室外

- object-group， 第 2 页
- object-group-search， 第 7 页
- object network， 第 10 页
- object network-service， 第 12 页
- object service， 第 15 页
- ocsp disable-nonce， 第 17 页
- ocsp interface， 第 19 页
- ocsp url， 第 21 页
- on屏幕键盘（已弃用），第 23 页
- ospf authentication， 第 24 页
- ospf authentication-key， 第 26 页
- ospf cost， 第 28 页
- ospf database-filter， 第 30 页
- ospf dead-interval， 第 31 页
- ospf hello-interval， 第 33 页
- ospf message-digest-key， 第 34 页
- ospf mtu-ignore， 第 36 页
- ospf network point-to-point non-broadcast， 第 37 页
- ospf priority， 第 39 页
- ospf retransmit-interval， 第 40 页
- ospf transmit-delay， 第 41 页
- otp expiration， 第 42 页
- output console， 第 44 页
- output file， 第 45 页
- output none， 第 47 页
- outstanding（已弃用），第 48 页
- override-account-disable (已弃用)，第 50 页
- override-svc-download， 第 52 页

object-group

要定义可用于优化配置的对象组，请在全局配置模式下使用 **object-group** 命令。使用此命 **no**令的形式从配置中删除对象组。

object-group {**protocol | network | icmp-type | security | user | network-service**} *grp_name*
object-group service*grp_name* ［**tcp | udp | tcp-udp**］

Syntax Description

grp_name	标识对象组（1 到 64 个字符），可以是字母、数字以及“_”、“-”、“。”的任意组合。个字符。
icmp-type	（不推荐，请使用 **service**。）定义一组 ICMP 类型，例如 echo 和 echo-reply。输入 **object-groupicmp-type**命令后，使用 **icmp-object** 和 **group-object** 命令添加 ICMP 对象。
network	定义一组主机或子网 IP 地址。输入 **object-groupnetwork**命令后，使用 **network-object** 和 **group-object**命令添加网络对象。您可以创建一个混合有 IPv4 和 IPv6 地址的组。 注释 不能使用混合对象组进行 NAT。
network-service	使用可选服务规范定义一组子网或域名。输入此命令后，使用 **network-service-member** 命令添加网络服务对象，或使用 **domain** 和 **subnet** 命令直接添加成员。
protocol	（不推荐，请使用 **service**。）定义一组协议，例如 TCP 和 UDP。输入 **object-groupprotocol**命令后，使用 **protocol-object** 和 **group-object**命令添加协议对象。
security	定义与思科 TrustSec 配合使用的安全组对象。输入 **object-groupprotocol**命令后，使用 **security-group** 和 **group-object**命令添加安全组对象。
service	根据协议、ICMP 类型和 TCP/UDP/SCTP 端口定义服务。
[tcp|udp|tcp-udp	要定义混合服务组或 SCTP 端口，请不要为对象组指定协议类型。输入命令 **object-groupservice** 后，使用 **service-object**和 命令将服务对象添加到服务组中。**group-object** 这是首选方法，即使对象旨在仅包含 TCP 或 UDP（或两者）端口列表。 不建议在 object-group service 命令中直接使用 **tcp**、 **udp**和 **tcp-udp** 关键字。相反，请将这些关键字放在命令之外，并在 **service-object** 命令上配置 TCP 和 UDP 端口。如果您包含其中一个关键字，请使用 **port-object** 和 **group-object**命令添加端口组。
user	定义可用于控制身份防火墙访问的用户和用户组。输入 **object-groupprotocol**命令后，使用 **user**、 **user-group**和 **group-object**命令添加用户和用户组对象。

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。
8.4(2)	添加了对 **user** 关键字的支持以支持身份防火墙。
9.0(1)	您现在可以创建支持 IPv4 和 IPv6 地址混合的网络对象组。 添加了对 **security** 关键字的支持以支持思科 TrustSec。
9.14	该关 **icmp-type**键字已被弃用。请使用 **service** 关键字，并在对象中指定 **serviceicmp** 。
9.17(1)	添加了 **network-service** 关键字。

使用指南

可以对主机或服务等对象进行分组，然后可以在 ACL (**access-list**) 和 NAT (**nat**) 等功能中使用对象组。此示例显示如何在 ACL 中使用网络对象组：

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group NWgroup1
```

您可以按层次结构对命令进行分组；；对象组可以是其他对象组的成员。

CR_Examples

以下示例显示如何使用 **object-groupnetwork** 命令创建网络对象组：

```
ciscoasa(config)# object-group network sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.eng.ftp.servcers
ciscoasa(config-network-object-group)# network-object host 172.23.56.194
ciscoasa(config-network-object-group)# network-object 192.1.1.0 255.255.255.224
ciscoasa(config-network-object-group)# exit
```

以下示例显示如何使用 **object-groupnetwork** 命令创建包含现有对象组的网络对象组：

```
ciscoasa(config)# object-group network sjc_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.ftp.servers

ciscoasa(config-network-object-group)# network-object host 172.23.56.195
ciscoasa(config-network-object-group)# network-object 193.1.1.0 255.255.255.224

ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# exit
```

以下示例显示如何使用**group-object**模式创建一个包含先前定义的对象的新对象组，以及如何在一个 ACL 中使用这些对象：

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network-object-group)# network-object host 192.168.1.1
ciscoasa(config-network-object-group)# network-object host 192.168.1.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network-object-group)# network-object host 172.23.56.1
ciscoasa(config-network-object-group)# network-object host 172.23.56.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network-object-group)# group-object host_grp_1
ciscoasa(config-network-object-group)# group-object host_grp_2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)#access-list all permit tcp object-group all_hosts any eq www
```

如果没有 **group-object** 命令，则需要定义 *all_hosts* 组，以包含 *host_grp_1* 和 *host_grp_2*中已定义的所有 IP 地址。使用 **group-object** 命令，可以消除主机的重复定义。

