mf – mz

mfib forwarding

要重新启用接口上的 MFIB 转发，请在 **mfibforwarding** 接口配置模式下使用该命令。要禁用接口上的 MFIB 转发，请使用此命 **no**令的形式。

mfibforwarding
nomfibforwarding

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下， **multicast-routing** 命令可在所有接口上启用 MFIB 转发。

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	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

当您启用组播路由时，默认情况下将在所有接口上启用 MFIB 转发。使用命令的 **no** 形式可在特定接口上禁用 MFIB 转发。只有 **no** 形式会出现在运行配置中。

在接口上禁用MFIB转发时，除非通过其他方法进行专门配置，否则该接口不接受任何组播数据包。当禁用 MFIB 转发时，也会阻止 IGMP 数据包。

CR_Examples

以下示例在指定接口上禁用 MFIB 转发：

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

Related Commands

命令	说明
multicast-routing	启用多播路由。
pim	在接口上启用PIM。

迁移

要将 LAN 间 (IKEv1) 或远程访问配置（SSL 或 IKEv1）迁移到 IKEv2，请在全局配置模式下使用 migrate 命令：

migrate {**l2l** | **remote-access** {**ikev2** | **ssl**} | **overwrite**}

Syntax Description

l2l	将 IKEv1 LAN 间配置迁移到 IKEv2。
remote-access	指定远程访问配置。
ikev2	将远程访问 IKEv1 配置迁移到 IKEv2。
ssl	将远程访问 SSL 配置迁移到 IKEv2。
覆盖	覆盖现有 IKEv2 配置。

Command Default

没有默认值或行为。

Command Modes

下表显示了输入命令的模式：

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
8.4(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

migratel2l 命令将所有 LAN 间 IKEv1 配置迁移到 IKEv2。

如果使用 **overwrite** 关键字，ASA 会使用迁移的命令覆盖任何现有 IKEv2 配置，而不是将其合并。

migrateremote-access 命令将 IKEv1 或 SSL 设置迁移到 IKEv2，但您仍必须执行以下配置任务：

- 在 webvpn 配置模式下加载 Secure Client 个软件包文件。
- 配置 Secure Client 配置文件，并为组策略指定它们。
- 请将用于 IKEv1 连接的任何自定义对象与用于 IKEv2 连接的隧道组关联。

- 使用 **cryptoikev2remote-accesstrust-point** 命令指定服务器身份验证身份证书（信任点）。ASA 使用信任点自行向通过 IKEv2 连接的远程 Secure Client进行身份验证。
- 除默认隧道组或组策略（DefaultWEBVPNGroup 隧道组和默认策略组配置为允许 IKEv2 或 SSL）外，请为您可能已配置的任何隧道组或组策略指定 IKEv2 和/或 SSL。
- 在隧道组中配置组别名或组 URL，以使客户端能够连接到默认组以外的组。
- 更新任何外部组策略和/或用户记录。
- 任何其他全局、隧道组、组策略设置来更改客户端行为。
- 使用 **cryptoikev2enable** 为 IKEv2 配置客户端用于下载文件和/或执行软件升级的端口。<interface> [client-services [port]] 命令设置 。

Related Commands

命令	说明
cryptoikev2enable	在 IPsec 对等体通信的接口上启用 IKEv2 协商。
showruncryptoikev2	显示 IKEv2 配置信息。

min-object-size

要设置 ASA 可为 WebVPN 会话缓存的最小对象大小，请在缓存模式下使用 min-object-size 命令。要更改大小，请再次使用 命令。要设置最小对象大小，请输入值零 (0)。

min-object-size整数范围

Syntax Description

整数范围	0 - 10000 KB。

Command Default

默认大小为 0 KB。

Command Modes

下表显示了输入命令的模式：

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
缓存配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

最小对象尺寸必须小于最大对象尺寸。如果已启用缓存压缩，ASA 会在压缩对象后计算大小。

CR_Examples

以下示例显示如何将最大对象大小设置为 40 KB：

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# min-object-size40
ciscoasa(config-webvpn-cache)#
```

Related Commands

命令	说明
cache	进入 WebVPN 缓存模式。
cache-compressed	配置 WebVPN 缓存压缩。

命令	说明
disable	禁用缓存。
expiry-time	配置缓存对象的到期时间而不重新验证它们。
lmfactor	为仅具有最后修改时间戳的缓存对象设置重新验证策略。
max-object-size	定义要缓存的对象的最大大小。

mkdir

要创建新目录，请在 **mkdir** 特权 EXEC 模式下使用该命令。

mkdir [/**noconfirm**] [**disk0:** | **disk1:** | | **flash:**] *path*

Syntax Description

noconfirm	（可选）抑制确认提示。
disk0:	（可选）指定内部闪存，后跟冒号。
disk1:	（可选）指定外部闪存，后跟冒号。
flash:	（可选）指定内部闪存，后跟冒号。在 ASA 5500 系列自适应安全设备中，该 **flash**关键字的别名为 。 **disk0**
path	要创建的目录的名称和路径。

Command Default

如果不指定路径，则会在当前工作目录中创建目录。

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
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果已存在同名目录，则不会创建新目录。

CR_Examples

以下示例显示如何创建名为“backup”的新目录：

