Radware DDos v1

最終更新日:2017 年 11 月 9 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect®

このソリューションについて

Radware DDos v1 は、Radware virtual DefensePro（vDP）の機能を実証するものです。これにより、ネットワーク レベルとアプリケーション レベルの最も一般的な DDoS 攻撃のいくつかを開始し、Radware の vDP 機能によって攻撃を自動的に検出し、軽減する様子を確認することができます。同じ攻撃ベクトルを FTD を使用して分析できる、オプションのコンポーネントも用意されています。

最初に、標的型の SYN フラッドと合わせて少数の基本的な UDP、ICMP フラッド ネットワーク攻撃を開始し、サンプル Web サイトに結果を表示します。続いて、Radware virtual DefensePro を設定してこれらの攻撃を阻止する方法を示します。さらに、複数のレイヤ 7 攻撃（HTTP GET、DNS、Low and Slow）によって複雑性を高め、もう一度 vDP を使用して、それらの攻撃の監視と阻止を行います。

最終的に、現実のマルチベクトル攻撃を行うことが可能になります。DDoS 攻撃がシンプルであることは稀です。現実の DDoS 攻撃では、通常 7 ～ 12 の個別の攻撃が組み合わされて、セキュリティ対策のバイパスが試みられます。さらに、これらの攻撃のパラメータは時間の経過とともに変わる場合があります。20 以上の DDoS スクリプトにアクセスして個別に実行することも、別のウィンドウを開いて vDP のフル機能を実証することもできます。

このモジュールの最終的な目標は、そうしたタイプの攻撃を vDP によって簡単にブロックできることを示し、適切なツールを使用して効果的な対策ができることを確認することです。それにより FTD は、本来の機能を十分に発揮できるようになります。いずれにしても DDoS 攻撃はマルチベクトル攻撃の一部になっていることが多いため、vDP がシステムの可用性確保に集中することで、FTD はさらに巧妙な侵入イベントに特化して対処できるようになります。FTD と vDP の連携によって大きな効果が得られます。

dCloud セッション

この環境は次の要素で構成されています。

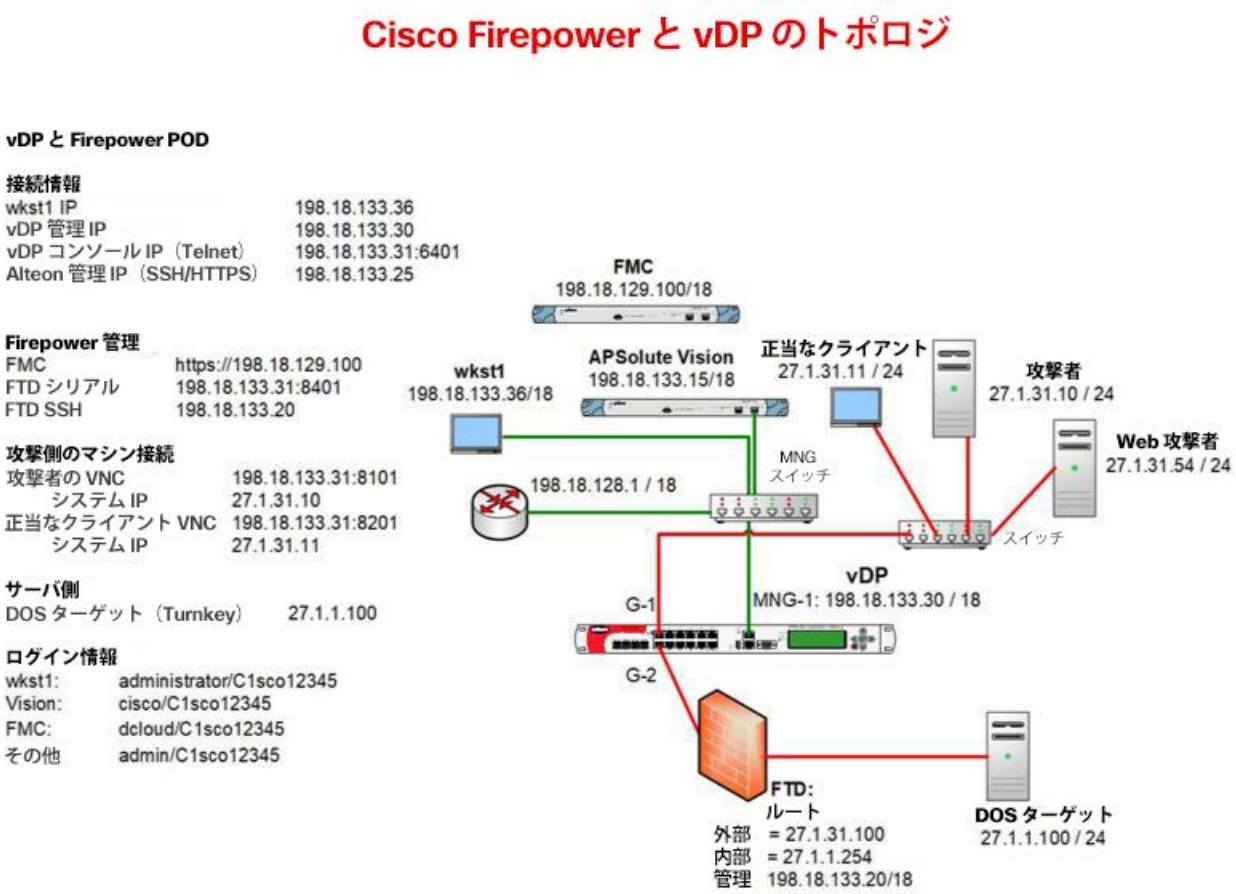
- Radware vDP インスタンス
- vDP に関する Vision 管理
- FTDv（次世代ファイアウォール）
- FMCv（Firepower Management Center）
- DOS スクリプトを使用した攻撃用マシン
- 正当なクライアント
- Web ページを運用する正当なサーバ

