

HCIE-Security 备考指南

应用安全（NIP）



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 应用安全（NIP）需要掌握的知识点.....	1
应用安全.....	1
接口对的策略应用.....	2
威胁防护简介.....	6
签名.....	6
威胁防护策略.....	8
威胁防护工作模式.....	10
威胁防护配置流程.....	11
配置威胁防护策略.....	13
配置全局参数.....	13
新建威胁防护策略.....	16
配置签名集.....	18
配置覆盖签名.....	20
查看策略模板.....	21
查看预定义签名.....	22
配置自定义签名.....	24
举例：配置威胁防护策略.....	27
举例：配置自定义签名.....	30
应用控制简介.....	33
配置应用控制策略.....	34
配置全局参数.....	34
新建应用控制策略.....	35
配置应用协议集.....	38
新建自定义应用协议.....	39
策略应用.....	41
在直路 IPS 接口对上应用策略.....	41
在 IDS 接口对上应用策略.....	43
在单臂 IPS 接口对上应用策略.....	44
调整策略优先级.....	46
举例：利用策略优先级满足多层次防护需求.....	47
HCIE-Security 模拟面试问题及面试建议.....	51

HCIE-Security 应用安全（NIP）需要掌握的知识点

- 掌握 NIP 应用安全的配置

应用安全

应用安全包括威胁防护、应用控制、反病毒和 URL 过滤功能。其中，威胁防护、应用控制和反病毒需要通过以策略的方式应用到接口对并针对具体接口对的流量生效，URL 过滤的配置则是全局生效。

威胁防护

威胁防护能够有效防御应用层攻击，如：缓冲区溢出攻击、木马、后门攻击、蠕虫等。

设备通过监控或者分析系统事件检测入侵，使用和匹配包含最新攻击特征的威胁防护签名库，判断该报文是否为攻击报文。如果检测到攻击，设备根据威胁防护策略进行响应，对攻击报文进行告警、阻断或攻击抓包等。

除了预定义的签名库外，用户还能根据实际网络情况和攻击特征定义自定义签名。但建议用户只在非常了解攻击特征的情况下才配置自定义签名，因为自定义签名设置错误不仅无法阻断攻击，而且还有可能导致报文误丢弃或业务不通等问题。

反病毒

设备通过扫描文件并将扫描结果与病毒库进行比较，判断文件中是否包含匹配病毒特征的信息。如果检测到病毒，则根据反病毒策略进行响应，响应动作包括阻断和告警等。如果没有检测到病毒，则放行文件。

旁路部署的 IPS 设备不支持反病毒功能。

应用控制

设备通过对数据流进行检测，可以识别几乎所有的应用层业务，并对指定类型的数据流量进行控制。通过分析设备收到的数据包并和应用控制知识库进行比对，对 P2P、IM、VoIP 等类型的网络数据流量进行分类，并对不同类型的协议进行相应的控制。

URL 过滤

URL 过滤可以对用户进行 URL 访问控制，从而防止用户随意访问网站而影响工作效率或者导致网络威胁。

设备通过分析用户的上网请求中的 URL，将 URL 和配置的 URL 过滤规则进行比较，根据规则对 HTTP 请求进行放行或阻断。

接口对的策略应用

应用安全功能需要通过以策略的方式应用到接口对上才能生效。一个接口对上可以应用多条应用安全策略，并且有一定的匹配顺序，配置前需要合理规划否则会达不到预期效果。

策略的组成

每一条应用安全策略都由基本的网络访问控制、威胁防护策略、应用控制策略和反病毒策略组成，如[图 1](#)所示。

图 1 应用安全策略举例

ID	VLAN ID	源地址	目的地址	服务	动作	应用控制策略	威胁防护策略	反病毒策略	描述
a01 → b01 (1 Item)									
0	any	any	any	ip	permit	--	default	--	--
b01 → a01 (2 Items)									
1	1	1.1.1.1/32	2.2.2.2/32	ip	permit	Default_IM	default	av_policy	--
2	1	1.1.1.0/24	2.2.2.2/32	ip	permit	--	default	--	--

基本的网络访问控制

基本的网络访问控制是优先级最高的应用安全策略。

基本的网络访问控制作为 NIP 的基本策略，将源地址、目的地址和动作（放行或阻断）等内容定义在策略中。

各种匹配条件如果需要引用相关其他资源，例如地址、服务等，需要提前创建好才可在策略中引用。

流量匹配了基本的网络访问控制后，如果被放行才能进行后续应用层处理；如果被拒绝通过，就直接被阻断。

威胁防护策略

威胁防护策略包含了不同的签名，设备能够通过签名对网络流量进行匹配。对于匹配流量根据预置的动作（比如告警、阻断、攻击抓包等）进行处理。签名可以为预定义签名，也可以为自定义签名。

设备提供了缺省的威胁防护策略 **default**，可以被修改。设备同时还提供了能够满足一些常见防护场景的策略模板，可以参考引用模板方式配置新的威胁防护策略。

应用控制策略

应用控制策略能够直接指定被监控的应用协议类型和管理动作。

NIP 提供了两个缺省应用控制策略，分别为 IM 类和 P2P 类，只能查看和应用。

- **Default_IM**: 阻断所有 IM 类应用
- **Default_P2P**: 限流所有 P2P 类应用

反病毒策略

NIP 通过扫描文件并将扫描结果与病毒库进行比较，判断文件中是否包含匹配病毒特征的信息。如果检测到病毒，则根据反病毒策略进行响应，响应动作包括阻断和告警等。如果没有检测到病毒，则放行文件。

当 IPS 接口切换到 IDS 模式后，IDS 接口对上不能应用反病毒策略。

策略的应用

策略应用到接口对上后才生效。



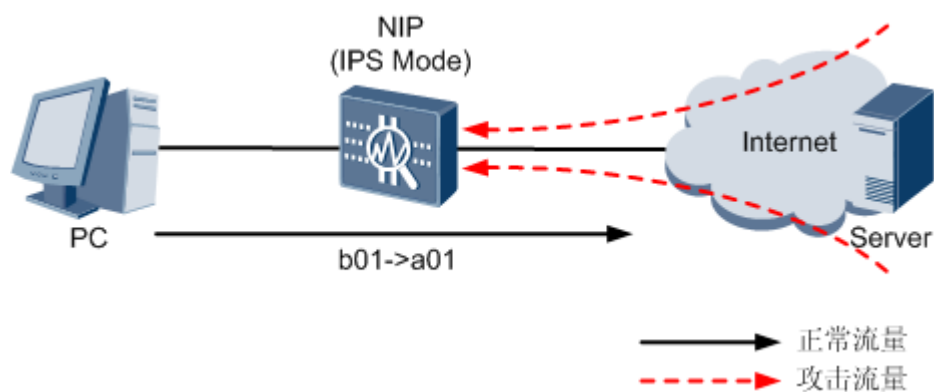
注意：

当策略应用到 IPS 接口对时，能有效防御攻击；当策略应用到 IDS 接口对时，通常只对攻击行为进行检测。

- IPS 接口对上的策略应用

在 IPS 接口对上应用策略，注意应用在访问发起的方向。如[图 2](#)所示，PC 访问 Server 时，PC 受到了来自网络的威胁。虽然产生攻击的方向是 a01->b01，但是应用策略的方向是 PC 访问 Server 的方向 b01->a01。

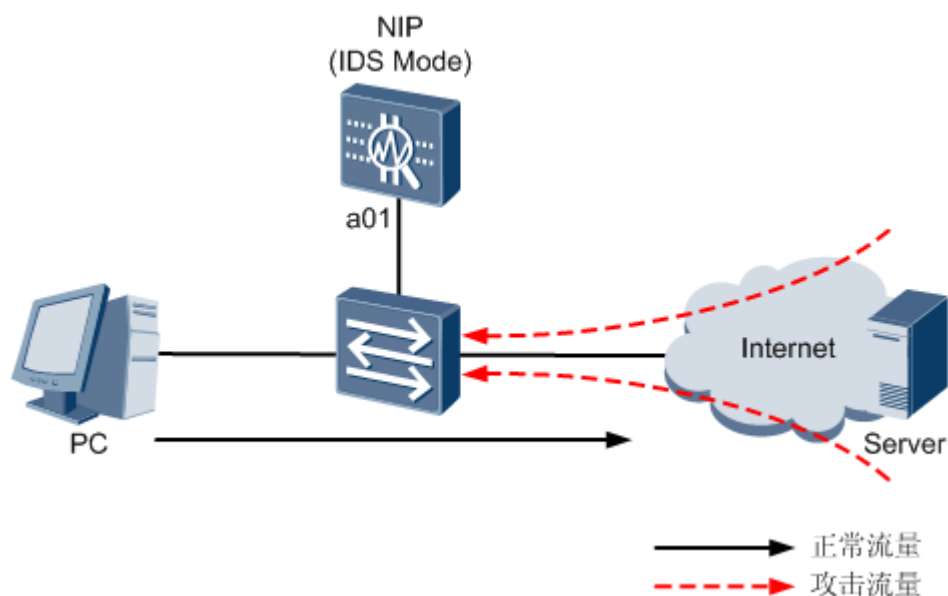
图 2 IPS 接口对上的策略应用



- IDS 接口对上的策略应用

IDS 旁路部署模式下虽然只使用一个物理接口，但是策略仍然是应用在接口对上的，策略对两个接口都生效。如图 3 所示，PC 访问 Server 时，PC 受到了来自网络的威胁。此时，应将策略应用到 a01-b01 接口对上，监控网络流量。

图 3 IDS 接口对上的策略应用



策略的匹配顺序

为了保证多层级的防护功能，应用安全策略需要满足一定的规划原则。

应用安全策略的规划原则：

1. 流量匹配了动作为 **deny** 的基本的网络访问控制后，将不再匹配威胁防护策略、应用控制策略和反病毒策略，所有流量将被阻断。

2. 流量匹配了动作为 **permit** 的基本的网络访问控制后，而且策略中没有威胁防护策略、应用控制策略或反病毒策略，所有流量将被允许放行。
3. 细化的策略要比宽泛的策略优先匹配，也就是说细化的策略需要放在列表的上边。否则一旦匹配到宽泛的策略，细化策略就不再匹配了。

IPS 接口对 b01→a01 上需要配置从 1.1.1.0/24 到 2.2.2.2/32 的应用安全策略。要求 1.1.1.0/24 网段中的所有用户都需要进行威胁防护和反病毒，而且其中 1.1.1.1/32 这个用户还要特殊进行应用控制。

图 4 b01→a01 上的策略列表 1

ID	VLAN ID	源地址	目的地址	服务	动作	应用控制策略	威胁防护策略	反病毒策略
a01 → b01 (1 Item)								
b01 → a01 (2 Items)								
0	1	1.1.1.0/24	2.2.2.2/32	ip	permit	--	default	av_policy
1	1	1.1.1.1/32	2.2.2.2/32	ip	permit	Default_IM	default	av_policy