```
ciscoasa# mkdir backup
```

Related Commands

命令	说明
cd	将当前工作目录更改为指定的目录。
dir	系统随即会显示目录的内容。

命令	说明
rmdir	删除指定的目录。
pwd	显示当前工作目录。

mobile-device portal

要将所有移动设备的无客户端 VPN 访问 Web 门户从迷你门户更改为完整浏览器门户，请在 webvpn 配置模式下使用 **mobile-deviceportal** 命令。您只需对运行 Windows CE 等旧版操作系统的智能手机进行此配置。使用现代智能手机则无需配置此选项，因为它们默认使用完整浏览器门户。

mobile-deviceportal {**full**}
nomobile-deviceportal {**full**}

Syntax Description

mobile-deviceportal{full}	为所有移动设备将无客户端 VPN 访问门户从迷你门户更改为支持完整浏览器的门户。

Command Default

运行 命令之前，默认行为是某些移动设备通过迷你门户获得无客户端 VPN 访问，而某些移动设备使用完整门户。

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
webvpn configuration	• 是	—	• 是	—	—

Command History

版本	修改
8.2(5)	此命令是在 8.2(5) 和 8.4(2) 中同时添加的。
8.4(2)	此命令是在 8.2(5) 和 8.4(2) 中同时添加的。

使用指南

仅当思科 Technical Assistance Center (TAC) 建议您使用时，才使用此命令。

CR_Examples

将无客户端 VPN 访问门户更改为所有移动设备的完整浏览器门户。

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

Related Commands

命令	说明
show running-config webvpn	显示 webvpn 的运行配置。

mode

要将安全情景模式设置为单一或多个，请在全局配置模式下使用 **mode** 命令。您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个环境都像一个独立的设备，有自己的安全策略、接口和管理员。多个环境类似于拥有多个独立设备。在单模式下，ASA具有单配置，并且作为单设备运行。在多模式下，您可以创建多个情景，每个情景都有自己的配置。允许的情景数量取决于您的许可证。

mode {**single** | **multiple**} [**noconfirm**]

Syntax Description

multiple	设置多情景模式。
noconfirm	（可选）设置模式而不提示您确认。该选项对于自动化脚本非常有用。
single	将情景模式设置为单情景模式。

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
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在多情景模式下，ASA 包含每个情景的配置，用于标识安全策略、接口以及您可以在独立设备上配置的几乎所有选项（请参阅命 **config-url**令以识别情景配置位置）。系统管理员可在系统配置中配置情景以添加和管理情景；系统配置类似于单模式配置，是启动配置。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

当您使用 **mode** 命令更改情景模式时，系统会提示您重新启动。

情景模式（单情景或多情景）不会存储在配置文件中，即使该模式经过重新启动也是如此。如果需要将配置复制到另一台设备，请使用命令将新设备上的模式设置为匹 **mode**配。

当您从单一模式转换为多模式时，ASA 会将运行配置转换为两个文件：包含系统配置的新启动配置和包含管理上下文的 admin.cfg（位于内部闪存的根目录中）。原始运行配置保存为old_running.cfg

（在内部Flash存储器的根目录中）。系统不会保存原始启动配置。ASA 自动向系统配置中添加一个管理情景的条目，名称为“admin”。

如果从多模式转换为单模式，可能需要先将完整的启动配置（如果可用）复制到 ASA。从多模式继承的系统配置并非单模式设备的完整运行配置。

并非所有功能都支持多上下文模式。有关详细信息，请参阅 CLI 配置指南。

CR_Examples

以下示例将模式设置为多：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

以下示例将模式设置为单一：

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

Related Commands

命令	说明
context	在系统配置中配置情景并进入情景配置模式。
showmode	显示当前情景模式（单模式或多模式）。

monitor-interface

要在特定接口上启用运行状况监控，请在全局配置模式下使用 **monitor-interface**命令。要禁用接口监控，请使用此命 **no**令的形式。

monitor-interface { *if_name* | **service-module** }
nomonitor-interface { *if_name***service-module** }

Syntax Description

if_name	指定被监控的接口的名称。
service-module	监控服务模块。如果您不希望硬件模块故障（例如 ASA FirePOWER 模块）触发故障转移，则可以使用此命令的 **no** 形式禁用模块监控。

Command Default

默认情况下，启用物理接口和服务模块监控；请参阅对逻辑接口的监控默认被禁用。

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
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。
9.3(1)	添加了 service-module 关键字。

使用指南

可以为 ASA 监控的接口数因平台而异，并且可通过查看 **showfailover** 命令输出来确定。

ASA 故障转移对之间在每个接口轮询频率时间段内交换 Hello 消息。故障转移接口轮询时间为 3 至 15 秒。例如，如果轮询时间设置为 5 秒，则如果在接口上未侦听到 5 个连续呼叫（25 秒），则开始在该接口上进行测试。

监测的故障切转移口可以具有以下状态：

- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。

• Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

在主用/主用故障转移中，此命令仅在某个情景中有效。

CR_Examples

以下示例对名为“inside”的接口启用监控：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

Related Commands

命令	说明
clearconfiguremonitor-interface	恢复所有接口的默认接口运行状况监控。
failoverinterface-policy	指定要进行故障转移，必须被监控的接口的数量或百分比。
failoverpolltime	指定接口上 hello 消息之间的间隔（主用/备用故障转移）。
polltimeinterface	指定接口上 hello 消息之间的间隔（主用/主用故障转移）。
showrunning-configmonitor-interface	显示正在 **monitor-interface**运行的配置中的命令。

more

要显示文件的内容，请在 **more** 特权 EXEC 模式下使用该命令。

more {**/ascii** | **/binary** | **/ebcdic** / **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:** } 文件名

Syntax Description

/ascii	（可选）在二进制模式下显示二进制文件和 ASCII 文件。
/binary	（可选）在二进制模式下显示任何文件。
/ebcdic	（可选）以 EBCDIC 显示二进制文件。
disk0:	（可选）显示内部闪存上的文件。
disk1:	（可选）显示外部闪存卡上的文件。
filename	指定要显示的文件的名称。
flash:	（可选）指定内部闪存，后跟冒号。在 ASA 5500 系列自适应安全设备中，该关 **flash** 键字的别名为 。 **disk0**
ftp:	（可选）显示 FTP 服务器上的文件。
http:	（可选）显示网站上的文件。
https:	（可选）显示安全网站上的文件。
system:	（可选）显示文件系统。
tftp:	（可选）显示 FTP 服务器上的文件。

Command Default

ASCII 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
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

morefilesystem: 命令提示您输入本地目录或文件系统的别名。

注释 当您查看使用 **more** 命令保存的配置文件时，配置文件中的隧道组密码以明文显示。

CR_Examples

以下示例显示如何显示名为“test.cfg”的本地文件的内容：

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
```

```
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

命令	说明
cd	更改为指定的目录。
pwd	系统随即会显示当前工作目录。

mount type cifs

要使安全设备可以访问通用互联网文件系统 (CIFS)，请在全局配置模式下使用 **mounttypecifs**命令。此命令允许您进入 mount cifs 配置模式。要卸载 CIFS 网络文件系统，请使用此命令的 **no**形式。

mount*name***type cifs server***server-name***share***share*{**status enable** | **status disable**} [**domain***domain-name*] **username***username***password***password*
[**no**] **mount***name***type cifs server***server-name***share***share*{**status enable** | **status disable**} [**domain***domain-name*] **username***username***password***password*

Syntax Description

域 域名	（可选）此参数仅用于 CIFS 文件系统，指定 Windows NT 域名。最多允许 63 个字符。
name	指定要分配给本地 CA 的现有文件系统的名称。
password密码	标识文件系统安装的授权密码。
server*server-name*	指定 CIFS 文件系统服务器的预定义名称（或 IP 地址，采用点分十进制表示法）。
share共享名称	按名称明确标识特定服务器共享（文件夹），以访问服务器中的文件数据。
status enable或者 **disable**	将文件系统的状态标识为已安装或已取消安装（可用或不可用）。
user*username*	用于安装文件系统的授权用户名。

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
8.0(2)	添加了此命令。

使用指南

mount 命令使用可安装文件系统 (IFS) 来安装 CIFS 文件系统。IFS 是文件系统 API，使安全设备能够识别并加载文件系统的驱动程序。

该 **mount**命令将安全设备上的 CIFS 文件系统附加到 UNIX 文件树。相反， **nomount** 命令会将其分离。

其他 CLI 命令使用 **mount** 命令中指定的 安装名称 来指代安全设备上已安装的文件系统。例如，为本地证书颁发机构设置文件存储的 **database**命令需要现有已安装文件系统的安装名称，以便将数据库文件保存到非闪存。

CIFS远程文件访问协议与应用在本地磁盘和网络文件服务器上共享数据的方式兼容。CIFS在TCP/IP上运行并使用互联网的全局DNS，是Microsoft的开放式跨平台服务器消息块(SMB)协议的增强版，SMB 协议是 Windows 操作系统中的本地文件共享协议。

使用 **mount**命令后，始终从根 shell 退出。在 mount-cifs-config 模式下使用 **exit** 关键字会使用户返回到全局配置模式。

要重新连接，请重新映射到存储的连接。

注释 支持安装 CIFS 和 FTP 文件系统。（请参阅 **mount***name* **typeftp**命令。）此版本不支持安装网络文件系统 (NFS) 卷。

CR_Examples

以下示例将 *cifs://amer;chief:BIG-Boy@myfiler02/my_share* 装载为标签 *cifs_share*：