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

図 2. 論理トポロジ



注:このトポロジには、他のデモンストレーションでも使用できるデバイスが含まれています。このガイドでは使用しない VM もあります。

表 2. ラボ用デバイス

システム	プロトコル	IP アドレス	宛先 TCP ポート
DefensePro シリアル接続	Telnet	198.18.133.31	6401
DefensePro SSH 接続	SSH	198.18.133.30	22
DefensePro 攻撃者サーバ	VNC	198.18.133.31	8101
Kali Web 攻撃者	VNC	198.18.133.31	3101
正当な PC	VNC	198.18.133.31	8201
次世代ファイアウォールコンソール接続	Telnet	198.18.133.31	8401
Firepower SSH 接続	SSH	198.18.133.20	22
Vision Appliance	HTTPS	198.18.133.15	443
FMC	HTTPS	198.18.129.100	443

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

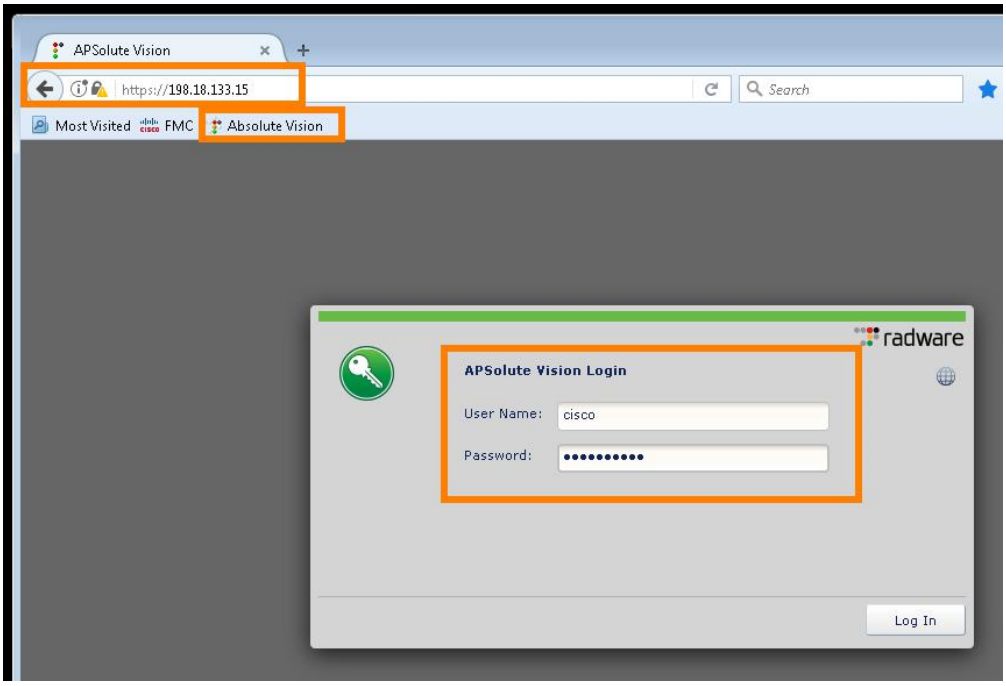
1. dCloud セッションを開始します。[手順を見る]

