inspect a – inspect z

inspect ctiqbe

要启用 CTIQBE 协议检测，请在类配置模式下使用 **inspectctiqbe** 命令。可以从 map configuration 模式访问 Class configuration 模式。要禁用检查，请使用此命 **no**令的形式。

inspect ctiqbe
no inspect ctiqbe

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	我们添加了此命令，它取代了之前已弃用的 **fixup** 命令。

使用指南

该 **inspectctiqbe**命令启用 CTIQBE 协议检查，支持 NAT、PAT 和双向 NAT。这使得 Cisco IP SoftPhone 和其他 Cisco TAPI/JTAPI 应用程序能够与 Cisco CallManager 成功协作，以便在 ASA 上设置呼叫。

许多思科 VoIP 应用都使用电话应用程序编程接口 (TAPI) 和 Java 电话应用程序编程接口 (JTAPI)。计算机电话接口快速缓冲编码 (CTIQBE) 由 Cisco TAPI 服务提供程序 (TSP) 用于与思科 CallManager 通信。

下面总结了使用 CTIQBE 应用检测时适用的限制：

- 不支持 CTIQBE 呼叫状态故障转移。
- 使用 **debugctiqbe** 命令可能会延迟消息传输，这可能会对实时环境中的性能造成影响。在启用此调试或日志记录功能且 Cisco IP SoftPhone 似乎无法通过 ASA 完成呼叫建立时，请在运行 Cisco IP SoftPhone 的系统上增加超时值。
- CTIQBE 应用检测不支持在多个 TCP 数据包中分段的 CTIQBE 消息。

下面总结了在特定情况下使用 CTIQBE 应用检测时的特殊注意事项：

- 如果两个 Cisco IP SoftPhone 注册到不同的 Cisco CallManager，并且连接到 ASA 的不同接口，则这两个电话之间的通话将会失败。

- 当 Cisco CallManager 位于比 Cisco IP SoftPhones 安全性更高的接口上时，如果 Cisco CallManager IP 地址需要 NAT 或外部 NAT，则映射必须是静态的，因为 Cisco IP SoftPhone 要求在 PC 上的 Cisco TSP 配置中明确指定 Cisco CallManager IP 地址。
- 使用 PAT 或外部 PAT 时，如果要转换 Cisco CallManager IP 地址，则必须将其 TCP 端口 2748 静态映射到 PAT（接口）地址的相同端口，以使 Cisco IP SoftPhone 注册成功。CTIQBE 监听端口 (TCP 2748) 是固定的，用户无法在 Cisco CallManager、Cisco IP SoftPhone 或 Cisco TSP 上配置。

检查信令消息

要检查信令消息，**inspect**ctiqbe命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和NAT状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，**inspect**ctiqbe命令不使用隧道默认网关路由。隧道默认网关路由是采用 **route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspect**ctiqbe命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用CTIQBE检测引擎，该引擎创建类映射来匹配默认端口（2748）上的CTIQBE流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map ctiqbe-port
ciscoasa(config-cmap)# match port tcp eq 2748
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ctiqbe_policy

ciscoasa(config-pmap)# class ctiqbe-port
ciscoasa(config-pmap-c)# inspect ctiqbe
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ctiqbe_policy interface outside
```

要对所有接口启用 CTIQBE 检测，请使用 **global** 参数代替 **interfaceoutside**。

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
showconn	显示不同连接类型的连接状态。
showctiqbe	显示有关跨 ASA 建立的 CTIQBE 会话和由 CTIQBE 检测引擎分配的媒体连接的信息。
timeout	为不同协议和会话类型设置最大空闲持续时间。

inspect dcerpc

要启用对流向终端映射器的DCERPC流量的检测，请在类配置模式下使用inspect dcerpc命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect dcerpc [*map_name*]
no inspect dceprc [*map_name*]

Syntax Description

map_name	（可选）DCERPC检测映射的名称。

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

该 **inspect dcerpc**命令启用或禁用 DCERPC 协议的应用程序检查。

CR_Examples

以下示例显示如何使用为 DCERPC 针孔配置的超时定义 DCERPC 检测策略映射。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
ciscoasa(config)# class-map dcerpc
ciscoasa(config-cmap)# match port tcp eq 135
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# class dcerpc
ciscoasa(config-pmap-c)# inspect dcerpc dcerpc_map
ciscoasa(config)# service-policy global-policy global
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。

命令	说明
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	创建检查策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。
timeoutpinhole	配置 DCERPC 针孔的超时并覆盖全局系统针孔超时。

inspect diameter

要启用 Diameter 应用程序检查，请在类配置模式下使用 inspect **diameter** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect diameter [*diameter_map*] [**tls-proxy***proxy_name*]
no inspect diameter [*diameter_map*] [**tls-proxy***proxy_name*]

注释 Diameter 检测需要运营商许可证。

Syntax Description

diameter_map	指定 Diameter 策略映射名称。
tls-proxy*proxy_name*	使用指定的 TLS 代理，以便检查加密连接。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.5(2)	添加了此命令。
9.6(1)	添加了 **tls-proxy** 关键字。

使用指南

Diameter 是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。

Diameter 使用 TCP 和 SCTP 作为传输层，并使用 TCP/TLS 和 SCTP/DTLS 保障通信安全。另外，它也可以选择性地提供数据对象加密。有关 Diameter 的详细信息，请参阅 RFC 6733。

Diameter应用执行服务管理任务，例如决定用户权限、服务授权、服务质量和收费率。虽然Diameter应用可出现在 LTE 架构的许多不同控制面板接口上，但 ASA 仅检测以下接口的 Diameter 命令编码和属性-值对 (AVP)：

- S6a：移动管理实体 (MME) - 家庭订用服务(HSS)。

- S9：PDN 网关 (PDG) - 3GPP AAA 代理/服务器。
- Rx：策略收费规则功能 (PCRF) - 呼叫会话控制功能 (CSCF)。

Diameter 检测为 Diameter 终端打开针孔，以允许通信。该检测支持 3GPP 版本 12，并符合 RFC 6733 要求。您可以将其用于 TCP/TLS（通过在启用检测时指定 TLS 代理），但不能将其用于 SCTP。使用 Ipsec 可保障 SCTP Diameter 会话的安全。

您可以选择性地使用 Diameter 检测策略映射根据应用 ID、命令代码和 AVP 来过滤流量，以便应用特殊操作，例如丢弃数据包或连接或记录它们。可以为新注册的 Diameter 应用创建自定义 AVP。通过过滤，您可以微调网络上允许的流量。

注释 默认情况下，允许其他接口上运行的应用的 Diameter 消息通过。虽然无法基于这些不支持应用的命令代码或 AVP 指定操作，但您可以配置 Diameter 检测策略映射，根据应用 ID 丢弃这些应用。

CR_Examples

以下示例在默认端口（TCP/3868、TCP/5868 和 SCTP/3868）上全局应用 Diameter 检测。

```
ciscoasa(config)# policy-map global_policy

ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect diameter
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
inspectsctp	启用 SCTP 检查。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
showservice-policyinspectdiameter	显示检查直径策略的状态和统计信息。
tls-proxy	定义 TLS 代理。

inspect dns

要启用 DNS 检测（如果以前已禁用）或配置 DNS 检测参数，请在类配置模式下使用 **inspectdns** 命令。可以从 map configuration 模式访问 Class configuration 模式。要禁用 DNS 检查，请使用此命 **no** 令的形式。

inspect dns [*map_name*] [**dynamic-filter-snoop**]
no inspect dns [*map_name*] [**dynamic-filter-snoop**]

Syntax Description

dynamic-filter-snoop	（可选）启用动态过滤器侦听，仅由僵尸网络流量过滤器使用。应仅在使用僵尸网络流量过滤时包含此关键字。我们建议仅在有外部 DNS 请求经过的接口上启用 DNS 监听。在所有 UDP DNS 流量（包括流向内部 DNS 服务器的流量）上启用 DNS 监听会为 ASA 形成不必要的负载。
map_name	（可选）指定 DNS 映射的名称。

Command Default

默认情况下会启用此命令。默认情况下会禁用僵尸网络流量过滤器侦听。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。
7.2(1)	此命令已修改为允许配置其他 DNS 检查参数。
8.2(1)	添加了 **dynamic-filter-snoop** 关键字。

使用指南

默认情况下，启用 DNS 检测，使用 preset_dns_map 检测类映射：

- 最大 DNS 消息长度为 512 字节。
- 最大客户端 DNS 消息长度是自动设置的，以与资源记录匹配。
- DNS Guard 已启用，因此 ASA 在转发 DNS 应答后立即终止与 DNS 查询相关的 DNS 会话。另外，ASA 还会监控消息交换，以确保 DNS 应答的 ID 与 DNS 查询的 ID 匹配。
- 根据 NAT 配置的 DNS 记录转换已启用。

- 协议执行已启用，使得可以进行 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。

DNS 重写需要 DNS 检测

当启用 DNS 检测时，DNS 重写将为源自任何接口的 DNS 消息的 NAT 提供全面支持。

如果内部网络上的客户端请求从外部接口上的 DNS 服务器对内部地址进行 DNS 解析，则正确转换 DNS A 记录。如果禁用 DNS 检测引擎，则不转换 A 记录。

DNS 重写执行两个功能：

- 当 DNS 客户端位于专用接口上时，将 *DNS* 应答 中的公共地址（可路由或“映射”地址）转换为专用地址（“实际”地址）。
- 当 DNS 客户端位于公用接口上时，将专用地址转换为公用地址。

只要 DNS 检测保持启用状态，您就可以为 NAT 配置 DNS 重写。

CR_Examples

以下示例显示如何设置最大 DNS 消息长度：

```
ciscoasa(config)# policy-map type inspect dns dns-inspect
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 1024
```

以下示例为所有 UDP DNS 流量创建类映射，使用默认 DNS 检测策略映射启用 DNS 检测和僵尸网络流量过滤器监听，并将其应用于外部接口：

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
dynamic-filterenable	为一个流量类或为所有流量（如果不指定访问列表）启用僵尸网络流量过滤器。
policy-map	将类映射与特定的安全操作相关联。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。

inspect esmtp

要启用 SMTP/ESMTP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspectesmtp** 命令。可以从策略图配置模式访问类配置模式。要删除配置，请使用此命令 **no**的形式。

inspect esmtp [*map_name*]
no inspect esmtp [*map_name*]

Syntax Description

map_name （可选）ESMTP 映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

默认情况下，ESMTP 检测已启用，其中会使用 _default_esmtp_map 检测策略映射。

- 会掩蔽服务器横幅。
- 检查加密流量。
- 不会查找发件人和收件人地址中的特殊字符，不会执行任何操作。
- 会丢弃并记录命令行长度大于 512 的连接。
- 会丢弃并记录有多于 100 个收件人的连接。
- 会记录正文长度超过 998 字节的消息。
- 会丢弃并记录报头行长度大于 998 的连接。
- 会丢弃并记录 MIME 文件名超过 255 个字符的消息。
- 会掩蔽匹配“others”的 EHLO 应答参数。