如图 4 所示，先为整个网段配置了威胁防护策略和反病毒策略，然后为特殊用户只配置了应用控制策略，这样配置的错误的。特殊用户发起的流量会先匹配到第一条宽泛的策略，就不往下继续匹配了。按照细化策略先配置，宽泛策略后配置的原则，应该先配置特殊用户的再配置所有用户的策略。而且注意特殊用户不能只配置应用控制策略还要配置威胁防护策略和反病毒策略，因为一旦匹配到特殊用户的策略就不会继续匹配所有用户的威胁防护策略和反病毒策略了。正确的策略配置如图 5 所示。

图 5 b01→a01 上的策略列表 2

ID	VLAN ID	源地址	目的地址	服务	动作	应用控制策略	威胁防护策略	反病毒策略
a01 → b01 (1 Item)								
b01 → a01 (2 Items)								
0	1	1.1.1.1/32	2.2.2.2/32	ip	permit	Default_IM	default	av_policy
1	1	1.1.1.0/32	2.2.2.2/32	ip	permit	--	default	av_policy

缺省应用安全策略

NIP 提供了缺省应用安全策略，该策略引用了缺省的基本的网络访问控制和缺省的威胁防护策略，未引用应用控制和反病毒策略，其取值如表 1 所示。

设备出厂时每个 IPS 接口对上都应用了缺省应用安全策略。当每个 IPS 接口对切换到 IDS 模式后，IDS 接口对上自动应用缺省应用安全策略。缺省应用安全策略能够满足用户的大部分防护需要，可以查看和修改。

表 1 缺省应用安全策略参数值		
参数	缺省值	说明
ID	0	-
VLAN ID	any	-
源地址	any	-
目的地址	any	-
服务	ip	-
动作	permit	表示所有 IP 报文都允许通过。
应用控制策略	-	未引用应用控制策略
威胁防护策略	default	引用了威胁防护策略为 default 。
反病毒策略	-	未引用反病毒策略

威胁防护简介

介绍威胁防护相关的概念。

- [签名](#)

签名用来描述网络中存在的攻击行为的特征，设备通过将报文内容和威胁防护签名进行比较来检测和防范攻击。

- [威胁防护策略](#)

威胁防护策略包含符合过滤条件的多个签名，通过签名识别攻击流量。

- [威胁防护工作模式](#)

威胁防护的工作模式包括 IPS 工作模式和 IDS 工作模式。

签名

签名用来描述网络中存在的攻击行为的特征，设备通过将报文内容和威胁防护签名进行比较来检测和防范攻击。

签名

威胁防护的签名分为两类：

- 预定义签名

NIP 中预先定义的签名。用户需激活 License 后升级签名库，即可获得包含预定义签名的签名库，并且能够不断地获取新的威胁防护签名库。

- 自定义签名



注意：

建议用户只在非常了解攻击特征的情况下才配置自定义签名。如果自定义签名设置错误不仅无法阻断攻击，而且还有可能导致报文被误丢弃或业务不通等问题。

用户根据网络流量特点对特定的入侵行为自行定义的签名。自定义签名的攻击特征使用正则表达式定义。正则表达式是一种模式匹配工具。

签名集

签名集是满足指定过滤条件的预定义签名的集合。签名集的过滤条件包括：签名的类别、方向、协议、可信度以及严重性。只有同时满足所有过滤条件的签名才能加入签名集中。例如，当只需要对 HTTP 类型的报文进行威胁防御，可以通过过滤条件只加入 HTTP 协议的签名。设备检测时不会执行其他的签名，提高运行效率。

创建威胁防护策略后，用户可通过配置签名集，以及签名集的启用状态和响应方式来满足特定需求。签名集之间存在优先关系，如一个策略中的两个签名集包含同一个签名，设备将根据优先级高的签名集的启用状态和响应方式对匹配该签名的报文进行处理。



说明：

一个签名集中只能有统一的动作，不能给不同的签名设置不同的动作。

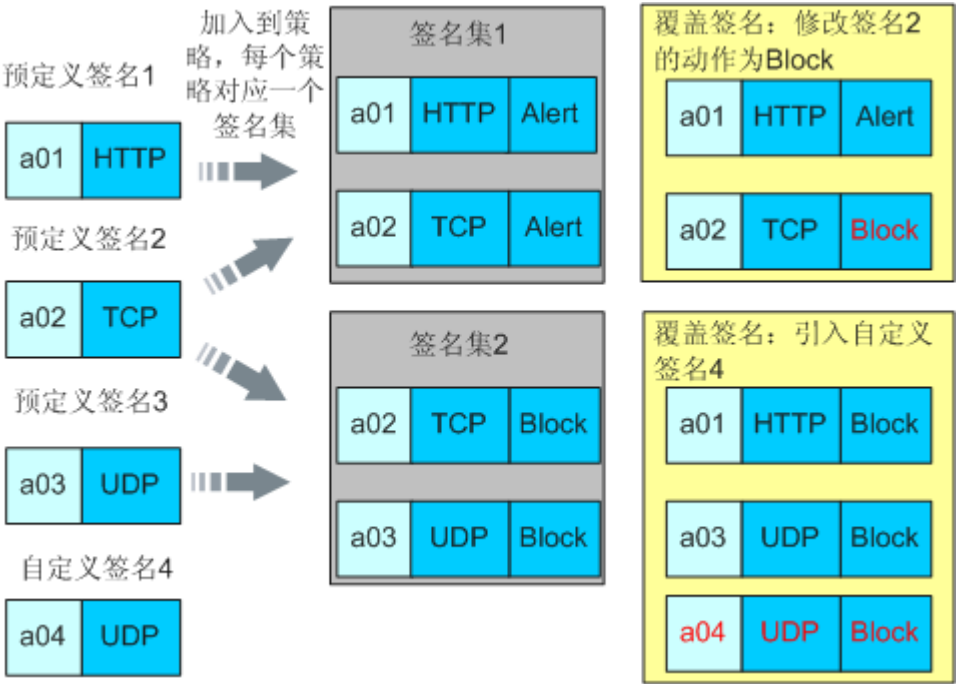
覆盖签名

覆盖签名用于修改指定策略中的签名，提供更加灵活的配置手段。覆盖签名只在本策略中有效，通常用于：

- 修改预定义签名的启用状态和响应方式。例如签名集的动作作为告警，而匹配某签名的动作应该是阻断。此时可以采用覆盖签名的方式，修改该签名的动作。
- 引入自定义签名。自定义签名只能通过覆盖签名的方式加入到策略中。

覆盖签名、签名、签名集的关系如[图 1](#)所示。

图 1 覆盖签名、签名、签名集关系



说明：

图 1 中红色部分即为覆盖签名，只在指定策略上生效。

a01~a04 为该签名特征码的通用化表示。TCP、UDP、HTTP 表示签名的协议。

威胁防护策略

威胁防护策略包含符合过滤条件的多个签名，通过签名识别攻击流量。

威胁防护策略的创建方式

根据用户的网络环境需求不同，用户对安全应用级别的要求不同，创建威胁防护策略存在以下几种方式：

- 缺省的威胁防护策略

NIP 提供了缺省的威胁防护策略 **default**。**default** 采用配置签名集的方式，可以被修改。

- 策略模板

NIP 提供了策略模板，模板内容为针对指定场景预先定义的签名集及其启用状态和响应方式。如果模板内容可满足安全需求，用户可以直接在威胁防护策略中引用模板，从而减少配置工作。用户在威胁防护策

略中引入模板后，模板中的签名集加入威胁防护策略中，该签名集与定义的签名集一样，用户可以修改启用状态、响应方式等配置。

- 签名集

用户根据需要配置各种过滤条件来过滤签名集中包含的签名，并配置签名集的启用状态和响应方式。

- 覆盖签名

用户可以根据需要在威胁防护策略里修改某个签名的响应方式，称为覆盖签名。配置了覆盖签名之后，这条签名在该策略中的响应方式临时被修改了。当用户取消覆盖签名之后，这条签名在此策略中的响应方式恢复成原签名的响应方式。自定义签名也需要通过覆盖签名的方式引入到威胁防护策略中。



说明：

在同一条威胁防护策略中，覆盖签名优先级高于签名集的配置，如果配置的覆盖签名和签名集中的配置有冲突，覆盖签名的配置生效。

- 复制威胁防护策略（同步策略）

新建的威胁防护策略可以复制已经存在的策略。复制后的威胁防护策略可以进行修改，以满足用户对安全性的需要。

完成威胁防护策略配置后，需要将威胁防护策略应用在指定的接口对后才能生效。

威胁防护策略的编译

对威胁防护策略的修改只有经过编译后才能生效。NIP 支持手动提交配置来编译威胁防护策略。另外，有些情况也能触发威胁防护策略的自动编译，而且与手动提交配置的编译效果相同。

- 手动编译

修改一个已经使用的威胁防护策略，而且没有被重新应用在其他接口对的操作时，需要手工编译。具体操作为：

- 增加、删除、修改签名集
- 增加、删除、修改覆盖签名
- 删除、修改被策略引用的自定义签名

- 自动编译

具体操作为：

- 接口对上应用威胁防护策略
- 配置特权策略或取消已配置的特权策略
- 升级签名库版本

威胁防护工作模式

威胁防护的工作模式包括 IPS 工作模式和 IDS 工作模式。

威胁防护工作模式

威胁防护工作模式是所有 IPS 接口对或 IDS 接口的全局工作模式。IPS 接口对用于直路接入，IDS 接口用于旁路接入，具体介绍参见[接口配置](#)。

威胁防护工作模式分为：

- IPS 工作模式

IPS 工作模式下，设备支持防护功能和告警功能。缺省情况下，设备支持防护功能。

- IDS 工作模式

IDS 工作模式下，设备支持防护功能和告警功能。缺省情况下，设备支持告警功能。

攻击响应方式

一个签名包含一种攻击特征，当报文命中签名时，NIP 将该报文识别为攻击报文。



说明：

匹配到攻击的实际动作受 IPS 或 IDS 的全局工作模式制约。

NIP 对攻击报文的响应方式如[表 1](#)所示。

表 1 攻击响应方式		
工作模式	签名动作	实际动作
防护模式	阻断	NIP 阻断报文，记录日志。
	告警	NIP 不对报文进行处理，记录日志。
告警模式	告警	NIP 不对报文进行处理，记录日志。
	阻断	

威胁防护配置流程

通过阅读威胁防护配置流程，可以全局掌握威胁防护配置过程，并可以指导如何进行具体配置。



注意：

配置威胁防护策略前，请确保已经完成升级签名库到最新版本。升级签名库的说明和操作请参见[知识库和病毒库升级](#)。

修改已应用到接口对上的威胁防护策略的签名集或覆盖签名后，需要提交编译来更新威胁防护策略的配置。

威胁防护配置流程根据选择签名的类型不同分为两种，使用预定义签名方式和使用自定义签名方式，分别如[图 1](#)和[图 2](#)所示。一个策略下可以同时引用预定义签名和自定义签名。

