Radware DDos v1

最后更新日期：2017 年 11 月 9 日

关于本演示

本预配置演示指南包括以下内容：

要求

下表列出了本预配置演示的要求。

表 1. 要求

必需	可选
• 笔记本电脑	• 思科 AnyConnect®

关于此解决方案

Radware DDos v1 用于演示 Radware virtual DefensePro (vDP) 的功能。您可以在此发起若干当今最常见的网络和应用级 DDoS 攻击，并亲眼目睹 Radware vDP 自动检测和缓解这些攻击的能力。还有一个可选组件：您可以使用 FTD 来分析同样的攻击媒介。

首先，您先发起几次基本的 UDP、ICMP 泛洪网络攻击以及一次针对性 SYN 泛洪攻击并使用示例网站查看结果，然后我们将向您介绍如何配置 Radware virtual DefensePro 来阻止这些攻击。接下来，我们用 HTTP GET、DNS、少量慢速攻击等几种第 7 层攻击增加复杂性，并再次使用 vDP 同样监控和阻止这些攻击。

最后，您能够发起一次真正的多媒介攻击。DDoS 攻击很少是简单的。在现实中，DDoS 攻击通常纠集了 7 到 12 起单独的攻击，企图绕过您的对策。此外，这些攻击的参数也会随时间而变化。您有权访问 20 多个 DDoS 脚本，一次发起一个，或者打开其他窗口来演示 vDP 的全部功能。

最后，本模块的目的是演示 vDP 阻止此类攻击有多么容易 - 它是完成正确任务的正确工具。这使 FTD 能够专注于它最擅长的方面。毕竟，DDoS 攻击通常是多媒介攻击的一部分，因此在 vDP 专注于保持系统可用时，FTD 可以将重点放到更精细的入侵事件上。FTD 和 vDP 配合使用能取得更好的效果。

dCloud 会话

此环境包括：

- Radware vDP 实例
- vDP 的 Vision 管理
- FTDv（下一代防火墙）
- FMCv（Firepower 管理中心）
- 包含 DOS 脚本的攻击计算机
- 合法客户端
- 运行网页的合法服务器

拓扑

本部分内容包括用于说明解决方案脚本化场景和功能的预配置用户和组件。大多数组件完全可以使用预定义的管理用户帐户进行配置。通过点击活动会话的**拓扑**菜单中的组件图标，您可以查看用于访问组件的 IP 地址和用户帐户凭证，在需要用到 IP 地址和用户帐户凭证的场景步骤中也同样如此。

图 1. dCloud 拓扑

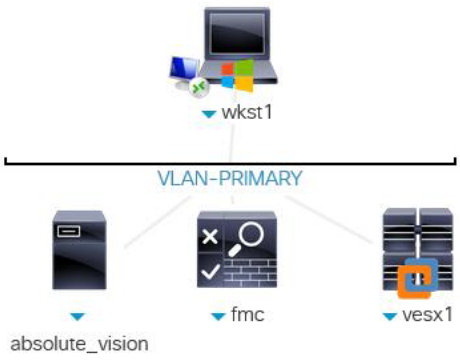
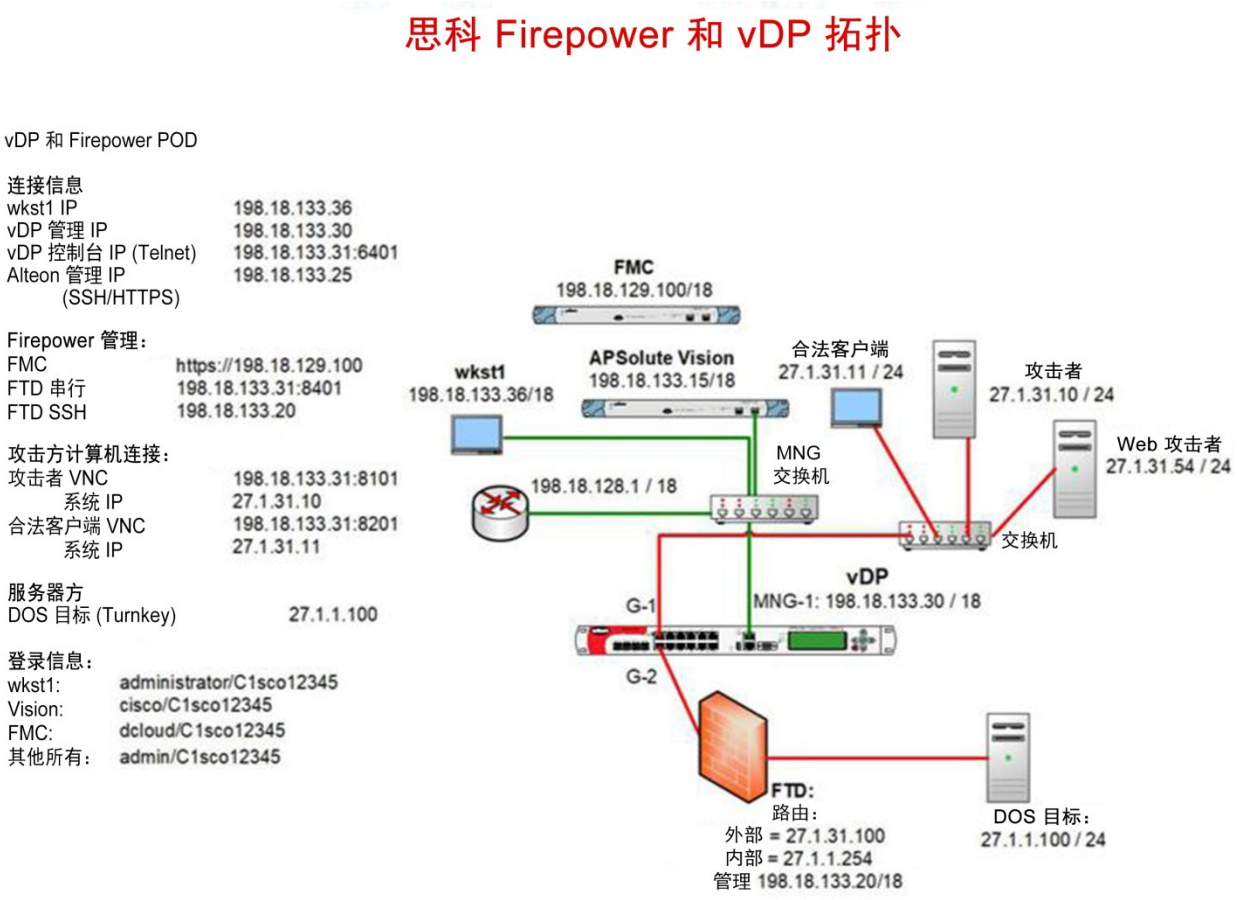


图 2. 逻辑拓扑



注意：此拓扑包含其他设备，可用于其他演示。本指南中未使用所有虚拟机 (VM)。

表 2. 实验设备

系统	协议	IP 地址	目的 TCP 端口
DefensePro 串行连接	Telnet	198.18.133.31	6401
DefensePro SSH 连接	SSH	198.18.133.30	22
DefensePro 攻击者服务器	VNC	198.18.133.31	8101
Kali Web 攻击者	VNC	198.18.133.31	3101
合法 PC	VNC	198.18.133.31	8201
下一代防火墙控制台连接	Telnet	198.18.133.31	8401
Firepower SSH 连接	SSH	198.18.133.20	22
Vision 设备	HTTPS	198.18.133.15	443
FMC	HTTPS	198.18.129.100	443

