目 录

1 应用层检测引擎

1.1 应用层检测引擎配置命令

1.1.1 app-profile

app-profile命令用来创建DPI应用profile，并进入DPI应用profile视图。如果指定的DPI应用profile已经存在，则直接进入DPI应用profile视图。

undo app-profile命令用来删除指定的DPI应用profile。

【命令】

app-profile *profile-name*

undo app-profile *profile-name*

【缺省情况】

不存在 DPI 应用 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：表示DPI应用profile的名称，为 1～63 个字符的字符串，不区分大小写，且只能为字母、数字、下划线。

【使用指导】

DPI（Deep Packet Inspection，深度报文检测）应用 profile 是一个安全业务模板，通过在 DPI 应用 profile 中引用 DPI 各业务策略（例如 IPS 策略、内容过滤策略、URL 过滤策略），并将其应用于对象策略规则中来实现基于安全域间实例的 IP 报文应用层检测功能。

【举例】

创建一个名称为 abc 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc]
```

1.1.2 authentication enable

authentication enable命令用来开启发送邮件的认证功能。

undo authentication enable命令用来关闭发送邮件的认证功能。

【命令】

authentication enable

undo authentication enable

【缺省情况】

发送邮件的认证功能处于开启状态。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【使用指导】

当通过命令 **email-server**指定的邮件服务器需要认证时，可以开启发送邮件的认证功能，否则不需要开启此功能。

【举例】

关闭发送邮件的认证功能。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] undo authentication enable
```

1.1.3 block-period

block-period命令用来配置报文源IP地址被阻断的时长。

undo block-period命令用来恢复缺省情况。

【命令】

block-period *period*

undo block-period

【缺省情况】

报文源 IP 被阻断的时长为 1800 秒。

【视图】

应用层检测引擎的源阻断动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

period：报文源IP地址被阻断的时长，取值范围为 1～86400，单位为秒。

【使用指导】

如果设备上同时开启了黑名单功能，则报文的源 IP 地址被添加到 IP 黑名单后的老化时间为源阻断动作参数 profile 中配置的阻断时长。报文的源 IP 地址被加入 IP 黑名单后，阻断时长之内，后续来自该源 IP 地址的报文将被丢弃。

如果设备上未开启黑名单功能，报文会被阻断，且报文的源IP地址会被添加到IP黑名单，但IP黑名单功能并未生效。实现IP黑名单功能需要执行 **blacklist enable**或 **blacklist global enable**命令，有关此命令的详细介绍请参见“安全命令参考”中的“攻击检测与防范”。

【举例】

在名称为 b1 的应用层检测引擎源阻断动作参数 profile 中，配置报文源 IP 地址被阻断的时长为 3600 秒。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-para-b1] block-period 3600
```

【相关命令】

- **blacklist global enable**（安全命令参考/攻击检测与防范）
- **inspect block-source parameter-profile**

1.1.4 capture-limit

capture-limit命令用来配置捕获报文的最大字节数。

undo capture-limit命令用来恢复缺省情况。

【命令】

capture-limit *kilobytes*

undo capture-limit

【缺省情况】

捕获报文的最大字节数为 512 千字节。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

kilobytes：表示捕获报文的最大字节数，取值范围为 0～1024，单位为千字节。

【使用指导】

捕获到的报文将被缓存到设备本地，当缓存的报文字节数达到指定上限值时，系统会将缓存的报文上传到指定的 URL 上，并清空本地缓存，然后重新开始捕获报文。如果配置捕获报文的最大字节数为 0，则系统会将捕获到的报文立刻上传到指定的 URL 上。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置捕获报文的最大值为 1024 千字节。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-c1] capture-limit 1024
```

【相关命令】

- **inspect capture parameter-profile**
- **export url**
- **export repeating-at**

1.1.5 display inspect status

display inspect status命令用来显示应用层检测引擎的工作状态。

【命令】

display inspect status

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示应用层检测引擎的运行状态。

```
<Sysname> display inspect status
Chassis 0 Slot 1:
 Running status: normal
```

表1-1 display inspect status 命令显示信息描述表

字段	描述
Running status	应用层检测引擎的运行状态，包括如下取值： • bypass by configure：因为配置原因引擎无法处理报文 • bypass by cpu busy：因为 CPU 使用率过高导致引擎无法处理报文 • normal：引擎工作正常