威胁防护策略配置完成后，需要与应用控制策略统一规划后，应用 IPS 接口对或 IDS 接口对上。

图 1 使用预定义签名的威胁防护配置流程图

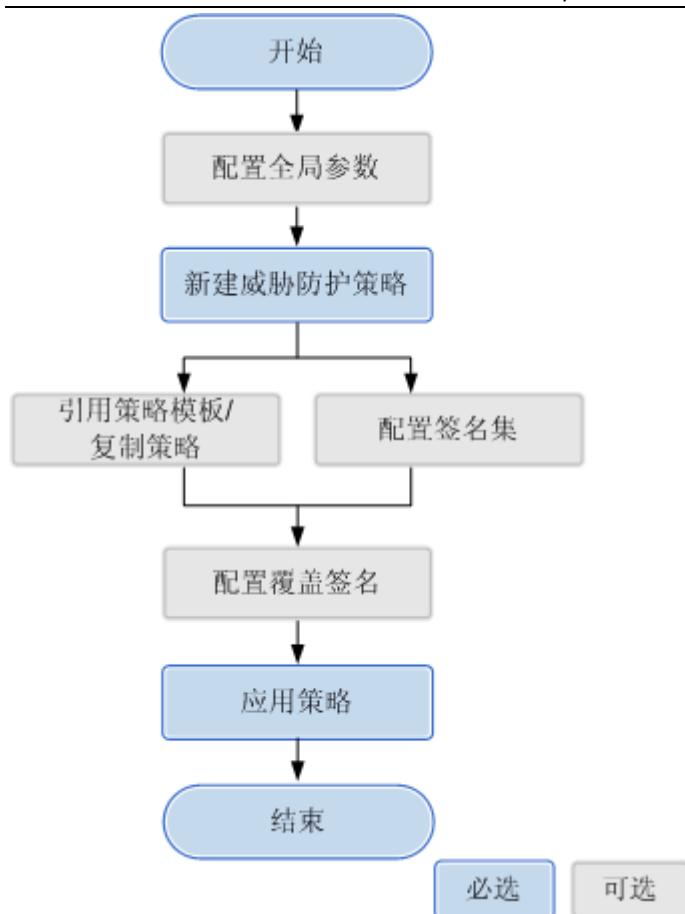
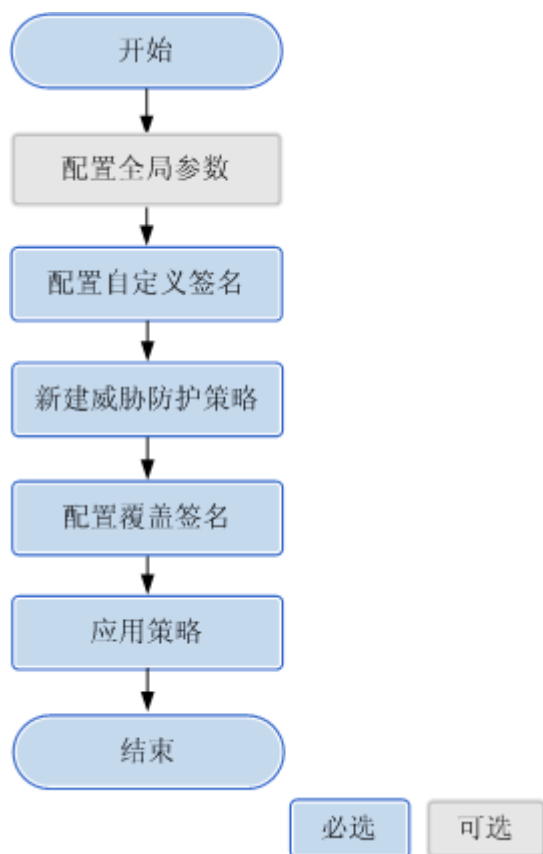


图 2 使用自定义签名的威胁防护配置流程图



配置威胁防护策略

根据网络防护需求不同，威胁防护策略可以通过配置签名集和覆盖签名完成。

- [配置全局参数](#)

介绍工作模式、IP 隔离、日志归并和攻击抓包的概念和配置。

- [新建威胁防护策略](#)

威胁防护可以采用同步策略或策略模板的方式创建新的策略。

- [配置签名集](#)

创建威胁防护策略后，用户可通过配置签名集，以及签名集的启用状态和响应方式来满足特定需求。一条策略可以配置多个签名集。签名集方式的策略只对预定义签名有效。

- [配置覆盖签名](#)

覆盖签名可以用来修改威胁防护策略中单个签名的启用状态和响应方式，也可以用来将自定义签名引入到威胁防护策略中。

- [查看策略模板](#)

设备提供威胁防护策略模板，模板中已定义签名集。如果模板能够满足应用场景或者与应用场景相似，则可直接在策略中引用模板。

配置全局参数

介绍工作模式、IP 隔离、日志归并和攻击抓包的概念和配置。

全局参数介绍

- 工作模式

威胁防护有 2 种工作模式：防护模式和告警模式。

防护模式下，签名的阻断响应方式生效并产生日志；告警模式下，签名的阻断响应方式无效只产生日志。



说明：

旁路部署的 IPS 设备在防护模式下的阻断动作仅是：在威胁防护检测到 TCP 协议类型的攻击后，发送 TCP

RST 报文中断连接。

- 非对称部署模式

正常情况下，NIP 会对双向的流量状态进行关联检测。在特殊场景下，受组网限制，来回路径不一致不可避免。此时可以开启非对称部署模式，对单边流量进行检测。

- IP 隔离

当攻击发生时，为了及时阻断攻击流量，可以开启 IP 隔离功能。此时，设备会将攻击者或受害者的 IP 地址加入到 IP 隔离列表中。在隔离时间内，阻断该 IP 地址发出的报文。

可以选择“监控 > IP 隔离”查看 IP 隔离列表。

- 日志归并

日志归并是指将同类的日志进行合并，以便减少数据量，节省空间。归并条件：签名 ID（必选）、源端口、目的端口、源 IP、目的 IP、VLAN ID 和动作。

归并的原则是在归并时间间隔内，对于相同归并条件的日志进行归并，其他项显示为 0。归并条件为签名 ID 和源 IP 的日志归并如[图 1](#)所示。



说明：

日志归并仅对于威胁防护日志有效。

图 1 日志归并示意图

签名ID	源IP地址	源端口	其他
24000	1.1.1.1	2000	a
24000	1.1.1.1	2000	b
24001	1.1.1.2	3000	c
24001	1.1.1.2	4000	d

归并后的日志

24000	1.1.1.1	0	0
24001	1.1.1.2	0	0

• 攻击抓包

设备提供抓包功能，可以对攻击报文进行抓包，便于对攻击报文进行分析。

配置全局参数

1. 选择“应用安全 > 威胁防护 > 策略”。
2. 选择“配置全局参数”页签。
3. 依次选择各项参数。具体参数描述请参见[表1](#)。
4. 单击“应用”。

表 1 威胁防护全局参数说明		
参数	说明	取值建议
工作模式设置		
IPS 工作模式（直路）	防护模式下，签名的阻断响应方式生效并产生日志。 告警模式下，签名的阻断响应方式无效只产生日志。	-
IDS 工作模式（旁路）	防护模式下，签名的阻断响应方式生效并产生日志。 告警模式下，签名的阻断响应方式无效只产生日志。	-
特权策略	配置全局特权策略或取消已配置的特权策略。 同一时间只能有一个特权策略生效。	配置特权策略时，特权策略必须从已配置的威胁防护列表中选取。
非对称部署模式	非对称部署模式启用开关。	设备部署在来回路径不一致的网络时，需要开启非对称部署模式。
检测方式	选择检测单边流量的方向。 开启“非对称部署模式”后，本配置才生效。	<ul style="list-style-type: none"> • 仅检测到服务器方向报文。 • 仅检测到客户端方向报文。 • 检测双向报文。
IP 隔离设置		
协议	指定攻击报文的协议，只对该协议的攻击报文进行 IP 隔离。	<ul style="list-style-type: none"> • TCP：TCP 协议 • 其他：除 TCP 外的所有其他协议
IP 地址	指定需要隔离的 IP 地址类型。 网络中部署了邮件服务器，如果配置的参数为“目的 IP”，一旦有攻击邮件服务器的报文到匹配威胁防护策略，将导致邮件服务器的 IP 地址列入隔离列表中而不能正常对外	<ul style="list-style-type: none"> • 源 IP 提取报文的源 IP 地址，隔离该 IP 的报文。 • 目的 IP 提取报文的源 IP 地址，隔离该 IP 的

表 1 威胁防护全局参数说明

参数	说明	取值建议
	提供服务。	报文。 <ul style="list-style-type: none"> 攻击者 设备根据报文判断出攻击者 IP 地址，隔离该 IP 的报文。 受害者 设备根据报文判断出受害者 IP 地址，隔离该 IP 的报文。 双向阻断 对源 IP 和目的 IP(即攻击者和受害者)同时进行隔离。
隔离时间	配置 IP 地址加入 IP 隔离列表的时间。	-
日志归并设置		
日志归并	开启或关闭日志归并。	-
归并条件	指定归并条件，相同条件的日志进行归并。	-
归并时间间隔	指定归并时间间隔（归并周期）。归并只在同一个归并周期内生效。例如指定归并时间为 10 秒，某攻击第 5 秒和第 20 秒依次达到，即使符合归并条件，也不会归并。	-
攻击抓包设置		
抓包个数	配置抓包的个数。检测到攻击事件后，如果抓包功能开启，可以根据配置的抓包数量对攻击报文及其后续报文进行抓取。	-

新建威胁防护策略

威胁防护可以采用同步策略或策略模板的方式创建新的策略。

在“威胁防护策略列表”中可以查看策略状态：

- 引用：策略是否正在被使用中。
- 状态：策略是否已经提交。威胁防护策略新建或修改后，需要提交后才能生效。

如果存在策略没有提交，可以单击“提交”，将所有策略一起提交。

新建威胁防护策略

1. 选择“应用安全 > 威胁防护 > 策略”。

2. 单击“新建”。
3. 依次输入或选择各项参数。具体参数描述请参见表1。
4. 单击“应用”。

表1 新建威胁防护策略参数说明

参数	说明	取值建议
名称	威胁防护策略的名称。	新建威胁防护策略的名称不能与设备已有威胁防护策略的名称相同。
描述	威胁防护策略的描述信息。	-
同步策略/策略模板	选择是否同步策略/策略模板。 同步策略/策略模板后，新建的策略将具有与原策略/策略模板相同的配置。 通过同步已经创建的策略或策略模板，将已有策略或策略模板中的签名引入到新建策略中，然后可以在此基础上进一步修改，方便配置。	如选择同步，则策略或策略模板的取值为： <ul style="list-style-type: none"> 策略：已经创建的策略。 策略模板：设备缺省已经存在，可以选择“策略模板”页签查看。

导出/导入威胁防护策略

威胁防护策略支持导入和导出。当网络中部署多台设备并且配置相同时，可以先在某台设备上配置，验证通过后导出策略，依次导入到其他设备。



说明：

导出的文件为 IPSPolicy.xml，可以通过文本工具或 XML 编辑工具打开和修改。

1. 选择“应用安全 > 威胁防护 > 策略”。
2. 单击“导出”，将策略导出到本地。
3. 在其他设备上单击“导入”。
4. 在“待导入策略列表”中勾选需要导入的策略。