开始演示

演示前的准备

思科 dCloud 强烈建议您事先使用活动会话执行本文档中的任务，然后再给现场观众演示。这样您将熟悉文档和内容的结构。

遵循本指南后，有必要安排一个新会话，以将环境重置为其原始配置。

细致的准备对于一场成功的演示至关重要

按照步骤安排内容会话并配置演示环境。

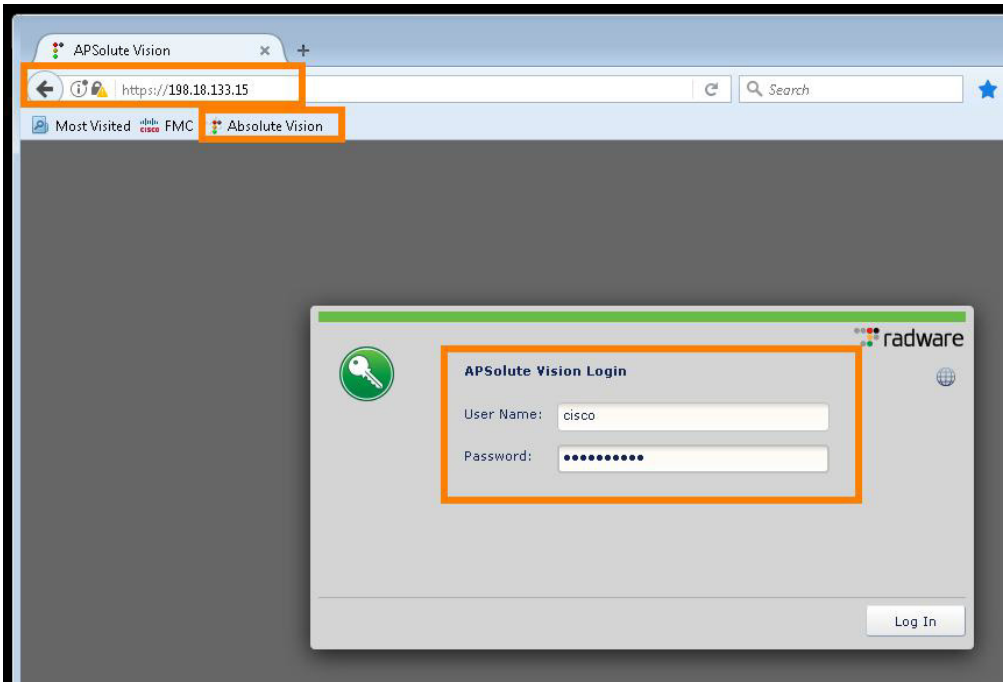
1. 启动 dCloud 会话。[查看具体操作]

注意：激活会话可能需要 10 分钟的时间。

2. 为了获得最佳性能，请通过**思科 AnyConnect VPN** [查看具体操作] 和**笔记本电脑上的本地 RDP 客户端** [查看具体操作] 连接到工作站。
   - 工作站 1：`198.18.133.36`，用户名：**administrator**，密码：`C1sco12345`

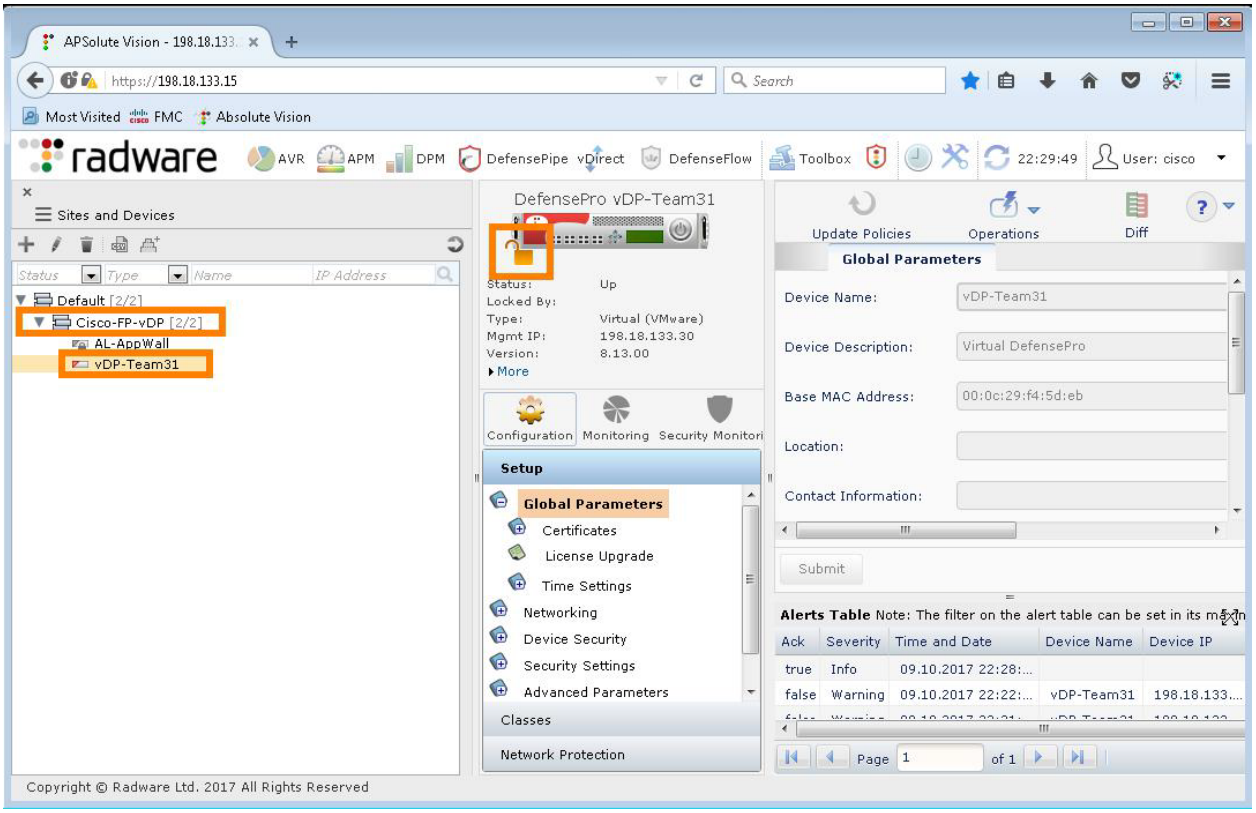
注意：您也可以使用思科 dCloud 远程桌面客户端 [查看具体操作] 连接到工作站。dCloud 远程桌面客户端非常适合于访问极少交互的活动会话。但是，许多用户在使用此方法时会遇到连接和性能问题。

3. 在浏览器中，转到 `https://198.18.133.15` 或点击 Absolute Vision 书签。使用用户名 cisco 和密码 `C1sco12345` 登录。