注: セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るために、**Cisco AnyConnect VPN** [手順を見る] およびラップトップの**ローカル RDP クライアント** [手順を見る] を使用してワークステーションに接続します。
   - Workstation 1: `198.18.133.36`、ユーザ名: **administrator**、パスワード: `C1sco12345`

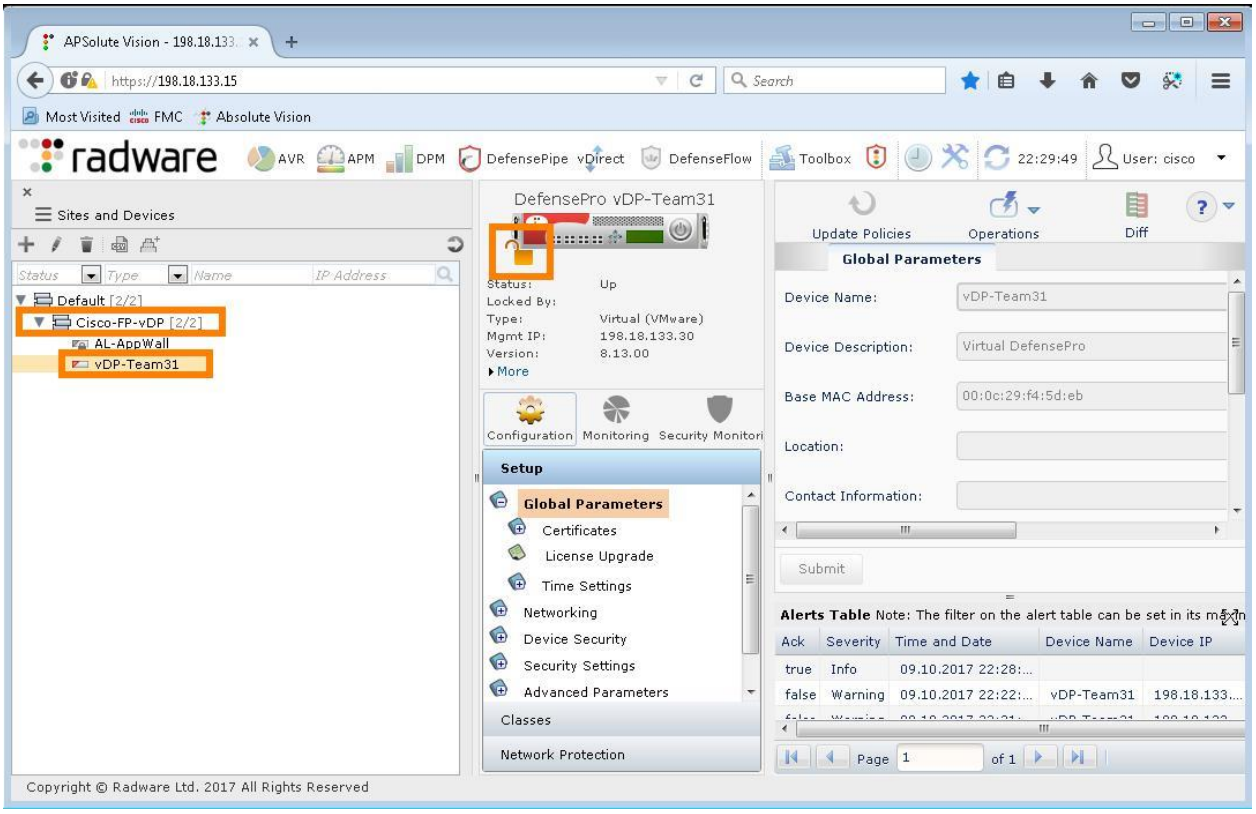
注: Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [手順を見る] 。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法には、接続ができない場合や、パフォーマンスが悪い場合があります。