1.1.6 dns-server

dns-server命令用来配置域名解析服务器的IPv4 地址。

undo dns-server命令用来恢复缺省情况。

【命令】

dns-server *ip-address*

undo dns-server

【缺省情况】

不存在域名解析服务器的 IPv4 地址。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

ip-address：表示域名服务器的IPv4 地址，为点分十进制格式。

【使用指导】

如果配置的邮件服务器的地址为主机名格式，当设备发送日志信息邮件时，需要通过域名解析服务器获取邮件服务器 IP 地址与主机名的映射关系。

【举例】

配置域名解析的服务器地址为 192.168.0.1。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] dns-server 192.168.0.1
```

1.1.7 email-server

email-server命令用来配置邮件服务器的地址。

undo email-server命令用来恢复缺省情况。

【命令】

email-server *address-string*

undo email-server

【缺省情况】

不存在邮件服务器的地址。

【视图】

应用层检测引擎的邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

address-string：表示邮件服务器的地址，为 3～63 个字符的字符串，区分大小写。

【使用指导】

配置的邮件服务器地址的地址既可以是邮件服务器的 IP 地址，也可以是邮件服务器的主机名。

在同一个邮件动作参数 profile 视图下，多次执行本命令，最后一次执行的命令生效。

说明

采用主机名时，需要确保设备能通过静态或动态域名解析方式获得邮件服务器的 IP 地址，并与之路由可达。否则邮件发送会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”

【举例】

配置邮件服务器地址为 rndcas.123.com。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server rndcas.123.com
```

配置邮件服务器地址为 192.168.1.1。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server 192.168.1.1
```

1.1.8 export repeating-at

export repeating-at命令用来配置每天定时上传捕获报文的时间。

undo export repeating-at命令用来恢复缺省情况。

【命令】

export repeating-at *time*

undo export repeating-at

【缺省情况】

每天凌晨 1 点定时上传捕获报文。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

time：表示每天上传捕获报文的时间，格式为hh:mm:ss，取值范围为 00:00:00～23:59:59。

【使用指导】

每天指定的时间到达时，无论本地缓存是否达到最大值，系统将向指定的 URL 上传缓存的捕获报文，并清空本地缓存。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置每天定时上传捕获报文的时间为凌晨 2 点。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-c1] export repeating-at 02:00:00
```

【相关命令】

- **inspect capture parameter-profile**
- **export url**
- **capture-limit**

1.1.9 export url

export url命令用来配置上传捕获报文的URL。

undo export url命令用来恢复缺省情况。

【命令】

export url *url-string*

undo export url

【缺省情况】

未指定上传捕获报文的 URL。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

url-string：表示用于上传捕获报文的URL，为 1～255 个字符的字符串。

【使用指导】

本地缓存的捕获的报文字节数达到指定上限值或者每天指定的时间到达时，系统会将缓存的报文上传到指定的 URL。如果未配置上传捕获报文的 URL，则系统依然会上传捕获到的报文，但是会上传失败。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置上传捕获报文的 URL 为 tftp://192.168.100.100/upload。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-c1] export url tftp://192.168.100.100/upload
```

【相关命令】

- **inspect capture parameter-profile**
- **capture-limit**
- **export repeating-at**

1.1.10 inspect activate

inspect activate命令用来激活DPI各业务模块的策略和规则配置。

【命令】

inspect activate

【缺省情况】

DPI 各业务模块的策略和规则被创建、修改和删除时不生效。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当DPI各业务模块（比如IPS和URL过滤等特性）的策略和规则被创建、修改和删除后，需要执行 **inspect activate**命令来使其策略和规则配置生效。

当 DPI 各业务模块的策略和规则被创建、修改和删除且保存配置的情况下，设备重启之后，其相关的所有策略和规则配置也会生效。

执行此命令会暂时中断 DPI 业务的处理，为了避免重复执行此命令对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一执行此命令。

【举例】

激活 DPI 各业务模块的策略和规则配置。