以下示例显示如何将 TCP 和 UDP 服务添加到服务对象组：

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

以下示例显示如何将多个服务对象添加到服务对象组：

```
ciscoasa(config)# object-group service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object-group service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object-group service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# group-object SSH
ciscoasa(config-service-object-group)# group-object EIGRP
ciscoasa(config-service-object-group)# group-object HTTPS
```

以下示例显示如何在服务对象组中添加协议、端口和 ICMP 混合规格：

```
ciscoasa(config)# object-group service mixed
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
```

以下示例显示如何使用 **service-object** 子命令，该命令对于对 TCP 和 UDP 服务进行分组非常有用：

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host kqk.suu.dri.ixx
ciscoasa(config-network-object-group)# network-object host kqk.suu.pyl.gnl
```

```
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service usr_svc
ciscoasa(config-service-object-group)# service-object tcp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object tcp destination eq pop3
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config)# access-list acl extended permit object-group usr_svc object-group locals
 object-group remote
```

以下示例显示如何使用 **object-groupuser**命令创建用户组对象：

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

（不建议使用，请改用服务对象。）以下示例显示如何使用 **object-groupicmp-type**模式创建 ICMP 对象组：

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

（不建议使用，请改用服务对象。）以下示例显示如何使用 **object-groupprotocol** 模式创建协议对象组：

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol-object-group)# protocol-object udp
ciscoasa(config-protocol-object-group)# protocol-object ipsec
ciscoasa(config-protocol-object-group)# exit
ciscoasa(config)# object-group protocol proto_grp_2
ciscoasa(config-protocol-object-group)# protocol-object tcp
ciscoasa(config-protocol-object-group)# group-object proto_grp_1
ciscoasa(config-protocol-object-group)# exit
```

（不建议使用，无需使用 **tcp** 关键字，而是使用 **service-object** 命令定义端口。）以下示例显示如何使用 **object-groupservice** 模式创建 TCP 端口对象组：

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service-object-group)# group-object eng_www_service
ciscoasa(config-service-object-group)# port-object eq ftp
ciscoasa(config-service-object-group)# port-object range 2000 2005
ciscoasa(config-service-object-group)# exit
```

以下示例显示如何使用对象组简化访问列表配置。此分组支持在1行中配置访问列表，而不是在不使用分组的情况下需要 24 行。

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host 10.1.1.15
ciscoasa(config-network-object-group)# network-object host 10.1.1.16
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service eng_svc tcp
ciscoasa(config-service-object-group)# port-object eq www
ciscoasa(config-service-object-group)# port-object eq smtp
ciscoasa(config-service-object-group)# port-object range 25000 25100
ciscoasa(config)# access-list acl extended permit tcp object-group remote object-group
locals object-group eng_svc
```

注释 **showrunning-configaccess-list** 命令显示配置的对象组名称的访问列表。 **showaccess-list**命令显示此信息以及使用组扩展为单个条目（不含其对象分组）的访问列表条目。

以下示例使用先前定义的网络服务对象配置一组 SaaS 应用程序。

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

Related Commands

命令	说明
clearconfigureobject-group	从配置中删除所有对象组命令。
group-object	添加网络对象组。
network-object	向网络对象组添加网络对象。
port-object	将端口对象添加到服务对象组。
security-group	将安全组添加到安全组对象组。
showrunning-configobject-group	显示当前对象组。
user	将用户名添加到用户组对象。
user-group	向用户组对象添加用户组名。

object-group-search

要启用 ACL 优化，请在 **object-group-search** 全局配置模式下使用该命令。使用此命 **no**令的形式可以禁用ACL优化。

object-group-search{**access-control | threshold**}
no object-group-search{**access-control | threshold**}

Syntax Description

access-control	启用对象组搜索访问控制规则。
threshold	为对象组搜索处理启用最大阈值。有关详细信息，请参阅使用说明。

Command Default

（9.18 之前）默 认情况下禁用对象组搜索。默认情况下，阈值也是禁用的。

从 9.18 开始，默认启用对象组搜索以控制新部署的访问。

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
8.3(1)	添加了此命令。
9.12(1)	添加了 **threshold** 关键字。9.8、9.9 和 9.10 的临时版本中还添加了 关键字。
9.18(1)	对于新部署，访问控制的默认设置已更改为启用。如果以前未启用此功能，则必须在升级时启用它。

使用指南

object-group-search命令优化入站方向的所有 ACL。

通过启用对象组搜索可降低搜索访问规则所需的内存，但此规则会影响查询性能及增加 CPU 使用量。启用后，对象组搜索不会扩展ASP表中使用网络或服务对象的ACL，而是根据这些组定义搜索访问规则以查找匹配项。您将在 **showaccess-list** 输出中看到这一点。

对象组搜索受限于一个阈值。对于每个连接，将根据网络对象匹配源和目标IP地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。此检查是为了防止性能降低。配置规则以防止过多的匹配项。避免创建重复的对象，以防止达到阈值。

从版本 9.12(1) 开始，在回到 9.8(x) 的临时版本中，默认情况下此阈值处于禁用状态。使用 **showrunning-configallobject-group-search** 命令来确定是否配置了阈值选项；如果已配置，则确定当前设置。

启用对象组搜索时，如果为访问组启用了大量功能、大量活动连接和大型 ACL，则在操作期间会断开连接，并且在建立新连接时性能会下降。即使您启用事务性提交 (**asprule-enginetransactional-commitaccess-group**)，也可能发生这些丢弃。

注释 对象组搜索仅适用于网络和服务对象。它不适用于安全组或用户对象。如果ACL包括安全组，请勿启用此功能。结果可能是非活动的 ACL 或其他意外行为。

CR_Examples

以下示例显示如何使用该 **object-group-search**命令启用 ACL 优化：

```
ciscoasa(config)# object-group-search access-control
```

以下是未启用时 **object-group-search**的**showaccess-list**命令示例输出：

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group BLK-LAN
 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=2) 0xce8596ec
    access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