选择时请注意查看策略的状态：

- 名称重复：导入的策略和已有的策略存在重名。请仔细检查，避免错误覆盖。
- 新建：导入全新的策略。请仔细检查，避免错误覆盖。

5. 单击“确定”。

其他操作

操作	说明
删除策略	被应用安全策略引用的威胁防护策略不能删除。可以通过“应用安全 > 策略应用”查看策略的引用情况。
提交	将所有策略提交设备进行编译、使之生效。当有多个策略需要修改，为了节省时间，可以全部策略修改完毕后，点击本按钮统一提交策略。

配置签名集

创建威胁防护策略后，用户可通过配置签名集，以及签名集的启用状态和响应方式来满足特定需求。一条策略可以配置多个签名集。签名集方式的策略只对预定义签名有效。

新建签名集

一个签名必须同时满足所有过滤条件才能加入签名集。


1. 选择“应用安全 > 威胁防护 > 策略”。
2. 在“威胁防护策略列表”区域框中单击，修改指定的策略。
3. 在“签名集列表”区域框中单击“新建”。
4. 依次输入或选择各项参数。具体参数描述请参见表1。
5. 单击“确定”。

表1 新建签名集参数说明



参数	说明	取值建议
名称	签名集的名称。	新建签名集的名称不能与设备已有签名集的名称相同。
方向	签名检测报文的方向，也就是说对指定方向的报文进行检测。	<ul style="list-style-type: none"> 去服务端：检测发往服务器端的报文的签名。 去客户端：检测发往客户端的报文的签名。 任意方向：检测发往任意方向的报文的签名。 <p>对于 HTTP 的请求报文，就是去服务端；HTTP 的回应报文就是去客户端；对于 TCP/UDP 协议报文，请求方为 Client 端，发出去的报文为去服务端。</p>

表 1 新建签名集参数说明		
参数	说明	取值建议
		<p>选中“全部”复选框后，该签名集包含所有方向的签名。</p> <p>取消选中“全部”复选框后，必需设置签名的方向。如果没有设置方向，签名集无效，该签名集不包含任何的签名。</p>
严重性	签名集中签名的严重性。	<p>选中“全部”复选框后，该签名集包含所有严重性的签名。</p> <p>取消选中“全部”复选框后，缺省情况下，严重性为“大于等于”“告警”。</p>
可信度	签名集中签名的可信度。	<p>选中“全部”复选框后，该签名集包含所有可信度的签名。</p> <p>取消选中“全部”复选框后，缺省情况下，可信度为“大于等于”“中”。</p>
协议	签名集中签名的协议。	<p>由威胁防护签名库动态生成。</p> <p>选中“全部”复选框后，该签名集包含所有协议的签名，包括升级后的新增协议。</p> <p>取消选中“全部”复选框后，必需设置签名的协议。如果没有设置协议，签名集无效，该签名集不包含任何的签名。</p>
类别	签名集中签名的类别。	<p>由威胁防护签名库动态生成。</p> <p>选中“全部”复选框后，该签名集包含所有类别的签名，包括升级后的新增类别。</p> <p>取消选中“全部”复选框后，必需设置签名的类别。如果没有设置类别，签名集无效，该签名集不包含任何的签名。</p> <p>设备还支持配置类别的模式：</p> <p>“与”表示同时满足全部设置的类别的签名可加入签名集。</p> <p>“或”表示满足任一设置的类别的签名就可加入签名集。</p>
状态	签名集的启用状态。	-
动作	签名集的响应动作。	<ul style="list-style-type: none"> • 阻断：当报文命中签名时，阻断该报文。 • 告警：当报文命中签名时，不阻断该报文只记录日志。 • 防火墙联动 • IP 隔离：开启 IP 隔离功能。 <p>注意： 不推荐在 MPLS、VLAN 网络中使用 IP 隔离功能。</p> <ul style="list-style-type: none"> • 攻击抓包：开启攻击抓包功能。

调整签名集的优先级

签名集（包括模板中的签名集）之间存在优先关系，在同一条 IPS 策略中，排在前面的签名集比排在后面的签名集的优先级高。如果一个签名包含在一条 IPS 策略的多个签名集中，则 NIP 按照优先级高的签名集所配置的启用状态和响应方式对匹配签名的报文进行处理。当安全威胁发生变化，用户可以调整签名集的优先级来满足新的安全需求。

调整签名集的位置可以实现调整签名集的优先级。

1. 选择“应用安全 > 威胁防护 > 策略”。
2. 在“威胁防护策略列表”区域框中单击，修改指定的策略。
3. 在“签名集列表”区域框中单击，输入目标位置签名集的名称，将该签名集排到目标签名集的前面或后面。
4. 单击“确定”。

配置覆盖签名

覆盖签名可以用来修改威胁防护策略中单个签名的启用状态和响应方式，也可以用来将自定义签名引入到威胁防护策略中。

新建覆盖签名

如果需要针对某个特定签名单独配置启用状态和响应方式，可配置此功能。覆盖签名比策略模板、签名集方式定义的策略优先级高。

只使用预定义签名的情况下，如果对特定签名没有优先要求，不需要配置覆盖签名。



1. 选择“应用安全 > 威胁防护 > 策略”。
2. 在“威胁防护策略列表”区域框中单击，修改指定的策略。
3. 在“覆盖(Overrides)列表”区域框中单击“新建”。
4. 依次输入或选择各项参数。具体参数描述请参见[表 1](#)。
5. 单击“确定”。
6. 单击“返回”，界面弹出是否立即提交的确认框，请根据提示信息操作。

表 1 覆盖签名参数说明		
参数	说明	取值建议
已选择签名	待修改启用状态或响应方式的预定义签名，或者待引入的自定义签名。	<p>单击 ，查询签名。</p> <p>查询方法分为两种：</p> <ul style="list-style-type: none"> 按组合条件查询：通过组合协议、方向、严重性、类别和可信度，查询符合条件的签名。 按 ID 查询。 <p>单击“选择”复选框，选择需要修改的签名。</p>
状态	覆盖签名的启用状态。	只有选中“启用”对应的复选框，配置的动作才生效。
动作	覆盖签名的响应动作。	<ul style="list-style-type: none"> 阻断：当报文命中签名时，阻断该报文。 告警：当报文命中签名时，不阻断该报文只记录日志。 防火墙联动。 IP 隔离：开启 IP 隔离功能。 <p>注意： 不推荐在 MPLS、VLAN 网络中使用 IP 隔离功能。</p> <ul style="list-style-type: none"> 攻击抓包：开启攻击抓包功能。

查看策略模板

设备提供威胁防护策略模板，模板中已定义签名集。如果模板能够满足应用场景或者与应用场景相似，则可直接在策略中引用模板。

背景信息


设备存在缺省的策略模板，如[表 1](#)所示。用户只能查看该策略模板的详细信息，不能对其进行其他操作。

新建威胁防护策略时，策略模板可以通过“同步策略/策略模板”选项被引用。生成的新威胁防护策略，具有与策略模板相同的配置信息，而且可以修改签名集和覆盖签名等信息。

表 1 策略模板	
策略模板名称	应用场景
default_ids	该模板适用于当设备以 IDS（旁路）模式部署时的通用场景。
outside_firewall	该模板适用于当设备部署在防火墙外面的场景。

表 1 策略模板	
策略模板名称	应用场景
all_inclusive_without_audit	该模板将所有的预定义签名（除了级别为审计的签名之外）都包含进来，这样能够明显减少审计日志，减轻运维工作量。
all_inclusive_with_audit	该模板将所有的预定义签名都包含进来，适用于高安全级别的应用场景。
default_inline_ips	该模板适用于当设备以 IPS（直路）模式部署时的通用场景。
dmz	该模板适用于当设备部署在 DMZ 区域前的场景。
inside_firewall	该模板适用于当设备部署在防火墙里面的场景。
web_server	该模板适用于当设备部署在 Web 服务器前面的场景。
mail_server	该模板适用于当设备部署在 Mail 服务器前面的场景。
dns_server	该模板适用于当设备部署在 DNS 服务器前面的场景。
file_server	该模板适用于当设备部署在 File 服务器前面的场景。

操作步骤

1. 选择“应用安全 > 威胁防护 > 策略”。
2. 选择“策略模板”页签。在“策略模板列表”区域框中单击，查看详细信息。

查看预定义签名

预定义签名为 NIP 预先定义的签名，无需用户自行配置，获取最新版本的威胁防护预定义签名。查看预定义签名可以了解目前设备支持的预定义签名详细情况。

查看预定义签名

1. 选择“应用安全 > 威胁防护 > 预定义签名”。
2. 单击“刷新”，刷新和查看预定义签名的最新列表。
3. **可选：**单击“高级查询”，选择查询条件，并输入待查询项的参数，单击“确定”，过滤出相应的签名信息。

查询条件包括：

- 按 ID 查询：按照预定义签名的 ID 进行查询。
- 按 CVE 名称查询：按照国际权威组织 CVE（Common Vulnerabilities & Exposures）为公开的安全漏洞定义的名称进行查询。
- 按组合条件查询：按照签名的协议、方向、严重、类别、可信度的任何组合进行查询。

4. 单击指定预定义签名的 ，查看该签名的详细信息。

预定义签名详细信息的说明如表 1 所示。

表 1 预定义签名参数说明		
参数	说明	取值建议
ID	预定义签名的 ID。	-
方向	预签名检测报文的方向，也就是说对指定方向的报文进行检测。	含义如下： <ul style="list-style-type: none"> • to-server：检测发往服务器端的报文。 • to-client：检测发往客户端方向的报文。 • any：检测发往任意方向的报文。
可信度	预定义签名的可信度，用来描述该签名的可信赖程度。可信度越高，说明命中签名的攻击误报的可能性越小。	-
严重性	预定义签名的严重性，用来描述攻击后果的严重性。签名的严重性越高，说明命中签名的攻击产生的后果越严重。	-
状态	预定义签名的状态。	<ul style="list-style-type: none"> • active：可用的预定义签名。 • deprecated：无效或不可用的预定义签名。
协议	预定义签名的协议，用来描述攻击特征所在报文使用的协议类型。	由威胁防护签名库动态生成。
类别	预定义签名的类别，用来描述攻击特征所属的攻击类别。 一个预定义签名可以属于多个不同的类别。	-
描述信息	预定义签名的描述信息。	-
对策	针对预定义签名需要采取的措施。	-
参考信息	第三方机构对该预定义签名的详细描述。	包括该漏洞的 BID 编号（网站 http://www.securityfocus.com 对该漏洞的编号）、CVE 名称和微软对该漏洞的编号、以及到 http://www.securityfocus.com 和 CVE 网

表 1 预定义签名参数说明

参数	说明	取值建议
		站的链接功能。例如，单击 CVE-2011-1220 链接即可弹出 CVE 网站上该漏洞的网页，如 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1220 。
被攻击厂商列表	指定被攻击厂商的列表。	包括厂商名称、产品名称和版本号。