```
<Sysname> system-view
[Sysname] inspect activate
```

1.1.11 inspect block-source parameter-profile

inspect block-source parameter-profile命令用来创建应用层检测引擎的源阻断动作参数profile，并进入源阻断动作参数profile视图。如果指定的源阻断动作参数profile已经存在，则直接进入源阻断动作参数profile视图。

undo inspect block-source parameter-profile命令删除应用层检测引擎的源阻断动作参数profile。

【命令】

inspect block-source parameter-profile *parameter-name*

undo inspect block-source parameter-profile *parameter-name*

【缺省情况】

不存在源阻断动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

parameter-name：源阻断动作参数profile的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入源阻断动作参数 profile 视图后，可以配置对报文执行源阻断动作时采用的特定参数，比如阻断时长。

【举例】

创建名称为 b1 的应用层检测引擎源阻断动作参数 profile，并进入源阻断动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-para-b1]
```

【相关命令】

- **block-period**

1.1.12 inspect bypass

inspect bypass命令用来关闭应用层检测引擎功能。

undo inspect bypass命令用来开启应层检测引擎功能。

【命令】

inspect bypass

undo inspect bypass

【缺省情况】

应用层检测引擎功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

应用层检测引擎对报文的检测是一个复杂且会占用一定的系统资源的过程。开启应用层检测功能后，如果出现 CPU 使用率过高等情况时，可以通过关闭此功能来保证设备的正常运行。

关闭应层检测引擎功能后，系统将不会对接收到的报文进行 DPI 深度安全处理。

【举例】

关闭应用层检测引擎功能。

```
<Sysname> system-view
[Sysname] inspect bypass
```

【相关命令】

- **display inspect status**

1.1.13 inspect cache-option maximum

inspect cache-option maximum命令用来配置应用层检测引擎缓存待检测规则的选项的最大数目。

undo cache-option命令用来恢复缺省情况。

【命令】

inspect cache-option maximum *max-number*

undo inspect cache-option

【缺省情况】

应用层检测引擎缓存待检测规则的选项的最大数目为 32。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-number：指定应用层检测引擎在检测报文时，对每条TCP/UDP流缓存待检测规则的选项的最大数目，取值范围为 1～254。

【使用指导】

应用层检测引擎中的检测规则是由各个 DPI 业务模块中的规则或特征转换而成。

有时应用层检测引擎在检测一条 TCP/UDP 数据流时，虽然匹配上了一个或多个关键字，但是只根据当前 TCP/UDP 报文的内容，不能确定检测规则是否能够被匹配上，因此需要对这些检测规则的选项进行缓存，通过继续检测后续报文是否能够匹配上这些检测规则的选项，来判断是否能识别出此条 TCP/UDP 数据流的应用或行为。

通常，使用缺省配置即可满足应用需求。但是在某些场景中，为了提高应用层检测引擎对 TCP/UDP 数据流应用或行为的识别能力和准确率，需要将应用层检测引擎当前缓存待检测选项的最大数调高，调高后，每条数据流占用的内存可能会上升。同理某些场景下，设备内存使用率偏高，可以调低这个参数，提高设备性能，以保证基础的数据转发正常进行。

例如当前应用层检测引擎有 5000 条检测规则，每条检测规则有一个关键字，那么当前应用层检测引擎中一共有 5000 个关键字。应用层检测引擎需要检测一条 TCP/UDP 数据流的报文的载荷部分是否存在这 5000 个关键字，一种可能的情况是当前报文中存在 10 个关键字。根据应用层检测引擎的工作原理可知，这 10 个关键字所属的 10 条检测规则，要求关键字之后的载荷部分各自需要匹配出 10 个不同的选项，因为每个选项都是对一个完整 TCP/UDP 数据流的检测，所以仅仅根据当前报文载荷就不能确定这些选项是否能被匹配上。因此需要针对这条 TCP/UDP 数据流缓存 10 个选项，通过继续检测后续报文是否能够匹配上这些检测规则的选项，来判断是否能识别出此条 TCP/UDP 数据流的应用层或行为。

一般一个检测规则可以对应多个关键字，每个关键字对应多个选项。

【举例】

配置应用层检测引擎缓存待检测规则的选项的最大数目为 4。

```
<Sysname> system-view
[Sysname] inspect cache-option maximum 4
```