ESMTP 应用程序检查通过限制可通过 ASA 的 SMTP 命令类型并添加监控功能，提供了针对基于 SMTP 的攻击的改进防护。

ESMTP 是增强型 SMTP 协议，在大多数方面和 SMTP 类似。为方便起见，本文档中用 SMTP 来同时指代 SMTP 和 ESMTP。扩展 SMTP 的应用检测流程类似于 SMTP 应用检测，这项检测支持 SMTP 会话。扩展 SMTP 会话中使用的大多数命令与 SMTP 会话中使用的命令相同，但 ESMTP 会话的速度快很多，而且提供了更多与可靠性和安全性相关的选项，例如，传送状态通知。

扩展SMTP应用检测增加了对如下扩展SMTP命令的支持：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS 和 VRFY。除了支持七个 RFC 821 命令（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）之外，ASA 还支持总共十五个 SMTP 命令。

不支持其他扩展 SMTP 命令（例如 ATRN、ONEX、VERB、CHUNKING）和专用扩展。不受支持的命令将被转换为X（内部服务器会拒绝这些命令）。这将会生成消息，例如“500 Command unknown: 'XXX'”。不完整的命令将被丢弃。

ESMTP 检测引擎将服务器 SMTP 横幅中的字符更改为星号，但对“2”、“0”、“0”字符除外。会忽略回车符 (CR) 和换行符 (LF)。

在 SMTP 检测启用的情况下，如果不遵守以下规则，用于交互式 SMTP 的 Telnet 会话可能会挂起：SMTP 命令长度必须至少为四个字符；必须以回车符和换行符终止；且必须在获得响应后才能发出下一个应答。

SMTP 服务器使用数字应答代码和（可选）人可读字符串来响应客户端请求。SMTP 应用检测控制和减少用户可使用的命令以及服务器返回的消息。SMTP 检测主要执行以下三项任务：

- 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。
- 监控 SMTP 命令-响应序列。
- 生成审核线索 - 邮件地址中嵌入的无效字符被替换时，会生成审核记录 108002。有关详细信息，请参阅 RFC 821。

SMTP 检测监控以下异常签名的命令-响应序列：

- 截断的命令。
- 命令终止错误（不是以 <CR><LR> 终止）。
- MAIL 和 RCPT 命令指定邮件的发件人和收件人。会扫描邮件地址以检测异常字符。竖线 (|) 将被删除（更改为空格）；“<”和“>”只能用于定义邮件地址（“>”前面必须有“<”）。
- SMTP 服务器执行的意外转换。
- 对于未知命令，ASA 会将数据包中的所有字符更改为 X。在这种情况下，服务器会向客户端生成错误代码。由于数据包发生了变化，因此必须重新计算或调整 TCP 校验和。
- TCP 数据流编辑。
- 命令管道。

CR_Examples

以下示例启用 SMTP 检测引擎，从而创建类映射来匹配默认端口（25）上的 SMTP 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map smtp-port
```

```
ciscoasa(config-cmap)# match port tcp eq 25
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map smtp_policy

ciscoasa(config-pmap)# class smtp-port
ciscoasa(config-pmap-c)# inspect esmtp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy smtp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
showconn	显示不同连接类型的连接状态，包括SMTP。

inspect ftp

要为 FTP 检测配置端口或启用增强检测，请在类配置模式下使用 **inspectftp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect ftp [**strict** [*map_name*]]
no inspect ftp [**strict** [*map_name*]]

Syntax Description

map_name	FTP 检测映射的名称。
strict	（可选）启用FTP流量的增强型检测，并强制遵守RFC标准。

Command Default

默认情况下启用 FTP 检测，并且 ASA 会侦听 FTP 的端口 21。

将 FTP 移至更高的端口时请谨慎。例如，如果将 FTP 端口设置为 2021，则向端口 2021 发起的所有连接都将其数据负载解释为 FTP 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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的**fixup** 命令。添加了 *map_name*选项。

使用指南

FTP 应用检测用于检测 FTP 会话和执行四种任务：

- 准备动态辅助数据连接
- 跟踪 FTP 命令-响应序列
- 生成审核线索
- 转换嵌入式 IP 地址

FTP 应用检测为 FTP 数据传输准备辅助信道。这些信道的端口是通过 PORT 或 PASV 命令协商的。这些信道根据文件上传、文件下载或目录列表事件进行分配。

注释 仅对 FTP 控制连接的端口而非数据连接的端口应用检测。ASA 状态检测引擎会根据需要动态准备数据连接。

如果使用该 **noinspectftp**命令禁用 FTP 检查引擎，则出站用户只能以被动模式启动连接，并且所有入站 FTP 都将被禁用。

严格 FTP

严格 FTP 可防止 Web 浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全性。要启用严格 FTP，请在命令中包含严格选 **inspectftp**项。

在使用严格 FTP 时，您可以选择指定 FTP 检测策略映射来指定不允许通过 ASA 的 FTP 命令。

在接口上启用该 **strict**选项后，FTP 检查将强制执行以下行为：

- 必须先确认 FTP 命令，然后 ASA 才允许使用新命令。
- ASA 丢弃发送嵌入式命令的连接。
- 检查 227 命令和 PORT 命令，以确保这些命令不显示在错误字符串中。

注意 使用该 **strict**选项可能会导致不严格遵守 FTP RFC 的 FTP 客户端失败。

如果启用该 **strict**选项，则会跟踪每个 FTP 命令和响应序列是否存在以下异常活动：

- 截断命令 - 检查 PORT 和 PASV 应答命令中逗号的数量是否是五个。如果不是五个，将会截断 PORT 命令并关闭 TCP 连接。
- 错误命令 - 检查 FTP 命令以确定它是否以 <CR><LF> 字符结尾（如 RFC 所要求）。如果不是，将会关闭连接。
- RETR 和 STOR 命令的大小 - 根据某个固定常数检查这些命令的大小。如果命令大小大于该固定常数，将会记录错误消息并关闭连接。
- 命令欺骗 - PORT 命令应始终从客户端发送。如果 PORT 命令是从服务器发送，将会拒绝 TCP 连接。
- 应答欺骗 - PASV 应答命令 (227) 应始终从服务器发送。如果 PASV 应答命令是从客户端发送，将会拒绝 TCP 连接。这样可防止用户执行“227 xxxxx a1, a2, a3, a4, p1, p2.”时出现安全漏洞
- TCP 流编辑 - 如果检测到 TCP 流编辑，ASA 将关闭连接。
- 无效的端口协商 - 检查协商的动态端口值是否小于 1024。由于 1 至 1024 范围内的端口号是为已知连接保留的，因此，如果协商的端口在这个范围内，将会释放 TCP 连接。
- 命令管道 - 将 PORT 和 PASV 应答命令中在端口号后显示的字符数与常数值 8 进行比较。如果该字符数大于 8，将会关闭 TCP 连接。

- ASA 将 FTP 服务器对 SYST 命令的响应替换为一系列 X，以防止服务器向 FTP 客户端泄露其系统类型。要覆盖此默认行为，请使用 FTP **nomask-syst-reply**映射中的命令。

FTP 日志消息

FTP 应用检测生成以下日志消息：

- 为检索或上传的每个文件生成审核记录 302002。
- 如果辅助动态信道准备因内存不足而失败，将会生成审核记录 201005。

CR_Examples

提交用户名和密码之前，所有 FTP 用户均可以看到问候横幅。默认情况下，该横幅包含对于试图发现系统缺陷的黑客来说很有用的版本信息。以下示例显示如何掩蔽该横幅：

```
ciscoasa(config)# policy-map type inspect ftp mymap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# class-map match-all ftp-traffic
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ftp-policy
ciscoasa(config-pmap)# class ftp-traffic
ciscoasa(config-pmap-c)# inspect ftp strict mymap
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy ftp-policy interface inside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
mask-syst-reply	隐藏来自客户端的FTP服务器响应。
policy-map	将类映射与特定的安全操作相关联。
policy-maptypeinspect	创建检查策略映射。
request-commanddeny	指定要禁止的 FTP 命令。
service-policy	将策略映射应用到一个或多个接口。

inspect gtp

要启用 GTP 检查，请在 **inspectgtp**类配置模式下使用该命令。可以从 map configuration 模式访问 Class configuration 模式。使用此命 **no**令的形式可以禁用 GTP 检查。

inspect gtp [*map_name*]
no inspect gtp [*map_name*]

注释 GTP 检查需要 GTP/GPRS 或运营商许可证。

Syntax Description

map_name （可选）GTP检测策略映射的名称。

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。
9.5(1)	增加了对 GTPv2 和 IPv6 地址的支持。

使用指南

GPRS 隧道协议用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。服务提供商网络使用 GTP 通过终端之间的 GPRS 主干隧道传输多协议数据包。

默认情况下，GTP检测未启用。但是，如果在未指定检测映射的情况下启用GTP检测，将会使用默认映射（默认映射提供以下处理）。仅在需要不同值的情况下，才需要配置映射。

- 不允许错误。
- 最大请求数为 200。
- 最大隧道数为 500。
- GSN/端点超时为 30 分钟。

- PDP 情景超时是 30 分钟。在 GTPv2 中，此值为承载情景超时。
- 请求超时为 1 分钟。
- 信令超时是 30 分钟。
- 隧道超时为 1 小时。
- T3 响应超时为 20 秒。
- 丢弃并记录未知消息 ID。此行为限于 3GPP 为 S5S8 接口定义的消息。可能允许为其他 GPRS 接口定义的消息，最大程度地减少对它们应用的检测。

使用 **policy-maptypeinspectgtp**命令定义 GTP 的参数。定义 GTP 映射后，可使用 **inspectgtp** 命令启用该映射。然后，使用 **class-map**、 **policy-map**和 **service-policy** 命令定义流量类，向该类应用 inspect 命令，并将策略应用到一个或多个接口。

已知的 GTP 端口是 UDP 3386、2123 和 2152。

检查信令消息

要检查信令消息，**inspectgtp**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和NAT状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspectgtp**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspectgtp**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例显示如何限制网络中隧道的数量：

```
ciscoasa(config)# policy-map type inspect gtpgmap

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# tunnel-limit 3000

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default

ciscoasa(config-pmap-c)# inspect gtp gmap

ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
clearservice-policyinspectgtp	将清除全局 GTP 统计数据。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。

命令	说明
showservice-policyinspectgtp	显示 inspect gtp 策略的状态和统计信息。

inspect h323

要启用 H.323 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspecth323** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect h323 {**h225** | **ras**} [*map_name*]
no inspect h323 {**h225** | **ras**} [*map_name*]

Syntax Description

h225	启用 H.225 信令检测。
map_name	（可选）H.323 映射的名称。
ras	启用 RAS 检查。

Command Default

默认端口分配如下：

- h323 h225 1720
- h323 RAS 1718-1719

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

inspect h323 命令为符合 H.323 的应用程序（例如 Cisco CallManager 和 VocalTec Gatekeeper）提供支持。H.323 是国际电信联盟 (ITU) 为 LAN 上的多媒体会议定义的一套协议。ASA 支持 H.323 至版本 6，包括 H.323 v3 功能“一个呼叫信令信道上的多个呼叫”。