以下是启用时 **object-group-search**命令的**showaccess-list** 示例输出：

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

Related Commands

命令	说明
clearconfigobject-groupsearch	清除 object-group-search 配置。
showobject-group	如果对象组是网络对象组类型，则显示命中计数。
showrunning-configobject-group	显示当前对象组。
showrunning-configobject-group-search	显示运行配置中的 object-group-search 配置。

object network

要配置命名网络对象，请在全局配置模式下使用 **objectnetwork**命令。使用此命 **no**令的形式从配置中删除对象。

name *object* `network` **renamenew_obj_name** *[]*
no object network*name*

Syntax Description

name	指定网络对象的名称。名称长度可以是 1 到 64 个字符，由字母、数字和以下特殊字符组成：下划线、连字符、逗号、正斜杠和句点。对象和对象组共享相同的命名空间。
rename*new_obj_name*	（可选）将对象重命名为新的对象名称。

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
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.3(1)	添加了此命令。
8.4(2)	添加了对完全限定域名 (FQDN) 的支持。请参阅 **fqdn** 命令。

使用指南

网络对象可以包含主机、网络、范围 IP 地址（IPv4 或 IPv6）或 FQDN。输入命令后，请使用 **host**、**fqdn**、 **subnet**或 **range** 命令向对象添加一个地址。

您还可以使用 **nat** 命令在此网络对象上启用 NAT 规则。您只能为给定对象定义一条 NAT 规则；如果要配置多条 NAT 规则，则需要创建多个指定相同 IP 地址的对象 **objectnetworkobj-10.10.10.1-01**，**objectnetworkobj-10.10.10.1-02**例如，等等。

如果使用不同的 IP 地址配置现有网络对象，则新配置将替换现有配置。

CR_Examples

以下示例显示如何创建网络对象：

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

Related Commands

命令	说明
clearconfigureobject	清除创建的所有对象。
description	向网络对象添加说明。
fqdn	指定完全限定域名网络对象。
host	指定主机网络对象。
nat	为网络对象启用 NAT。
object-group network	创建网络对象组。
range	指定网络对象的地址范围。
showrunning-configobjectnetwork	显示网络对象配置。
subnet	指定子网网络对象。

object network-service

要配置命名的网络服务对象，请在全局配置模式下使用 **object network-service** 命令。使用此命 **no**令的形式从配置中删除对象。

object network-service *name* [**dynamic**]
no object network-service *name*

Syntax Description

dynamic	（可选。） **dynamic** 关键字意味着对象不会保存到运行配置，它将仅显示在 **show object** 输出中。 **dynamic** 关键字主要供外部设备管理器使用。
name	名称最多可包含 128 个字符，并且可以包含空格。如果包含空格，则必须用双引号将名称引起来。

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
9.17(2)	添加了此命令。

使用指南

网络服务对象定义了一个应用。它通过子网规范或更常见的DNS域名来定义应用的位置。您也可以选择包括协议和端口，以缩小应用的范围。

只能在网络服务组对象中使用这些对象；不能在访问控制列表条目(ACE)中直接使用网络服务对象。

使用以下命令之一向对象添加一个或多个应用程序位置和可选服务。使用命令的 **no** 形式来删除对象。您可以多次输入这些命令。

- **domain** *domain_name* [*service*] - DNS 名称，最多 253 个字符。名称可以是完全限定的（例如 www.example.com）或部分名称（例如 example.com），在后一种情况下，对象会匹配所有子域，即使用部分名称的服务器（如 www.example.com、www1.example.com、long.server.name.example.com 等）。如果存在完全匹配的名称，则将根据最长名称对连接进行匹配。域名可以解析到多个 IP 地址。

- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。

这些命令的服务规范相同。只有当您想限制匹配的连接范围时，才指定服务。默认情况下，与已解析 IP 地址的任何连接都与对象相匹配。

protocol [*operator port*]

其中：

- *protocol* 是连接中使用的协议，例如 tcp、udp、ip 等。使用 ? 查看协议列表。
- （仅限 TCP/UDP。）*operator* 为以下选项之一：
  - **eq** 等于指定的端口号。
  - **lt** 表示小于指定端口号的任何端口。
  - **gt** 表示大于指定端口号的任何端口。
  - **range** 表示两个指定端口之间的任何端口。
- （仅限 TCP/UDP。）*port* 是端口号 1-65535 或助记符，例如 www。使用 ? 查看助记符。对于范围，必须指定两个端口，并且第一个端口号要小于第二个端口号。

示例

以下是网络服务对象的示例。

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

Related Commands

命令	说明
app-id	指定对象的应用 ID。
clear object	清除网络服务对象的命中计数。
description	为对象添加描述。
domain	指定对象的域名。
object-group network-service	创建网络服务对象组。
show object	显示网络服务对象。

命令	说明
subnet	指定对象的子网。

object service

要将某个服务对象配置为自动反映在使用该对象的所有配置中，请在全局配置模式下使用**objectservice**命令。使用此命 **no**令的形式来删除对象。

object service*name*[**rename***new_obj_name*]
no object service对象名称[**rename***new_obj_name*]

Syntax Description

name	指定服务对象的名称。名称长度可以是 1 到 64 个字符，由字母、数字和以下特殊字符组成：下划线、连字符、逗号和句点。对象名称必须以字母开头。
rename*new_obj_name*	（可选）将对象重命名为新的对象名称。

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
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

服务对象可以包含协议、ICMP、ICMPv6 或 TCP /UDP/SCTP 端口或端口范围。输入命令后，使用 **service** 命令向对象添加一个服务规格。

如果使用不同的协议和端口（或多个端口）配置现有的服务对象，则新配置将用新的协议和端口（或多个端口）替换现有的协议和端口（或多个端口）。

CR_Examples

以下示例显示如何创建服务对象：

```
ciscoasa(config)# object service SERVOBJECT1
ciscoasa(config-service-object)# service tcp source eq www destination eq ssh
```