配置自定义签名

自定义签名是用户根据网络流量特点对特定的入侵行为自行定义的签名。

在“自定义签名列表”中的“状态”列，可以查看状态：

- **modified**：自定义签名创建后的状态。
- **applied**：自定义签名通过覆盖签名引用到指定威胁防护策略并编译后的状态。
- **deleted**：删除状态为“**applied**”的自定义签名后的状态。如果需要完全删除该自定义签名，需要在引用该自定义签名的威胁防护策略中提交编译。

新建自定义签名

自定义签名的攻击特征使用正则表达式定义。正则表达式是一种模式匹配工具。最简单的正则表达式只匹配字符串，如 hello。正则表达式还提供了一些具有特殊含义的专用字符，也称为元字符（metacharacter）。用户可以使用这些元字符灵活地配置自定义签名。

1. 选择“应用安全 > 威胁防护 > 自定义签名”。
2. 在“自定义签名列表”区域框中单击“新建”。
3. 依次输入或选择各项参数，如[表 1](#)所示。
4. 单击“应用”。

表 1 新建自定义签名参数说明

参数	说明	取值建议
ID	自定义签名的 ID。	新建自定义签名的 ID 不能与设备已有自定义签名的 ID 相同。
名称	自定义签名的名称。	-

表 1 新建自定义签名参数说明

参数	说明	取值建议
协议	自定义签名的协议类型，用来描述攻击特征所在报文使用的协议类型。	由威胁防护签名库动态生成。
严重性	自定义签名的严重性，用来描述攻击后果的严重性。签名的严重性越高，说明命中签名的攻击产生的后果越严重。	-
方向	自定义签名检测报文的方向，也就是说对指定方向的报文进行检测。	<ul style="list-style-type: none"> 去服务端：检测发往服务器端的报文的签名。 去客户端：检测发往客户端的报文的签名。 任意方向：检测发往任意方向的报文的签名。 <p>对于 HTTP 的请求报文，就是去服务端；HTTP 的回应报文就是去客户端；对于 TCP/UDP 协议报文，请求方为 Client 端，发出去的报文为去服务端。</p>
源地址	自定义签名的源 IP 地址。	-
源地址掩码	自定义签名的源 IP 地址的掩码。 配置“源地址”后，必需配置“源地址掩码”。	-
源端口	自定义签名的源端口。	<p>设备还支持指定源端口的范围：</p> <ul style="list-style-type: none"> 任意：任意端口号。 低端口：端口号为 1~1023。 高端口：端口号为 1024~65535。
目的地址	自定义签名的目的 IP 地址。	-
目的地址掩码	自定义签名的目的 IP 地址的掩码。 配置“目的地址”后，必需配置“目的地址掩码”。	-
目的端口	自定义签名的目的端口。	<p>设备还支持指定目的端口的范围：</p> <ul style="list-style-type: none"> 任意：任意端口号。 低端口：端口号为 1~1023。 高端口：端口号为 1024~65535。
搜索长度	最大搜索长度。配置了搜索长度后，设备只搜索流中指定长度的内容来检查是否匹配签名，超过指定长度的部分不再处理。	-
搜索偏移	特征码出现的开始位置。当攻击特征明确时，通过配置“搜索偏移”可以提高检测率和性能。	<ul style="list-style-type: none"> 报文：基于报文的偏移值。指特征码必须在报文的指定偏移值处出现才会匹配签名。 流：基于流的偏移值。指特征码必须在流的指定偏移值处出现才会匹

表 1 新建自定义签名参数说明

参数	说明	取值建议
		<p>配签名，只对当前运行于 TCP 之上的应用层协议的会话有效。</p> <ul style="list-style-type: none"> 任意：建议使用本参数。此时，关键字需要至少输入 2 个字符。
关键字	关键字是指攻击报文的特征码，采用正则表达式配置。	<p>说明： 配置正则表达式时，需要注意以下事项：</p> <ul style="list-style-type: none"> { }只能用于{n,m}和{ }。 ,只能出现在{ }中，如果出现在其他地方，前面必须加转义符\。 +, *, ?, {}为修饰词，之前的字符必须为正常字符。 ()、[]、{}必须成对出现。
描述	自定义签名的描述信息。	-

自定义签名中元字符的描述

元字符应用在自定义签名中，能够被灵活应用，方便用户配置特定规则的签名。

元字符	含义	说明
\	转义符。	<p>匹配以下字符时前面需要使用转义符：</p> <ul style="list-style-type: none"> 定义为元字符的字符 <和>
+	前一个字符在目标对象中出现 1 次或连续多次。	-
*	前一个字符在目标对象中出现 0 次或连续多次。	-
?	前一个字符在目标对象中出现 0 次或 1 次。	<p>配置自定义签名的正则表达式时使用\q 代替元字符?。如正则表达式 abc?，在 NIP 上需要输入 abc\q。</p> <p>说明：</p> <ul style="list-style-type: none"> 当正则表达式中匹配\q 本身时，需要使用转义符\。如 abc\q，在 NIP 上输入 abc\\q。 当正则表达式中匹配?本身时，需要使用 \x3f 代替。如 ab?，在 NIP 上输入 ab\x3f。
.	匹配除\n 之外任何单个字符，包括空格。	-
	左边和右边的字符为或的关系。	的前后必须有字符或表达式，如写成 ab 是不正确的。

元字符	含义	说明
\x	16 进制。	\x 表示 16 进制时,后面必须有两个字符,如\x0a。另外,只能包含 0~9 和 a~f 这 16 个字符。匹配字符?、"时需要使用 16 进制。
[xyz]	匹配方括号内列出的任意字符。	-
[^xyz]	匹配除了方括号内列出的字符外的任意字符。	^在字符前。
[a-z]	匹配指定范围内的任意字符。	<ul style="list-style-type: none"> []里面不能出现字符(、)、[、]、\、{、}、+、*、?、.、 。 []里面至少包含一个确定的字符。
[^a-z]	匹配不在指定范围内的任意字符。	<ul style="list-style-type: none"> []里面不能出现字符(、)、[、]、\、{、}、+、*、?、.、 。 在[]里面至少有一个确定的字符。 ^只能出现在[]的开始处。
()	标记一个子表达式的开始和结束位置。	-
{n,m}	m 和 n 均为非负整数, $n \leq m$ 。匹配连续出现的次数为 $n \sim m$ 次。	,与 n 和 m 之间不能有空格。
{i}	前一个字符不区分大小写。	<ul style="list-style-type: none"> {i}前面的字符个数必须是确定的。如 <code>abc+{i}</code>、<code>abc*{i}</code>、<code>abc?{i}</code>、<code>abc{2,10}{i}</code>都是错误的。 {i}不能连续出现多次。

举例：配置威胁防护策略

对攻击特征已经明确的攻击行为,采用预定义签名的方式,通过签名集和覆盖签名配置威胁防护策略,满足安全性的需求。

前提条件

为确保威胁防护策略的有效性,请确保已经完成威胁防护签名库升级。

需求

保护企业内网的 HTTP 服务器,使得 HTTP 服务器避免受到来自 Internet 的攻击。要求禁用 ID 为 24109 的签名。



说明:

此处的禁用 ID 仅为举例，请用户根据网络的实际攻击特征进行配置。

配置思路

配置使用签名集和覆盖签名的威胁防护策略的思路如下：

1. 配置全局参数。（本例以缺省值为例）
2. 新建一条威胁防护策略后，新建签名集，保护 HTTP 服务器。
3. 使用覆盖签名修改 ID 为 24109 的签名为禁用。

操作步骤

1. 配置全局参数。
 - a. 选择“应用安全 > 威胁防护 > 策略”。
 - b. 在“配置全局参数”中配置威胁防护全局参数，选择缺省值。具体参数配置如下：
 - IPS 工作模式（直路）：防护模式
 - IDS 工作模式（旁路）：告警模式
 - 特权策略：None
 - c. 单击“应用”。
2. 新建威胁防护策略，名称为 policy_http。
 - a. 在“威胁防护策略列表”中单击“新建”。
 - b. 依次输入或选择各项参数。具体参数配置如下：
 - 名称：policy_http
 - 描述：Threat prevention policy for HTTP server
 - 同步策略/策略模板：无
 - c. 单击“应用”。
3. 新建签名集 set_http。
 - a. 在“签名集列表”区域框中单击“新建”。
 - b. 依次输入或选择各项参数。具体参数配置如下：

- 名称：set_http
 - 方向：去服务端
 - 严重性：大于等于错误
 - 可信度：全部（缺省值）
 - 协议：HTTP
 - 类别：全选（缺省值）
 - 状态：启用（缺省值）
 - 动作：阻断（缺省值）
- c. 单击“确定”。
4. 配置覆盖签名，修改预定义签名的状态。
- a. 在“覆盖(Overrides)列表”中单击“新建”。
- b. 依次输入或选择各项参数，配置如下：
- 已选择签名：24109
 - 状态：未启用
 - 动作：告警（缺省值）
- c. 单击“确定”。
5. 单击“返回”，界面弹出是否立即提交的确认框。单击“是”，等提交成功后单击“确定”。

结果验证

配置完成后，创建的签名集如[图 1](#)所示。

图 1 签名集配置结果

签名集列表								
+ 新建 刷新								
名称	协议	方向	严重性	可信度	类别	状态	动作	配置
set_http	HTTP	to-server	>= error	all	all	已启用	阻断	  

覆盖签名如[图 2](#)所示。

图 2 覆盖签名配置结果

覆盖(Overrides)列表				
  				
<input type="checkbox"/> 签名ID	签名名称	状态	动作	配置
<input type="checkbox"/> 24109	Web Attack: Sun Java Webstart BasicServiceImpl CVE-2010-3563	未启用	告警	

创建的威胁防护策略如[图 3](#)所示。

图 3 威胁防护策略配置结果

威胁防护策略列表				
  				
名称	引用	描述	状态	配置
default	是	Threat prevention policy	已提交	 
policy_http	否	Threat prevention policy for HTTP server	已提交	 

后续处理

威胁防护策略配置完成后，选择“应用安全 > 策略应用 > 接口对”，将策略应用在指定的 IPS 接口对或 IDS 接口对上才能生效。

用户可以根据“同步策略/策略模板”，复制策略 policy_http，并根据实际需求修改签名集或覆盖签名，新建一条威胁防护策略。

举例：配置自定义签名

用户已知某类攻击依靠预定义签名无法检测出，可根据攻击报文的特征及实际网络情况编写自定义签名，从而快速地阻挡攻击。

需求

很多攻击者在攻击 HTTP 服务器前会先执行命令 GET/server-status HTTP/1.1 或 GET/server-info HTTP/1.1 获取要攻击的服务器基本信息。根据服务器信息找到相关漏洞，再进行攻击。设备需要阻挡这类攻击，可以通过自定义签名的方式将攻击加入威胁防护策略中进行防护。