```
ciscoasa
(config)#
mount cifs_share type CIFS

ciscoasa (config-mount-cifs)#
server myfiler02a
```

Related Commands

命令	说明
调试 cif	记录 CIFS 调试消息。
debug ntdomain	记录 Web VPN NT 域调试消息
debugwebvpncifs	记录 WebVPN CIFS 调试消息。
dir all-filesystems	显示 ASA 上安装的所有文件系统的文件。

mount type ftp

要使安全设备可访问文件传输协议 (FTP) 文件系统，请在全局配置模式下使用 **mounttypeftp**命令进入 mount FTP 配置模式。 **nomounttypeftp**命令用于卸载 FTP 网络文件系统。

[**no**] **mount***name* **typeftp** **server***server-name* **path***pathname* {**statusenable** | **statusdisable**} {**modeactive** | **modepassive**} **username***username* **password***password*

Syntax Description

modeactive或者 **passive**	将 FTP 传输模式标识为主动或被动。
否	删除已安装的 FTP 文件系统，使其不可访问。
password密码	标识文件系统安装的授权密码。
path路径名	指定 FTP 文件系统服务器的目录路径名。路径名不能包含空格。
server*server-name*	指定FTPFS文件系统服务器的预定义名称（或采用点分十进制表示法的IP地址）。
statusenable或者 **disable**	将文件系统的状态标识为已安装或已卸载（可用或不可用）。
username*username*	指定用于文件系统安装的授权用户名。

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
8.0(2)	添加了此命令。

使用指南

mount*name* **typeftp**命令使用可安装文件系统 (IFS) 挂载指定的网络文件系统。IFS 是文件系统 API，使安全设备能够识别并加载文件系统的驱动程序。

要确认实际已安装 FTP 文件系统，请使用 **dirall-filesystems** 指令

当其他 CLI 命令引用已在安全设备上安装的文件系统时，将使用 **mount** 命令中指定的安装名称。例如，为本地证书颁发机构设置文件存储的 **database**命令需要已安装文件系统的安装名称，以便将数据库文件保存到非闪存。

注释 创建 FTP 类型安装时使用 **mount** 命令要求 FTP 服务器必须为 UNIX 目录列表样式。Microsoft FTP 服务器默认采用 MS-DOS 目录列表样式。

注释 支持安装 CIFS 和 FTP 文件系统。（请参阅 **mount***name* **typeftp**命令。）此版本不支持安装网络文件系统 (NFS) 卷。

CR_Examples

此示例将 *ftp://amor;chief:Big-kid@myfiler02* 装载为标签 *my ftp*：