3. ブラウザから `https://198.18.133.15` にアクセスするか、[APSolute Vision] ブックマークをクリックします。ユーザ名 cisco およびパスワード `C1sco12345` を使用してログインします。



4. 画面左側にある [Cisco-FP-vDP] を選択します。

5. vDP を選択し、デバイスを管理するために**ロック** アイコンをクリックします。

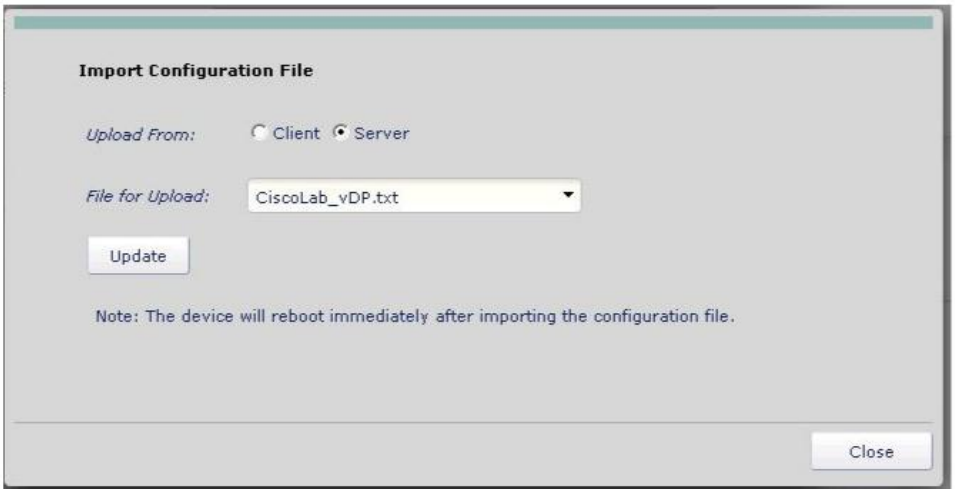


6. [動作（Operations）] を選択します。オプションがアクティブになっている場合は、[設定ファイルのインポート（Import Configuration File）] をクリックして、最新の設定をダウンロードします。

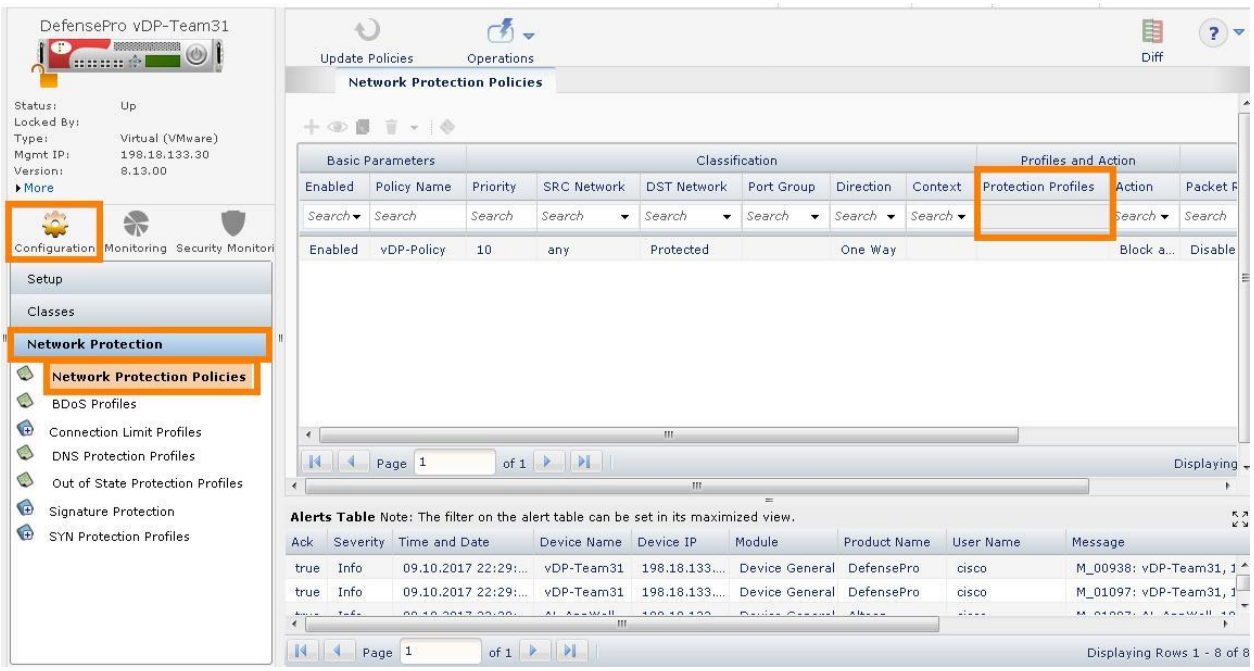
7. [サーバ（Server）] オプション ボタンをオンにして、**CiscoLab_vDP.txt** を選択します。