Related Commands

命令	说明
clearconfigureobject	清除创建的所有对象。

命令	说明
service	配置服务对象的协议和端口。

ocsp disable-nonce

要禁用 nonce 扩展，请在 crypto ca trustpoint 配置模式下使用 ocsp disable-nonce 命令。要重新启用随机数扩展，请使用此命令的 **no** 形式。

ocsp disable-nonce
no ocsp disable-nonce

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，OCSP 请求包括一个随机数扩展。

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。

使用指南

使用此命令时，OCSP 请求不包括 OCSP 随机数扩展，ASA 也不会检查。默认情况下，OCSP 请求包含一个 nonce 扩展，它以加密方式绑定请求和响应以避免重放攻击。但是，某些 OCSP 服务器使用不包含此匹配随机数扩展的预生成响应。要将 OCSP 用于这些服务器，必须禁用 nonce 扩展。

CR_Examples

以下示例显示如何禁用名为 newtrust 的信任点的随机数扩展。

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# ocsp disable-nonce
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
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。
match certificate	配置 OCSP 覆盖规则。
ocspinterface*nameif*	指定可用于 OCSP 吊销检查的接口。

命令	说明
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。

ocsp interface

要配置使 ASA 访问 OCSP 的源接口，请在 crypto ca trustpool 配置模式下使用 **interface** *nameif* 命令。要从配置中删除接口，请使用此 命 令的no形式。

ocsp interface *nameif*
no ocsp interface *nameif*

Syntax Description

interface *nameif*	指定 ASA 用于访问 OCSP 服务器的接口。

Command Default

此命令没有默认值。

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
Crypto ca trustpoint 配置。	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
9.5(1)	添加了此命令。

使用指南

默认情况下，OCSP 使用不包括管理接口条目的全局路由表。如果 OCSP 位于管理接口之后，则 OCSP 吊销检查不会成功。当您使用此命令时，可以将 OCSP 吊销检查配置为使用接口，包括管理接口（视需要而定）。

CR_Examples

以下示例显示如何配置 OCSP 的源接口。

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
```

```
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt  url
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url  ?

crypto-ca-trustpoint mode commands/options:
  LINE < 500 char  URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url http://lal-bagh:8888
```

Related Commands

命令	说明
ocsp url	指定要用于检查与信任点关联的所有证书的OCSP服务器。
ocsp disable-nonce	禁用 OCSP 请求的 nonce 扩展。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

ocsp url

要为 ASA 配置 OCSP 服务器以用于检查与信任点（而不是客户端证书的 AIA 扩展中指定的服务器）关联的所有证书，请在 **ocspurl**crypto ca trustpoint 配置模式下使用该命令。要从配置中删除服务器，请使用此命 **no** 令的形式。

ocsp url*URL*
no ocsp url

Syntax Description

URL 指定 OCSP 服务器的 HTTP URL。

注释
同时支持 IPv4 和 IPv6 OCSP URL。将 IPv6 地址括在方括号中，例如：*http://[0:0:0:0:0.18:0a01:7c16]*。

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。
9.20(1)	添加了对 IPv6 OCSP URL 的支持。

使用指南

ASA 仅支持 HTTP URL，而您只能为每个信任点指定一个 URL。

ASA 提供三种定义 OCSP 服务器 URL 的方法，并且 ASA 会按照您的定义方式尝试使用 OCSP 服务器，顺序如下：

- 您使用 **matchcertificate** 命令设置的 OCSP 服务器。
- 使用 **ocspurl** 命令设置的 OCSP 服务器。
- 客户端证书的 AIA 字段中的 OCSP 服务器。

如果您不通过 **matchcertificate** 命令或 **ocspurl** 命令配置 OCSP URL，ASA 将使用客户端证书的 AIA 扩展中的 OCSP 服务器。如果证书没有 AIA 扩展，则吊销状态检查失败。

CR_Examples

以下示例显示如何使用 URL http://10.1.124.22 配置 OCSP 服务器。

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://10.1.124.22
ciscoasa(config-ca-trustpoint)#
```

以下示例显示如何使用 IPv6 URL 配置 OCSP：

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# ocsp url  http://[0:0:0:0:0:ffff:0a01:7c16]
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
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。
match certificate	配置 OCSP 覆盖规则。
ocspdisable-nonce	禁用 OCSP 请求的 nonce 扩展。
ocspinterface*nameif*	指定可用于 OCSP 吊销检查的接口。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

on屏幕键盘（已弃用）

要将屏幕键盘插入登录窗格或具有登录名/密码要求的所有窗格，请在 webvpn 模式下使用 **onscreen-keyboard** 命令。要删除以前配置的屏幕键盘，请使用此命令的 **no** 版本。

onscreen-keyboard {**logon** | **all**}
no onscreen-keyboard [**logon** | **all**]

Syntax Description

logon	为登录窗格插入屏幕键盘。
all	为登录窗格以及有登录名/密码要求的所有其他窗格插入屏幕键盘。

Command Default

没有屏幕键盘。

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配置模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.17(1)	由于取消了对 Web VPN 的支持，此命令已被弃用。

使用指南

通过屏幕键盘，您可以输入用户凭证而无需按键。

CR_Examples

以下示例显示如何为登录页面启用屏幕键盘：

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 onscreen-keyboard logon
ciscoasa(config-webvpn)#
```

Related Commands

命令	说明
webvpn	进入 webvpn 模式，该模式让您配置无客户端 SSLVPN 连接的属性。

ospf authentication

要启用 OSPF 验证，请在接口配置模式下使用 **ospfauthentication** 命令。要恢复默认的身份验证立场，请使用此命令的 **no**形式。

ospfauthentication {**key-chain key-chain-name** | **message-digest** | **null**}
no ospf authentication

Syntax Description

key-chain *key-chain-name*	（可选）指定用于身份验证的密钥链。key-name 参数最多可以为 63 个字母数字字符。
message-digest	（可选）指定使用 OSPF 消息摘要身份验证。
null	（可选）指定不使用 OSPF 身份验证。

Command Default

默认情况下，未启用 OSPF 身份验证。

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	• 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。
9.12(1)	添加了密钥链功能，以支持OSPF身份验证的轮换密钥。

使用指南

在使用 **ospfauthentication** 命令之前，使用 **ospfauthentication-key** 命令为接口配置密码。如果您使用 **message-digest** 关键字，请为带有 **ospfmessage-digest-key** 命令的接口配置 message-digest key。

为了获得后向兼容性，仍然支持区域的身份验证类型。如果没有为接口指定身份验证类型，则将使用区域的身份验证类型（区域默认为空身份验证）。

使用不带任何选项的此命令时，将启用简单密码身份验证。

CR_Examples

以下示例显示如何在所选接口上为 OSPF 启用简单密码身份验证：