```
ciscoasa
(config)#
mount myftp type ftp server myfiler02a path status enable username chief password big-kid
```

Related Commands

命令	说明
debugwebvpn	记录 WebVPN 调试消息。
ftp mode passive	控制 ASA 上的 FTP 客户端与 FTP 服务器之间的交互。

mroute

要配置静态多播路由，请在**mroute**全局配置模式下使用该命令。要删除静态多播路由，请使用此命**no**令的形式。

mroute*srcsmask*{*in_if_name*[**dense***output_if_name*]|*rpf_addr*}[*distance*]
no*mroute srcsmask*{*in_if_name*[**dense***output_if_name*]|*rpf_addr*}[*distance*]

Syntax Description

dense*output_if_name*	（可选）密集模式输出的接口名称。 **dense***output_if_name*关键字和参数对仅支持SMR存根多播路由（igmp转发）。
distance	（可选）路由的管理距离。距离较短的路由具有优先权。默认值为0。
in_if_name	指定组播路由的传入接口名称。
rpf_addr	指定组播路由的传入接口。如果RPF地址PIM邻居，则会向其发送PIM加入消息、移植消息和删除消息。*rpf-addr*参数可以是直接连接的系统的主机IP地址，也可以是网络/子网号。如果是路由，则会从单播路由表中执行递归查找，以查找直连系统。
smask	指定组播源网络地址掩码。
src	指定组播源的IP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	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令允许您静态配置组播源所在的位置。ASA希望在其用于将单播数据包发送到特定源的同一接口上接收组播数据包。在某些情况下，例如绕过不支持多播路由的路由，多播数据包可能会采用与单播数据包不同的路径。

静态组播路由不能通告或重分布。

使用该**showmroute**命令显示多播路由表的内容。使用该**showrunning-configmroute**命令显示运行配置中的 mroute 命令。

CR_Examples

以下示例显示如何使用 **mroute** 命令配置静态组播路由：

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

Related Commands

命令	说明
clearconfiguremroute	从配置中**mroute**删除命令。
showmroute	显示 IPv4 多播路由表。
showrunning-configmroute	显示配**mroute**置中的命令。

mschapv2-capable

要对 RADIUS 服务器启用 MS-CHAPv2 身份验证请求，请在 aaa-server 主机配置模式下使用 **mschapv2-capable**命令。要禁用 MS-CHAPv2，请使用此命 **no**令的形式。

mschapv2-capable
nomschapv2-capable

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 MS-CHAPv2。

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
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.2(1)	添加了此命令。

使用指南

要启用 MS-CHAPv2 作为 ASA 和 RADIUS 服务器之间用于 VPN 连接的协议，必须在隧道组常规属性中启用密码管理。启用密码管理会生成一个从 ASA 向 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 **password-management** 命令的描述。

如果在隧道组中使用双重身份验证并启用密码管理，则主身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则可以使用该命令配置该服务器发送非 MS-CHAPv2 身份验证请 **nomschapv2-capable** 求。

CR_Examples

以下示例为 RADIUS 服务器 authsrv1.cisco.com 禁用 MS-CHAPv2：

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

Related Commands

命令	说明
aaa-server host	标识 AAA 服务器组的 AAA 服务器。
password-management	当您配置密码管理命令时，ASA 会在远程用户登录时通知用户当前密码即将过期或已过期。然后，ASA 为用户提供机会更改密码。
secondary-authentication-server-group	指定备用AAA服务器组，不能是SDI服务器组。

msie-proxy except-list

要在客户端设备上配置本地旁路的浏览器代理例外列表设置，请在**msie-proxyexcept-list**策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy except-list {**value***server* [*:port*] | **none**}
nomsie-proxyexcept-list

Syntax Description

none	表示没有 IP 地址/主机名或端口，并阻止继承例外列表。
value*server:port*	指定适用于此客户端设备的 MSIE 服务器和端口的 IP 地址或名称。端口号可选。

Command Default

默认情况下，会禁用 msie-proxy except-list。

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
策略组配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南*3.1* 版》 或移动设备的 版本说明 。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略设置 Microsoft Internet Explorer 代理例外列表，该列表由 IP 地址为 192.168.20.1、使用端口 880 的服务器组成：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。

命令	说明
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy local-bypass

要为客户端设备配置浏览器代理本地旁路设置，请在 **msie-proxylocal-bypass**策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxylocal-bypass {**enable** | **disable**}
nomsie-proxylocal-bypass {**enable** | **disable**}

Syntax Description

disable	禁用客户端设备的浏览器代理本地绕行设置。
enable	启用客户端设备的浏览器代理本地绕行设置。

Command Default

默认情况下，会禁用 msie-proxy local-bypass。

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
策略组配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南*3.1* 版》 或移动设备的 版本说明 。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略启用 Microsoft Internet Explorer 代理本地旁路：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy lockdown