4. 在屏幕左侧，选择 **Cisco-FP-vDP**。

5. 选择 vDP 并点击**锁定**图标管理设备。

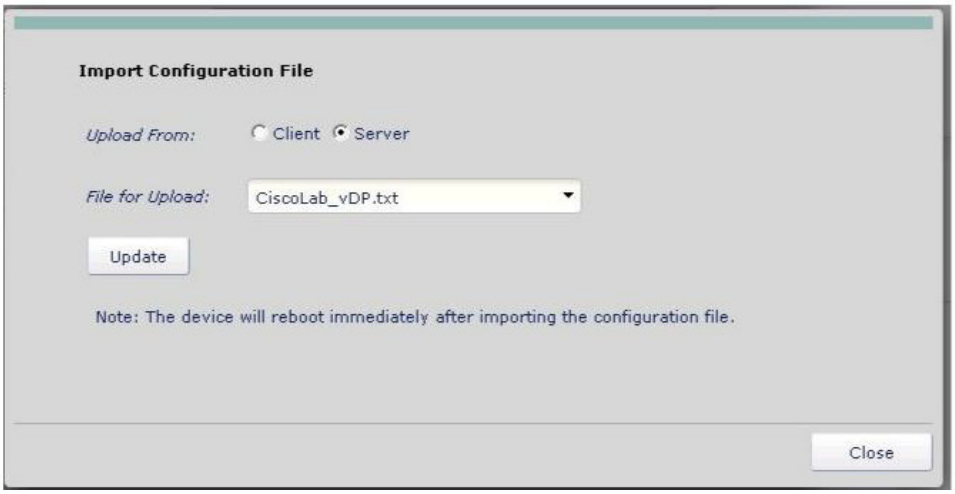


6. 选择**操作**。如果选项处于活动状态，点击**导入配置文件**下载最新配置。

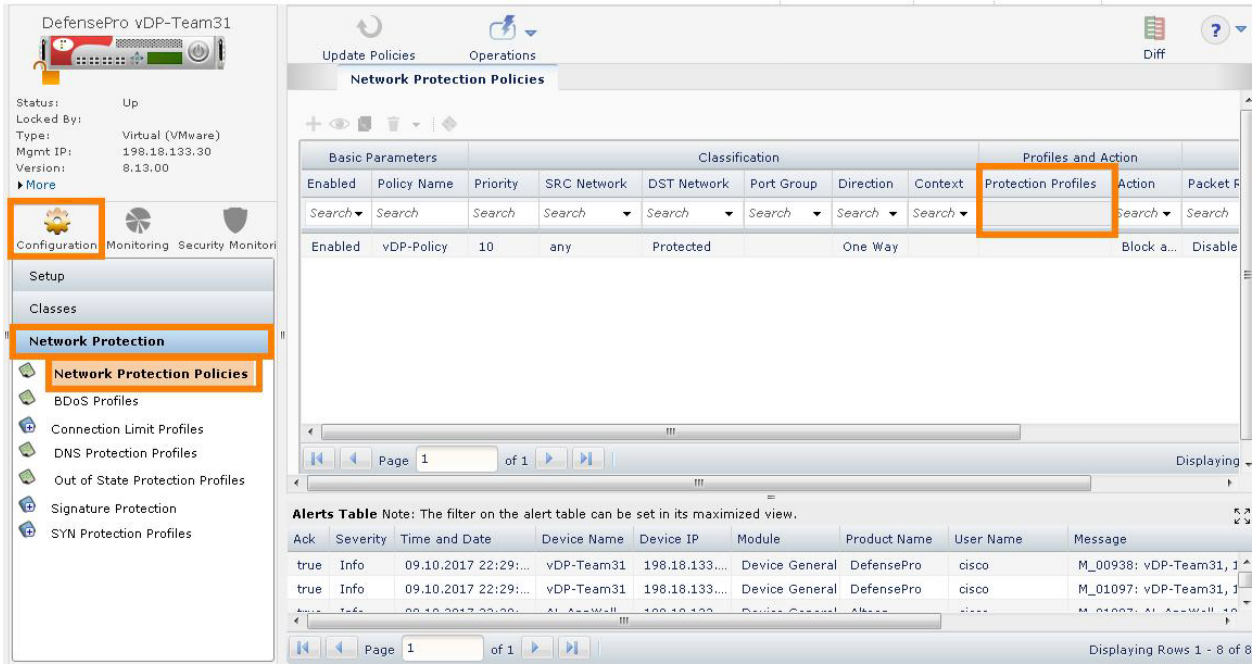
7. 选择**服务器**单选按钮，然后选择 **CiscoLab_vDP**。

8. 点击**更新**（并重置 vDP）。如果选项显示为灰色，请转到下一步。

注意：因为 vDP 会重新启动，所以此操作可能需要 5 分钟时间。



9. 依次点击**配置 > 网络保护 > 网络保护策略**验证配置，并确定没有附加保护配置文件。



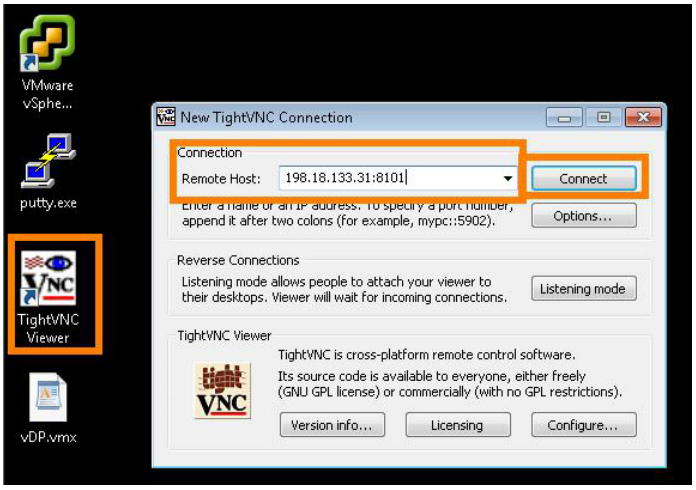
场景 1： BDoS 攻击

在这段演示中，您将向端口 80 发起两次 BDoS 攻击，一次是 TCP RST 泛洪，一次是 UDP 泛洪。尽管状态设备可以缓解这些泛洪，但此类泛洪的目标是用庞大的每秒数据包数让系统不堪重负。

