使用SDWAN的配置组启用安全功能

目录

简介

本文档介绍如何通过配置组配置NGFW、URL过滤、AMP和IPS/IDS，包括统一日志记录的说明。

先决条件

实现流可视性和应用可视性

如果使用策略组定义策略：

- 选择Policy group，然后选择Application priority and SLA。
- 选择新增
- 点击其他设置(Additional settings)并启用应用可视性和流可视性(Application visibility and Flow visibility)

如果您使用的是旧策略

- 在配置组中选择Cli附加配置文件并添加以下命令

```
policy
app-visibility
flow-visibility
```

确保您符合此处提供的功能的必备条件
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/url-filtering.html

```
Note: If you are using the legacy policy along with Configuration groups :

Select Configuration and Click Security
Click Custom Options and select Policies/Profiles and then access these features to enable
```

本文档重点介绍使用策略组启用的功能

下一代防火墙(NGFW)

要启用NGFW，请执行以下步骤：

- 选择Policy group，然后点击NGFW，然后点击Add NGFW Policy
- 为其指定策略名称，然后点击“下一步”
- 选择要与NGFW策略关联的配置组
- 添加规则，然后点击“下一步”
- 创建您的NGFW策略

要启用日志记录，请编辑NGFW策略，然后选择其他设置并打开统一日志记录

URL 过滤

要为20.18之前的版本启用URL过滤，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后单击Groups of Interest
- 选择安全，然后展开配置文件

要为版本20.18及更高版本启用url过滤，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后点击Objects and Profiles
- 选择安全配置文件

选择add url filtering，输入详细信息并点击save

高级恶意软件保护 (AMP)

要为20.18之前的版本启用AMP，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后单击Groups of Interest
- 选择安全，然后展开配置文件

要为版本20.18及更高版本启用AMP，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后点击Objects and Profiles
- 选择安全配置文件

选择Advanced Malware Protection并点击Add Advanced Malware Protection

添加详细信息并点击save

入侵防御系统(IPS)/入侵检测系统(IDS)

要为20.18之前的版本启用IPS/IDS，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后单击Groups of Interest
- 选择安全，然后展开配置文件

要为版本20.18及更高版本启用IPS/IDS，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后点击Objects and Profiles
- 选择安全配置文件

选择Intrusion Prevention并单击Add Intrusion Prevention

添加详细信息并点击save

创建高级检测配置文件(AIP)

要为20.18之前的版本启用AIP，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后单击Groups of Interest
- 选择安全，然后展开配置文件

要为版本20.18及更高版本启用AIP，请执行以下操作：

- 选择UI上的Configuration，然后选择Policy group，然后点击Objects and Profiles
- 选择安全配置文件

选择Advanced Inspection Profile，然后点击Add Advanced Inspection Profile

- 输入在前面的步骤中创建的AMP/IPS/Url过滤名称，然后点击save

AIP与NGFW的关联

- 选择Configuration，然后选择Policy groups，然后点击NGFW
- 编辑之前创建的NGFW策略
- 对于之前创建的NGFW规则，请编辑并关联之前创建的AIP配置文件，然后点击保存

日志记录

对于日志记录，使用cli add on通过配置组在路由器上启用此功能

```
policy
ip visibility features
ulogging enable

parameter-map type inspect-global
log dropped-packets
log flow-export fnf
log flow
!
utd engine standard unified-policy
utd global
flow-logging all
```

确认

```
show  flow monitor sdwan-flow-monitor cache

IPV4 SOURCE ADDRESS:                          10.100.10.75
```

```
IPV4 DESTINATION ADDRESS:                       10.10.10.25
TRNS SOURCE PORT:                               53
TRNS DESTINATION PORT:                          34796
IP VPN ID:                                      10
IP PROTOCOL:                                    17
tcp flags:                                      0x00
interface input:                                Gi2
interface output:                               Gi3
flow cts source group tag:                      0
flow cts destination group tag:                 0
counter bytes long:                             125
counter packets long:                           1
timestamp abs first:                            14:59:47.613
timestamp abs last:                             14:59:47.613
flow end reason:                                Not determined
connection initiator:                           Reverse initiator
interface overlay session id input:             10
interface overlay session id output:            0
connection connection id long:                  0x000000000050D9CC
drop cause id:                                  0
counter bytes drop long:                        0
sdwan sla not met :                             0
sdwan preferred color not met :                 0
sdwan queue id :                                2
counter packets drop long:                      0
ulogging fw zp id:                              4
ulogging fw zone id array:                      3 3
ulogging fw class id:                           12544961
ulogging fw policy id:                          5559936
ulogging fw proto id:                           25
ulogging fw action:                             2
ulogging fw drop reason id:                     0
ulogging fw source ipv4 address translated:     0.0.0.0
ulogging fw destination ipv4 address translated:  0.0.0.0
ulogging fw source port translated:             0
ulogging fw destination port translated:        0
ulogging utd ips pri:                           1
ulogging utd ips sid:                           57756
ulogging utd ips gid:                           1
ulogging utd ips cid:                           21
ulogging utd urlf url hash:                     00000000000000000000000000000000
ulogging utd urlf url category:                 0
ulogging utd urlf url reputation:               0
ulogging utd urlf application name:
ulogging utd amp dispos:                        0
ulogging utd amp filename hash:                 00000000000000000000000000000000
ulogging utd amp file type:                     0
ulogging utd amp file hash:                     0000000000000000000000000000000000000000000000000000000000000000
ulogging utd amp malname hash:                  00000000000000000000000000000000
ulogging utd drop reason id:                    0
ulogging sdvt drop reason id:                   0
ulogging utd ips policy id:                     1
ulogging utd ips action id:                     1
ulogging utd urlf policy id:                    N/A
ulogging utd urlf action id:                    N/A
ulogging utd amp policy id:                     N/A
ulogging utd amp action id:                     N/A
ulogging utd urlf reason id:                    0
ulogging ulogging flow direction:               Reverse initiator
ulogging fw user name:
ulogging fw source ipv6 address translated:     ::
ulogging fw destination ipv6 address translated:  ::
```

```
ip dscp:                                  0x00
application name:                         port dns
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。