8. [更新（Update）] をクリックして vDP をリセットします。オプションがグレー表示になっている場合は、次の手順に進みます。

注：vDP の再起動には 5 分ほどかかる場合があります。



9. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] の順に選択して、保護プロファイルが設定されていないことを確認します。



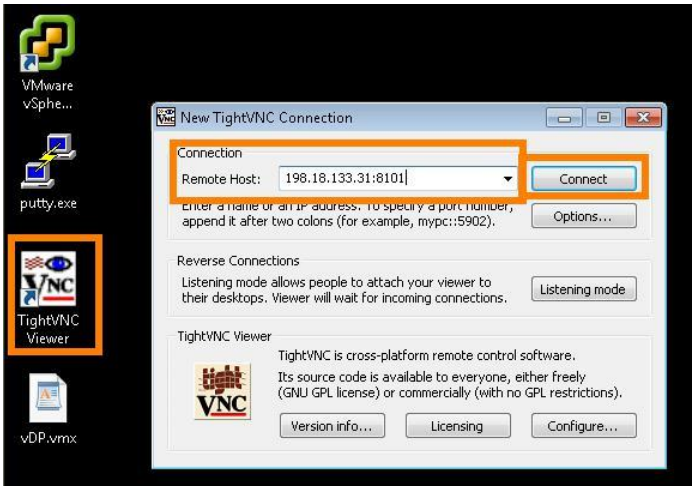
シナリオ 1.　BDoS 攻撃

このデモでは、ポート 80 に対して TCP RST フラッドと UDP フラッドの 2 つの BDoS 攻撃を開始します。これらのフラッドはステートフル デバイスによって軽減できますが、こうしたフラッドは、1 秒あたりのパケット数を過大にしてシステムを過負荷にすることを目的にしています。

