matchport	指定 TCP/UDP 端口作为该接口上接收的数据包的比较条件。
showrunning-configclass-map	显示有关类映射配置的信息。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。