因此，当设备收到的报文具有以下特征时，即认为是攻击报文。分析攻击特征可以知道攻击报文具有如下属性：

- 报文的协议是 HTTP
- 报文的方向是从客户端到服务器

- 报文的内容包含 GET/server-status HTTP/1.1 或 GET/server-info HTTP/1.1



说明：

- 不同的客户端在发出 GET 请求时，GET 后面可以带的字符为空格，Tab 键或空格与 Tab 键的任意组合，并且均可以重复多次。
- 请用户根据网络的实际攻击特征进行配置。建议用户只在非常了解攻击特征的情况下进行配置，因为设置错误不仅无法阻断攻击，还有可能导致报文误丢弃或业务不通等问题。

配置思路

配置自定义签名的思路如下：

1. 新建一条自定义签名，保护 HTTP 服务器的信息不被攻击者获取。协议为 HTTP，方向为发往服务器的报文，即 HTTP 请求信息，关键字定义为获取服务器信息。
2. 覆盖签名中引用新建的自定义签名。（假设威胁防护策略已经创建，名为 ips_policy，并已应用在 IPS 接口对上。）

操作步骤

1. 新建一条自定义签名。
 - a. 选择“应用安全 > 威胁防护 > 自定义签名”。
 - b. 在“自定义签名列表”中单击“新建”。
 - c. 依次输入或选择各项参数，配置如下：
 - ID：10
 - 名称：user_defined
 - 协议：HTTP
 - 方向：去服务端
 - 关键字：GET[\x20\x09]+/server-(info|status)



说明：


1. GET 为字符串，表示报文中包含 GET。

2. [\x20\x09]+表示空格、Tab 键或者是空格和 Tab 键的任意组合在报文中出现一次或者多次。[]表示匹配其中的任意字符。\\x20 是 16 进制，表示空格；\\x09 也是 16 进制，表示 Tab 键。+表示前一个字符在目标对象中出现 1 次或连续多次。
3. /server-为字符串，表示报文中包含/server-。
4. (info|status)表示报文中包含 info 或者 status 这两个字符串的任意一个。

其他参数均为缺省值。

- d. 单击“应用”。

2. 引用签名。

- a. 选择“应用安全 > 威胁防护 > 策略”。
- b. 在“威胁防护策略列表”区域框中单击，修改策略 ips_policy。
- c. 在“覆盖(Overrides)列表”中单击“新建”。
- d. 依次输入或选择各项参数，配置如下：
 - 已选择签名：10
 - 状态：启用
 - 动作：阻断
- e. 单击“确定”。

3. 单击“返回”，界面弹出是否立即提交的确认框。单击“是”，等提交成功后单击“确定”。

结果验证

配置完成后，自定义签名如[图 1](#)所示。

图 1 自定义签名配置结果

<input type="checkbox"/> ID	名称	协议	方向	严重性	状态	命中次数	配置
<input type="checkbox"/> 10	user_defined	HTTP	to-server	warning	modified	0	

配置完成后，自定义签名如[图 2](#)所示。

图 2 覆盖签名配置结果

<input type="checkbox"/> 签名ID	签名名称	状态	动作
<input type="checkbox"/> 10	user_defined	已启用	阻断

应用控制简介

NIP 利用业务感知技术，检测和识别流经报文的应用层协议。

随着互联网的飞速发展，随时随地享受网络带来的便捷已经成为人们生活中不可或缺的一部分。但是一些网络应用（如 BT，PPLive 等）的出现，占用了大量的网络带宽，使得本就并不宽裕的网络资源变得更加紧张，用户的上网体验度也与日俱下。因此，控制网络应用，提高用户上网体验度成了迫在眉睫的问题。

NIP 利用业务感知技术对网络中的流量进行协议识别，并针对协议实施不同的控制策略。业务感知技术能够对网络中的流量进行协议解析，并与应用控制知识库中的规则进行匹配，识别出具体的协议。

预定义应用协议

缺省情况下，设备中存在一个知识库文件。知识库中包含了大部分常见的网络报文的特征协议，即预定义应用协议。预定义应用协议分为：

- 大类

大类是对一类协议的总称，包括 P2P，IM，VoIP，Video 等大类。

- 小类

小类是对大类的分解，是具体的应用协议。

自定义应用协议

自定义应用协议是用户根据报文的源端口、目的端口和关键字等信息，定义出来的对报文进行更精确的定位控制的应用规则。

一般情况下，通过更新知识库获取的自定义应用协议，已基本可以满足应用需求。当预定义应用协议无法满足对流量的应用控制需求，或者需要对流量进行更精准的控制时，可以配置自定义的应用协议规则，针对应用程序产生的报文的源或者目的端口、关键字等信息进行来对报文进行检测识别，然后对应用程序进行阻断或放行控制。

应用控制方式

NIP 的应用控制即可对网络中不同的流量类型实施不同的控制策略。您可以对一个大类实施应用控制，也可以对具体的小类实施应用控制，通常情况下都是针对协议大类实施应用控制。

应用控制方式分为：

- 阻断

阻断指定应用协议的报文通过设备。如果某企业网内需要阻断 IM 大类的应用，此时将控制方式设置为阻断。

- 允许

允许放行指定应用协议的报文通过设备。为了保证正常 Web 浏览业务，通常将 Web_Browsing 大类设置为放行。

- 限流及连接数限制

针对指定应用协议报文，限制流量或连接数。P2P 大类通常被设置为限流，以保证网络流量能正常运行其他业务。

配置应用控制策略

应用控制策略能够直接指定监控的应用协议类型和管理动作。

- [配置全局参数](#)

启用应用识别增强功能会一定程度地影响设备性能，请根据协议的选择正确地启用该功能。

- [新建应用控制策略](#)

应用控制策略可以选择通过基本规则或高级规则创建。

配置全局参数

启用应用识别增强功能会一定程度地影响设备性能，请根据协议的选择正确地启用该功能。

背景信息

启用应用识别增强功能后，不仅能够实现对某些多通道协议的快速识别，而且能够实现对特定类型报文的所有字节的检测。应用识别增强功能提高了协议识别的速度和准确率。



说明：

由于应用识别增加功能会对性能有所影响，因此请对照[应用协议速查表](#)确认是否需要启用该功能。

操作步骤

1. 选择“应用安全 > 应用控制 > 策略”。
2. 选择“配置全局参数”页签。
3. 选择“启用”，应用识别增强功能启用。

新建应用控制策略

应用控制策略可以选择通过基本规则或高级规则创建。



注意：

配置应用控制策略前，请确保已经完成升级应用控制知识库到最新版本。

在一个应用控制策略中，可以定义一条或多条规则，进行顺序匹配。

在一条应用控制策略内部，可以直接指定协议大类或小类来匹配（基本规则），也可以引用应用协议集来匹配（高级规则）。

设备将首先匹配基本规则，然后匹配高级规则。基本规则的先后顺序不可调整；高级规则的先后顺序可以调整。

设备提供了两个缺省应用控制策略，分别为 IM 类的 **Default_IM** 和 P2P 类的 **Default_P2P**，只能查看和使用，不可编辑或删除。

新建应用控制策略

1. 选择“应用安全 > 应用控制 > 策略”。

2. 单击“应用控制策略列表”区域框中的“新建”。
3. 依次输入或选择各项参数，如表 1 所示。
4. 单击“应用”。

表 1 新建应用控制策略参数说明

参数	说明	取值建议
名称	策略的名称。	-
描述	策略的描述信息。	-

5. 配置应用控制策略规则。根据不同需要，进行以下配置：

- 直接指定应用协议类型。（基本规则）
 - a. 单击需要配置的协议名称，进入“应用协议”界面。
 - b. 依次输入或选择各项参数，如表 2 所示。
 - c. 单击“确定”。
 - d. 单击“应用”。

表 2 应用协议参数说明

参数	说明	取值建议
协议名称	应用协议或协议大类的名称。	-
控制方式	对采用指定协议传输的报文的处理方式。	<ul style="list-style-type: none"> ▪ 阻断：阻断采用指定协议传输的报文。 ▪ 允许：放行采用指定协议传输的报文。 ▪ 限流及连接数限制：对采用指定协议传输的报文限流或连接数限制。 <p>说明： 接口在 IPS 模式下三种控制方式均生效；而接口在 IDS 模式下，阻断和限流及连接数限制均不生效，因此选择“允许”即可。</p>
限流速率	当“控制方式”为限流及连接数限制时，需要设置此项。 对采用指定应用协议集中的协议传输的报文限制传输时的最大速率。	-
连接数限制	当“控制方式”为限流及连接数限制时，需要设置此项。 对采用指定应用协议集中的协议传输的报文做基于 IP 的连接数限制。	-
连接数限制方向	当配置“连接数限制”后，需要设置此项。	<ul style="list-style-type: none"> ▪ 源：对源地址进行连接数限制。

表 2 应用协议参数说明		
参数	说明	取值建议
	基于 IP 地址，对指定方向的连接进行连接数限制。	<ul style="list-style-type: none"> 目的：对目的地址进行连接数限制。 双向：对源和目的地址同时进行连接数限制。
时间段	指定规则生效的时间段。	<ul style="list-style-type: none"> 已经创建的时间段，或者新建的时间段。 all：表示所有时间。

- 引用指定的应用协议集。（高级规则）
 - 单击“应用协议集引用”中的“新建”。
 - 依次输入或选择各项参数，如表 3 所示。
 - 单击“应用”。

表 3 新建应用协议集引用参数说明		
参数	说明	取值建议
应用协议集	任意应用协议或协议大类的集合。	-
控制方式	对采用指定应用协议集中的协议传输的报文的处理方式。	<ul style="list-style-type: none"> 阻断：阻断采用指定应用协议集中的协议传输的报文。 允许：放行采用指定应用协议集中的协议传输的报文。 限流及连接数限制：对采用指定应用协议集中的协议传输的报文限流或连接数限制。 <p>说明： 接口在 IPS 模式下三种控制方式均生效；而接口在 IDS 模式下，阻断和限流及连接数限制均不生效，因此选择“允许”即可。</p>
限流速率	当“控制方式”为限流及连接数限制时，需要设置此项。 对采用指定应用协议集中的协议传输的报文限制传输时的最大速率。	-
连接数限制	当“控制方式”为限流及连接数限制时，需要设置此项。 对采用指定应用协议集中的协议传输的报文做基于 IP 的连接数限制。	-
连接数限制方向	当配置“连接数限制”后，需要设置此项。 基于 IP 地址，对指定方向的连接进行连接数限制。	<ul style="list-style-type: none"> 源：对源地址进行连接数限制。 目的：对目的地址进行连接数限制。

表 3 新建应用协议集引用参数说明		
参数	说明	取值建议
		<ul style="list-style-type: none"> 双向：对源和目的地址同时进行连接数限制。
时间段	该规则生效的时间段。	已经创建的时间段，或者新建的时间段。 all：表示所有时间。