1.1.14 inspect capture parameter-profile

inspect capture parameter-profile命令用来创建应用层检测引擎的捕获动作参数profile，并进入捕获动作参数profile视图。如果指定的捕获动作参数profile已经存在，则直接进入捕获动作参数profile视图。

undo inspect capture parameter-profile命令用来删除应用层检测引擎的捕获动作参数profile。

【命令】

inspect capture parameter-profile *parameter-name*

undo inspect capture parameter-profile *parameter-name*

【缺省情况】

不存在捕获动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：捕获动作参数profile的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入捕获动作参数 profile 视图后，可以配置执行报文捕获动作时采用的特定参数，比如本地缓存报文的最大值字节数。

【举例】

创建名称为 c1 的应用层检测引擎捕获动作参数 profile，并进入捕获动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-b1]
```

【相关命令】

- **capture-limit**
- **export repeating-at**
- **export url**

1.1.15 inspect cpu-threshold disable

inspect cpu-threshold disable命令用来关闭CPU门限响应功能。

undo inspect cpu-threshold disable命令用来恢复CPU门限响应功能。

【命令】

inspect cpu-threshold disable

undo inspect cpu-threshold disable

【缺省情况】

CPU 门限响应功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

应用层检测引擎对报文的检测是一个比较复杂且会占用一定系统资源的过程。当设备的 CPU 利用率低于配置的 CPU 利用率阈值或恢复到 CPU 利用率恢复阈值时，系统对整条数据流的内容进行检测。当 CPU 利用率达到设备上配置的 CPU 利用率阈值时，系统触发 CPU 门限响应功能，系统会根据如下情况对数据流做出不同的处理：

- 若固定长度数据流检测功能处于关闭状态，则系统会自动关闭应用层检测引擎的检测功能来保证设备的正常运行。

- 若固定长度数据流检测功能处于开启状态，则应用层检测引擎只对一条数据流首包后固定长度内的数据进行检测，超出固定长度后的的数据不再进行检测。
- 若应用层检测引擎 CPU 门限响应功能处于关闭状态，则系统仍然对整条数据流的内容进行检测。

在系统 CPU 占用率较高的情况下，不建议用户关闭此功能。

【举例】

关闭 CPU 门限响应功能。

```
<Sysname> system-view
[Sysname] inspect cpu-threshold disable
```

【相关命令】

- **display inspect status**
- **inspect bypass**
- **inspect stream-fixed-length disable**

1.1.16 inspect email parameter-profile

inspect email parameter-profile命令用来创建应用层检测引擎的邮件动作参数profile，并进入邮件动作参数profile视图。如果指定的邮件动作参数profile已经存在，则直接进入邮件动作参数profile视图。

undo inspect email parameter-profile命令删除应用层检测引擎邮件动作参数profile。

【命令】

inspect email parameter-profile *parameter-name*

undo inspect email parameter-profile *parameter-name*

【缺省情况】

不存在邮件动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

parameter-name：邮件动作参数profile的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入邮件动作参数 profile 视图后，可以配置执行发送邮件动作时采用的特定参数，比如邮件服务器的地址、发件人与收件人的地址和登录邮件服务器的用户名和密码等信息。

【举例】

创建名称为 c1 的应用层检测引擎邮件动作参数 profile，并进入邮件动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1]
```

1.1.17 inspect logging parameter-profile

inspect logging parameter-profile命令用来创建应用层检测引擎的日志动作参数profile，并进入日志动作参数profile视图。如果指定的日志动作参数profile已经存在，则直接进入日志动作参数profile视图。

undo inspect logging parameter-profile命令用来删除应用层检测引擎的日志动作参数profile。

【命令】

inspect logging parameter-profile *parameter-name*

undo inspect logging parameter-profile *parameter-name*

【缺省情况】

不存在日志动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：日志动作参数profile的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入日志动作的参数 profile 视图后，可以配置生成报文日志时采用的特定参数，比如输出日志的方式。