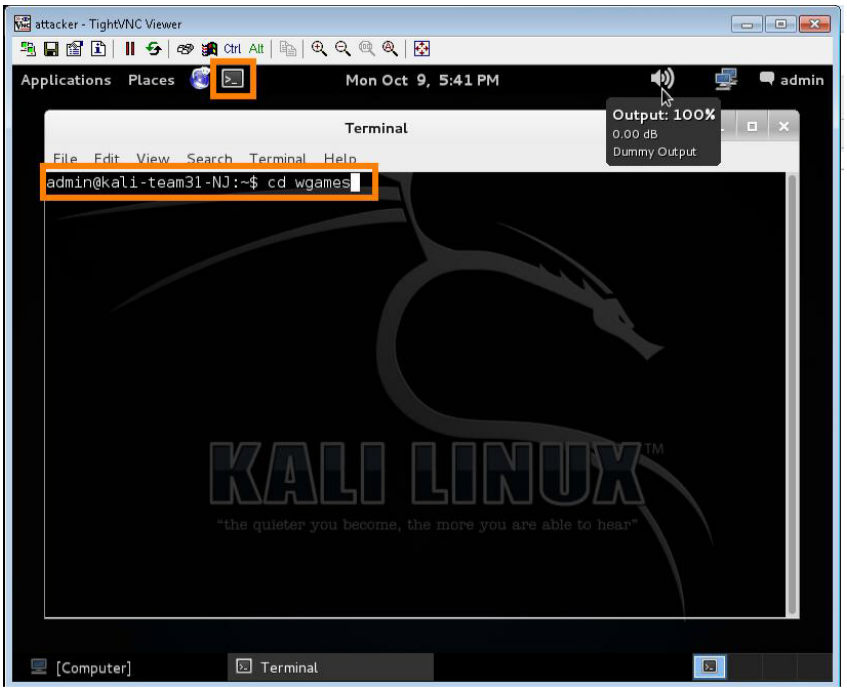
步骤

TCP 泛洪

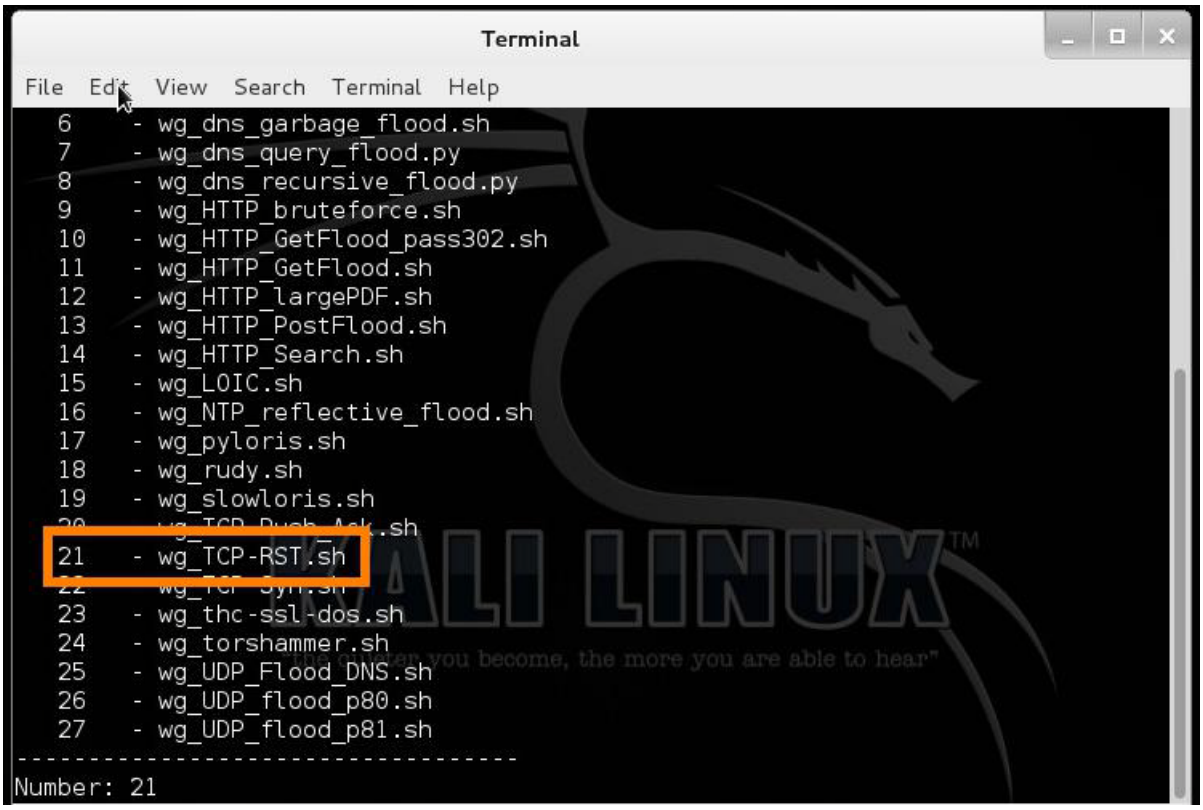
1. 在桌面上，打开 TightVNC 查看器。使用 VNC 连接至位于 `198.18.133.31:8101` 的 Kali 计算机。使用用户 ID admin 和密码 `C1sco12345` 登录。



2. 选择左上方的终端图标，然后在提示符后输入 **`cd wgames`**。



3. 输入 `sudo ./start.sh`，然后输入根密码 C1sco12345。输入 21 并按 **Enter** 键，即可选择 **第 21 项**（TCP-RST 攻击）。



4. 在工作站上使用 Putty，通过 Telnet 连接到 vDP 的控制台 = **`198.18.133.31 端口 = 6401`**。

5. 在提示符后，输入：

```
system inf-stats reset
```

注意：如果收到提示您需要登录的消息，请输入命令 `login`，然后输入用户名 admin 和密码 C1sco12345。

6. 然后，输入 `system`

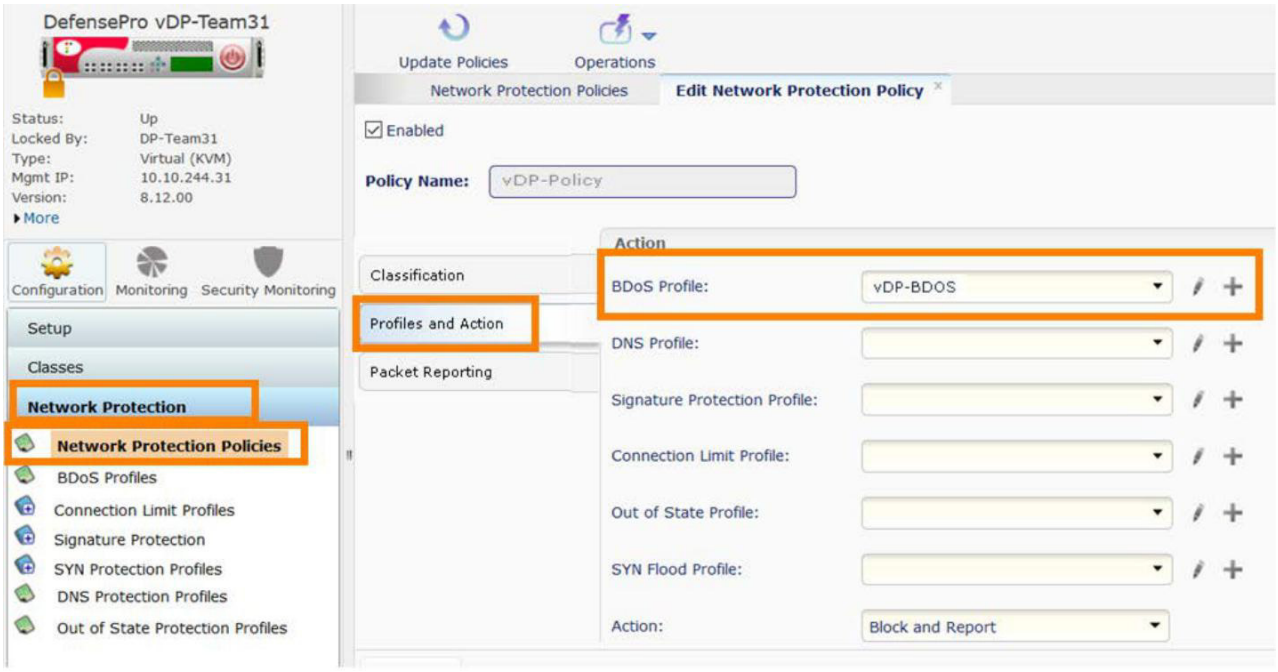
```
inf-stats
```

您应该看到大量从端口 1（外部端口）传入的流量，以及使用 TCP 端口 0 作为源或目的端口的数据包被 vDP 自动阻止的消息。

7. 在攻击计算机上，使用 **Ctrl+C** 停止攻击。

DefensePro

1. 在 Vision 中，依次选择**配置 > 网络保护 > 网络保护策略**，在您的会话中启用 BDOS 保护配置文件。
2. 双击 vDP-Policy 策略并选择“配置文件和操作”。