配置应用协议集

配置应用控制策略时，如果希望在一条规则中完成配置对多个类型应用协议的检测，需要配置应用协议集。

NIP 支持检测多种类型的应用协议。当创建多个应用协议集时，建议使用有意义的名字命名应用协议集以方便记忆和管理。

将需要检测的应用协议类型加入应用协议集的两种方法：

- 只指定大类：将大类中包括的所有应用协议类型全部加入应用协议集。
- 指定小类：将某一小类定义的应用协议类型加入应用协议集。

新建应用协议集

- 选择“应用安全 > 应用控制 > 应用协议集”。
- 单击“应用协议集列表”区域框中的“新建”。
- 依次输入或选择各项参数，如表 1 所示。
- 单击“应用”。

如果操作成功，则界面返回“应用协议集”，且列表中添加新配置项。

表 1 新建应用协议集参数说明		
参数	说明	取值建议
名称	应用协议集的名称。	-
描述	应用协议集的描述信息。	-
应用协议	设备提供的可供选择的应用协议，包含预定义应用协议和自定义的应用协议（在最后 userdefine 项中显示）。	预定义应用协议获取自应用控制知识库文件，应用控制知识库的版本不同，包含的应用层协议也会不同。

表 1 新建应用协议集参数说明

参数	说明	取值建议
已选应用	已经选择的需要控制的应用协议。	增加应用协议：选中“应用协议”中应用协议对应的复选框。 删除应用协议：选中“已选应用”中应用协议，单击“取消选择”。

新建自定义应用协议

当预定义应用协议无法满足对流量的应用控制需求，或者需要对流量进行更精准的控制时，可以通过配置自定义应用协议来对流量进行控制，可以指定协议类型、源端口、目的端口、关键字等信息。

新建自定义应用协议

1. 选择“应用安全 > 应用控制 > 自定义应用协议”。
2. 单击“自定义应用协议列表”中的“新建”。
3. 配置自定义应用协议的“名称”和“描述”。
4. 单击“应用”。
5. **可选：**配置自定义应用协议的端口信息。

依次输入或选择各项参数，如[表 1](#)所示。

表 1 新建自定义应用协议参数说明

参数	说明	取值建议
协议	需要匹配的协议类型，分为 TCP、UDP 两种协议。	-
源端口	配置自定义应用协议的源端口。	-
目的端口	配置自定义应用协议的目的端口。	-

6. **可选：**配置自定义应用协议的关键字信息。
 - a. 在“关键字列表”中，单击“新建”。
 - b. 依次输入或选择各项参数，如[表 2](#)所示。

表 2 添加关键字参数说明		
参数	说明	取值建议
类型	指定关键字的类型，可配置如下两种类型。 <ul style="list-style-type: none"> 十六进制 字符串 	-
关键字	指定关键字的内容，通过报文内容和关键字的是否匹配来判断报文的转发和阻断。 <ul style="list-style-type: none"> 当关键字的类型为十六进制类型时，关键字的内容字符类型必须为[0～9]，[a～f]和[A～F]，并且内容长度必须是偶数且不大于 62 个字符。 当关键字的类型为字符串类型时，关键字的内容不区分大小写，内容长度取值范围 1～31 个字符。 	-
匹配位置	指定关键字的偏移方向。 <ul style="list-style-type: none"> None：从数据区域起始位置开始匹配 64 字节，并且同时从结束位置往回匹配 64 字节。 载荷头：以数据区域起始位置为 0 点，开始计算偏移量。 载荷尾：以数据区域结束位置为 0 点，往回计算偏移量。 	如果关键字包含在距离数据区域起始位置 64 字节范围内，则需要选择 None 或者载荷头。 如果关键字包含在距离数据区域结束位置 64 字节范围内，则需要选择 None 或者载荷尾。
偏移量	指定关键字的偏移量。 <ul style="list-style-type: none"> “匹配位置”选择 None 时无需配置。 “匹配位置”选择载荷头时表示从数据区域起始位置到所配置“关键字”起始位置的字节数。 “匹配位置”选择载荷尾时表示从数据区域结束位置到所配置“关键字”结束位置的字节数。 	配置偏移量后只从偏移量开始匹配特征字字节长度的范围。

c. 单击“确定”。

7. 单击“应用”。

界面中显示新建的自定义应用协议，则表明操作成功。

说明：

例如某报文整个数据区域的十六进制格式如下所示：

```

27 3B 89 BB 01 16 B3 1D 6E A7 63 A9 D3 48 C3 F1
CC D0 5E 2B 40 43 E5 C3 07 D5 48 7D 16 8A B4 0E
9B D8 98 9E 42 7F 7D A0 D1 6C 0F CC F4 62 F0 1F
9B 14 87 C1 EC CC 82 BA C9 09 A9 7D 0A C2 AA 1F
42 B0 FA 25 94 1C 22 C3 15 1C E9 14 56 17 E8 3E
39 F2 2F CD 69 67 E0 23 72 56 B1 8F 41 06 3E 87
70 96 98 00 07 D2 BE 16 33 01 F4 21 58 F8 A6 89
AC 3F AA DC 05 56 0B E9 9F 13 3F 84 E0 E8 5D C2
7B 00 00 E2 18 E0 F4 B8 9A 9C 57 5F AE 88 F0 AD
48 64 AF D4 E8 7E A8 5B EB A2 3F 4A B8 0C 25 8C
6E 04 2E 18 C9 18 E4 EC B2 6E 45 4C 9B C0 BE B2
2B 04 E4 86 4E 15 BF 52 B8 2B F6 AA 00 07 E9 6C
    
```

- 前后两个蓝框内的内容均可以作为关键字内容，关键字类型选择十六进制。
- 如果关键字配置为 B31D，那么“匹配位置”需要选择 None 或者载荷头，选择载荷头时“偏移量”设置为 6。
- 如果关键字配置为 B82B，那么“匹配位置”需要选择 None 或者载荷尾，选择载荷尾时“偏移量”设置为 6。

策略应用

应用安全策略配置后，需要应用在 IPS 接口对或 IDS 接口对上。

- [在直路 IPS 接口对上应用策略](#)

应用策略需要应用到接口对上后才生效。新的应用安全策略可以通过新建或者复制已有策略完成。

- [在 IDS 接口对上应用策略](#)

应用策略需要应用到接口对上后才生效。新的应用安全策略可以通过新建或者复制已有策略完成。

- [在单臂 IPS 接口对上应用策略](#)

应用策略需要应用到接口对上后才生效。新的应用安全策略可以通过新建或者复制已有策略完成。

在直路 IPS 接口对上应用策略

应用策略需要应用到接口对上后才生效。新的应用安全策略可以通过新建或者复制已有策略完成。

在直路 IPS 接口对上新建应用安全策略

1. 选择“应用安全 > 策略应用 > 接口对”。

 表示是直路 IPS 接口对； 表示是 IDS 接口对； 表示是单臂 IPS 接口对。

2. 在“策略列表”区域框中，单击“新建”。
3. 依次输入或选择各项参数，如表 1 所示。
4. 单击“应用”。

表 1 新建应用安全策略参数说明

参数	说明	取值建议
方向	策略应用的接口对方向。每个接口对有两个方向。 复制或插入后的应用安全策略不能修改方向。	方向指的是访问发起的方向，也就是报文首包的方向。
VLAN ID	报文 Tag 中 VID 字段的值。	-
源地址	报文的源 IP 地址，可以是一个或多个 IP 地址/IP 地址范围、地址组。	<ul style="list-style-type: none"> IP 地址/IP 地址范围。 已经创建的地址、地址组名称，或者新建的地址、地址组。 不设置或者选择 any 表示可以为任意 IP 地址。
目的地址	报文的目的 IP 地址，可以是一个或多个 IP 地址/IP 地址范围、地址组。	<ul style="list-style-type: none"> IP 地址/IP 地址范围。 已经创建的地址、地址组名称，或者新建的地址、地址组。 不设置或者选择 any 表示可以为任意 IP 地址。
服务	设备提供的服务类型。	<ul style="list-style-type: none"> 设备中已存在的自定义服务、服务组及预定义服务。 新建的自定义服务、服务组。
动作	设备对符合策略报文的处理方式。	<ul style="list-style-type: none"> permit: 表示允许符合条件的报文通过。 deny: 表示拒绝符合条件的报文通过。
应用控制策略	已配置的应用控制策略。	根据安全需求，选择是否应用该策略。
威胁防护策略	缺省的和已配置的威胁防护策略。	根据安全需求，选择是否应用该策略。
反病毒策略	已配置的反病毒策略。	根据安全需求，选择是否应用该策略。
自定义连接时长	对特定应用的数据流定义连接时长，保证报文在长时间没有到达设备后再次到达时，仍然能够通过设备，从而使这些应用不中断。	选择“开启”，自定义连接功能启用。
记录日志	是否启用会话日志记录功能。 启用后设备将记录允许通过的符合条件的数据流量。	选择“开启”，日志记录功能启用。
描述	应用安全策略的描述信息。	建议根据安全需求，详细描述策略的功能，

表 1 新建应用安全策略参数说明

参数	说明	取值建议
		方便后续维护。

其他操作



操作	说明
删除	被应用安全策略引用的威胁防护策略不能删除。可以通过“应用安全 > 策略应用”查看策略的引用情况。
启用	选择并单击待启用策略的复选框。策略被应用后，状态为启用。取消启用后，策略将失效。
复制	单击  ，复制指定策略。 复制已有的应用安全策略可以简化配置过程。当安全需求与已有策略相似时，可以采用此方法，然后根据具体需求修改。
移动	单击  ，移动策略的位置，调整策略的优先级。
插入	单击  后，将新建一条策略。新建策略插入在该策略前。

在 IDS 接口对上应用策略

应用策略需要应用到接口对上后才生效。新的应用安全策略可以通过新建或者复制已有策略完成。

在 IDS 接口对上新建应用安全策略

1. 选择“应用安全 > 策略应用 > 接口对”。

 表示是直路 IPS 接口对； 表示是 IDS 接口对； 表示是单臂 IPS 接口对。

2. 在“策略列表”中，单击“新建”。
3. 依次输入或选择各项参数，如[表 1](#)所示。
4. 单击“应用”。




表 1 新建应用安全策略参数说明

参数	说明	取值建议
VLAN ID	报文 Tag 中 VID 字段的值。	-
源地址	报文的源 IP 地址，可以是一个或多个 IP 地址/IP 地址范围、地址组。	<ul style="list-style-type: none"> IP 地址/IP 地址范围。

表 1 新建应用安全策略参数说明

参数	说明	取值建议
		<ul style="list-style-type: none"> 已经创建的地址、地址组名称，或者新建的地址、地址组。 不设置或者选择 any 表示可以为任意 IP 地址。
目的地址	报文的目的 IP 地址，可以是一个或多个 IP 地址/IP 地址范围、地址组。	<ul style="list-style-type: none"> IP 地址/IP 地址范围。 已经创建的地址、地址组名称，或者新建的地址、地址组。 不设置或者选择 any 表示可以为任意 IP 地址。
服务	设备提供的服务类型。	<ul style="list-style-type: none"> 设备中已存在的自定义服务、服务组及预定义服务。 新建的自定义服务、服务组。 缺省情况下，为 IP 服务。
应用控制策略	已配置的应用控制策略。	根据安全需求，选择是否应用该策略。
威胁防护策略	缺省的和已配置的威胁防护策略。	根据安全需求，选择是否应用该策略。
记录日志	是否启用会话日志记录功能。 启用后设备将记录允许通过的符合条件的数据流量。	选择“开启”，日志记录功能启用。
描述	应用安全策略的描述信息。	建议根据安全需求，详细描述策略的功能，方便后续维护。