启用 H.323 检查后，ASA 支持在同一呼叫信令信道上进行多个呼叫，这是 H.323 版本 3 添加的功能。此功能可缩短呼叫建立时间并减少 ASA 上端口的使用。

H.323 检测具有如下两个主要功能：

- 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消息以 PER 编码格式编码，所以 ASA 使用 ASN.1 解码器来解码 H.323 消息。
- 动态分配协商的 H.245 和 RTP/RTCP 连接。

检查信令消息

要检查信令消息，**inspecth323**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和NAT状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspecth323**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用**route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果VPN流量需要**inspecth323**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 H.323 检测引擎，该引擎创建类映射来匹配默认端口 (1720) 上的 H.323 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map h323-port
ciscoasa(config-cmap)# match port tcp eq 1720
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map h323_policy

ciscoasa(config-pmap)# class h323-port
ciscoasa(config-pmap-c)# inspect h323
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy h323_policy interface outside
```

Related Commands

命令	说明
policy-maptypeinspect	创建检查策略映射。
showh225	显示通过 ASA 建立的 H.225 会话的信息。
showh245	显示终端使用慢启动通过 ASA 建立的 H.245 会话的信息。
showh323ras	显示通过 ASA 建立的 H.323 RAS 会话的信息。
timeout {h225 | h323}	配置关闭 H.225 信令连接或 H.323 控制连接前的空闲时间。

inspect http

要启用 HTTP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspecthttpcommand**。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect http [*map_name*]
no inspect http [*map_name*]

Syntax Description

map_name	（可选）HTTP检测映射的名称。

Command Default

HTTP 的默认端口为 80。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

提示 可以安装执行应用和URL过滤（包括HTTP检测）的服务模块，例如ASA CX或ASA FirePOWER。ASA上运行的HTTP检测与这些模块不兼容。请注意，使用专用模块配置应用过滤比尝试使用HTTP检测策略映射在 ASA 上手动配置要简单的多。

使用 HTTP 检测引擎可防御特定攻击以及与 HTTP 流量相关的其他威胁。

HTTP应用检测扫描HTTP报头和正文，并对数据执行各种检查。这些检查可防止各种HTTP构造、内容类型、隧道协议和消息传送协议通过安全设备。

增强型 HTTP 检测功能（又称为应用防火墙，在配置 HTTP 检测策略映射时可使用此功能）有助于防止攻击者使用 HTTP 消息来避开网络安全策略。

HTTP 应用检测可阻止通过隧道传送的应用以及 HTTP 请求和响应中的非 ASCII 字符，从而防止恶意内容到达 Web 服务器。还支持对 HTTP 请求和响应报头中的各个元素进行大小限制、URL 拦截以及 HTTP 服务器报头类型欺骗。

增强型 HTTP 检测验证所有 HTTP 消息是否满足以下条件：

- 符合 RFC 2616 的要求
- 仅使用 RFC 定义的方法。
- 符合其他条件。

CR_Examples

在本例中，任何通过 any 接口进入 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。由于采用了全局策略，检测仅在流量流入每个接口时发生。

```
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map http_traffic_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# inspect http
ciscoasa(config)# service-policy http_traffic_policy global
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
policy-maptypeinspect	创建检查策略映射。

inspect icmp

要配置 ICMP 检测引擎，请在类配置模式下使用 **inspecticmp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect icmp
no inspect icmp

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

ICMP 检查引擎允许像 TCP 和 UDP 流量一样检查 ICMP 流量。如果没有 ICMP 检测引擎，我们建议您在 ACL 中不要允许 ICMP 通过 ASA。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检查引擎确保每个请求只有一个响应，并且序列号是正确的

当禁用 ICMP 检查时（默认配置），系统会拒绝从较低安全性接口至较高安全性接口的 ICMP 回应应答消息，即使该接口是对 ICMP 回应请求的响应。

CR_Examples

如以下示例所示启用 ICMP 应用检测引擎，该引擎创建一个使用 ICMP 协议 ID（对于 IPv4 为 1，对于 IPv6 为 58）匹配 ICMP 流量的类映射。然后，服务策略会被应用到外部接口。要对所有接口启用 ICMP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
icmp	为在 ASA 接口终止的 ICMP 流量配置访问规则。
policy-map	定义将安全操作与一个或多个流量类别关联的策略。
service-policy	将策略映射应用到一个或多个接口。

inspect icmp error

要启用 ICMP 错误消息的应用检测，请在类配置模式下使用 **inspecticmp** error 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect icmp error
no inspect icmp error

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

当启用 ICMP 错误检测时，ASA 将基于 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。ASA 将使用转换的 IP 地址覆盖数据包。

禁用时，ASA 不会为生成 ICMP 错误消息的中间节点创建转换会话。内部主机与 ASA 之间的中间节点生成的 ICMP 错误消息将会到达外部主机，而不占用任何其他 NAT 资源。如果外部主机使用 traceroute 命令来跟踪连接 ASA 内部目标的跃点，这种方式则不合适。当 ASA 不转换中间跃点时，显示的所有中间跃点将带有映射目标 IP 地址。

会扫描 ICMP 负载，以从原始数据包检索五元组。然后，会使用检索到的五元组进行查找，以确定客户端的原始地址。ICMP 错误检测引擎会对 ICMP 数据包进行以下更改：

- 在 IP 报头中，映射 IP 更改为实际 IP（目标地址）并修改 IP 校验和。
- 在 ICMP 报头中，会根据 ICMP 数据包的变化修改 ICMP 校验和。
- 在负载中，会进行以下更改：
  - 原始数据包映射 IP 更改为实际 IP
  - 原始数据包映射端口更改为实际端口
  - 重新计算原始数据包 IP 校验和

CR_Examples

以下示例启用 ICMP 错误应用检测引擎，该引擎创建一个使用 ICMP 协议 ID（对于 IPv4 为 1，对于 IPv6 为 58）匹配 ICMP 流量的类映射。然后，服务策略会被应用到外部接口。要对所有接口启用 ICMP 错误检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp error
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
icmp	为在 ASA 接口终止的 ICMP 流量配置访问规则。
inspecticmp	启用或禁用 ICMP 检查引擎。
policy-map	定义将安全操作与一个或多个流量类别关联的策略。
service-policy	将策略映射应用到一个或多个接口。

inspect ils

要启用 ILS 应用检测，请在类配置模式下使用 inspect **ilscommand**。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect ils
no inspect ils

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

该 **inspectils**命令为使用 LDAP 与 ILS 服务器交换目录信息的 Microsoft NetMeeting、SiteServer 和 Active Directory 产品提供 NAT 支持。

ASA 支持 ILS 的 NAT，用于在 ILS 或 SiteServer 目录中注册和定位端点。因为 LDAP 数据库仅存储 IP 地址，所以，无法支持 PAT。

对于搜索响应，当 LDAP 服务器位于外部时，应考虑使用 NAT，以允许内部对等设备在注册到外部 LDAP 服务器时进行本地通信。对于此类搜索响应，会先搜索 xlate，然后搜索 DNAT 条目以获得正确地址。如果上述两种搜索都失败，则地址未更改。对于使用 NAT 0（无 NAT）且不期望 DNAT 交互的站点，建议关闭检测引擎以提供更佳性能。

当 ILS 服务器位于 ASA 边界内时，可能需要进行其他配置。这就需要提供一个孔来让外部客户端在指定的端口（通常为 TCP 389）上访问 LDAP 服务器。

由于 ILS 流量仅发生在辅助 UDP 通道上，因此 TCP 连接在 TCP 不活动间隔后断开。默认情况下，此间隔为 60 分钟，可以使用命令进行调 **timeout**整。

ILS/LDAP 遵循客户端/服务器模式，通过单个 TCP 连接处理会话。根据客户端的操作，将可能创建多个上述会话。

在连接协商期间，BIND PDU 会从客户端发送至服务器。一旦收到来自服务器的成功 BIND RESPONSE，系统就可能交换其他操作消息（例如 ADD、DEL、SEARCH 或 MODIFY），以对 ILS 目录执行多项操作。ADD REQUEST 和 SEARCH RESPONSE PDU 可能包含 NetMeeting 对等设备的

IP 地址，H.323（SETUP 和 CONNECT 消息）使用它建立 NetMeeting 会话。Microsoft NetMeeting v2.X 和 v3.X 提供 ILS 支持。

ILS 检测将执行以下操作：

- 使用 BER 解码功能解码 REQUEST/RESPONSE PDU。
- 解析 LDAP 数据包。
- 提取 IP 地址。
- 根据需要转换 IP 地址。
- 使用 BER 编码功能，用已转换地址对 PDU 进行编码。
- 将新编码的 PDU 复制回 TCP 数据包。
- 执行递增 TCP 校验和与序列号调整。

ILS 检测存在如下局限性：

- 不支持推荐请求和响应。
- 多个目录中的用户不统一。
- NAT 无法标识多个目录中具有多个身份的单一用户。

注释 由于 H.225 呼叫信令流量仅发生在辅助 UDP 通道上，因此 TCP 连接会在 TCP 命令指定的时间间隔后断 **timeout**开。默认情况下，此间隔设置为 60 分钟。

CR_Examples

如以下示例所示启用ILS检测引擎，该引擎创建一个类映射来匹配默认端口（389）上的ILS流量。然后，服务策略会被应用到外部接口。要对所有接口启用 ILS 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map ils-port
ciscoasa(config-cmap)# match port tcp eq 389
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ils_policy

ciscoasa(config-pmap)# class ils-port
ciscoasa(config-pmap-c)# inspect ils
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ils_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。

命令	说明
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。

inspect im

要启用 Instant Messenger 流量检测，请在类配置模式下使用 inspect im 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect im*map_name*
no inspect im*map_name*

Syntax Description

map_name IM 映射的名称。

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

该 **inspect im**命令启用或禁用 IM 协议的应用程序检查。使用即时消息 (IM) 检测引擎可以控制 IM 的网络使用情况，以及阻止机密数据泄露、蠕虫传播和针对公司网络的其他威胁。