要在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的连接 (Connections) 选项卡和“设置”(Settings) 应用中的系统代理选项卡或保持不变，请在 group-policy 配置模式下使用 **msie-proxylockdown** 命令。

msie-proxylockdown [**enable** | **disable**]

Syntax Description

disable	保持 Microsoft Internet Explorer 中的“连接”选项卡和“设置”应用中的“系统代理”选项卡不变。
enable	在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡和“设置”应用中的系统代理选项卡。

Command Default

默认组策略中该命令的默认值是enable。每个组策略都从默认组策略继承其默认值。

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
策略组配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
8.2(3)	添加了此命令。

使用指南

启用此功能将会在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡。此外，从 Windows 10 版本 1703（或更高版本）开始，启用此功能还会在 AnyConnect VPN 会话期间隐藏“设置”应用中的系统代理选项卡。禁用该功能将使 Microsoft Internet Explorer 中的“连接”选项卡和“设置”应用中的系统代理选项卡的显示保持不变。

要使用此功能，您还必须指定私有端代理。

注释 在 AnyConnect VPN 会话期间隐藏“设置”应用中的系统代理选项卡需要 AnyConnect 版本 4.7.03052 或更高版本。

此命令可在 AnyConnect VPN 会话期间临时更改用户注册表。当 AnyConnect 关闭 VPN 会话时，它将注册表返回到会话开始前的状态。

您可以启用此功能以防止用户指定代理服务和更改 LAN 设置。防止用户访问这些设置可增强 AnyConnect 会话期间的终端安全。

有关代理设置的详细信息，请参阅 Cisco 安全客户端 管理员指南，或者参阅您的移动设备的 版本说明 。

CR_Examples

以下示例在 AnyConnect 会话期间隐藏 Connections 选项卡：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

以下示例保持 Connections 选项卡不变：

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

Related Commands

命令	说明
msie-proxyexcept-list	为客户端设备上的浏览器指定一个代理服务器例外列表。
msie-proxylocal-bypass	绕过客户端设备上配置的本地浏览器代理设置。
msie-proxymethod	指定客户端设备的浏览器代理操作。
msie-proxypac-url	指定要从中检索定义代理服务器的代理自动配置文件的URL。
msie-proxyserver	为客户端设备上的浏览器配置代理服务器。
show running-config group-policy	显示运行配置中的组策略设置。

msie-proxy method

要为客户端设备配置浏览器代理操作（“方法”），请在 **msie-proxymethod**策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxymethod [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]
no msie-proxymethod [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**}

注释 有关适用于此语法的限定条件，请参阅使用指南部分。

Syntax Description

auto-detect	允许在客户端设备的浏览器中使用自动代理服务器检测。
no-modify	对于此客户端设备，保持浏览器中的 HTTP 浏览器代理服务器设置不变。
no-proxy	禁用客户端设备浏览器中的 HTTP 代理设置。
use-pac-url	指示浏览器从 **msie-proxypac-url** 命令中指定的代理自动配置文件 URL 检索 HTTP 代理服务器设置。
use-server	设置浏览器中的 HTTP 代理服务器设置以使用命令中配置的 **msie-proxyserver**值。

Command Default

默认方法是 use-server。

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
组策略配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(2)	添加了 use-pac-url 选项。

使用指南

包含代理服务器 IP 地址或主机名和端口号的行最多可包含 100 个字符。

该命令支持以下选项组合：

- **[no]msie-proxymethodno-proxy**

- **[no]msie-proxymethodno-modify**
- **[no]msie-proxymethod[auto-detect][use-server][use-pac-url]**

可以使用文本编辑器为浏览器创建代理自动配置 (.pac) 文件。.pac 文件是一个 JavaScript 文件，其中包含用于根据 URL 的内容来指定要使用的一个或多个代理服务器的逻辑。.pac 文件位于 Web 服务器上。当您指定时 **use-pac-url**，浏览器将使用.pac 文件来确定代理设置。使用 **msie-proxypac-url**命令指定从中检索 .pac 文件的 URL。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南*3.1* 版》 或移动设备的 版本说明 。

CR_Examples

以下示例显示如何将自动检测配置为名为FirstGroup 的组策略的 Microsoft Internet Explorer 代理设置：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

以下示例将名为FirstGroup 的组策略的 Microsoft Internet Explorer 代理设置配置为使用服务器 QAserver、端口 1001 作为客户端 PC 的服务器：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
msie-proxypac-url	指定要从中检索代理自动配置文件的 URL。
msie-proxyserver	配置客户端设备的浏览器代理服务器和端口。
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy pac-url

要指示浏览器查找代理信息的位置，请在 group-policy 配置模式下输入 **msie-proxypac-url** 命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxypac-url {**none** | **value***url*}
nomsie-proxypac-url

Syntax Description

无	指定没有 URL 值。
value*url*	指定浏览器可获取代理自动配置文件的网站，该代理自动配置文件定义要使用的代理服务器。

Command Default

默认值为 none。

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
组策略配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

要求

要使用代理自动配置功能，远程用户必须使用 Cisco AnyConnect VPN 客户端。要启用代理自动配置 URL 的使用，还必须使用 **msie-proxymethod**] 选项配置 **use-pac-url** 命令。