其他操作

操作	说明
删除	被应用安全策略引用的威胁防护策略不能删除。可以通过“应用安全 > 策略应用”查看策略的引用情况。
启用	选择并单击待启用策略的复选框。策略被应用后，状态为启用。取消启用后，策略将失效。
复制	单击  ，复制指定策略。 复制已有的应用安全策略可以简化配置过程。当安全需求与已有策略相似时，可以采用此方法，然后根据具体需求修改。
移动	单击  ，移动策略的位置，调整策略的优先级。
插入	单击  后，将新建一条策略。新建策略插入在该策略前。

在单臂 IPS 接口对上应用策略

应用策略需要应用到接口对上后才生效。新的应用安全策略可以通过新建或者复制已有策略完成。

在单臂 IPS 接口对上新建应用安全策略

1. 选择“应用安全 > 策略应用 > 接口对”。

 表示是直路 IPS 接口对； 表示是 IDS 接口对； 表示是单臂 IPS 接口对。

2. 在“策略列表”区域框中，单击“新建”。
3. 依次输入或选择各项参数，如表 1 所示。
4. 单击“应用”。




表 1 新建应用安全策略参数说明

参数	说明	取值建议
VLAN ID	报文 Tag 中 VID 字段的值。	-
源地址	报文的源 IP 地址，可以是一个或多个 IP 地址/IP 地址范围、地址组。	<ul style="list-style-type: none"> IP 地址/IP 地址范围。 已经创建的地址、地址组名称，或者新建的地址、地址组。 不设置或者选择 any 表示可以为任意 IP 地址。
目的地址	报文的目的 IP 地址，可以是一个或多个 IP 地址/IP 地址范围、地址组。	<ul style="list-style-type: none"> IP 地址/IP 地址范围。 已经创建的地址、地址组名称，或者新建的地址、地址组。 不设置或者选择 any 表示可以为任意 IP 地址。
服务	设备提供的服务类型。	<ul style="list-style-type: none"> 设备中已存在的自定义服务、服务组及预定义服务。 新建的自定义服务、服务组。
动作	设备对符合策略报文的处理方式。	<ul style="list-style-type: none"> permit: 表示允许符合条件的报文通过。 deny: 表示拒绝符合条件的报文通过。
应用控制策略	已配置的应用控制策略。	根据安全需求，选择是否应用该策略。
威胁防护策略	缺省的和已配置的威胁防护策略。	根据安全需求，选择是否应用该策略。
反病毒策略	已配置的反病毒策略。	根据安全需求，选择是否应用该策略。
自定义连接时长	对特定应用的数据流定义连接时长，保证报文在长时间没有到达设备后再次到达时，仍然能够通过设备，从而使这些应用不中断。	选择“开启”，自定义连接功能启用。

表 1 新建应用安全策略参数说明

参数	说明	取值建议
记录日志	是否启用会话日志记录功能。 启用后设备将记录允许通过的符合条件的数据流量。	选择“开启”，日志记录功能启用。
描述	应用安全策略的描述信息。	建议根据安全需求，详细描述策略的功能，方便后续维护。

其他操作

操作	说明
删除	被应用安全策略引用的威胁防护策略不能删除。可以通过“应用安全 > 策略应用”查看策略的引用情况。
启用	选择并单击待启用策略的复选框。策略被应用后，状态为启用。取消启用后，策略将失效。
复制	单击  ，复制指定策略。 复制已有的应用安全策略可以简化配置过程。当安全需求与已有策略相似时，可以采用此方法，然后根据具体需求修改。
移动	单击  ，移动策略的位置，调整策略的优先级。
插入	单击  后，将新建一条策略。新建策略插入在该策略前。

调整策略优先级

当安全威胁发生变化，用户可以调整应用安全策略的优先级来满足新的安全需求。

背景信息


在同一个接口对，可以配置多个应用安全策略。

应用安全策略之间存在优先关系。在“策略列表”区域框中，排在上面的应用安全策略优先级比排在下面的应用安全策略的优先级高。

调整应用安全策略的位置可以实现调整应用安全策略的优先级。

操作步骤

1. 选择“应用安全 > 策略应用”。

2. 在“策略列表”区域框中单击 ，输入目标位置应用安全策略的 ID，将该应用安全策略排到目标应用安全策略的前面或后面。

举例：利用策略优先级满足多层次防护需求

企业用户针对业务的不同，有不同的安全需求。因此在配置策略时根据优先级规划出多级防护需求。

组网需求

某企业内网地址为 172.16.0.0/16 网段，根据该企业不同部门的应用及安全需求，进行多级防护。

安全需求如下：

- 部门 A：172.16.1.0/24，检测 P2P 流量，需进行应用控制检测。
- 部门 A：特权用户（172.16.1.2/32）不进行任何检测，直接放行。
- 部门 B：172.16.2.0/24，不进行应用控制。
- 部门 C：172.16.3.0/24，不允许上网。
- 所有用户（特权用户除外）需要进行威胁防护检测。
- Web 服务器：172.16.4.1/32，Web 服务器通过 80 端口对外网用户提供 Web 服务，只针对访问 80 端口的流量进行威胁防护检测。

配置思路

配置多级防护的配置思路如下：

1. 策略的匹配顺序自上而下。
2. 部门 A 的特权用户优先级最高，不进行检测。因此将部门 A 的策略分为两个，特权用户优先级高。
3. 阻断的流量优先级高。因此部门 C 的策略优先级高于所有部门上网的优先级。




说明：

举例中使用了缺省的威胁防护策略 **default** 和缺省的应用控制策略 **Default_P2P**。

假设流量经过 NIP 的方向为 a01->b01，因此所有策略定义在 a01->b01 上。

操作步骤


1. 配置部门 A 的特权用户的应用安全策略。

- a. 选择“应用安全 > 策略应用 > 接口对”。
- b. 在“策略列表”区域框中，单击，新建 a01->b01 方向上的策略。
- c. 依次输入或选择各项参数。具体参数配置如下：

- 源地址：172.16.1.2/32
- 目的地址：any
- 动作：permit（缺省值）

其余参数配置为缺省值。


2. 配置部门 C 的应用安全策略。

- a. 在“策略列表”区域框中，单击，新建 a01->b01 方向上的策略。
- b. 依次输入或选择各项参数。具体参数配置如下：

- 源地址：172.16.3.0/24
- 目的地址：any
- 动作：deny

其余参数配置为缺省值。

3. 配置部门 A 的应用安全策略。

- a. 在“策略列表”区域框中，单击，新建 a01->b01 方向上的策略。
- b. 依次输入或选择各项参数。具体参数配置如下：

- 源地址：172.16.1.0/24
- 目的地址：any
- 动作：permit（缺省值）
- 应用控制策略：Default_P2P
- 威胁防护策略：default


其余参数配置为缺省值。



注意：

针对所有用户上网策略，部门 A 的应用安全策略为细化的策略，因此部门 A 配置了威胁防护策略 **default** 后，所有用户上网策略中仍然需要配置威胁防护策略 **default**，才能保证策略应用的正确性。

4. 配置 Web 服务器的应用安全策略。


a. 在“策略列表”区域框中，单击，新建 a01->b01 方向上的策略。

b. 依次输入或选择各项参数。具体参数配置如下：

- 源地址：any
- 目的地址：172.16.4.1/32
- 服务：http
- 动作：permit（缺省值）
- 威胁防护策略：default

其余参数配置为缺省值。

5. 对所有用户（特权用户除外）进行威胁防护策略。

a. 在“策略列表”区域框中，单击，新建 a01->b01 方向上的策略。


b. 依次输入或选择各项参数。具体参数配置如下：

- 源地址：172.16.0.0/16
- 目的地址：any
- 服务：ip
- 动作：permit（缺省值）
- 威胁防护策略：default

其余参数配置为缺省值。

6. **可选：**配置不受任何限制的策略，作为应急情况下，保障所有用户业务访问 Internet 的策略。

缺省情况下，设备上已经存在该策略。

- a. 在“策略列表”区域框中，单击，新建 a01->b01 方向上的策略。
- b. 依次输入或选择各项参数。具体参数配置如下：

- 源地址：any
- 目的地址：any
- 服务：ip（缺省值）
- 动作：permit（缺省值）

其余参数配置为缺省值。

后续处理


配置完成后，单击 移动策略的位置，将策略“0”移动到“策略列表”的最下面，应用安全策略如[图 1](#)所示。

图 1 应用安全策略配置结果

<input type="checkbox"/>	ID	VLAN ID	源地址	目的地址	服务	动作	应用控制策略	威胁防护策略	反病毒策略	描述
a01 → b01 (7 Items)										
<input type="checkbox"/>	1	any	172.16.1.2/32	any	ip	permit	--	--	--	--
<input type="checkbox"/>	2	any	172.16.3.0/24	any	ip	deny	--	--	--	--
<input type="checkbox"/>	3	any	172.16.1.0/24	any	ip	permit	Default_P2P	default	--	--
<input type="checkbox"/>	4	any	any	172.16.4.1/32	http	permit	--	default	--	--
<input type="checkbox"/>	5	any	172.16.0.0/16	any	ip	permit	--	default	--	--
<input type="checkbox"/>	6	any	any	any	ip	permit	--	--	--	--
<input type="checkbox"/>	0	any	any	any	ip	permit	--	default	--	--

当网络故障发生时，可以通过移动各策略的位置，来满足网络的不同安全需求。

例如，当需要所有用户不进行时，将策略 6 移动至列表首位。流量匹配策略 6 后，将不再匹配其他策略。

移动完成后，应用安全策略如[图 2](#)所示。

图 2 应急状态下的应用安全策略配置结果

<input type="checkbox"/>	ID	VLAN ID	源地址	目的地址	服务	动作	应用控制策略	威胁防护策略	反病毒策略	描述
a01 → b01 (7 Items)										
<input type="checkbox"/>	6	any	any	any	ip	permit	--	--	--	--
<input type="checkbox"/>	1	any	172.16.1.2/32	any	ip	permit	--	--	--	--
<input type="checkbox"/>	2	any	172.16.3.0/24	any	ip	deny	--	--	--	--
<input type="checkbox"/>	3	any	172.16.1.0/24	any	ip	permit	Default_P2P	default	--	--
<input type="checkbox"/>	4	any	any	172.16.4.1/32	http	permit	--	default	--	--
<input type="checkbox"/>	5	any	172.16.0.0/16	any	ip	permit	--	default	--	--
<input type="checkbox"/>	0	any	any	any	ip	permit	--	default	--	--

HCIE-Security 模拟面试问题及面试建议

1. NIP 设备上能够提供哪些应用安全？