```
ciscoasa(config-if)# ospf authentication
ciscoasa(config-if)#
```

以下示例显示如何在所选接口上为 OSPF 启用密钥链密码身份验证：

```
ciscoasa(config)# interface gigabitEthernet 0/0
ciscoasa(config-if)# ospf authentication key-chain CHAIN-INT-OSPFKEYS
```

Related Commands

命令	说明
ospf **authentication-key**	指定相邻路由设备使用的密码。
ospfmessage-digest-key	启用 MD5 身份验证并指定 MD5 密钥。

ospf authentication-key

要指定相邻路由设备使用的密码，请在接口配置模式下使用 **ospfauthentication-key** 命令。要删除密码，请使用此命 **no**令的形式。

ospfauthentication-key [**0** | **8** } *password*
no ospf authentication-key

Syntax Description

0	指定将遵循未加密的密码
8	指定将遵循的加密密码。
password	分配 OSPF 身份验证密码，供相邻路由设备使用。密码必须少于 9 个字符。可以在两个字符之间包含空格。密码开头或结尾的空格将被忽略。

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	• 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。

使用指南

该命令创建的密码将用作密钥，在发起路由协议数据包时直接插入到 OSPF 报头中。可以为每个接口的每个网络指定单独的密码。同一网络上的所有相邻路由器都必须具有同一密码才能交换 OSPF 信息。

CR_Examples

以下示例显示如何指定 OSPF 身份验证的密码：

```
ciscoasa(config-if)# ospf authentication-key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

Related Commands

命令	说明
areaauthentication	为指定区域启用OSPF 身份验证。

命令	说明
ospfauthentication	启用 OSPF 身份验证。

ospf cost

要指定通过接口发送数据包的开销，请在接口配置模式下使用 **ospfcost** 命令。要将接口成本重置为默认值，请使用此命令的 **no**形式。

ospf cost*interface_cost*
no ospf cost

Syntax Description

interface_cost	通过接口发送数据包的开销（一种链路状态度量）。这是一个无符号整数，范围介于 0 至 65535 之间。0 表示直接连接到接口的网络，并且接口带宽越高，通过该接口发送数据包的关联开销就越低。换句话说，较大的开销值表示低带宽接口，而较低开销值表示高带宽接口。 ASA 上的 OSPF 接口默认成本为 10。此默认值与 Cisco IOS 软件不同，后者的默认开销为 1（适用于快速以太网和千兆以太网）和 10（适用于 10BaseT）。如果您在网络中使用 ECMP，则必须此情况考虑在内。

Command Default

默认接 口成本为 10。

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	• 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。

使用指南

该 **ospfcost** 命令允许您明确指定在接口上发送数据包的成本。 *interface_cost* 参数是一个从 0 到 65535 的无符号整数值。

noospfcost命令允许您将路径开销重置为默认值。

CR_Examples

以下示例展示如何指定在所选接口上发送数据包的开销：

```
ciscoasa(config-if)# ospf cost 4
```

Related Commands

命令	说明
showrunning-configinterface	显示指定接口的配置。

ospf database-filter

要在同步和泛洪期间过滤掉到OSPF接口的所有传出LSA，请在**ospfdatabase-filter**接口配置模式下使用该命令。要恢复LSA，请使用此命**no**令的形式。

ospf database-filterallout
no ospf database-filterallout

Syntax Description

allout	过滤所有传出到OSPF接口的LSA。

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
7.0(1)	添加了此命令。

使用指南

该 **ospfdatabase-filter**命令过滤发往 OSPF 接口的 LSA。 **noospfdatabase-filterallout** 命令恢复将 LSA 转发到接口。

CR_Examples

以下示例显示如何使用 **ospfdatabase-filter** 命令过滤传出 LSA：

```
ciscoasa(config-if)# ospf database-filter all out
```

Related Commands

命令	说明
showinterface	显示接口状态信息。

ospf dead-interval

要指定邻居声明路由器关闭之前的间隔，请在接口配置模式下使用 **ospfdead-interval**命令。要恢复默认值，请使用此命 **no**令的形式。

ospf dead-interval{秒**minimal** | **hello-multiplier**乘数}
no ospf dead-interval

Syntax Description

seconds	未发现呼叫数据包的时间长度。 *seconds* 的默认值是 **ospfhello-interval** 命令设置的间隔的四倍（其范围为 1 至 65535）。
最低	将 dead 间隔设置为 1 秒。使用此关键字要求还配置了 hello-multiplier 关键字和 multiplier 参数。
hello-multiplier 乘数	范围为 3 至 20 的整数值，表示 1 秒内发送的呼叫数据包的数量。

Command Default

秒 的默认值是命令设置的间隔的 **ospfhello-interval**四倍。

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	• 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。
9.2(1)	添加了对 Fast Hello 数据包的支持。

使用指南

通过 ospf dead-interval 命令，您可以设置 dead 间隔之前邻居的声明路由器关闭（看不到呼叫数据包的时间长度）。 *seconds* 参数用于指定 dead 间隔，它对于网络上的所有节点都必须相同。 *seconds* 的默认值是 **ospfhello-interval** 命令设置的间隔的四倍，范围为 1 到 65535。

no ospf dead-interval 命令可恢复默认间隔值。

Dead 间隔在 OSPF 呼叫数据包中通告。此值对于特定网络上的所有网络设备都必须相同。

指定较小的死亡间隔（秒）将更快地检测到邻居关闭并改善收敛，但可能会导致更多的路由不稳定性。

快速呼叫数据包 OSPF 支持

通过指定带有 multiplier 参数的 maximum 和 hello-multiplier 关键字，可以启用 OSPF 快速呼叫数据包。minimal 关键字将死间隔设置为 1 秒，hello-multiplier 值设置在该 1 秒内发送的 hello 数据包的数量，从而提供亚秒级或“快速”hello 数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为1秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