CR_Examples

以下示例显示如何定义 IM 检查策略图：

```
ciscoasa(config)# regex loginname1 “user1\@example.com”
ciscoasa(config)# regex loginname2 “user2\@example.com”
ciscoasa(config)# regex loginname3 “user3\@example.com”
ciscoasa(config)# regex loginname4 “user4\@example.com”
ciscoasa(config)# regex yahoo_version_regex “1\.0”
ciscoasa(config)# regex gif_files “.*\.gif”
ciscoasa(config)# regex exe_files “.*\.exe”
ciscoasa(config)# class-map type regex match-any yahoo_src_login_name_regex
ciscoasa(config-cmap)# match regex loginname1
ciscoasa(config-cmap)# match regex loginname2
ciscoasa(config)# class-map type regex match-any yahoo_dst_login_name_regex
ciscoasa(config-cmap)# match regex loginname3
ciscoasa(config-cmap)# match regex loginname4
ciscoasa(config)# class-map type inspect im match-any yahoo_file_block_list
ciscoasa(config-cmap)# match filename regex gif_files
```

```
ciscoasa(config-cmap)# match filename regex exe_files

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy
ciscoasa(config-cmap)# match login-name regex class yahoo_src_login_name_regex
ciscoasa(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex
ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy2
ciscoasa(config-cmap)# match version regex yahoo_version_regex
ciscoasa(config)# class-map im_inspect_class_map
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# policy-map type inspect im im_policy_all
ciscoasa(config-pmap)# class yahoo_file_block_list
ciscoasa(config-pmap-c)# match service file-transfer
ciscoasa(config-pmap)# class yahoo_im_policy
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap)# class yahoo_im_policy2
ciscoasa(config-pmap-c)# reset
ciscoasa(config)# policy-map global_policy_name
ciscoasa(config-pmap)# class im_inspect_class_map
ciscoasa(config-pmap-c)# inspect im im_policy_all
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
policy-map	创建第 3/4 层策略映射。
policy-maptypeinspect	创建检查策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。
matchprotocol	匹配检测类或策略映射中的特定 IM 协议。

inspect ip-options

要启用数据包报头中 IP 选项的检测，请在类或策略映射类型检查配置模式下使用 inspect ip-options 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect ip-options [*map_name*]
no inspect ip-options*map_name*

Syntax Description

map_name （可选。）IP选项映射的名称。

Command Default

默认情况下，此命令在全局策略中启用。默认检测映射会允许带有 router-alert 选项的数据包，但会丢弃带有任何其他选项的数据包。

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
策略或类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.2(2)	添加了此命令。支持的选项有 **eoolnop**、、和 **router-alert**选项。如果 IP 报头包含除 EOOL、NOP 或 RTRALT 之外的其他选项，无论 ASA 是否配置为允许这些选项，ASA 都会丢弃该数据包。
9.5(1)	增加了对所有 IP 选项的支持。

使用指南

在数据包中，IP 报头包含选项 (Options) 字段。选项字段，通常称为 IP 选项，提供在某些情况下需要但对于大多数常见通信来说不必要的控制功能。具体来说，IP 选项提供了时间戳、安全性和特殊路由。IP 选项的使用是可选的，并且该字段可以包含零个、一个或多个选项。

您可以配置 IP 选项检测，以便基于数据包信头 IP Options 字段的内容控制允许的 IP 数据包。您可以丢弃包含不需要选项的数据包、清除选项（并允许数据包）或者允许该数据包而不做任何更改。

如果希望进行非默认处理，请创建 IP 选项检测策略映射，输入 **parameter** 命令，然后指定要对各个选项采取的操作。可以检测以下选项。在所有情况下，allow 操作允许包含指定选项且未经过修改的数据包；clear 操作允许包含指定选项的数据包，但会从报头中删除该选项。

使用命 **no**令的形式从地图中删除选项。任何包含映射中未包括的选项的数据包都会被丢弃，即使数据包中包含其他允许或清除的选项。

有关 IP 选项的列表以及相关 RFC 的引用，请参阅 IANA 页面：
http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml 。

- {**defaultactionallow**| **clear**}—为地图中未明确包含的任何选项设置默认操作。如果您未设置允许或清除的默认操作，则包含不允许选项的数据包将被丢弃。
- {**basic-securityactionallow**| **clear**}—允许或清除安全 (SEC) 选项。
- {**commercial-securityactionallow**| **clear**}—允许或清除商业安全 (CIPSO) 选项。
- {**eoolactionallow**| **clear**}—允许或清除选项列表末尾选项。此选项仅包含一个零字节，出现在所有选项的末尾，以标记选项列表的结束。根据标题长度，这可能与标题的末端不一致。
- {**exp-flow-controlactionallow**| **clear**}—允许或清除实验流控制 (FINN) 选项。
- {**exp-measurementactionallow**| **clear**}—允许或清除实验测量 (ZSU) 选项。
- {**extended-securityactionallow**| **clear**}—允许或清除扩展安全 (E-SEC) 选项。
- {**imi-traffic-descriptoractionallow**| **clear**}—允许或清除 IMI 流量描述符 (IMITD) 选项。
- {**nopactionallow**| **clear**}—允许或清除无操作选项。IP 报头中的选项字段可以包含零个、一个或多个选项，这使得该字段的总长度可变。但是，IP报头必须是32位的倍数。如果所有选项的位数不是 32 位的倍数，NOP 选项将被作为“内部填充”，用于对齐 32 位边界上的选项。
- {**quick-startactionallow**| **clear**}—允许或清除快速启动 (QS) 选项。
- {**record-routeactionallow**| **clear**}—允许或清除记录路线 (RR) 选项。
- {**router-alertactionallow**| **clear**}.— 允许或清除路由器警报 (RTRALT) 选项。默认 IP 选项 (IP Options) 检测策略映射允许此选项。此选项通知传输路由器检测数据包的内容，即使数据包未流向该路由器。在实施 RSVP 和类似协议时，这种检查很有价值，因为这些协议需要数据包传送路径上的路由器进行相对复杂的处理。丢弃包含 Router Alert 选项的 RSVP 数据包可能会导致 VoIP 的实施出现问题。
- {**timestampactionallow**| **clear**}—允许或清除时间戳 (TS) 选项。
- {**0-255**} **action**{**allow**| **clear**}—允许或清除由选项类型编号标识的选项。该编号是完整的选项类型，八位数（副本、类和选项编号），而不只是八位数的选项编号部分。这些选项类型可能不代表实际选项。非标准选项必须采用 Internet 协议 RFC 791 (http://tools.ietf.org/html/rfc791) 中定义的预期类型长度值格式。

CR_Examples

以下示例显示如何定义 IP 选项检测策略映射，以允许 ASA 传输数据包报头中包含 EOOL、NOP 和 RTRALT 选项的数据包。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow

ciscoasa(config-pmap-p)# nop action allow

ciscoasa(config-pmap-p)# router-alert action allow
```

以下示例显示如何设置新的默认操作，以允许具有任何 IP 选项的数据包。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action allow
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
policy-map	创建第 3/4 层策略映射。
policy-maptypeinspect	创建检查策略映射。

inspect ipsec-pass-thru

要启用 IPsec 直通检测，请在类映射配置模式下使用 inspect ipsec-pass-thru 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect ipsec-pass-thru [*map_name*]
no inspect ipsec-pass-thru [*map_name*]

Syntax Description

map_name	（可选）IPsec 直通映射的名称。

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

inspect ipsec-pass-thru 命令可以启用或禁用应用检测。IPsec 直通应用程序检查可方便地遍历与 IKE UDP 端口 500 连接相关的 ESP（IP 协议 50）和/或 AH（IP 协议 51）流量。它避免了冗长的访问列表配置以允许 ESP 和 AH 流量，并且还使用超时和最大连接提供安全性。

使用 IPsec 传递参数映射来标识要用于定义检测参数的特定映射。使用 policy-map type inspect 命令访问参数配置，它允许您指定 ESP 或 AH 流量的限制。您可以在参数配置模式下设置每客户端最大连接数和空闲超时。

使用 class-map、policy-map 和 service-policy 命令定义流量类，向该类应用 inspect 命令，以及将策略应用到一个或多个接口。定义的参数映射与 inspect ipsec-pass-thru 命令一起使用时启用。

允许 NAT 流量和非 NAT 流量。但是，不支持 PAT。

注释 在 ASA 7.0(1) 中， **inspect ipsec-pass-thru** 命令仅允许 ESP 流量通过。如果在未指定任何参数的情况下指定 **inspect ipsec-pass-thru** 命令，要在更高版本中保留相同的行为，则会创建并附加一个允许 ESP 的默认映射。此映射可在 show running-config all 命令的输出中看到。

CR_Examples

它避免了冗长的访问列表配置以允许 ESP 和 AH 流量，并且还使用超时和最大连接提供安全性。

```
ciscoasa(config)# access-list ipsecpassthruacl permit udp any any eq 500
ciscoasa(config)# class-map ipsecpassthru-traffic
ciscoasa(config-cmap)# match access-list ipsecpassthruacl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru iptmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
ciscoasa(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
ciscoasa(config)# policy-map inspection_policy
ciscoasa(config-pmap)# class ipsecpassthru-traffic
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru iptmap
ciscoasa(config)# service-policy inspection_policy interface outside
```

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。
matchprotocol	匹配检测类或策略映射中的特定 IM 协议。

inspect ipv6

要启用 IPv6 检测，请在类配置模式下使用 inspect ipv6 命令。可从策略映射配置模式访问类配置模式。要删除配置，请使用此命令 **no**的形式。

inspect ipv6 [*map_name*]
no inspect ipv6 [*map_name*]

Syntax Description

map_name	（可选。）IPv6检测策略映射的名称。

Command Default

默认情况下，IPv6 检查是禁用的。

如果启用 IPv6 检测但不指定检测策略映射，将会使用默认 IPv6 检测策略映射并执行以下操作：

- 仅允许已知的 IPv6 扩展报头。丢弃并记录不符合要求的数据包。
- 按照 RFC 2460 规范的规定实施 IPv6 扩展报头顺序。丢弃并记录不符合要求的数据包。
- 丢弃带有路由类型报头的任何数据包。

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

IPv6 检测根据扩展报头有选择性地记录或丢弃 IPv6 流量。此外，IPv6 检测可以检查 Pv6 数据包中扩展报头的类型和顺序是否符合 RFC 2460 的要求。

CR_Examples

以下示例丢弃所有带有逐跳、目标选项、路由地址和路由类型 0 标头的 IPv6 流量：

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop
 match header destination-option
  drop
 match header routing-address count gt 0
```

```
  drop
 match header routing-type eq 0
  drop
policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
匹配报头	匹配 IPv6 检测策略映射中的 IPv6 报头。
policy-maptypeinspectipv6	为 IPv6 创建检查策略图。
policy-map	创建第 3/4 层策略映射。
verify-header	配置 IPv6 检测参数。

inspect lisp

要启用 LISP 检查，请在 **inspectlisp** 类配置模式下使用该命令。您可以通过首先输入命令来访问类配置 **policy-map**模式。要禁用 LISP 检查，请使用此**no**命令的形式。

inspect lisp [*inspect_map_name*]
no inspect lisp [*inspect_map_name*]

Syntax Description

inspect_map_name	如果要限制 EID 或需要为 LISP 消息指定预共享密钥，请指定 LISP 检测映射名称 (**policy-maptypeinspectlisp**)。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.5(2)	我们添加了此命令。

使用指南

ASA 会检测 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。

关于集群流移动性的 LISP 检查

ASA 检测 LISP 流量是否发生位置更改，然后使用此信息进行无缝集群操作。如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