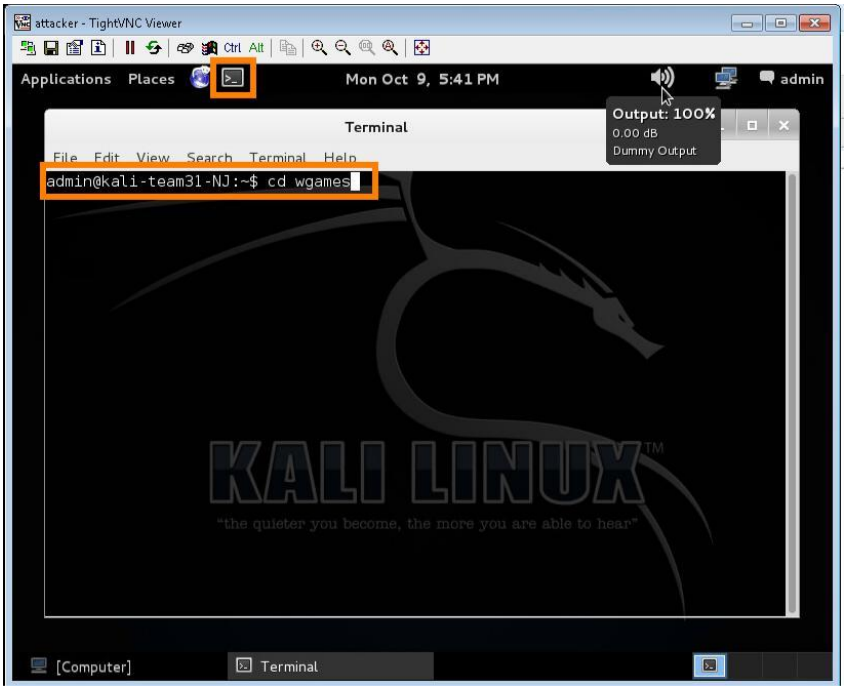
手順

TCP フラッド

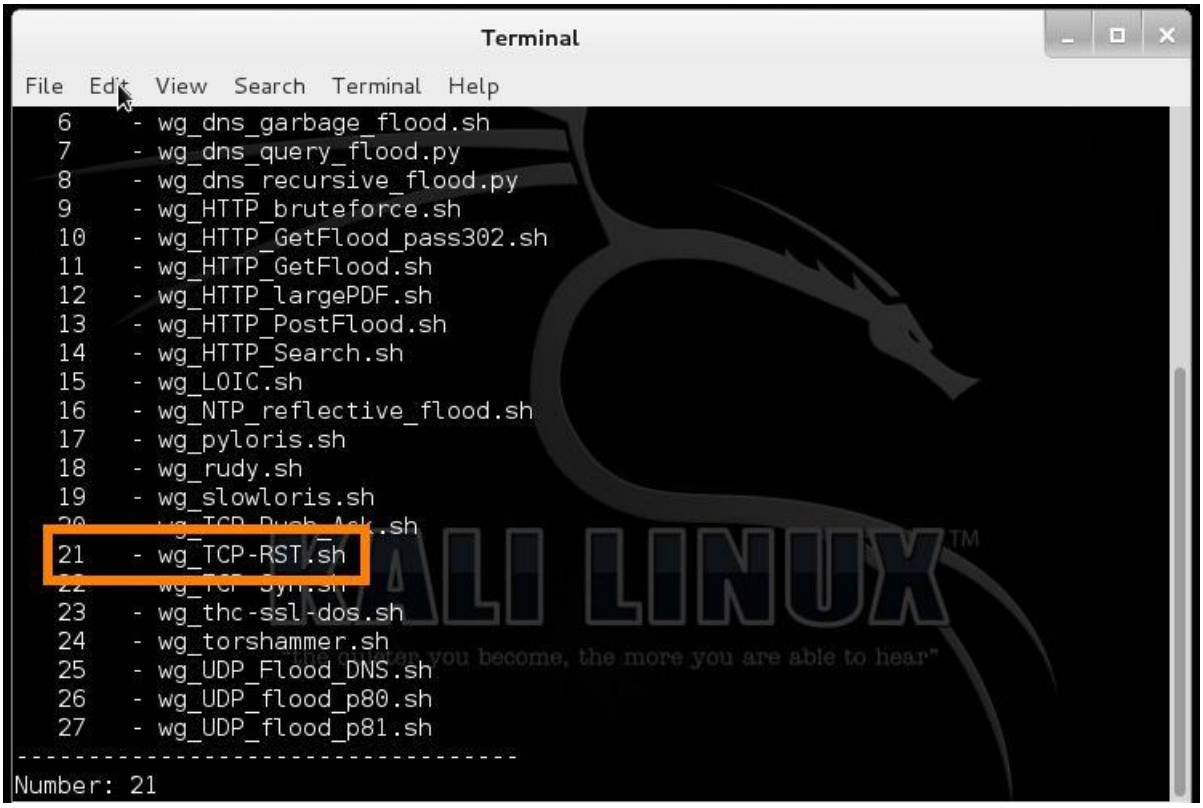
1. デスクトップで TightVNC Viewer を開きます。Kali マシンに `198.18.133.31:8101` で VNC 接続します。ユーザ ID admin とパスワード `C1sco12345` でログインします。