使用 show ospf interface 命令验证 dead 间隔和 fast hello 间隔。

CR_Examples

在以下示例中，通过指定 minimal 关键字以及 hello-multiplier 关键字和值来启用 OSPF 对快速 Hello 数据包的支持。由于乘数设置为 5，因此每秒将发送五个呼叫数据包。

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

Related Commands

命令	说明
ospfhello-interval	指定接口发送hello数据包的间隔。
showospfinterface	显示OSPF相关的接口信息。

ospf hello-interval

要指定接口上发送的 hello 数据包之间的间隔，请在 **ospfhello-interval**接口配置模式下使用该命令。要将呼叫间隔恢复为默认值，请使用此命令的 **no** 形式。

ospfhello-interval秒
no ospf hello-interval

Syntax Description

seconds	指定在接口上发送呼叫数据包的间隔；其有效值范围为 1 至 65535 秒。

Command Default

秒的默认 值为 **hello-interval**10 秒。

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	• 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。

使用指南

该值在hello数据包中公布。问候间隔越小，检测到的拓扑变化就越快，但随之而来的路由流量也越多。对于特定网络上的所有路由器和接入服务器，此值必须相同。

CR_Examples

以下示例将 OSPF 呼叫间隔设置为 5 秒：

```
ciscoasa(config-if)# ospf hello-interval 5
```

Related Commands

命令	说明
ospfdead-interval	指定邻居声明路由器关闭之前的间隔。
showospfinterface	显示OSPF相关的接口信息。

ospf message-digest-key

要启用 OSPF MD5 验证，请在接口配置模式下使用 **ospfmessage-digest-key** 命令。要删除 MD5 密钥，请使用此命 **no**令的形式。

ospfmessage-digest-key*key-id***md5**[**0**|**8**] *key*
no ospf message-digest-key

Syntax Description

key-id	启用 MD5 身份验证并指定数字身份验证密钥 ID 号码；有效值为 1 到 255。
md5密钥	最多 16 个字节的字母数字密码。您可以在关键字符之间添加空格。密钥开头或结尾的空格将被忽略。MD5 身份验证负责验证通信的完整性、认证信源并检查时效性。
0	指定将遵循未加密的密码
8	指定将遵循的加密密码。

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	• 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。

使用指南

ospf message-digest-key 命令允许您启用 MD5 身份验证。通过该命令的 **no** 形式，可删除旧的 MD5 密钥。 *key_id* 是身份验证密钥的数字标识符，范围介于 1 到 255 之间。 *key* 是最多 16 字节的字母数字密码。MD5 负责验证通信的完整性、认证信源并检查时效性。

CR_Examples

以下示例显示如何指定用于 OSPF 身份验证的 MD5 密钥：

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

Related Commands

命令	说明
areaauthentication	启用OSPF区域验证。
ospfauthentication	启用OSPF身份验证。

ospf mtu-ignore

要禁用接收数据库数据包时的 OSPF 最大传输单元 (MTU) 不匹配检测，请在 **ospfmtu-ignore**接口配置模式下使用该命令。要恢复 MTU 不匹配检测，请使用此命令的 **no** 形式。

ospfmtu-ignore
no ospf mtu-ignore

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，处于启 **ospfmtu-ignore**用状态。

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
7.0(1)	添加了此命令。

使用指南

OSPF 检查邻居在公用接口上是否使用同一 MTU。当邻居交换数据库描述符 (DBD) 数据包时，将执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU，则不会建立 OSPF 邻接。该命令禁用接收 DBD 数据包时的 **ospfmtu-ignore**OSPF MTU 不匹配检测。该类别在默认情况下已启用。

CR_Examples

以下示例显示如何禁用该 **ospfmtu-ignore**命令：

```
ciscoasa(config-if)# ospf mtu-ignore
```

Related Commands

命令	说明
showinterface	显示接口状态信息。

ospf network point-to-point non-broadcast

要将 OSPF 接口配置为点对点非广播网络，请在接口配置模式下使用 **ospfnetworkpoint-to-pointnon-broadcast** 命令。要从配置中删除此命令，请使用此命 **no**令的形式。

ospf network point-to-point non-broadcast
no ospf network point-to-point non-broadcast

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
接口配置	• 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。

使用指南

该 **ospfnetworkpoint-to-pointnon-broadcast**命令允许您通过 VPN 隧道传输 OSPF 路由。

将接口指定为点对点接口时，必须手动配置 OSPF 邻居；无法进行动态发现。要手动配置 OSPF 邻居，请在路由器配置模式下使用 **neighbor** 命令。

当接口配置为点对点时，适用以下限制：

- > 您只能为接口定义一个邻居。
- 您无需定义指向加密终端的静态路由。
- 除非显式配置邻居，否则接口无法形成邻接关系。
- 如果接口上运行着基于隧道的 OSPF，则不能在同一接口上运行具有上游路由器的常规 OSPF。
- 您应该在指定 OSPF 邻居之前将加密映射绑定到接口，以确保 OSPF 更新通过 VPN 隧道传递。如果在指定 OSPF 邻居后将加密映射绑定到接口，请使用该**clearlocal-hostall**命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接关系。

CR_Examples

以下示例显示如何将所选接口配置为点对点非广播接口：

```
ciscoasa(config-if)# ospf network point-to-point non-broadcast
ciscoasa(config-if)#
```

Related Commands

命令	说明
neighbor	指定手动配置的OSPF邻居。
showinterface	显示接口状态信息。

ospf priority

要更改OSPF路由器优先级，请在接口配置模式下使用 **ospfpriority** 命令。要恢复默认优先级，请使用此命 **no**令的形式。

ospf priority编号
no ospf priority[*number*]

Syntax Description

number	指定路由器的优先级；有效值为 0 到 255。

Command Default

数字的默认值为 1。

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	• 支持	—

使用指南

如果连接到网络的两台路由器同时尝试成为指定路由器，则优先采用具有较高优先级的路由器。如果优先级相同，则优先采用具有较高路由器ID的路由器。优先级设置为0的路由器没有资格成为指定路由器或备用指定路由器。只为多路访问网络（即，不为点对点网络）的接口配置路由器优先级。