集群流移动性包含多种相互关联的配置：

1. （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。请参阅 **policy-maptypeinspectlisp**、 **allowed-eid,** 和 **validate-key**命令。
2. LISP 流量检查 - ASA 检查 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。查看 **inspectlisp**命令。

3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。查看命令。 **clusterflow-mobilitylisp**
4. 站点 ID - ASA 使用每个集群设备的站点 ID 确定新的所有者。查看命令。 **site-id**
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。查看命令。 **flow-mobilitylisp**

CR_Examples

以下示例检查位于 192.168.50.89 的 LISP 路由器（位于内部）与位于 192.168.10.8 的 ITR 或 ETR 路由器（位于另一个 ASA 接口上）之间的 LISP 流量（UDP 4342）：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

Related Commands

命令	说明
allowed-eids	基于 IP 地址限制检测到的 EID。
clear cluster info flow-mobility counters	清除流移动性计数器。
clear lisp eid	从 ASA EID 表中删除 EID。
cluster flow-mobility lisp	为服务策略启用流移动性。
flow-mobility lisp	为集群启用流移动性。
inspect lisp	检测 LISP 流量。
policy-map type inspect lisp	定制 LISP 检测。
site-id	为集群机箱设置站点 ID。
show asp table classify domain inspect-lisp	显示 LISP 检测的 ASP 表。
show cluster info flow-mobility counters	显示流移动性计数器。
show conn	显示受 LISP 流移动性影响的流量。
show lisp eid	显示 ASA EID 表。
show service-policy	显示服务策略。
validate-key	输入预共享密钥以验证 LISP 消息。

inspect m3ua

要启用 M3UA 检测，请在类配置模式下使用 **inspectm3ua** 命令。可以从 map configuration 模式访问 Class configuration 模式。使用此命令的 **no** 形式可禁用 M3UA 检测。

inspect m3ua [*map_name*]
no inspect m3ua [*map_name*]

注释 M3UA 检查需要运营商许可证。

Syntax Description

map_name （可选）M3UA 检测策略映射的名称。

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

MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接 SS7 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。M3UA 在 RFC 4666 中定义。

M3UA 使用 SCTP 作为传输层。SCTP 端口 2905 是预期端口，但可以配置信令网关使用不同的端口。

MTP3 层提供网络功能，例如路由和节点寻址，但使用点代码来识别节点。M3UA 层可交换源点码 (OPC) 和目标点码 (DPC)。这与 IP 使用 IP 地址识别节点的方式类似。

M3UA 检测提供的协议符合具有限制性。

您可以选择创建 M3UA 检查策略图，以根据点代码或服务指标 (SI) 应用访问策略。此外，还可以基于消息类和类型应用速率限制。

CR_Examples

以下示例显示了 M3UA 检测策略映射和检测策略。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasahostname(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect m3ua m3ua-map
ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
showservice-policyinspectm3ua	显示检查M3UA策略的状态和统计信息。

inspect mgcp

要启用 MGCP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect **mgcp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect mgcp [*map_name*]
no inspect mgcp [*map_name*]

Syntax Description

map_name （可选）MGCP映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

要使用MGCP，您通常至少需要配置至少两个**inspect**命令：一个用于网关接收命令的端口，另一个用于呼叫代理接收命令的端口。通常，呼叫代理将命令发送到网关的默认 MGCP 端口 (2427)，而网关将命令发送到呼叫代理的默认 MGCP 端口 (2727)。

MGCP 用于从称为媒体网关控制器或呼叫代理的外部呼叫控制元件控制媒体网关。媒体网关通常是一个网络元素，用于在电话电路上传送的音频信号和互联网上或其他数据包网络上传送的数据包之间提供转换。借助具有 MGCP 的 NAT 和 PAT，可以使用一组有限的外部（全局）地址来支持内部网络中的大量设备。

媒体网关示例如下：

- 中继网关：用于在电话网络和IP语音网络之间建立连接。这种网关通常管理大量的数字电路。
- 家庭网关：提供用于连接到IP语音网络的传统模拟(RJ11)接口。住宅网关的示例包括电缆调制解调器/电缆机顶盒、xDSL 设备和宽带无线设备。
- 商业网关，为 IP 语音网络提供传统的数字 *PBX* 接口或集成的软 PBX 接口。

MGCP 消息通过 UDP 传输。响应会发送回命令的源地址（IP 地址和 UDP 端口号），但响应可能不会到达收到命令的同一地址。如果在同一故障转移配置中使用多个呼叫代理，且接收命令的呼叫代理已经将控制转交给备用呼叫代理，由备用呼叫代理来发送响应，可能会发生这种情况。

注释 MGCP呼叫代理发送AUEP消息，以确定MGCP终端是否存在。这样将通过ASA建立一个数据流，并允许 MGCP 终端注册到呼叫代理。

在 MGCP 映射配置模式下使用 **call-agent** 和 **gateway** 命令配置一个或多个呼叫代理和网关的 IP 地址。在MGCP映射配置模式下，使用**command-queue**命令可指定命令队列中一次允许的最大MGCP命令数。

检查信令消息

要检查信令消息，**inspectmgcp**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和NAT状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspectmgcp**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用**route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspectmgcp**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

可排队的 MGCP 命令的最大数量为 150。

CR_Examples

以下示例显示如何识别 MGCP 流量、定义 MGCP 检查图、定义策略以及将策略应用于外部接口。这样将创建一个类映射，以便匹配默认端口（2427 和 2727）上的 MGCP 流量。然后，服务策略会被应用到外部接口。此配置允许呼叫代理 10.10.11.5 和 10.10.11.6 控制网关 10.10.10.115，并允许呼叫代理 10.10.11.7 和 10.10.11.8 控制两个网关 10.10.10.116 和 10.10.10.117。要对所有接口启用 MGCP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2427

ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2727
ciscoasa(config)# class-map mgcp_port
ciscoasa(config-cmap)# match access-list mgcp_acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect mgcp inbound_mgcp
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-agent 10.10.11.5 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.6 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.7 102
ciscoasa(config-pmap-p)# call-agent 10.10.11.8 102
ciscoasa(config-pmap-p)# gateway 10.10.10.115 101
ciscoasa(config-pmap-p)# gateway 10.10.10.116 102
ciscoasa(config-pmap-p)# gateway 10.10.10.117 102
ciscoasa(config-pmap-p)# command-queue 150
ciscoasa(config-mgcp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class mgcp_port
ciscoasa(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-maptypeinspectmgcp	为 MGCP 创建检查策略图。
showmgcp	显示通过 ASA 建立的 MGCP 会话的相关信息。
timeout	为不同协议和会话类型设置最大空闲持续时间。

inspect mmp

要配置 MMP 检测引擎，请在类配置模式下使用 **inspectmmp** 命令。要删除 MMP 检查，请使用此 **no** 命令的形式。

inspect mmp tls-proxy [名称]
no inspect mmp tls-proxy [名称]

Syntax Description

name	指定 TLS 代理实例名称。
tls-proxy	为 MMP 检测启用 TLS 代理。MMP 协议可以额外使用 TCP 传输；但是，CUMA 客户端仅支持 TLS 传输。因此，要启用 MMP 检测，必须使用 **tls-proxy** 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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.0(4)	命令已添加。

使用指南

ASA 包括用于验证 CUMA 移动多路复用协议 (MMP) 的检测引擎。MMP 是一种用于在 CUMA 客户端与服务器之间传输数据实体的数据传输协议。当 ASA 部署在 CUMA 客户端与 服务器之间并需要检测 MMP 数据包时，请使用 **inspectmmp** 命令。

由于 MMP 流量只能通过 TLS 连接传输，因此必须带 TLS 代理启用 MMP 检测。

注释 请注意，在配置 MMP 检测引擎时，它只能添加到非默认检测类下。

CR_Examples

以下示例展示如何使用 **inspectmmp**命令检测 MMP 流量：

```
ciscoasa
(config)#
class-map mmp
```

```
ciscoasa
(config-cmap)#
match port tcp eq 5443
ciscoasa
(config-cmap)#
exit
ciscoasa
(config)#
policy-map mmp-policy
ciscoasa
(config-pmap)#
class mmp
ciscoasa(config-pmap-c)# inspect mmp tls-proxy myproxy
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa
(config)#
service-policy mmp-policy interface outside
```

Related Commands

命令	说明
tls-proxy	配置 TLS 代理实例。

inspect netbios

要启用 NetBIOS 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect netbios **command**。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect netbios [*map_name*]
no inspect netbios [*map_name*]

Syntax Description

map_name （可选）NetBIOS 映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

inspectnetbios 命令启用或禁用 NetBIOS 协议的应用检查。默认情况下，NetBIOS 检测处于启用状态。NetBIOS 检查引擎根据 ASA NAT 配置转换 NetBIOS 名称服务 (NBNS) 数据包中的 IP 地址。或者可以创建策略映射以便丢弃或记录 NetBIOS 协议违规情况。