2. 左上部の端末アイコンをクリックし、プロンプトに「**`cd wgames`**」と入力します。



3. 「`sudo ./start.sh`」と入力し、ルート パスワード C1sco12345 を入力します。「21」と入力して [item 21]（TCP-RST 攻撃）を選択し、Enter を押します。



4. ワークステーションで PuTTY を使用し、vDP= `198.18.133.31 Port = 6401` のコンソールに Telnet 接続します。

5. プロンプトに「`system inf-stats reset`」と入力します。

注：ログインを要求するメッセージが表示された場合は `login` コマンドを入力し、ユーザ名 admin とパスワード C1sco12345 を入力します。

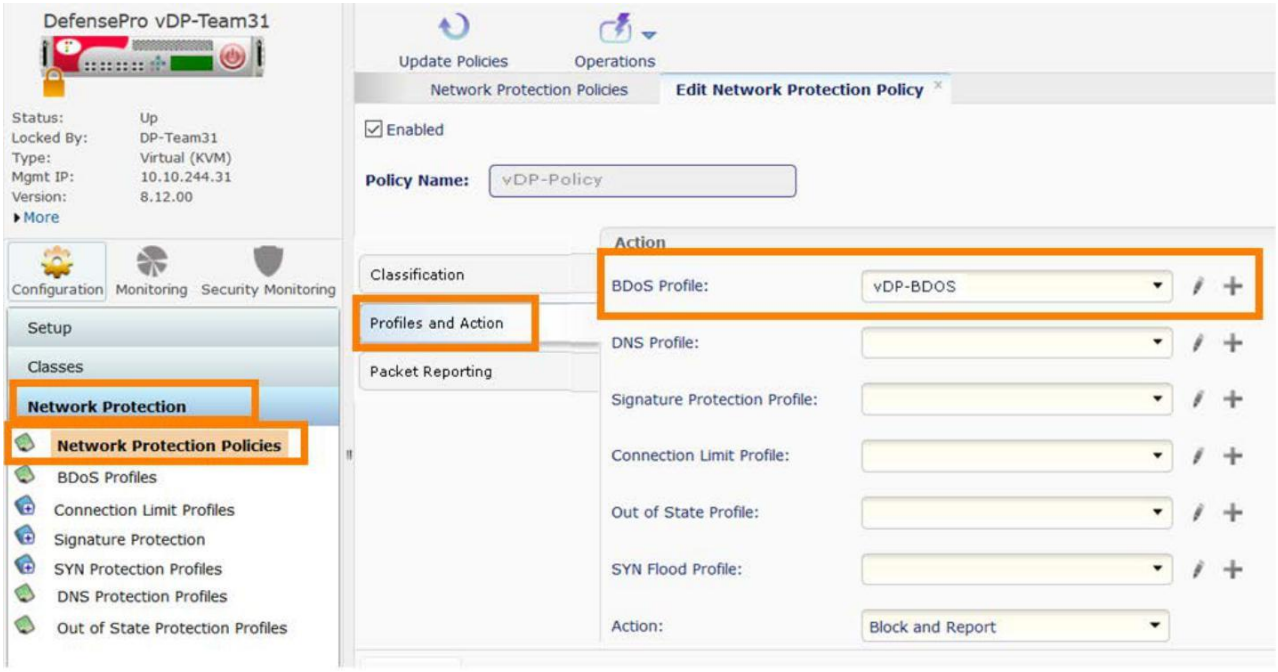
6. 次に「`system inf-stats`」と入力します。

   ポート 1（外部ポート）に大量のトラフィックが着信し、TCP ポート 0 を送信元ポートまたは宛先ポートとして使用するパケットが vDP によって自動的にブロックされることを示すメッセージが表示されます。

7. 攻撃用マシンで、Ctrl+C を押して攻撃を停止します。

Defense Pro

1. Vision で、[設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択し、セッションの BDOS 保護プロファイルを有効にします。
2. vDP-Policy ポリシーをダブルクリックし、[プロファイルとアクション（Profiles and Action）] を選択します。