在多情景模式下，对于共享接口，请指定0以确保设备不会成为指定路由器。OSPFv2实例无法跨共享接口相互建立邻接关系。

CR_Examples

以下示例显示如何更改所选接口上的 OSPF 优先级：

```
ciscoasa(config-if)# ospf priority 4
ciscoasa(config-if)#
```

Related Commands

命令	说明
showospfinterface	显示OSPF相关的接口信息。

ospf retransmit-interval

要指定属于该接口的邻接关系的LSA 重新传输之间的时间，请在**ospfretransmit-interval**接口配置模式下使用该命令。要恢复默认值，请使用此命 **no**令的形式。

ospf retransmit-interval [*seconds*]
no ospf retransmit-interval [*seconds*]

Syntax Description

seconds	指定属于接口的相邻路由器的LSA 重新传输的间隔时间；；其有效值范围为 1 至 65535 秒。

Command Default

秒的默认 **retransmit-interval**值为 5 秒。

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	• 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。

使用指南

当一台路由器向其邻居发送LSA 时，它将保留该LSA，直至收到确认消息。如果路由器没有收到确认，它将重新发送 LSA。

此参数设置应保守，否则将导致不必要的重新传输。串行线路和虚拟链路的值应较大。

CR_Examples

以下示例显示如何更改 LSA 的重新传输间隔：

```
ciscoasa(config-if)# ospf retransmit-interval 15
ciscoasa(config-if)#
```

Related Commands

命令	说明
showospfinterface	显示OSPF相关的接口信息。

ospf transmit-delay

如要设置在接口上发送链路状态更新数据包所需的估计时间，请在接口配置模式下使用 **ospftransmit-delay** 命令。要恢复默认值，请使用此命 **no**令的形式。

ospf transmit-delay [秒]
no ospf transmit-delay [秒]

Syntax Description

seconds	设置在接口上发送链路状态更新数据包所需的估计时间。默认值为 1 秒，范围为 1 至 65535 秒。

Command Default

秒的默认值为 1 秒。

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	• 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。

使用指南

更新数据包中的LSA在传输之前必须将其年龄增加秒数参数中指定的量。分配的值应将接口的传输和传播延迟考虑在内。

如果在通过链路进行传输之前未添加延迟，则不考虑LSA 通过该链路进行传播的时间。此设置对于超低速链路意义更大。

CR_Examples

以下示例将选定接口的传输延迟设置为 3 秒：

```
ciscoasa(config-if)# ospf restransmit-delay 3
ciscoasa(config-if)#
```

Related Commands

命令	说明
showospfinterface	显示OSPF相关的接口信息。

otp expiration

要为本地证书颁发机构(CA)注册页面指定一次性密码(OTP)的有效持续时间（以小时为单位），请在 ca 服务器配置模式下使用 **otpexpiration**命令。要将持续时间重置为默认小时数，请使用此命令的 **no**形式。

otp expiration*timeout*
no otp expiration

Syntax Description

timeout	指定在注册页面的OTP到期之前，用户必须从本地CA注册证书的时间（以小时为单位）。有效值范围为 1 至 720 小时（30 天）。

Command Default

默认情况下，证书注册的 OTP 过期时间为 72 小时（3 天）。

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 服务器配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

OTP 过期期限指定用户必须登录到 CA 服务器注册页面的小时数。在用户登录并注册证书之后，**enrollmentretrieval** 命令指定的时间段开始。

注释 用户在注册界面页面上注册证书时使用的 OTP 也用作解锁包含为该用户颁发的证书和密钥对的 PKCS12 文件的密码。

CR_Examples

以下示例指定注册页面的 OTP 应用 24 小时：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# otp expiration 24
ciscoasa
(config-ca-server)
#
```

以下示例将 OTP 持续时间重置为默认值 72 小时：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# no otp expiration
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
crypto ca server	提供对 ca 服务器配置模式命令集的访问，允许您配置和管理本地 CA。
enrollment-retrieval	指定注册用户可以检索 PKCS12 注册文件的时间（以小时为单位）。
showcryptocaserver	显示证书颁发机构配置。

output console

要将 **action** 命令的输出发送到控制台，请在事件管理器小程序配置模式下使用 **outputconsole** 命令。要删除控制台作为输出目的地，请使用此命令的 **no**形式。

output console
no output console

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
事件管理器小程序配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

使用此命令可将 **action** 命令的输出发送到控制台。

CR_Examples

以下示例将命令的输出发 **action**送到控制台：

```
ciscoasa(config-applet)# output console
```

Related Commands

命令	说明
输出文件附加	将命令输出写入单个文件，但每次都会附加到该**action**文件。
outputfilenew	将命令的输出发 **action**送到每个被调用的小程序的新文件。
outputfileoverwrite	将 **action**命令输出写入单个文件，每次都会被截断。
outputfilerotate	创建一组轮换的文件。
outputnone	丢弃命令的 **action**所有输出。

output file

要将 **action** 命令输出重定向到指定文件，请在事件管理器小程序配置模式下使用 **outputfile**命令。要删除指定操作，请使用此命 **no**令的形式。

output file [**append***filename* | **new** | **overwrite***filename* | **rotate***n*]
no output file [**append***filename* | **new** | **overwrite***filename* | **rotate***n*]

Syntax Description

append*filename*	连续将输出附加到指定的文件名，该文件是本地（到 ASA）文件名。
new	创建一个名为 eem-*applet -timestamp .log* 的新输出文件，其中 *applet* 是事件管理器小程序的名称， *timestamp* 是 YYYYMMDD-hhmmss 格式的时间戳。
覆盖文件名	将输出写入指定的文件，但每次调用事件管理器小程序时都会截断输出。
rotate*n*	创建一个名为 eem-*applet -x .log* 的输出文件，其中 *applet* 是事件管理器小程序的名称， *x* 是文件编号。当要写入新文件时，最旧的文件会被删除，且所有的后续文件都会在写入第一个文件之前进行重新编号。最新的文件用 0 表示，最旧的文件用最高数字 (*n* -1) 表示。 *n* 参数指定轮换值。有效值范围为 2 到 100。

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
事件管理器小程序配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

使用 **outputfile**命令将 **action** 命令输出重定向到指定文件。

CR_Examples

以下示例将输出附加到单个文件：