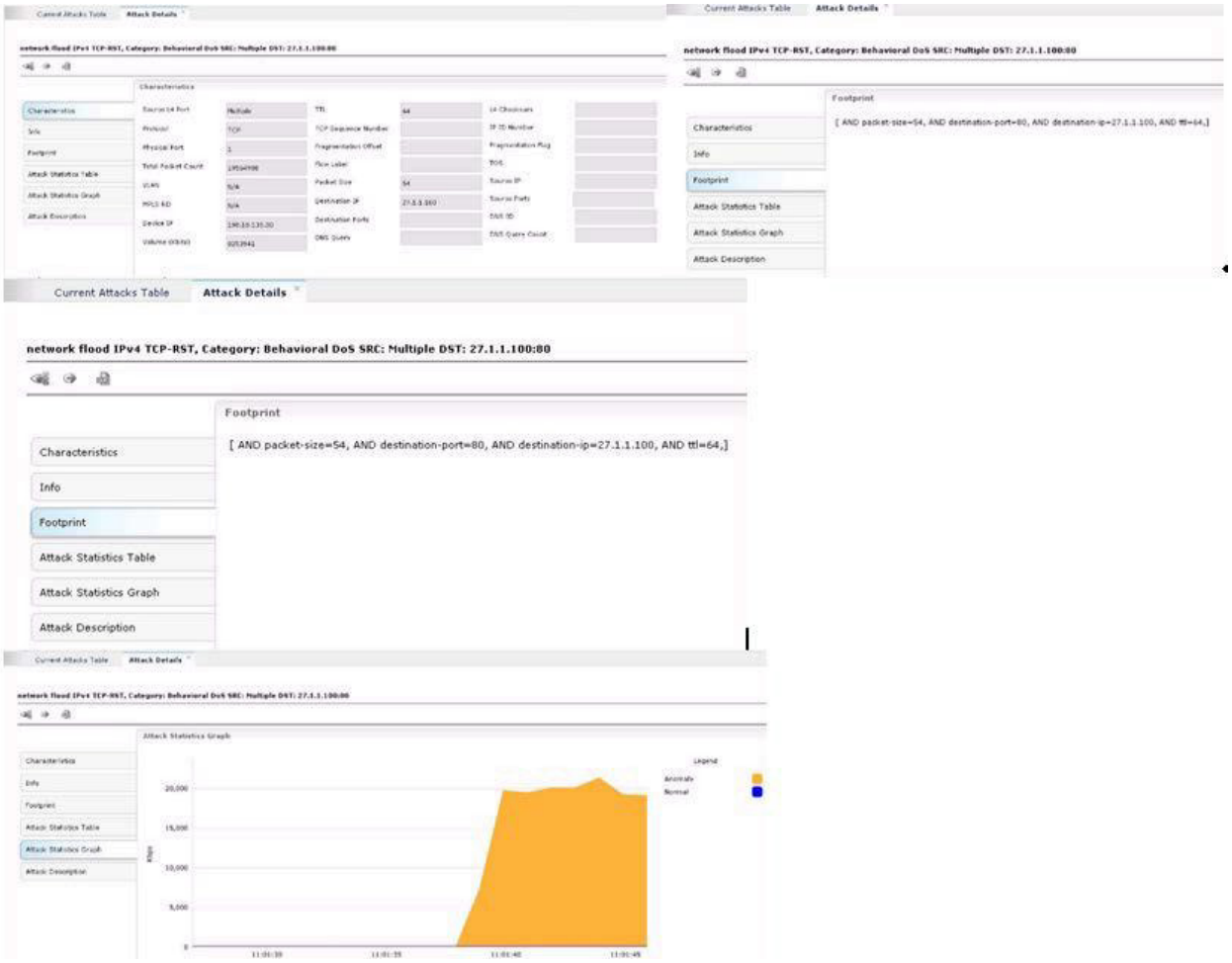


3. 在“BDoS 配置文件”中选择 **Lab-BDOS**，然后点击**提交**。
4. 点击**更新策略**激活配置更改。在攻击者计算机上再次发起攻击。
5. 在控制台上，您将看到 BDOS 丢弃攻击数据包。

```
DefensePro#07-04-2017 20:25:02 WARNING 74 Behavioral-DoS "network flood IPv4 TCP
-RST" TCP 0.0.0.0 0 27.1.31.100 80 2 Regular "Cisco-VDP" ongoing 686544 289635 N
```

6. 在 Vision 中，依次选择**安全监控 > 当前攻击表**，您将看到显示的攻击。

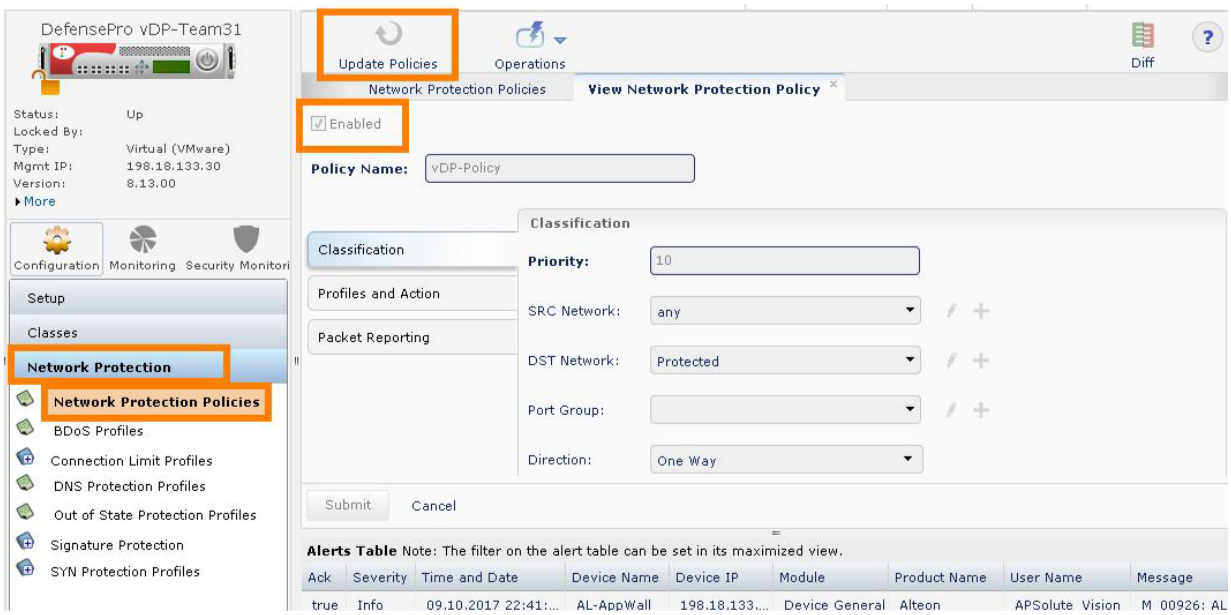
7. 双击攻击，查看更多详细信息。



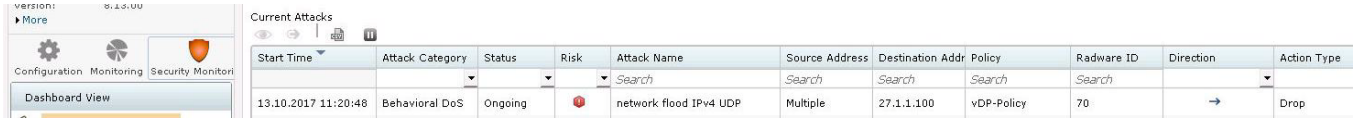
8. 在攻击计算机上，使用 **Ctrl+C** 停止攻击。

UDP 泛洪

1. 依次选择**配置 > 网络保护 > 网络保护策略**，禁用当前策略。双击您的策略。
2. 取消选中**启用**复选框，然后点击**提交**。
3. 点击**更新策略**。



4. 从攻击计算机上，在终端中运行 `./start.sh`。选择选项 26 wg_UDP_flood_p80.sh。



5. 在 vDP 上，使用 `system inf-stats` 查看统计信息（首先使用 `system inf-stats reset` 将其重置）。

DefensePro

1. 返回到策略，然后依次选择**配置 > 网络保护 > 网络保护策略**重新打开策略。双击您的策略。
2. 选中**启用**复选框，然后点击**提交**。
3. 点击**更新策略**。

4. vDP 现在将缓解攻击，您可以从合法计算机浏览至位于 http://27.1.1.100 的演示计算机。
5. 在攻击计算机上，使用 **Ctrl+C** 停止攻击。
6. 在继续下一个场景之前，我们要删除 BDoS 保护。转到您的策略，然后依次选择**配置 > 网络保护 > 网络保护策略**，删除 **BDoS 配置文件**。双击您的策略。
7. 选择**配置文件和操作**。
8. 在 **BDoS 配置文件**中，点击下拉列表并选择空白配置文件。
9. 点击**提交**，然后点击**更新策略**。