CR_Examples

以下示例显示如何定义 NetBIOS 检查策略映射：

```
ciscoasa(config)# policy-map type inspect netbios netbios_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation drop
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
policy-maptypeinspectnetbios	为 NetBIOS 创建检查策略图。
service-policy	将策略映射应用到一个或多个接口。

inspect pptp

要启用 PPTP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect **pptp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect pptp
no inspect pptp

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

点对点隧道协议 (PPTP) 是用于通过隧道传送 PPP 流量的协议。PPTP 会话通常包括一个 TCP 信道和两个 PPTP GRE 隧道。TCP 信道是用于协商和管理 PPTP GRE 隧道的控制信道。GRE 隧道承载两台主机之间的 PPP 会话。

启用后，PPTP 应用检测会检查 PPTP 协议数据包，并动态创建允许 PPTP 流量所需的 GRE 连接和转换。仅支持 RFC 2637 中定义的版本 1。

仅当通过 PPTP TCP 控制通道进行协商时，才会对 GRE 的修改版本 [RFC 2637] 执行 PAT。未修改版本的 GRE [RFC 1701、RFC 1702] 不执行端口地址转换。

特别是，ASA 会检测 PPTP 版本通知和对外呼叫请求/响应序列。仅检查 RFC 2637 中定义的 PPTP 版本 1。如果任一端公布的版本不是版本 1，将会禁用对 TCP 控制信道的进一步检测。此外，还会跟踪传出呼叫请求和应答序列。连接和 xlate 根据需要动态分配，以允许后续的辅助 GRE 数据流量。

要以 PAT 方式转换 PPTP 流量，必须启用 PPTP 检测引擎。此外，仅对符合如下条件的 GRE 版本执行 PAT：经过修改的（如 RFC2637 所要求）；且是通过 TCP 控制信道协商的。未修改版本的 GRE（RFC 1701 和 RFC 1702）不会执行 PAT。

如 RFC 2637 中所述，PPTP 协议主要用于将从调制解调器组 PAC（PPTP 访问集中器）发起的 PPP 会话隧道传送到头端 PNS（PPTP 网络服务器）。按这种方式使用时，PAC 为远程客户端，而 PNS 为服务器。

但是，当 Windows 用于 VPN 时，交互作用是反向的。PNS 是一种远程单用户 PC，用于启动与头端 PAC 的连接以获取对中央网络的访问权限。

要对所有接口启用 PPTP 检测，请使用 **global** 参数代替 **interfaceoutside**。

CR_Examples

如以下例所示，启用 PPTP 检测引擎，该引擎创建一个类映射来匹配默认端口 (1723) 上的 PPTP 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map pptp-port
ciscoasa(config-cmap)# match port tcp eq 1723
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pptp_policy
ciscoasa(config-pmap)# class pptp-port
ciscoasa(config-pmap-c)# inspect pptp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy pptp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect radius-accounting

要启用或禁用 RADIUS 计费检测，或者要定义用于控制流量或隧道的映射，请在类配置模式下使用 **inspectradius-accounting** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect radius-accounting*map_name*
no inspect radius-accounting [*map_name*]

Syntax Description

map_name	RADIUS计费映射的名称。

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

RADIUS 计费检测是为了防止使用 RADIUS 服务器的 GPRS 网络上出现过度计费攻击。虽然实施 RADIUS 计费检测无需 GTP/GPRS or Carrier 许可证，但它毫无意义，除非您正在实施 GTP 检测并已设置 GPRS。

使用 **policy-maptypeinspectradius-accounting**命令创建检测映射，以用于定义 RADIUS 计费的参数。输入 parameters 命令后，您可以使用 **sendresponse**、 **host**、 **validate-attribute**、 **enablegprs**和 **timeoutusers** 命令定义检测特征和行为。

然后使用 **class-maptypemanagement**、 **policy-map**和 **service-policy** 命令定义流量类，向该类应用 inspect radius-accounting 命令，并将策略应用到一个或多个接口。

注释 **inspectradius-accounting** 命令只能与 **class-maptypemanagement** 命令一起使用。

CR_Examples

以下示例显示如何配置 RADIUS 计费检测映射并全局启用检测。

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

Related Commands

命令	说明
parameters	定义要应用的安全操作的流量类。
class-maptypemanagement	用于标识流向要应用操作的 ASA 的第 3 层或第 4 层管理流量。
policy-maptypeinspectradius-accounting	为 RADIUS 计费创建检查策略图。
show和**clearservice-policy**	允许您查看和清除服务策略设置。
service-policy	将策略映射应用到一个或多个接口。

inspect rsh

要启用 RSH 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect **rsh** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect rsh
no inspect rsh

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务器协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要，RSH 检测支持协商端口号的 NAT。

CR_Examples

以下示例启用 RSH 检测引擎，创建类映射以匹配默认端口 (514) 上的 RSH 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 RSH 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map rsh-port
ciscoasa(config-cmap)# match port tcp eq 514
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rsh_policy

ciscoasa(config-pmap)# class rsh-port
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rsh_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect rtsp

要启用 RTSP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect **rtsp** 命令。可从策略映射配置模式访问类配置模式。要删除配置，请使用此命令 **no**的形式。

inspect rtsp [*map_name*]
no inspect rtsp [*map_name*]

Syntax Description

map_name （可选）RTSP 映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

inspectrtsp 命令允许 ASA 传递 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer 和思科 IP/TV 连接都使用 RTSP。

注释 对于 Cisco IP/TV，使用 RTSP TCP 端口 554 和 TCP 8554。

RTSP 应用使用已知 TCP（很少用 UDP）端口 554 作为控制信道。根据 RFC 2326 要求，ASA 仅支持 TCP。此 TCP 控制通道用于协商将用于传输音频/视频流量的数据通道，具体取决于客户端上配置的传输模式。

支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp 和 x-pn-tng/udp。

ASA 解析状态代码为 200 的设置响应消息。如果响应消息要入站，服务器需相对于 ASA 处于外部，并需要为连接从服务器进入站内打开动态信道。如果响应消息要出站，则 ASA 无需打开动态信道。

由于 RFC 2326 不要求客户端和服务器端口必须位于设置响应消息中，因此 ASA 需要保持状态并记住设置消息中的客户端端口。QuickTime 将客户端端口放在设置消息中，然后服务器仅使用服务器端口进行响应。

使用 RealPlayer

使用RealPlayer时，正确配置传输模式非常重要。对于ASA，从服务器向客户端添加命**access-list**令语句，反之亦然。对于 RealPlayer，请通过以下选择更改传输模式 **Options**： 、 **Preferences**、**Transport**、 **RTSPSettings**。

如果 RealPlayer 使用 TCP 模式，请选中 **UseTCPtoConnecttoServer** 和 **AttempttouseTCPforallcontent** 复选框。在 ASA 上无需配置检测引擎。

If using UDP mode on the RealPlayer, check the **UseTCPtoConnecttoServer** and **AttempttouseUDPforstaticcontent** check boxes, and for live content not available via Multicast. 在 ASA 中添加 **inspectrtsp**端口 命令语句。

限制和局限性

RSTP 检测有以下局限性。

- ASA 不支持通过 UDP 的组播 RTSP 或 RTSP 消息。
- ASA 无法识别 RTSP 消息隐藏在 HTTP 消息中的 HTTP 掩蔽技术。
- ASA 无法对 RTSP 消息执行 NAT，因为嵌入式 IP 地址作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中。数据包可以分段，但 ASA 无法对分段的数据包执行 NAT。
- 对于思科 IP/TV，ASA 对消息 SDP 部分可执行的转换数与内容管理器中的程序列表数呈正比（每个程序列表至少可包含六个嵌入式 IP 地址）。
- 可以为 Apple QuickTime 4 或 RealPlayer 配置 NAT。如果查看器和内容管理器位于外部网络，而服务器位于内部网络，则思科 IP/TV 只能采用 NAT。

CR_Examples

以下示例启用RTSP检测引擎，该引擎创建类映射来匹配默认端口（554和8554）上的RTSP流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 554

ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 8554
ciscoasa(config)# class-map rtsp-traffic

ciscoasa(config-cmap)# match access-list rtsp-acl

ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rtsp_policy

ciscoasa(config-pmap)# class rtsp-traffic
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rtsp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect scansafe

要对类中的流量启用云网络安全检测，请在类配置模式下使用 **inspectscansafe**命令。您可以通过首先输入命令来访问类配置 **policy-map**模式。要删除检查操作，请使用此命 **no**令的形式。

inspect scansafe*scansafe_policy_name* [**fail-open** | **fail-close**]
no inspect scansafe*scansafe_policy_name* [**fail-open** | **fail-close**]

Syntax Description

scansafe_policy_name	指定由 **policy-maptypeinspectscansafe** 命令定义的检测类映射名称。
fail-open	（可选）如果云网络安全服务器不可用，则允许流量通过 ASA。
fail-close	（可选）如果云网络安全服务器不可用，则丢弃所有流量。**fail-close**是默认设置。

Command Default

fail-close 为默认值。

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	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

思科云网络安全通过软件即服务 (SaaS) 模式提供 Web 安全和 Web 过滤服务。如果企业的网络中配备 ASA，不必额外安装硬件即可使用云网络安全服务。

注释 此功能也称为“ScanSafe”，因此某些命令中会显示 ScanSafe 名称。

使用模块化策略框架配置此命令：

1. 使用**policy-maptypeinspectscansafe**命令创建检测策略映射，至少一个用于 HTTP，一个用于 HTTPS（假设您要检测两种类型的流量）。
2. （可选）使 **class-maptypeinspectscansafe**用命令配置白名单。
3. 使用 the **class-map** 命令定义要检测的流量。您必须为 HTTP 和 HTTPS 流量配置单独的类映射。

4. 输入 **policy-map** 命令以定义策略。
5. 对于 HTTP，请输入 **class** 命令以引用 HTTP 类映射。
6. 输入引用 HTTP 检测策略映射的 **inspectscansafe**命令。
7. 对于 HTTPS，请输入 **class** 命令以引用 HTTPS 类映射。
8. 输入引用 HTTPS 检测策略映射的 **inspectscansafe**命令。
9. 最后，使用命令将策略映射应用到接 **service-policy**口。

CR_Examples

以下示例配置两个类：一个是 HTTP 流量类，一个是 HTTPS 流量类。每个 ACL 都可以使 HTTP 和 HTTPS 流量免于被发送到 www.cisco.com 和 tools.cisco.com，以及 DMZ 网络。所有其他流量将被发送到云网络安全，但来自若干白名单用户和组的流量除外。然后，策略将被应用到内部接口。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# object network cisco1
ciscoasa(config-object-network)# fqdn www.cisco.com
ciscoasa(config)# object network cisco2
ciscoasa(config-object-network)# fqdn tools.cisco.com
ciscoasa(config)# object network dmz_network
ciscoasa(config-object-network)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
ciscoasa(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443
ciscoasa(config)# class-map cws_class1
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTP
ciscoasa(config)# class-map cws_class2
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTPS
ciscoasa(config)# policy-map cws_policy
ciscoasa(config-pmap)# class cws_class1
```

```
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
ciscoasa(config-pmap)# class cws_class2
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
ciscoasa(config)# service-policy cws_policy inside
```

Related Commands

命令	说明
class-maptypeinspectscansafe	为加入白名单的用户和组创建检查类映射。
defaultusergroup	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和/或组。
[**https**]（参数）	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspectscansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器的身份验证密钥，以指示请求来自哪个组织。
matchusergroup	匹配白名单的用户或组。
policy-maptypeinspectscansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前等待的时间。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafegeneral-options	配置常规云网络安全服务器选项。
server{**primary**| **backup**}	配置主或备份云网络安全代理服务器的完全限定域名或 IP 地址。
showconnscansafe	显示所有云网络安全连接，标有大写 Z 标志。
showscansafeserver	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
showscansafestatistics	显示总计和当前 HTTP 连接数。
user-identitymonitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

检查 SCTP

要启用或禁用流控制传输协议 (SCTP) 检测，请在类配置模式下使用 **inspectsctp** 命令。可以从 map configuration 模式访问 Class configuration 模式。使用此命 **no**令的形式可以禁用 SCTP 检查。

inspect sctp [*map_name*]
no inspect sctp [*map_name*]

注释 SCTP 检查需要运营商许可证。

Syntax Description

map_name （可选）SCTP 检测策略映射的名称。

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

SCTP（流控制传输协议）支持电话信令协议 SS7，也是 4G LTE 移动网络架构中多个接口的传输协议。如果有移动网络流量通过 设备，则可以使用 SCTP 检测以及 GTP 和 Diameter 检测。

如果要过滤 SCTP 应用以提供可变服务，可以选择性地指定 SCTP 策略映射。您可以根据负载协议标识符 (PPID)，选择性地丢弃、记录或按速率限制 SCTP 流量类。使用 **policy-maptypeinspectsctp** 命令创建策略映射。