为什么使用此命令

许多网络环境都定义将 Web 浏览器连接到特定网络资源的 HTTP 代理。仅当在浏览器中指定了代理并且客户端将 HTTP 流量路由到代理时，HTTP 流量才可以到达网络资源。SSL VPN 隧道会将 HTTP 代理的定义复杂化，因为在通过隧道传送到企业网络时所需的代理与通过宽带连接来连接到互联网时或位于第三方网络上时所需的代理不同。

此外，具有大型网络的公司可能需要配置多个代理服务器并让用户根据瞬态条件在其之间进行选择。通过使用 .pac 文件，管理员可以编写一个脚本文件来确定众多代理中的哪些代理将用于整个企业内的所有客户端计算机。

以下是如何使用 PAC 文件的一些示例：

- 从列表中随机选择一个代理以实现负载均衡。
- 按时刻或星期几轮换代理以适应服务器维护计划。
- 指定在主代理发生故障的情况下使用的备份代理服务器。
- 根据本地子网为漫游用户指定位置最近的代理。

如何使用代理自动配置功能

可以使用文本编辑器为浏览器创建代理自动配置 (.pac) 文件。.pac 文件是一个 JavaScript 文件，其中包含用于根据 URL 的内容来指定要使用的一个或多个代理服务器的逻辑。使用 **msie-proxypac-url**命令指定从中检索 .pac 文件的 URL。然后，当您 **use-pac-url**在命令中 **msie-proxymethod** 指定时，浏览器会使用.pac 文件来确定代理设置。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南*3.1* 版》 或移动设备的 版本说明 。

CR_Examples

以下示例显示如何配置浏览器以从 URL www.example.com 获取名为FirstGroup 的组策略的代理设置：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

以下示例为名为FirstGroup 的组策略禁用代理自动配置功能：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
msie-proxymethod	配置客户端设备的浏览器代理操作（“方法”）。
msie-proxyserver	配置客户端设备的浏览器代理服务器和端口。
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy server

要为客户端设备配置浏览器代理服务器和端口，请在**msie-proxyserver**策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy server {**value***server* [*:port*] | **none**}
nomsie-proxyserver

Syntax Description

none	表示没有为代理服务器指定 IP 地址/主机名或端口并防止继承服务器。
value服务器：端口	指定适用于此客户端设备的MSIE服务器和端口的IP地址或名称。端口号可选。

Command Default

默认情况下，未指定 msie-proxy 服务器。

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
组策略配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南*3.1* 版》 或移动设备的 版本说明 。

CR_Examples

以下示例显示如何将 IP 地址 192.168.10.1 配置为 Microsoft Internet Explorer 代理服务器，使用端口 880，用于名为FirstGroup 的组策略：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。

命令	说明
clearconfiguregroup-policy	删除所有已配置的组策略属性。

mtu

要指定接口的最大传输单位，请在全局配置模式下使用 **mtu** 命令。要将以太网接口的 MTU 块大小重置为 1500，请使用此命令的 **no** 形式。此命令支持 IPv4 和 IPv6 流量。

mtu*interface_namebytes*
nomtu*interface_namebytes*

Syntax Description

bytes	MTU 中的字节数；有效值为 64 到 9198 字节（对于 Secure Client 和 Firepower 9300 ASA 安全模块为 9000 字节）。
interface_name	内部或外部网络接口名称。

Command Default

以太网接口的默认 字节数为 1500。

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	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.1(6)	最大 MTU 已从 65535 更改为 9198（或 9000，具体取决于型号）。

使用指南

mtu 命令可以设置在连接上发送的负载大小（不包括第 2 层报头或 VLAN 标记）。大于 MTU 值的数据将分片后再发送。以太网接口的默认 MTU 为 1500 字节（这也是没有巨帧预留的最大值）。在这种情况下，带有第 2 层报头（14 字节）和 VLAN 标记（4 字节）的数据包大小是 1518 字节。对于大多数应用而言，此值已足够，但如果网络条件需要，也可选择较小的数字。

ASA 支持 IP 路径 MTU 发现（如 RFC 1191 中所定义），使主机能够动态发现和处理路径沿途各种链路的最大允许 MTU 大小差异。有时，由于数据包大于为接口设置的 MTU，ASA 无法转发数据报，但已设置“不分段”(DF) 位。网络软件向发送主机发送一条消息，提醒其注意该问题。主机必须为目标对数据包进行分片，以适应路径上所有链路中最小数据包的大小。

使用第 2 层隧道协议 (L2TP) 时，我们建议您将 MTU 大小设置为 1380，以考虑 L2TP 报头和 IPsec 报头长度。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密会产生开销，因此 MTU 值不应设置为低于 1380。将接口设置为低于 1380 字节可能会导致数据包丢失。

从版本 9.1(6) 开始，ASA 可以使用的最大 MTU 为 9198 字节。此值不包括第 2 层报头。以前，ASA 允许您将最大 MTU 指定为 65535 字节，这不准确，并可能引发问题。如果您的 MTU 设置为高于 9198 的值，则升级后 MTU 会自动降低。在某些情况下，这种 MTU 变化可能导致 MTU 不匹配；请务必将连接的所有设备设置为使用新的 MTU 值。

CR_Examples

此示例显示如何为接口指定 MTU：

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

Related Commands

命令	说明
clearconfiguremtu	清除所有接口上已配置的最大传输单位值。
showrunning-configmtu	显示当前最大传输单元块大小。

mtu cluster

要设置集群控制链路的最大传输单位，请在全局配置模式下使用**mtucluster**命令。要恢复默认设置，请使用此命 **no**令的形式。

mtucluster*bytes*
nomtucluster [*bytes*]

Syntax Description

字节	指定集群控制链路接口的最大传输单元，介于 64 到 65,535 字节之间。我们不建议将集群控制链路 MTU 设置在 2561 和 8362 之间；由于块池处理，此 MTU 大小对于系统操作来说不是最佳的。默认 MTU 为 1500 字节。

Command Default

默认 MTU 为 1500 字节。

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

我们建议将MTU设置为1600字节或更大，这需要您使用命令启用巨型帧预**jumbo-framereservation**留。

该命令是全局配置命令，但也是引导配置的一部分，不会在单元之间复制。

CR_Examples

以下示例将集群控制链路 MTU 设置为 9000 字节：