【举例】

创建名称为 log1 的应用层检测引擎的日志动作参数 profile，并进入日志动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-logging-para-log1]
```

【相关命令】

- **log**

1.1.18 inspect optimization disable

inspect optimization disable命令用来关闭指定的应用层检测引擎的优化调试功能。

undo inspect optimization disable命令用来开启指定的应用层检测引擎的优化调试功能。

【命令】

inspect optimization [**chunk** | **no-acsignature** | **raw** | **uncompress** | **url-normalization**] **disable**

undo inspect optimization [**chunk** | **no-acsignature** | **raw** | **uncompress** | **url-normalization**] **disable**

【缺省情况】

应用层检测引擎的所有优化调试功能均处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

chunk：表示应用层检测引擎对Chunk格式报文进行解码的优化调试功能。

no-acsignature：表示应用层检测引擎对没有关键字检测规则进行检测的优化调试功能。

raw：表示应用层检测引擎对未经解码TCP/UDP的应用层载荷字段进行检测的优化调试功能。

uncompress：表示应用层检测引擎对HTTP Body字段进行解压缩的优化调试功能。

url-normalization：表示应用层检测引擎对HTTP URL字段进行正规化校准的优化调试功能。

【使用指导】

如果不指定任何参数，则表示关闭或开启应用层检测引擎的所有优化调试功能。

有关应用层检测引擎的各种优化调试功能的详细介绍如下：

应用层检测引擎对 Chunk 格式报文进行解码的优化调试功能：Chunk 是 HTTP 协议载荷(Body)的一种传输方式，对于以 Chunk 方式传输的 HTTP 协议的载荷，需要先对其进行解码以获取真正的载荷内容。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来关闭应层检测引擎解码 Chunk 格式报文的功能，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

应用层检测引擎对没有关键字检测规则进行检测的优化调试功能：没有关键字的检测规则是指此规则不是基于字符串匹配进行检测，而是基于报文的端口号、错误码等字段进行检测。缺省情况下应用层检测引擎对没有关键字的检测规则进行检测，但是在某些场景下，如果设备的吞吐量较差，不能满足客户基本的通信需求，此时可以配置应用层检测引擎对没有关键字的检测规则不进行检测，以提高设备的性能，保证用户最基础的网络通信。

应用层检测引擎对未经解码 TCP/UDP 的应用层载荷字段进行检测的优化调试功能：有些 TCP/UDP 数据流的应用层协议（例如 HTTP、SMTP、POP3、IMAP4）涉及编码和解码处理，而对该类数据流的应用层内容的检测需要在对报文载荷进行解码之后进行。如果当前设备的处理性能不能满足用户基本的通信需求，可以通过该命令取消对未解码的应用层载荷字段的检测，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对报文载荷内容的应用或行为的识别能力会受到影响。

应用层检测引擎对 HTTP Body 字段进行解压缩的优化调试功能：如果报文的 HTTP Body 字段是压缩编码，应用层检测引擎需要先对 HTTP Body 字段进行解压缩后，才能对此字段的内容进行检测。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来取消对 HTTP Body 字段的压缩编码进行解压缩处理，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

应用层检测引擎对 HTTP URL 字段进行正规化校准的优化调试功能：对 HTTP URL 字段进行正规化校准功能是指把 URL 中绝对路径字调整为常规路径格式，对特殊的路径字段进行调整和正确性检查。例如报文 URL 中绝对路径部分输入的是 test/dpi/../index.html，正规化处理后是 test/index.html。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命

令来取消对 HTTP URL 字段进行正规化校准处理，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

【举例】

关闭应用层检测引擎的所有优化调试功能。

```
<Sysname> system-view
[Sysname] inspect optimization disable
```

1.1.19 inspect packet maximum

inspect packet maximum命令用来配置应用层检测引擎可检测有载荷内容的报文的最大数目。

undo inspect packet命令用来恢复缺省情况。

【命令】

inspect packet maximum *max-number*

undo inspect packet

【缺省情况】

应用层检测引擎可检测有载荷内容的报文的最大数目为 32。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-number：指定应用层检测引擎检测有载荷内容的报文的最大数目，取值范围为 1～254。

【使用指导】

应用层检测引擎在对一个数据流的第一个有载荷内容的报文进行检测时，如果没有匹配上任何检测规则，则需要继续检测此数据流的第二个有载荷内容的报文，以此类推。如果直到设备设置的最大报文检测个数还未匹配上任何检测规则，则表示对此数据流匹配失败，并直接允许此数据流通过。通常，使用缺省配置即可满足应用需求。但是在某些应用场景中，应用层检测引擎在检测有载荷内容的报文的个数达到指定的个数之后，仍然不能识别当前报文应用层信息的应用或行为，此时需要调高这个参数。调高此参数后，设备的吞吐量性能会下降，但是应用识别的成功率会增加。同理在设备吞吐量较差，不能满足客户需求的应用场景中，此时需要调低这个参数，调低参数后，吞吐量会增加，但是应用识别成功率会降低。

【举例】

配置应用层检测引擎可检测有载荷内容的报文的最大数目为 16。