CR_Examples

以下示例创建的检测策略映射将丢弃未分配的 PPID（写入此示例时未分配）、按速率限制 PPID 32-40，并记录 Diameter PPID。该服务策略会对向匹配所有 SCTP 流量的 inspection_default 类应用检测。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
```

```
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log
policy-map global_policy
 class inspection_default
  inspect sctp sctp-pmap
!
service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
clearservice-policyinspectsctp	清除全局 SCTP 统计信息。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
showservice-policyinspectsctp	显示 inspect sctp 策略的状态和统计信息。

inspect sip

要启用 SIP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect **sip**命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect sip [*sip_map*] [**tls-proxy***proxy_name*] [**phone-proxy***proxy_name*] [**uc-ime***proxy_name*]
no inspect sip [*sip_map*] [**tls-proxy***proxy_name*] [**phone-proxy***proxy_name*] [**uc-ime***proxy_name*]

Syntax Description

phone-proxy*proxy_name*	为指定的检测会话启用电话代理。
sip_map	指定 SIP 策略映射名称。
tls-proxy*proxy_name*	为指定的检测会话启用 TLS 代理。关键字 **tls-proxy** 不能用作第 7 层策略映射名称。
uc-ime*proxy_name*	为 SIP 检查启用思科公司间媒体引擎代理。

Command Default

默认情况下，SIP 检测已通过默认检测映射启用，具体以下：

- SIP 即时消息 (IM) 扩展：已启用。
- SIP 端口的非 SIP 流量：允许。
- 隐藏服务器和终端的 IP 地址：已禁用。
- 掩蔽软件版本和非 SIP URI：已禁用。
- 确保到目标的跳数大于 0：已启用。
- RTP 符合性：未执行。
- SIP 符合性：不执行状态检查和报头验证。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

SIP 的默认端口分配是 5060。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。
8.0(2)	添加了 tls-proxy 关键字。
9.4(1)	删除了 **phone-proxy** 和 **uc-ime** 关键字。

使用指南

SIP是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。部分原因是SIP本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。

SIP 应用检测会在消息信头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。SIP应用检测还支持应用安全和协议符合性（此功能强制对SIP消息进行健全性检查，以及检测基于 SIP 的攻击）。

默认情况下，SIP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。

为了支持 SIP 呼叫通过 ASA，必须检测媒体连接地址、媒体端口和媒体初期连接的信令消息，因为在已知目标端口 (UDP/TCP 5060) 上发送信令时，系统会动态分配媒体流。此外，SIP 还会在 IP 数据包的用户数据部分嵌入 IP 地址。SIP 检查对这些嵌入式 IP 地址应用 NAT。

SIP 检查的限制

SIP 检测适用于嵌入式 IP 地址的 NAT。但是，如果配置 NAT 来转换源地址和目标地址，将不会重写外部地址（“trying”响应消息的 SIP 报头中的“from”）。因此，在处理 SIP 流量时应使用对象 NAT，从而避免转换目标地址。

当与 SIP 结合使用 PAT 时，有以下限制和限定：

- 如果远程终端尝试在 ASA 保护的网络上注册 SIP 代理，在非常特殊的条件下注册会失败，如下所示：
  - 对远程终端配置了 PAT。
  - SIP 注册服务器位于外部网络。
  - 在终端发送给代理服务器的 REGISTER 消息中，联系人字段中的端口缺失。
- 如果在 SIP 设备传输数据包时，该数据包的 SDP 部分的所有者/创建者字段 (o=) 中的 IP 地址与连接字段 (c=) 中的 IP 地址不同，则可能未正确转换 o= 字段中的 IP 地址。这是 SIP 协议的如下局限性造成的：不在 o= 字段中提供端口值。
- 使用 PAT 时，任何包含无端口的内部 IP 地址的 SIP 报头字段都可能不会转换，因此，内部 IP 地址将向外泄漏。如果要避免这种泄漏，请配置 NAT 来代替 PAT。

检查信令消息

要检查信令消息，**inspectsip**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和NAT状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspectsip**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspectsip**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 SIP 检测引擎，该引擎创建类映射来匹配默认端口 (5060) 上的 SIP 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 SIP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map sip-port
ciscoasa(config-cmap)# match port tcp eq 5060
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sip_policy

ciscoasa(config-pmap)# class sip-port
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sip_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-maptypeinspectsip	为 SIP 创建检查策略图。
showsip	显示通过 ASA 建立的 SIP 会话的相关信息。
showconn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。
tls-proxy	定义 TLS 代理实例并设置最大会话数。

inspect skinny

要启用 SCCP（瘦客户端）应用检测，请在类配置模式下使用 inspect **skinny**命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect skinny[*skinny_map*][**tls-proxy***proxy_name*][**phone-proxy***proxy_name*]
no inspect skinny[*skinny_map*][**tls-proxy***proxy_name*][**phone-proxy***proxy_name*]

Syntax Description

phone-proxy*proxy_name*	为检测会话启用电话代理。
Skinny_map	指定 Skinny 策略映射名称。
tls-proxy*proxy_name*	为检测会话启用 TLS 代理。

Command Default

默认情况下，SCCP 检测已启用，默认设置如下：

- 注册：未执行。
- 最大消息 ID：0x181。
- 最小前缀长度：4
- 媒体超时：00:05:00
- 信令超时：01:00:00。
- RTP 符合性：未执行。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。
8.0(2)	已添加关键 **tls-proxy**字。
9.4(1)	该关 **phone-proxy**键字已被弃用。
9.13(1)	该关**tls-proxy**键字已被弃用。该关键字将在未来的版本中被删除。

版本	修改
9.14(1)	已删除 **tls-proxy** 关键字，以及对 SCCP/Skinny 加密检测的支持。

使用指南

瘦客户端 (SCCP) 是用于 VoIP 网络的简化协议。使用 SCCP 的思科 IP 电话可共存于 H.323 环境中。与 Cisco CallManager 一起使用时，SCCP 客户端可以与符合 H.323 的终端进行互操作。

对于 SCCP，ASA 支持 PAT 和 NAT。如果要使用的 IP 电话多于 IP 电话可使用的全局 IP 地址，必须进行 PAT。通过支持 SCCP 信令数据包的 NAT 和 PAT，瘦应用检测可确保所有 SCCP 信令和媒体数据包均可通过 ASA。

Cisco CallManager 与思科 IP 电话之间的正常流量使用 SCCP，这些流量由 SCCP 检测处理，无需任何特殊配置。另外，ASA 还支持 DHCP 选项 150 和 66，将 TFTP 服务器的位置发送到思科 IP 电话及其他 DHCP 客户端即可完成操作。思科 IP 电话可能在请求中还包含 DHCP 选项 3（该选项用于设置默认路由）。

注释 ASA 支持检测来自运行 SCCP 协议版本 22 及更早版本的思科 IP 电话的流量。

支持 Cisco IP 电话

在思科 CallManager 位于思科 IP 电话较高安全性接口的拓扑中，如果需要对思科 CallManager IP 地址执行 NAT，则映射必须为静态，因为思科 IP 电话需要在其配置中显式指定思科 CallManager IP 地址。静态身份条目使位于安全性较高的接口的 Cisco CallManager 可以接受来自思科 IP 电话的注册。

Cisco IP 电话需要访问 TFTP 服务器来下载连接到 Cisco CallManager 服务器所需的配置信息。

当思科 IP 电话位于比 TFTP 服务器低的安全接口上时，必须使用 ACL 来与 UDP 端口 69 上的受保护 TFTP 服务器连接。虽然需要对 TFTP 服务器使用静态条目，但该静态条目不一定必须是身份静态条目。使用 NAT 时，身份静态条目会映射到同一 IP 地址。使用 PAT 时，它会映射到同一 IP 地址和端口。

当 Cisco IP 电话位于比 TFTP 服务器和 Cisco CallManager 安全性更高的接口上时，不需要 ACL 或静态条目即可允许 Cisco IP 电话发起连接。

限制和局限性

如果将内部 Cisco CallManager 的地址配置为通过 NAT 或 PAT 指向不同的 IP 地址或端口，则外部 Cisco IP 电话的注册将失败，因为 ASA 当前不支持通过 TFTP 传输文件内容的 NAT 或 PAT。虽然 ASA 支持 TFTP 消息的 NAT 并会为 TFTP 文件打开针孔，但在电话注册期间，ASA 无法转换通过 TFTP 传输的思科 IP 电话配置文件中嵌入的思科 CallManager IP 地址和端口。

注释 ASA 支持 SCCP 呼叫的状态故障转移，但呼叫建立过程中的呼叫除外。

检查信令消息

要检查信令消息，**inspectskinny**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和NAT状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspectskinny**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspectskinny**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 SCCP 检测引擎，创建类映射以匹配默认端口 (2000) 上的 SCCP 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 SCCP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map skinny-port
ciscoasa(config-cmap)# match port tcp eq 2000
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map skinny_policy

ciscoasa(config-pmap)# class skinny-port
ciscoasa(config-pmap-c)# inspect skinny
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy skinny_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-maptypeinspectskinny	为 SCCP 创建检查策略图。
showskinny	显示通过 ASA 建立的 SCCP 会话的相关信息。
showconn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。
tls-proxy	定义 TLS 代理实例并设置最大会话数。

inspect snmp

要启用 SNMP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspect **snmp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect snmp [*map_name*]
no inspect snmp [*map_name*]

Syntax Description

map_name	SNMP映射的名称。

Command Default

从 9.14(1) 开始，此命令默认启用。它在以前的版本中默认被禁用。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.14(1)	命令默认已启用，并且 SNMP 映射变为可选项。

使用指南

从 9.14(1) 开始，SNMP 应用程序检查适用于到设备的流量和通过设备的流量。如果您配置的 SNMP v3 将用户限制在特定 SNMP 主机上，则必须进行此检测。如果未检测，定义的 v3 用户可以从任何允许的主机轮询设备。默认端口已启用 SNMP 检测，因此只有在使用非默认端口时才需要进行配置。默认端口为 UDP/161、162（适用于所有设备类型）和 UDP/4161（适用于同时运行安全防火墙可扩展操作系 统 (FXOS) 的设备），因为 FXOS 在 UDP/161 上监听。

在 9.14(1) 之前的版本中，默认情况下未启用 SNMP 检测，并且它仅适用于通过设备的流量。

SNMP 应用程序检查还允许您将 SNMP 流量限制为特定版本的 SNMP。SNMP 早期版本的安全性较低；因此，安全策略可能要求拒绝使用某些 SNMP 版本。系统可能会拒绝 SNMP 1、2、2c 或 3 版本。要拒绝特定版本的 SNMP，请在您使用 **denyversion** 命令创建的 SNMP 映射中使用 **snmp-map** 命令。配置 SNMP 映射后，您可使用 **inspectsnmp** 命令启用映射，然后使用 **service-policy** 命令将其应用到一个或多个接口。