```
ciscoasa(config)# mtu cluster 9000
```

Related Commands

命令	说明
cluster-interface	标识集群控制链路接口。
jumbo frame-reservation	允许使用巨型以太网帧。

multicast boundary

要为管理范围的组播地址配置组播边界，请在接口配置模式下使用 **multicastboundary**命令。要删除边界，请使用此命 **no**令的形式。组播边界限制组播数据包流，并允许在不同的管理域中重复使用相同的组播组地址。

multicastboundary*acl* [**filter-autorp**]
nomulticastboundary*acl* [**filter-autorp**]

Syntax Description

acl	指定访问列表名称或编号。访问列表定义受边界影响的地址范围。在此命令中仅使用标准 ACL；不支持扩展 ACL。
filter-autorp	过滤边界 ACL 拒绝的 Auto-RP 消息。如果未指定，则允许所有 Auto-RP 消息通过。

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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

使用此命令可在接口上配置管理权限范围的边界，以过滤 *acl* 参数定义范围内的组播组地址。标准访问列表定义了受影响的地址范围。配置此命令后，不允许任何多播数据包在任何一个方向跨越边界。限制组播数据包流量可以在不同的管理域中重复使用相同的组播组地址。

如果配置**filter-autorp** 关键字，则管理范围边界还会检查 Auto-RP 发现和通知消息，并从边界 ACL 拒绝的 Auto-RP 数据包中删除任何 Auto-RP 组范围通知。仅在 Auto-RP 组范围中的所有地址获边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界。如果有任何地址未获允许，在 Auto-RP 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

CR_Examples

以下示例为所有具有管理作用域的地址设置边界并过滤 Auto-RP 消息：

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
```