场景 2： SYN 泛洪攻击

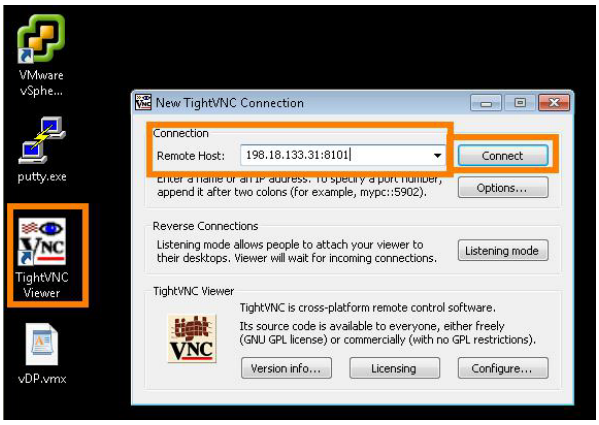
在此场景中，您要生成两次攻击，其一是向端口 80 发起简单的 SYN 泛洪攻击，此攻击是为了用大量 SYN 数据包淹没防火墙状态表，BDOS 引擎和 SYN 泛洪保护均可缓解此攻击。

第二次攻击是 HTTP GET 泛洪。此攻击作为合法的 TCP 流量绕过防火墙，让服务器不堪重负。
请使用 SYN 泛洪保护来缓解攻击。

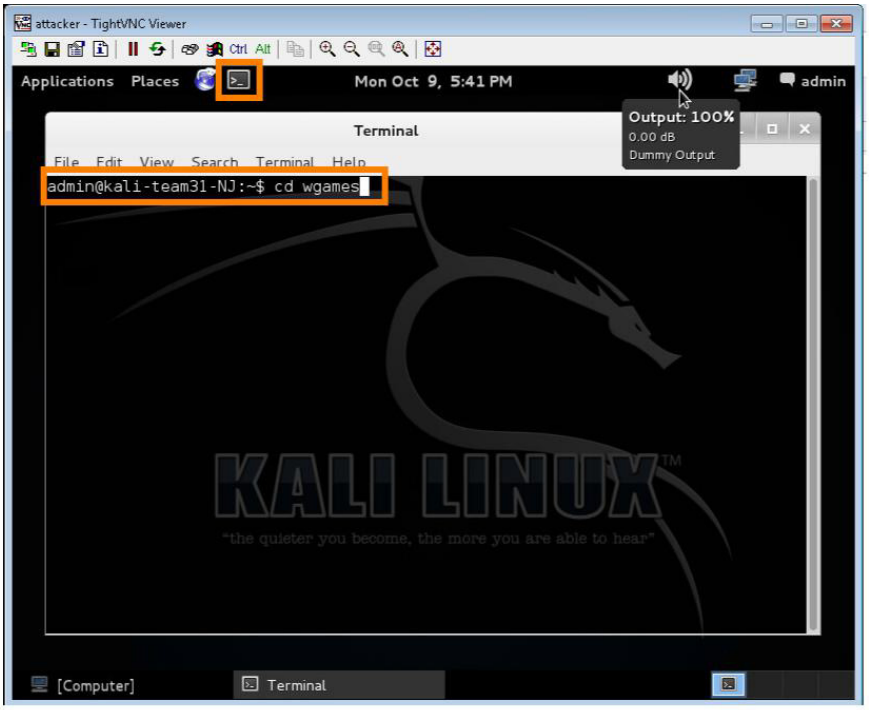
步骤

SYN 泛洪

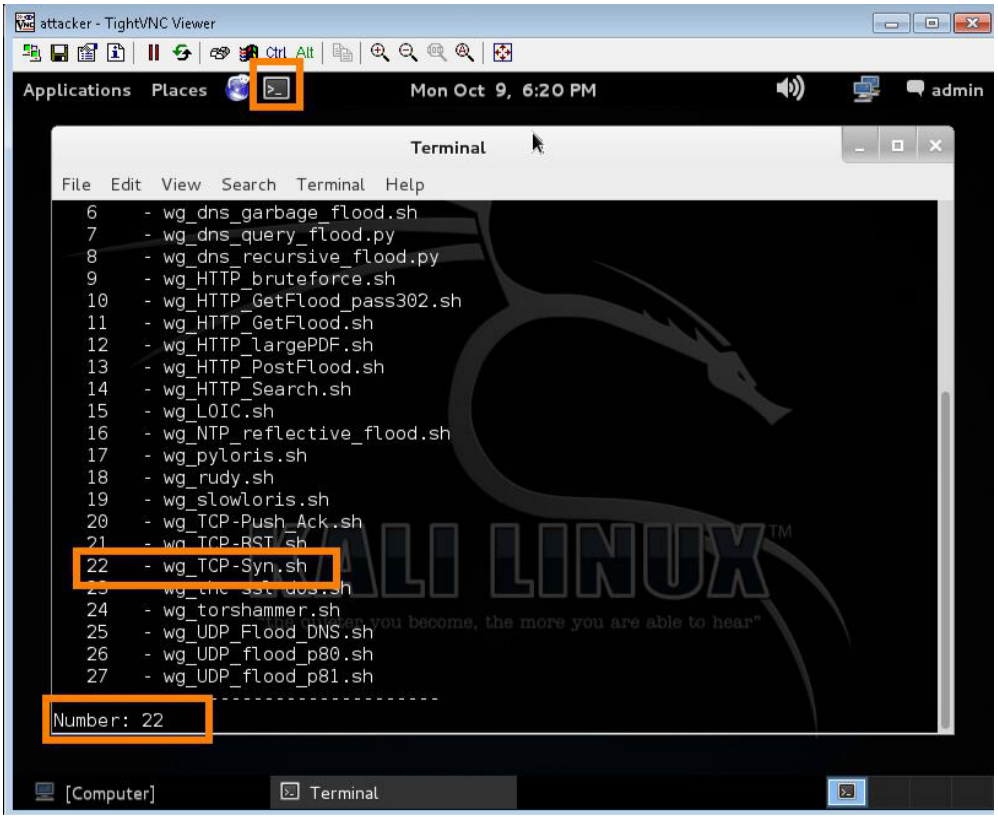
1. 在桌面上，打开 TightVNC 查看器。使用 VNC 连接至位于 `198.18.133.31:8101` 的 Kali 计算机。使用用户 ID admin 和密码 `C1sco12345` 登录。



2. 选择左上方的**终端**图标，然后在提示符后输入 **`cd wgames`**。



3. 在终端上，输入 `sudo ./start.sh` 并选择**选项 22 wg_TCP-Syn.sh**，发起基本 SYN 攻击。



4. 请注意 `system inf-stats` 表中的该攻击。

启用 BDOS 保护

1. 依次选择**配置 > 网络保护 > 网络保护策略**，双击策略并再次启用 BDoS 配置文件。按**更新策略**激活更改。
2. 查看 `dp rtm-stats` 表，注意已传入并正被丢弃的数据包。
3. 依次选择**配置 > 网络保护 > 网络保护策略**，在策略中关闭 BDOS 保护。双击您的策略。
4. 选择**配置文件和操作**。
5. 在“BDoS 配置文件”中，点击下拉列表并选择空白配置文件。
6. 点击**提交**，然后点击**更新策略**。
7. 保持攻击继续运行。

启用 SYN 保护配置文件

1. 依次选择**配置 > 网络保护 > 网络保护策略**，然后双击您的策略。
2. 选择**配置文件和操作**。
3. 在“SYN 泛洪配置文件”选项中，选择 **Lab-SYN-nocookie**。
4. 点击**提交**，然后点击**更新策略**。
5. vDP 将缓解攻击，但这次会标记攻击：

```
DefensePro#19-04-2017 23:56:27 WARNING 200000 SynFlood "SYN Flood HTTP" TCP 0.0.0.0 0 27.1.31.100 80 0 Regular "Cisco-VDP" ongoing 728268 341375 N/A 0 N/A medium challenge FFFFFFFF-FFFF-FFFF-0023-000058F7DC9D
```