从9.14(1)开始，如果您不需要控制版本，只需启用SNMP检查而无需地图。在以前的版本中，需要使用映射。

CR_Examples

以下示例识别 SNMP 流量，定义 SNMP 映射，定义策略，启用 SNMP 检测，并将策略应用到外部接口：

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy

ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
denyversion	禁止使用特定版本 SNMP 的流量。
snmp-map	定义 SNMP 映射并启用 SNMP 映射配置模式。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect sqlnet

要启用 Oracle SQL*Net 应用检测，请在类配置模式下使用 inspect **sqlnet** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect sqlnet
no inspect sqlnet

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。

默认端口分配为 1521。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

SQL*Net 协议由不同的数据包类型组成，ASA 处理这些数据包类型，以使数据流对于 ASA 两侧的 Oracle 应用程序而言保持一致。

SQL*Net 的默认端口赋值为 1521。这是 Oracle 用于 SQL*Net 的值，但是，该值与结构化查询语言 (SQL) 的 IANA 端口赋值不符。使用该 **class-map**命令将 SQL*Net 检查应用于一系列端口号。

注释 当与 SQL 控制 TCP 端口 1521 相同的端口上发生 SQL 数据传输时，请禁用 SQL*Net 检测。当启用 SQL*Net 检查时，ASA 充当代理，并将客户端窗口大小从 65000 减少到大约 16000，从而导致数据传输问题。

ASA NAT 所有地址并在数据包中查找为 SQL*Net 版本 1 打开的所有嵌入式端口。

对于 SQL*Net 版本 2，系统将修复紧跟 REDIRECT 数据包且数据长度为零的所有 DATA 或 REDIRECT 数据包。

需要修复的数据包包含以下格式的嵌入式主机/端口地址：

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

将不在 SQL*Net 版本 2 TNSFrame 类型（连接、接受、拒绝、重新发送和标记）中扫描 NAT 地址，检测也将不为数据包中的任何嵌入式端口打开动态连接。

如果负载前面是数据长度为零的 REDIRECT TNSFrame 类型，则将在 SQL*Net 版本 2 TNSFrames、Redirect 和 Data 数据包中扫描要打开的端口和 NAT 地址。当数据长度为零的重定向消息通过 ASA 时，将在连接数据结构中设置一个标志，以期望随后的数据或重定向消息被 NAT 并且端口被动态打开。如果前段中的一个 TNS 帧在 Redirect 消息后到达，则会重置标志。

SQL*Net 检测引擎将使用新旧消息的长度差异，重新计算校验和，更改 IP、TCP 长度，并重新调整序列号和确认号。

在所有其他情况下假设使用 SQL*Net 版本 1。系统将在 TNSFrame 类型（连接、接受、拒绝、重新发送、标记、重定向和数据）和所有数据包中扫描端口和地址。地址将被 NAT 并且端口连接将被打开。

CR_Examples

以下示例启用 SQL*Net 检测引擎，该引擎创建类映射以匹配默认端口 (1521) 上的 SQL*Net 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 SQL*Net 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map sqlnet-port
ciscoasa(config-cmap)# match port tcp eq 1521
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sqlnet_policy

ciscoasa(config-pmap)# class sqlnet-port
ciscoasa(config-pmap-c)# inspect sqlnet
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sqlnet_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。
showconn	显示不同连接类型的连接状态，包括 SQL*net。

inspect stun

要启用 NAT 会话实用程序 (STUN) 应用检测，请在类配置模式下使用 inspect **stun** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect stun
no inspect stun

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

默认端口分配为 TCP/3478 和 UDP/3478。

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

WebRTC 客户端使用 RFC 5389 中定义的 NAT 会话穿越工具 (STUN) 进行基于浏览器的实时通信，因而不需要插件。WebRTC 客户端通常使用云 STUN 服务器获悉它们的公共 IP 地址和端口。WebRTC 使用交互式连接建立（ICE，RFC 5245）来验证客户端之间的连接。虽然这些客户端可以使用 TCP 或其他协议，但它们通常使用 UDP。

由于防火墙通常会阻止传出 UDP 流量，所以思科 Spark 等 WebRTC 产品在完成连接时可能会遇到问题。如果两端已确认连接检查，STUN 检测可为 STUN 终端打开针孔并实现基本的 STUN 和 ICE 合规，以便允许进行客户端通信。由此，可避免在访问规则中开放新端口来启用这些应用。

对于默认检测类启用 STUN 检测时，系统会监视 TCP/UDP 端口 3478 中的 STUN 流量。该检测仅支持 IPv4 地址和 TCP/UDP。

STUN 检测在 NAT 方面存在一些局限性。对于 WebRTC 流量，支持静态 NAT/PAT44。由于思科 Spark 不需要针孔，所以 Spark 可以支持其他类型的 NAT。您还可以使用 NAT/PAT64，包括带有 Cisco Spark 的动态 NAT/PAT。

故障转移和集群模式支持STUN检查，因为针孔被复制。但是，设备之间不进行事务ID的复制。如果设备在收到 STUN 请求后发生故障，并且另一台设备收到 STUN 响应，则该 STUN 响应将被丢弃。

CR_Examples

以下示例启用 STUN 检测作为默认全局检测规则的一部分。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect stun
ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。
showconn	显示不同连接类型的连接状态，包括STUN。
showservice-policyinspectdiameter	显示检查直径策略的状态和统计信息。

inspect sunrpc

要启用 Sun RPC 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 inspectsunrpc命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect sunrpc
no inspect sunrpc

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

要启用 Sun RPC 应用检测或更改 ASA 侦听的端口，请在策略映射类配置模式下使用 inspect sunrpc 命令，也可以在策略映射配置模式下通过使用 **class** 命令访问该模式。要删除配置，请使用此命令 **no**的形式。

该 **inspectsunrpc**命令启用或禁用 Sun RPC 协议的应用程序检查。Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可以在系统上的任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，它必须找出该服务正在哪个端口上运行。它通过查询知名端口 111 上的端口映射器进程来实现此目的。

客户端发送服务的 Sun RPC 程序号，并获取返回的端口号。从此时起，客户端程序将其 Sun RPC 查询发送到该新端口。当服务器发出回复时，ASA 会拦截该数据包并在该端口上打开初始 TCP 和 UDP 连接。

注释 不支持 Sun RPC 负载信息的 NAT 或 PAT。

CR_Examples

以下示例启用 RPC 检测引擎，创建类映射以匹配默认端口 (111) 上的 RPC 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 RPC 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map sunrpc-port
ciscoasa(config-cmap)# match port tcp eq 111
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sample_policy
ciscoasa(config-pmap)# class sunrpc-port
ciscoasa(config-pmap-c)# inspect sunrpc
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sample_policy interface outside
```

Related Commands

命令	说明
clearconfiguresunrpc_server	删除使用该命令执行的 **sunrpc-server**配置。
clearsunrpc-serveractive	清除 Sun RPC 应用程序检查为特定服务（例如 NFS 或 NIS）打开的针孔。
showrunning-configsunrpc-server	显示有关 Sun RPC 服务表配置的信息。
sunrpc-server	允许以面向 Sun RPC 服务（如 NFS 或 NIS）的指定超时创建针孔。
showsunrpc-serveractive	显示为 Sun RPC 服务打开的针孔。EXTE

inspect tftp

要禁用 TFTP 应用检测（如果之前已禁用），请在类配置模式下使用 inspect **tftp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect tftp
no inspect tftp

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。

默认端口分配为 69。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

简单文件传输协议 (TFTP) 在 RFC 1350 中描述，是一种在 TFTP 服务器和客户端之间读取和写入文件的简单协议。

ASA 检查 TFTP 流量并在必要时动态创建连接和转换，以允许 TFTP 客户端和服务器之间的文件传输。具体来说，检查引擎检查 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。

只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务器之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。

如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检测。

CR_Examples

以下示例启用 TFTP 检测引擎，创建类映射来匹配默认端口 (69) 上的 TFTP 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 TFTP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map tftp-port
```

```
ciscoasa(config-cmap)# match port udp eq 69
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map tftp_policy

ciscoasa(config-pmap)# class tftp-port
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy tftp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect vxlan

要启用虚拟可扩展局域网 (VXLAN) 应用检查，请在类配置模式下使用 **inspectvxlan** 命令。可以从策略图配置模式访问类配置模式。要删除配置，请使用此命令 **no**的形式。

inspect vxlan
no inspect vxlan

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

默认端口分配是 UDP/4789。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.4(1)	添加了此命令。

使用指南

虚拟可扩展局域网 (VXLAN) 检测适用于流经 ASA 的 VXLAN 封装流量。该检测可确保 VXLAN 报头格式符合标准，丢弃所有格式错误的数据包。系统对于将 ASA 用作 VXLAN 隧道终端 (VTEP) 或 VXLAN 网关的流量不执行 VXLAN 检测，因为在解除 VXLAN 数据包封装的正常环节中会执行那些检测。

VXLAN 数据包为 UDP，通常在端口 4789 上。该端口是 default-inspection-traffic 类的一部分，因此您只需将 VXLAN 检查添加到 Inspection_default 全局服务策略规则中即可。或者，也可以使用端口或 ACL 匹配创建一个类。

CR_Examples

以下示例启用 VXLAN 检测作为全局检测默认规则的一部分。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect vxlan
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect waas

要启用 WAAS 应用检测，请在类配置模式下使用 **inspectwaas** 命令。可以从策略图配置模式访问类配置模式。要删除配置，请使用此命令 **no**的形式。

inspect waas
no inspect waas

Syntax Description

此命令没有任何参数或关键字。

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
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。

CR_Examples

以下示例显示如何在默认检测类上启用 WAAS 应用检测。

```
policy-map global_policy
 class inspection_default
  inspect waas
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect xdmcp

要启用 XDMCP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect xdmcp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no**的形式。

inspect xdmcp
no inspect xdmcp

Syntax Description

此命令没有任何参数或关键字。

Command Default

从 9.16 开始，此命令默认是禁用的。在先前版本中，它默认启用。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

inspect **xdmcp**命令启用或禁用 XDMCP 协议的应用检查。

XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。

为了成功协商和启动 XWindows 会话，ASA 必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许反向连接，请使用**established**ASA 上的命令。一旦 XDMCP 协商好端口来发送显示，就会查**established** 阅命令来验证是否应该允许这个反向连接。

在 XWindows 会话期间，管理器通过知名端口 6000 | n 与显示器 Xserver 进行通信。由于以下终端设置，每个显示器都与 Xserver 建立单独的连接：

```
setenv DISPLAY Xserver:n
```

其中 *n* 为显示器编号。

使用 XDMCP 时，系统将使用 IP 地址协商显示，以便 ASA 可在需要时应用 NAT。XDCMP 检测不支持 PAT。

CR_Examples

以下示例启用 XDMCP 检测引擎，创建类映射以匹配默认端口 (177) 上的 XDMCP 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 XDMCP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map xdmcp-port
ciscoasa(config-cmap)# match port tcp eq 177
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map xdmcp_policy

ciscoasa(config-pmap)# class xdmcp-port
ciscoasa(config-pmap-c)# inspect xdmcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy xdmcp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

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。