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

Related Commands

命令	说明
multicast-routing	在ASA上启用组播路由。

multicast-routing

要在 ASA 上启用 IP 多播路由，请在全局配置模式下使用该 **multicastrouting**命令。要禁用 IP 多播路由，请使用此命 **no**令的形式。

multicast-routing
nomulticast-routing

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下， **multicast-routing** 命令可在所有接口上启用 PIM 和 IGMP。

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	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

multicast-routing 命令可在所有接口上启用 PIM 和 IGMP。

注释 PAT 不支持 PIM。PIM 协议不使用端口，而 PAT 仅适用于使用端口的协议。如果安全设备是 PIM RP，请使用安全设备未转换的外部地址作为 RP 地址。

多播路由表中的条目数量受系统 RAM 数量限制。<xref> 根据安全设备上的 RAM 数量列出特定多播表的最大条目数。一旦达到这些限制，系统将会丢弃所有新条目。

表 *1:* 多播表的条目限制（组合静态和动态条目）

表	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP 组	1000	3000	5000

表	16 MB	128 MB	128+ MB
PIM 路由	3000	7000	12000

CR_Examples

以下示例在 ASA 上启用 IP 组播路由：

```
ciscoasa(config)# multicast-routing
```

Related Commands

命令	说明
igmp	启用接口上的IGMP。
pim	在接口上启用 PIM。

mus

要指定 ASA 标识 WSA 的 IP 范围和接口，请在全局配置模式下使用 **mus** 命令。要关闭该服务，请使用此命令的 **no** 形式。此命令支持 IPv4 和 IPv6 流量。仅注册在指定的子网和接口上找到的 WSA。

mus*IPv4*地址*IPv4*掩码*interface_name*
nomus*IPv4*地址*IPv4*掩码*interface_name*

注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提 供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南 可以使用以下命令：

- ABCD - 获授权访问 ASA 的 WSA IP 地址。
- host - 客户端通过向虚拟主机发送请求，定期检查与网络安全设备的连接。默认情况下，虚拟主机 URL 为 mus.cisco.com。启用 AnyConnect 安全移动性后，网络安全设备会拦截发往虚拟主机的请求并回复客户端。
- password - 配置 WSA 密码。
- server - 配置 WSA 服务器

CR_Examples 以下示例允许 1.2.3.x 子网上的 WSA 服务器访问 内部 接口上的安全移动解决方案：

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

Related Commands

命令	说明
mus password	为 AnyConnect 安全移动通信设置共享密钥。
mus server	指定 ASA 侦听 WSA 通信的端口。
show webvpn mus	显示有关活动 WSA 连接安全设备的信息。

mus host

要在 ASA 上指定 MUS 主机名，请在全局配置模式下输入命 **mushost** 令。这是从 ASA 发送到 Secure Client的遥测 URL。 Secure Client使用此 URL 与专用网络中的 WSA 联系，以获得 MUS 相关服务。要删除使用此命令输入的任何命令，请使用该 **nomushost** 命令。

mushost*hostname*
nomushost

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

您可以为给定端口启用 AnyConnect 安全移动。WSA 端口值为 1 到 21000。如果未在命令中指定端口，则将使用端口 11999。

您必须在执行此命令之前配置 AnyConnect 安全移动共享密钥。

注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提 供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

CR_Examples

以下示例显示如何进入 AnyConnect Secure Mobility 主机和 WebVPN 命令子模式：

```
ciscoasa(config)# webvpn

ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside

ciscoasa(config-webvpn)# mus password abcdefgh123
```

```
ciscoasa(config-webvpn)# mus server enable 960 # non-default port
ciscoasa(config-webvpn)# mus host mus.cisco.com
```

Related Commands

命令	说明
mus	指定 ASA 识别 WSA 的 IP 范围和接口。
muspassword	为 AnyConnect 安全移动通信设置共享密钥。
showwebvpnmus	显示有关活动 WSA 连接安全设备的信息。

mus password

要为 AnyConnect 安全移动通信设置共享安全，请在全局配置模式下输入**muspassword** 命令。要删除共享密钥，请使用 **nomuspassword** 命令。

muspassword
nomuspassword

注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提 供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

Syntax Description

此命令没有任何参数或关键字。

Command Default

。有效的密码由正则表达式 [0-9, az, AZ,:;_/-]{8,20} 定义。共享密钥密码的整体长度最少为 8 个字符，最多为 20 个字符。

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	—	—

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

此 WebVPN 子模式允许您配置 WebVPN 的全局设置。您可以设置 AnyConnect 安全移动通信的共享密钥。

CR_Examples

以下示例显示如何进入 AnyConnect 安全移动密码和 WebVPN 命令子模式：

```
ciscoasa
(config)#
 mus password <password_string>
ciscoasa
(config-webvpn)#
```

Related Commands

命令	说明
mus	指定 ASA 识别 WSA 的 IP 范围和接口。
musserver	指定 ASA 侦听 WSA 通信的端口。
showwebvpnmus	显示有关活动 WSA 连接安全设备的信息。

mus server

要指定 ASA 侦听 WSA 通信的端口，请在全局配置模式下输入 **musserver**命令。要删除使用此命令输入的任何命令，请使用该 **nomusserver** 命令。

musserverenable
nomusserverenable

注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提 供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

您必须指定 AnyConnect 安全移动服务使用的端口。ASA 与 WSA 之间的通信通过管理员指定的端口（范围为 1 至 21000）上的安全 SSL 连接进行。

您必须在执行此命令之前配置 AnyConnect 安全移动共享密钥。

CR_Examples

以下示例显示如何进入 AnyConnect 安全移动密码和 WebVPN 命令子模式：

```
ciscoasa
(config-webvpn)#
mus server enable
?
webvpn mode commands/options
 port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

Related Commands

命令	说明
mus	指定 ASA 识别 WSA 的 IP 范围和接口。
muspassword	为 AnyConnect 安全移动通信设置共享密钥。
showwebvpnmus	显示有关活动 WSA 连接安全设备的信息。

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。