```
<Sysname> system-view
[Sysname] inspect packet maximum 16
```

1.1.20 inspect redirect parameter-profile

inspect redirect parameter-profile命令用来创建应用层检测引擎的重定向动作参数profile，并进入重定向动作参数profile视图。如果指定的重定向动作参数profile已经存在，则直接进入重定向动作参数profile视图。

undo inspect redirect parameter-profile命令删除应层检测引擎的重定向动作参数profile。

【命令】

inspect redirect parameter-profile *parameter-name*

undo inspect redirect parameter-profile *parameter-name*

【缺省情况】

不存在重定向动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

parameter-name：重定向动作参数profile的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入重定向动作参数 profile 视图后，可以配置对报文执行重定向动作时采用的特定参数，比如对报文重定向的 URL。

【举例】

创建名称为 r1 的应用层检测引擎重定向动作参数 profile，并进入重定向动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1]
```

1.1.21 inspect signature auto-update proxy

inspect signature auto-update proxy命令用来配置DPI业务特征库在线升级所使用的代理服务器。

undo inspect signature auto-update proxy命令用来恢复缺省情况。

【命令】

inspect signature auto-update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* **password** { **cipher** | **simple** } *string*]

undo inspect signature auto-update proxy

【缺省情况】

未配置 DPI 业务特征库在线升级所使用的代理服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*：指定代理服务器的域名。*domain-name*表示代理服务器的域名，为 3～63 个字符的字符串，不区分大小写。

ip *ip-address*：指定代理服务器的IP地址，仅支持IPv4 类型地址。

port *port-number*：指定代理服务器的端口号，取值范围为 1～65535，缺省值为 80。

user *user-name*：指定登录代理服务器的用户名。*user-name*表示用户名，为 1～31 个字符的字符串，不区分大小写。

password：指定登录代理服务器的用户密码。

cipher：表示以密文方式设置密码。

simple：表示以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～31 个字符的字符串，密文密码为 1～73 个字符的字符串。

【使用指导】

当 DPI 业务模块（例如 IPS 和 URL 过滤）的特征库进行在线升级时，若设备不能连接到 H3C 官方网站，则可配置一个代理服务器使设备连接到 H3C 官方网站上的特征库服务专区，进行特性库在线升级。有关特征库在线升级功能的详细介绍，请参见各 DPI 业务配置指导手册中的“特征库升级与回滚”。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DPI 业务特征库在线升级所使用的代理服务器域名为 www.abc.com，端口号为 8888，登录代理服务器的用户名和密码均为 admin。

```
<Sysname> system-view
[Sysname] inspect signature auto-update proxy domain www.abc.com port 8888 user admin
password simple admin
```

1.1.22 inspect stream-fixed-length disable

inspect stream-fixed-length disable命令用来关闭应用层检测引擎检测固定长度数据流功能。

undo inspect stream-fixed-length disable命令用来开启应用层检测引擎检测固定长度数据流功能。

【命令】

inspect stream-fixed-length disable

undo inspect stream-fixed-length disable

【缺省情况】

应用层检测引擎检测固定长度数据流功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

应用层检测引擎检测固定长度数据流功能，是指当设备的 CPU 利用率达到设备上配置的 CPU 利用率阈值时，应用层检测引擎只检测每条数据流首包后固定长度内的数据，不再检测超出固定长度后的数据。当设备的 CPU 利用率恢复到设备上配置的 CPU 利用率恢复阈值时，系统会对整条数据流的内容进行检测。有关 CPU 利用率的详细配置请参见“基础配置指导”中的“设备管理”。

开启应用层检测引擎 CPU 门限响应功能，此功能才会生效。

当设备的 CPU 利用率较高的情况下，建议关闭此功能，此时应用层检测引擎 CPU 门限响应功能开启的情况下，系统会自动关闭应用层检测引擎的检测功能来保证设备的正常运行。

【举例】

关闭应用层检测引擎检测固定长度数据流功能。

```
<Sysname> system-view
[Sysname] inspect stream-fixed-length disable
```