```
ciscoasa(config-applet)# output file append examplefile1
```

以下示例将 **action** 命令的输出发送到新文件：

```
ciscoasa(config-applet)# output file new
```

以下示例将输出写入单个截断文件：

```
ciscoasa(config-applet)# output file overwrite examplefile1
```

以下示例创建一组轮换的文件：

```
ciscoasa(config-applet)# output file rotate 50
```

Related Commands

命令	说明
outputconsole	将命令的输出发 **action**送到控制台。
outputnone	丢弃命令的 **action**所有输出。

output none

要放弃 **action** 命令的任何输出，请在事件管理器小程序配置模式下使用 **outputnone** 命令。要保留 **action** 命令的输出，请使用此命令的 **no** 形式。

output none
no output none

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认设置为丢弃来自 **action** 命令的任何输出。

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
事件管理器小程序配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

使用此命令可丢弃来自 **action** 命令的任何输出。

CR_Examples

以下示例丢弃 **action** 命令的任何输出：

```
ciscoasa(config-applet)# output none
```

Related Commands

命令	说明
outputconsole	将命令的输出发 **action**送到控制台。
输出文件附加	将命令输出写入单个文件，但每次都会附加到该**action**文件。
outputfilenew	将命令的输出发 **action**送到每个被调用的小程序的新文件。
outputfileoverwrite	将 **action**命令输出写入单个文件，每次都会被截断。
outputfilerotate	创建一组轮换的文件。

outstanding（已弃用）

注释 支持此命令的最后一个版本是版本 9.5(1)。

要限制未经身份验证的邮件代理会话的数量，请在相应的邮件代理配置模式下使用 **outstanding**命令。要从配置中删除属性，请使用此命 **no** 令的形式。

outstanding{ *number*}
no outstanding

Syntax Description

number 允许的未经身份验证的会话数。范围是从1到1000。

Command Default

默认值为 20。

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
Pop3s	• 是	—	• 是	•	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.5(2)	此命令已弃用。

使用指南

使用此命令的no版本可从配置中删除此属性，此配置允许无限数量的未经身份验证的会话。这也会限制邮件端口上的 DOS 攻击。

电子邮件代理连接有三种状态：

- **1.** 新的邮件连接进入“unauthenticated”状态。
- **2.** 当连接出现用户名时，它进入“正在验证”状态。
- **3.** 当 ASA 对连接进行身份验证时，它会进入“已验证”状态。

如果处于未经身份验证状态的连接数超过配置的限制，ASA 将终止最早的未经身份验证的连接，以防止过载。它不会终止经过身份验证的连接。

CR_Examples

以下示例显示如何为 POP3S 邮件代理设置 12 个未经身份验证的会话的限制。

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)
#
 outstanding 12
```

override-account-disable (已弃用)

注释 支持此命令的最后一个版本是版本 9.5(1)。

要覆盖来自 AAA 服务器的帐户禁用指示，请在**override-account-disable**隧道组常规属性配置模式下使用该命令。要禁用覆盖，请使用此命 **no**令的形式。

override-account-disable
no override-account-disable

Syntax Description

此命令没有任何参数或关键字。

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
隧道组常规属性配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。
9.5(2)	此命令已弃用。

使用指南

此命令适用于返回“account-disabled”指示的服务器，例如使用 NT LDAP 的 RADIUS 和 Kerberos。

您可以为 IPsec RA 和 WebVPN 隧道组配置此属性。

CR_Examples

以下示例允许从 AAA 服务器为 WebVPN 隧道组“testgroup”覆盖“account-disabled”指示符：

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

以下示例允许从 AAA 服务器为 IPsec 远程访问隧道组“QAgroup”覆盖“account-disabled”指示符：

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

Related Commands

命令	说明
clearconfiguretunnel-group	清除隧道组数据库或特定隧道组的配置。
tunnel-group general-attributes	配置隧道组常规属性值。

override-svc-download

要配置连接配置文件以覆盖下载 AnyConnect 或 SSL VPN 客户端的组策略或用户名属性配置，请在 tunnel-group webvpn attributes 配置模式下使用 **override-svc-download** 命令。要从配置中删除命令，请使用以 **no**下命令形式：

override-svc-downloadenable
no override-svc-downloadenable

Command Default

默认设置为禁用。ASA 不会覆盖组策略或用户名属性配置来下载客户端。

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
Tunnel-group webvpn 配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

安全设备允许远程用户进行无客户端、AnyConnect 或 SSL VPN 客户端连接，具体取决于是否在组策略或用户名属性中使用命令启用了无客户端和/或 SSL **vpn-tunnel-protocol**VPN。该 **svcask**命令通过提示用户下载客户端或返回 WebVPN 主页来进一步修改客户端用户体验。

但是，您可能希望在特定隧道组下登录的无客户端用户不会遇到等待下载提示过期然后才显示无客户端 SSL VPN 主页的延迟。可以使用 **override-svc-download** 命令在连接配置文件级别防止这些用户遇到延迟。此命令使通过连接配置文件登录的用户立即看到无客户端 SSL VPN 主页，无论 **vpn-tunnel-protocol**或 **svcask**命令设置如何。

CR_Examples

在以下示例中，用户进入连接配置文件 >*engineering* 的隧道组 webvpn 属性配置模式，并启用连接配置文件来覆盖客户端下载提示的组策略和用户名属性设置：

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# override-svc-download
```

Related Commands

命令	说明
showwebvpnsvc	显示有关已安装的 SSL VPN 客户端的信息。

命令	说明
svc	为特定组或用户启用或需要 SSL VPN 客户端。
svcimage	指定 ASA 在缓存内存中扩展的客户端包文件，以便下载到远程 PC。

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。