6. 查看 `system inf-stats`。

```
DefensePro#system inf-stats
Port ifInPkts    ifInDiscards  ifInErrors  ifOutPkts  ifOutDiscards  ifOutErrors
1        194812             0           0      194809              0            0
2             0             0           0           0              0            0
MNG-1         0             0           0          20              0            0
```

7. 数据包从传入数据包的同一个接口被退回。vDP 正在为检测到的此次 SYN 泛洪发送 SYN 质询，而非如 BDOS 那样丢弃数据包。
8. 在攻击计算机上，使用 **Ctrl+C** 停止攻击。

HTTP GET 泛洪

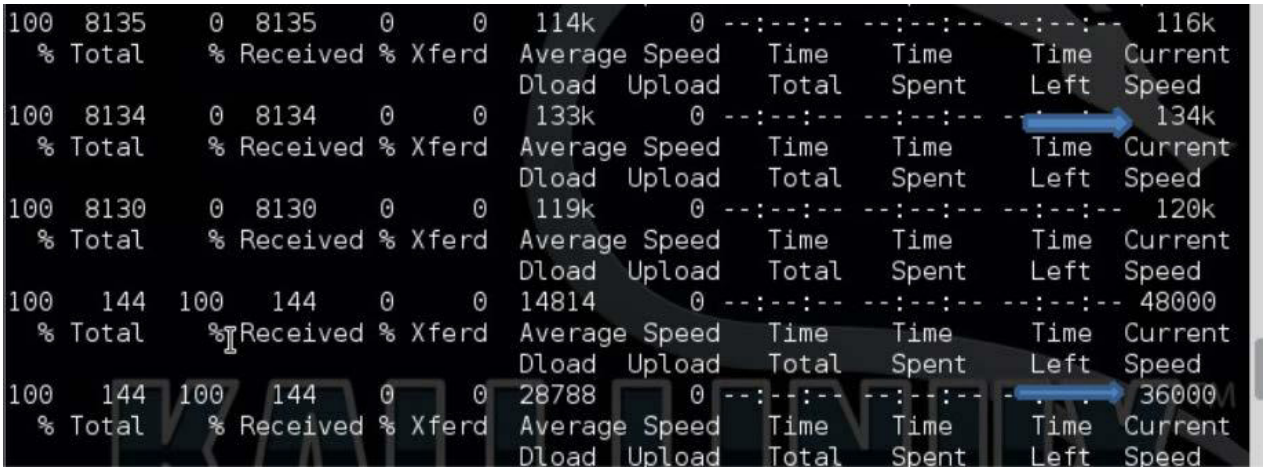
1. 在攻击计算机上，输入 `sudo ./start.sh` 并选择**选项 11 wg_HTTPGetFlood.sh**，发起新的攻击。
2. 这次将发起 **HTTP GET** 泛洪攻击。

注意：HTTP GET 通过具有基本 SYN 保护的 SYN 质询不会有问题，也不会被防火墙和 vDP 检测到。

DefensePro

1. 要缓解攻击，请依次选择**配置 > 网络保护 > 网络保护策略**，然后双击您的策略。
2. 选择**配置文件和操作**。
3. 在“SYN 泛洪配置文件”选项中，选择 **Lab-SYN-cookie**。
4. 点击**提交**，然后点击**更新策略**。

5. 一旦启用保护，您就可以在攻击计算机上看到攻击速度明显下降。您也可以在“安全监控”中看到 SYN 泛洪保护。
6. 如果无法看到 vDP 检测攻击，请将 **SYN 泛洪**配置文件更改为使用 **HTTP_Low 保护**而非标准的 **HTTP 保护**，或将标准的 HTTP 保护更改为较低的激活阈值。



7. 在攻击计算机上，使用 **Ctrl+C** 停止攻击。

场景 3： DNS 攻击

步骤

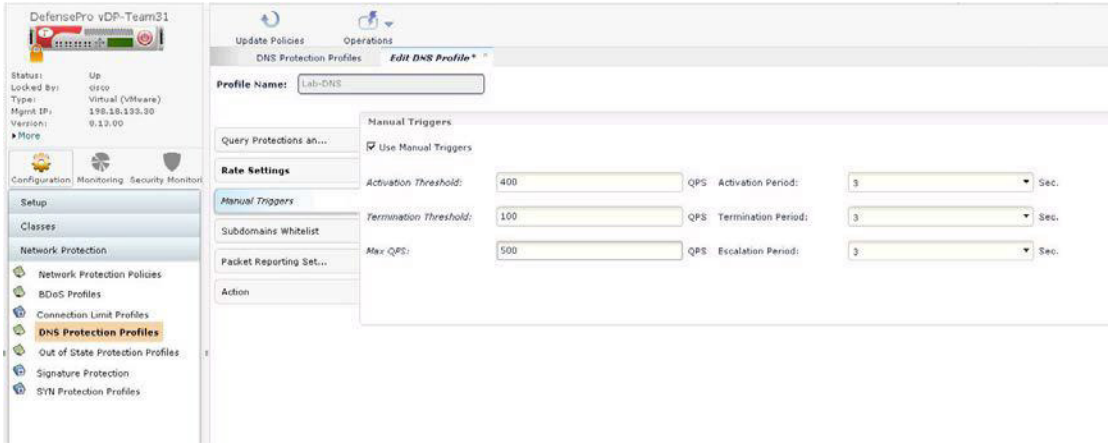
缓解攻击

DNS 攻击也可以采用两种方式来缓解。BDOS 能够阻止针对没有 DNS 服务器的网络的 DNS 泛洪攻击。但是，如果泛洪攻击针对的是 DNS 服务器，BDOS 会创建签名并阻止合法 DNS 请求。

1. 在攻击计算机上，输入 `sudo ./start.sh` 并选择**选项 7**，发起 **DNS 查询**泛洪。
2. 运行 `system inf -stats reset` 命令。
3. 攻击开始后，在 vDP 控制台上查看 `system inf-stats` 表。

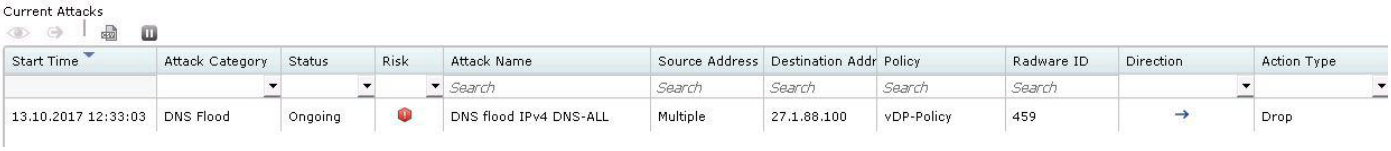
DefensePro

1. 依次选择**配置 > 网络保护 > 网络保护策略**。
2. 双击您的策略并点击**操作**。
3. 选择 **DNS 配置文件**，然后从下拉列表中选择 **Lab-DNS**。
4. 点击**提交**，然后点击**更新策略**。
5. 如果未检测到 DNS，问题可能出在攻击工具每秒生成的查询不足。
6. 转到**配置 > 网络保护 > DNS 保护配置文件**，然后双击现有配置文件。
    a. 选择“手动触发器”选项卡，将阈值更改为较低的值
    b. 激活阈值 = 40 QPS，终止阈值 = 10 QPS，将最大 QPS 更改为 50。
    c. 点击**提交**，然后点击**更新策略**。



7. 您很快就可以在“安全监控”窗口中看到，攻击现在已得到缓解。

8. 完成后，使用 **Ctrl+C** 停止攻击。


Current Attacks

Start Time	Attack Category	Status	Risk	Attack Name	Source Address	Destination Addr	Policy	Radware ID	Direction	Action Type
				Search	Search	Search	Search	Search		
13.10.2017 12:33:03	DNS Flood	Ongoing		DNS flood IPv4 DNS-ALL	Multiple	27.1.88.100	vDP-Policy	459	→	Drop