【相关命令】

- **inspect cpu-threshold disable**
- **inspect stream-fixed-length**

1.1.23 inspect stream-fixed-length

inspect stream-fixed-length命令用来配置应用层检测引擎检测数据流的固定长度。

undo inspect stream-fixed-length命令用来恢复缺省情况。

【命令】

inspect stream-fixed-length { **email** | **ftp** | **http** } * *length*

undo inspect stream-fixed-length

【缺省情况】

应用层检测引擎对 FTP 协议、HTTP 协议和与 E-mail 相关协议数据流的固定检测长度均为 32 千字节。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

email：表示设置检测与E-mail协议相关类型数据流的固定长度，支持的E-mail协议包括SMTP、POP3 和IMAP。

ftp：表示设置检测FTP协议类型数据流的固定长度。

http：表示设置检测HTTP协议类型数据流的固定长度。

length：表示设置检测指定协议类型数据流的固定长度，取值范围为 1～128，单位为千字节。

【使用指导】

调高此参数后，设备的吞吐量性能会下降，但是应用层信息识别的成功率会提高；同理调低参数后，设备的吞吐量会增加，但是应用层信息识别的成功率会降低。

【举例】

配置应用层检测引擎检测 FTP 协议类型数据流的固定长度为 35 千字节，检测 HTTP 协议类型数据流的固定长度为 40 千字节。

```
<Sysname> system-view
[Sysname] inspect stream-fixed-length ftp 35 http 40
```

【相关命令】

- **inspect cpu-threshold disable**
- **inspect stream-fixed-length disable**

1.1.24 inspect tcp-reassemble enable

inspect tcp-reassemble enable命令用来开启TCP数据段重组功能。

undo inspect tcp-reassemble enable命令用来关闭TCP数据段重组功能。

【命令】

inspect tcp-reassemble enable

undo inspect tcp-reassemble enable

【缺省情况】

TCP 数据段重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

大量的 TCP 乱序数据段极有可能会造成应用层检测引擎对此 TCP 数据流检测失败。例如应用层检测引擎需要检测 TCP 载荷中是否包含关键字“this is a secret”，由于数据段乱序，可能含有“a secret”的数据段先到达设备，含有“this is”的数据段后到达设备，这样就会造成应用层检测引擎对此 TCP 数据流检测失败。

为了提高应用层检测引擎对 TCP 数据流检测的准确率，可以在设备上开启 TCP 数据段重组功能。当接收到乱序的 TCP 数据段时，设备会将此数据段和来自于同一条数据流的后续数据段暂时保存至缓冲区，进行 TCP 数据段重组，完成数据段重组再送往后续流程处理。

若缓冲区中已缓存的数据段数目达到最大值（可以通过 **inspect tcp-reassemble max-segment**命令来配置）时仍无法成功重组，则设备直接将已缓存的乱序数据段和此条数据流的所有后续TCP数据段送往后续流程处理，不再进行TCP重组。这样可以降低对设备转发性能的影响。

【举例】

开启 TCP 数据段重组功能。

```
<Sysname> system-view
```

```
[Sysname] inspect tcp-reassemble enable
```

【相关命令】

- **inspect tcp-reassemble max-segment**

1.1.25 inspect tcp-reassemble max-segment

inspect tcp-reassemble max-segment命令用来配置TCP重组缓冲区可缓存的TCP数据段最大数目。

undo inspect tcp-reassemble max-segment命令用来恢复缺省情况。

【命令】

inspect tcp-reassemble max-segment *max-number*

undo inspect tcp-reassemble max-segment

【缺省情况】

TCP 重组缓冲区可缓存的 TCP 数据段最大数目为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-number：表示TCP重组缓冲区可缓存的TCP数据段最大数目，取值范围为 10～50。

【使用指导】

在存在大量 TCP 乱序数据段的网络环境中，调高此参数，则可提高应用层检测引擎对 TCP 数据段检测的准确率，但是设备转发性能可能会下降。若调低此参数可避免因长时间缓存 TCP 数据段而造成设备转发性能下降，但是应用层检测引擎对 TCP 数据段检测的准确率会降低。请根据实际情况调整此参数。

仅开启 TCP 数据段重组功能后，此命令才生效。

【举例】

配置 TCP 重组缓冲区中可缓存的 TCP 数据段最大数目为 20 个

```
<Sysname> system-view
[Sysname] inspect tcp-reassemble max-segment 20
```