场景 4： 少量慢速攻击

步骤

发起攻击

少量慢速攻击与 HTTP GET 泛洪类似，只是它以慢速连接开始，首先发送几个连接，然后使用不完整的 GET 请求逐渐增加连接。

1. 在攻击计算机上，输入 `./start.sh` 并选择选项 **19 wg_slowloris,sh**，发起少量慢速攻击。
2. 攻击开始后，在 vDP 控制台上使用命令 `system inf-stats table` 查看统计信息。
3. 使用 VNC 连接到合法客户端。不久后，位于 http://27.1.1.100 的服务器就会因攻击而停止响应或响应速度显著变慢。

DefensePro

1. 依次选择**配置 > 网络保护 > 网络保护策略**。
2. 双击您的策略并点击**操作**。
3. 选择**签名保护配置文件**，然后从下拉列表中选择 **DOS-All**。
4. 点击**提交**，然后点击**更新策略**。
5. 您很快就可以在**安全监控**窗口中看到，攻击现在已得到缓解。
6. 查看合法客户端。服务器应该已经重新开始响应。
7. 完成后，在攻击者计算机上使用 **Ctrl+C** 停止攻击。

注意：除 DOS-All 签名外，还可以通过 SYN 保护来缓解此攻击，如果选择 LAB-SYN-Cookie 选项，工具就无法通过 HTTP 质询。

场景 5： 多媒介攻击

在此部分，您将成为黑客。以下是 Kali 设备上的脚本及其说明的列表。尝试在启用所有现有 vDP 策略的情况下再运行几个脚本。尝试在单独的 cmd 窗口中同时运行几个脚本，并在 Vision 中监控结果。

脚本名称	攻击/攻击工具	说明
wg_apache_Killer.sh	Apache Killer	https://security.radware.com/ddos-knowledge-center/ddospedia/apache-killer/
wg_botnet.sh	BoNeSi	DDoS 僵尸网络模拟器 https://github.com/Markus-Go/bonesi
wg_dnsflood_STAS.py	DNS 泛洪	向 DNS 服务器发送随机数据包
wg_dns_flood.py	DNS 查询泛洪	向服务器发送针对 www.radware.com 的 DNS 请求
wg_dns_garbage_flood.sh	DNS 垃圾泛洪	向 DNS 服务器的端口 53 发送垃圾（HTML 页面）
wg_dns_query_flood.py	DNS 泛洪	与 wg_dns_flood.py 相同，此条多余，应删除
wg_dns_recursive_flood.py	DNS 递归泛洪	向服务器发送递归 DNS 请求
wg_HTTP_bruteforce.sh	HTTP 泛洪/Siege	向需要身份验证的页面 (/accounts.aspx) 发送 HTTP 泛洪
wg_HTTP_GetFlood.sh	HTTP 泛洪	向服务器的启动页面发送大量 HTTP GET 请求
wg_HTTP_GetFlood_pass302.sh	HTTP 泛洪	与 GetFlood.sh 类似，但增加了通过 HTTP-302 质询的能力
wg_HTTP_largePDF.sh	HTTP 泛洪	向服务器上的一个大文件发送大量 HTTP 请求，占用全部上游带宽，致使服务器对合法客户端响应缓慢
wg_HTTP_PostFlood.sh	HTTP 泛洪	向服务器的启动页面发送大量 HTTP POST 请求
wg_HTTP_Search.sh	HTTP 泛洪	向服务器的搜索页面发送大量 HTTP GET 请求，造成极高的 CPU 使用率
wg_LOIC.sh	LOIC	Low Orbit Ion Cannon (LOIC) 最初是 Praetox Technologies 开发的一种开源网络压力测试工具。借助该工具，开发人员可以出于诊断目的让服务器承受沉重的网络流量负载。但是，后来该工具在公共域中被匿名者通过各种更新进行修改并广泛用作 DDoS 工具。https://security.radware.com/ddos-knowledge-center/ddospedia/loic-low-orbit-ion-cannon/
wg_NTP_reflective_flood.sh	NTP 反射型泛洪	https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/ntp-reflected-flood/
wg_pyloris.sh	Pyloris	Pyloris 是慢速 HTTP DoS 工具。https://security.radware.com/ddos-knowledge-center/ddospedia/pyloris/
wg_rudy.sh	R.U.D.Y	R.U.D.Y.攻击 (R-U-Dead-Yet?) 是慢速 HTTP POST（第 7 层）拒绝服务工具。https://security.radware.com/ddos-knowledge-center/ddospedia/rudy-r-u-dead-yet/
wg_slowloris.sh	Slow Loris	Slowloris 是灰帽黑客“RSnake”开发的拒绝服务 (DoS) 工具，使用非常慢的 HTTP 请求造成 DoS。https://security.radware.com/ddos-knowledge-center/ddospedia/slowloris/
wg_TCP-Ack_flood.sh	TCP 泛洪	使用状态不相称的 TCP-ACK 数据包淹没服务器
wg_TCP-Push_Ack.sh	TCP 泛洪	使用状态不相称的 TCP-Push-ACK 数据包淹没服务器
wg_TCP-RST.sh	TCP 泛洪	使用状态不相称的 TCP-RST 数据包淹没服务器
wg_TCP-Syn.sh	TCP 泛洪	使用发起新会话的 TCP-SYN 数据包淹没服务器
wg_thc-ssl-dos.sh	THC-SSL-DOS	THC-SSL DOS 由名为 The Hacker's Choice 的黑客组织作为概念验证开发，旨在鼓励供应商修补一个严重的 SSL 漏洞。https://security.radware.com/ddos-knowledge-center/ddospedia/thc-ssl-dos/
wg_torshammer.sh	TORSHAMMER	Torshammer 是 phiral.net 创建的慢速 HTTP POST（第 7 层）DoS 工具 https://security.radware.com/ddos-knowledge-center/ddospedia/tors-hammer/
wg_UDP_Flood_DNS.sh	DNS 泛洪	使用随机的 DNS 数据包淹没服务器
wg_UDP_flood_p80.sh	UDP 泛洪	在端口 80 上使用随机数据包淹没服务器，假设端口 80 因防火墙上的错误配置而打开。这会给服务器的 IP 协议栈造成负载
wg_UDP_flood_p81.sh	UDP 泛洪	在端口 81 上使用 UDP 数据包淹没服务器

附录 A　　思科下一代防火墙访问权限

此环境中部署了思科下一代防火墙供您用于其他用途，展示 Radware 并不需要它。目前它处于路由内联模式，但所有策略均设置为只发出警报。有些特殊配置已启用，以便在发生某些攻击时显示这些攻击，但并非所有攻击都能看到。您将获得完全访问权限，可随意展示与 Radware 配合使用的思科 Firepower 解决方案。

1. 要打开 Firepower 管理控制台，请在 wkst1 上打开 Google Chrome 浏览器，并浏览至工具栏中的 **FMC** 快捷方式。

   Firepower 登录凭证是用户名 **dcloud** 和密码 **C1sco12345**

注意：如果出现运行状况警告，称 FTD 接口上没有流量，这是正常问题，因为只有手动发起的攻击才会产生流量。一旦您开始攻击场景，任何警告都将清除。您可能还会收到许可警报，说明看到的主机数超出授予许可的数量。这是预期行为，因为如果未将 Radware 解决方案设置为阻止 DDoS 攻击主机，则到达 NGFW 的 DDoS 攻击主机数量可能非常庞大。

在现实中，您可以只将 Kali 设备转发到黑洞中就罢手，然而现实并非那么简单。DDoS 攻击可能来自由数千台或几百万台设备组成的僵尸网络，也可能来自一个 IP 地址，您根本不能像运行您的应用的 AWS 或者（如果您是一所大学）学生宿舍那样关闭。Radware vDP 旨在自动检测并缓解此类攻击。思科 FTD 和 vDP 配合使用能取得更好的效果。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。