【相关命令】

- **inspect tcp-reassemble enable**

1.1.26 log

log命令用来配置记录报文日志的方式。

undo log命令用来取消指定的记录报文日志的方式。

【命令】

log { **email** | **syslog** }

undo log { **email** | **syslog** }

【缺省情况】

报文日志被输出到信息中心。

【视图】

应用层检测引擎的日志动作的参数 profile 视图

【缺省用户角色】

network-admin

【参数】

email：表示将日志以邮件的方式发送到指定的收件人邮箱。

syslog：表示将日志输出到信息中心。

【举例】

在名称为log1的应用层检测引擎日志动作参数profile中，配置将生成的报文日志输出到信息中心。

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-log-para-log1] log syslog
```

【相关命令】

- **inspect logging parameter-profile**

1.1.27 password

password命令用来配置登录邮件服务器的密码。

undo password命令用来恢复缺省情况。

【命令】

password { **cipher** | **simple** } *string*

undo password

【缺省情况】

不存在登录邮件服务器的密码。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

cipher：表示以密文方式设置用户密码。

simple：表示以明文方式设置用户密码，该密码将以密文形式存储。

string：表示登录邮件服务器的密码。明文密码为 1～63 个字符的字符串，密文密码为 1～117 个字符的字符串，区分大小写。

【使用指导】

在同一个邮件动作参数 profile 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置登录邮件服务器的明文密码为 abc123。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] password simple abc123
```

【相关命令】

- **authentication enable**

1.1.28 receiver

receiver命令用来配置收件人地址。

undo receiver命令用来恢复缺省情况。

【命令】

receiver *address-string*

undo receiver

【缺省情况】

不存在收件人地址。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

address-string：表示收件人地址，为 3～511 个字符的字符串，区分大小写。

【使用指导】

收件人地址可以同时输入多个，且每个收件人地址之间用英文“;”号隔开。

【举例】

配置收件人的地址为 123@abc.com 和 nnn@abc.com。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] receiver 123@abc.com;nnn@abc.com
```

1.1.29 redirect-url

redirect-url命令用来配置重定向URL。

undo redirect-url命令用来恢复缺省情况。

【命令】

redirect-url *url-string*

undo redirect-url

【缺省情况】

不存在重定向 URL。

【视图】

应层检测引擎的重定向动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

url-string：表示重定向URL，为 9～63 个字符的字符串，区分大小写。该URL必须以http:// 或https:// 开头，例如http://www.baidu.com。

【使用指导】

当需要把匹配成功的报文重定向到某个 Web 界面时，可以通过执行此命令来指定重定向 URL。

【举例】

配置重定向 URL 为 http://www.abc.com/upload。

```
<Sysname> system-view
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1] redirect-url http://www.abc.com/upload
```

【相关命令】

- **inspect redirect parameter-profile**

1.1.30 secure-authentication enable

secure-authentication enable命令用开启安全传输登录邮件服务器密码功能。

undo secure-authentication enable命令用来关闭安全传输登录邮件服务器密码功能。

【命令】

secure-authentication enable

undo secure-authentication enable

【缺省情况】

安全传输登录邮件服务器密码功能处于关闭状态。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【使用指导】

开启此功能后，首先在设备与邮件服务器之间创建一条安全通道，然后再在此通道中传输登录邮件服务器的密码。

【举例】

开启安全传输登录邮件服务器密码功能。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] secure-authentication enable
```

【相关命令】

- **authentication enable**

1.1.31 sender

sender命令用来配置发件人地址。

undo sender命令用来恢复缺省情况。

【命令】

sender *address-string*

undo sender

【缺省情况】

不存在发件人地址。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

address-string：表示发件人地址，为 3～63 个字符的字符串，区分大小写。

【使用指导】

发件人地址是指设备向目的地发送邮件时使用的源地址。

【举例】

配置发件人的地址为 abc@123.com。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] sender abc@123.com
```

1.1.32 username

username命令用来配置登录邮件服务器的用户名。

undo username命令用来恢复缺省情况。

【命令】

username *name-string*

undo username

【缺省情况】

不存在登录邮件服务器的用户名。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

【参数】

name-string：表示登陆邮件服务器的用户名。为 1～63 个字符的字符串，区分大小写。

【使用指定】

在同一个邮件动作参数 profile 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置登录邮件服务器的用户名为 han。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] username han
```

【相关命令】

- **authentication enable**