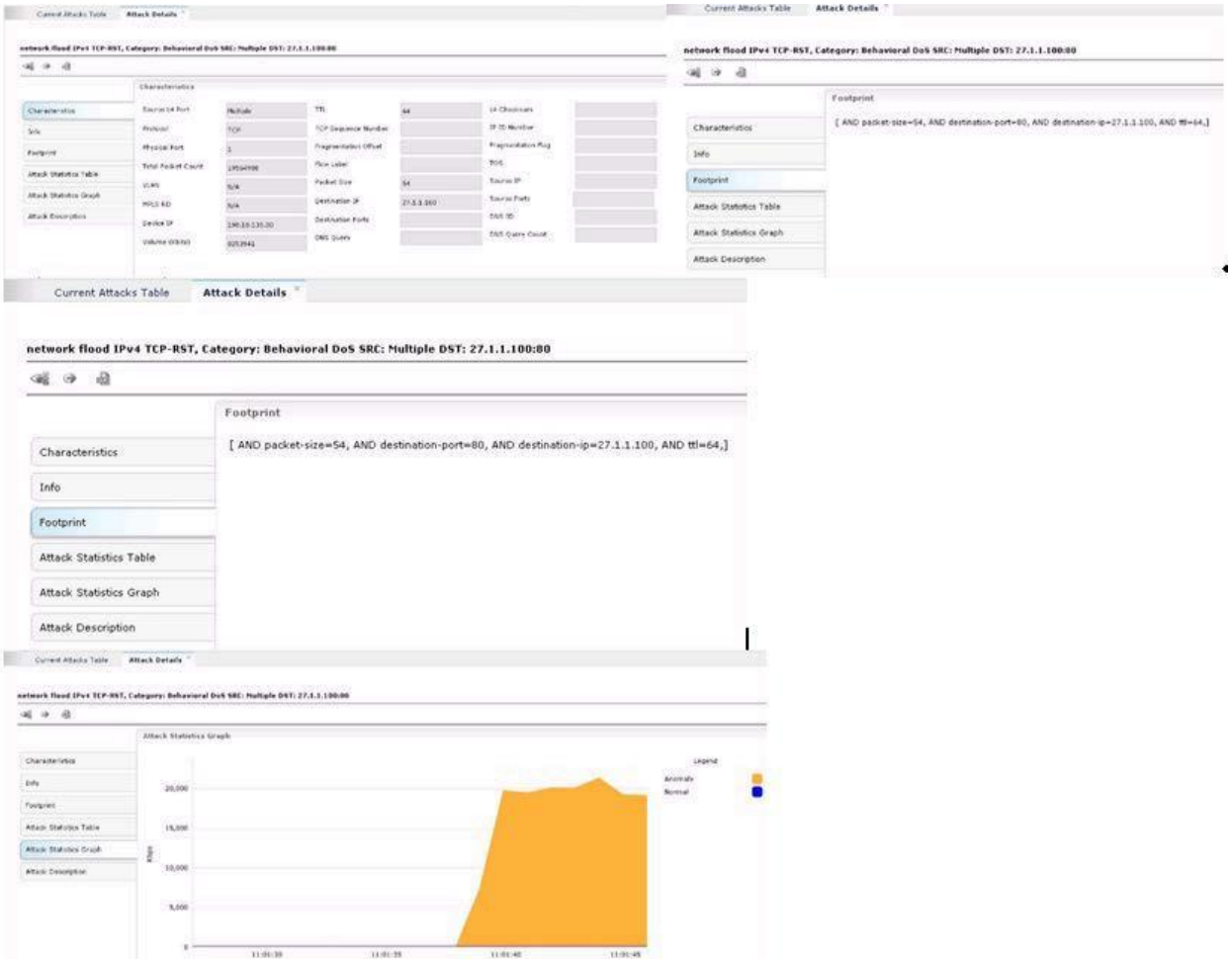


3. [BDoS プロファイル（BDoS Profile）] で [Lab-BDOS] を選択し、[送信（Submit）] をクリックします。
4. [ポリシーの更新（Update Policies）] をクリックし、設定変更を有効化します。攻撃用のマシンで攻撃を再開します。
5. コンソールで、BDOS が攻撃をドロップするのがわかります。

```
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. Vision で [セキュリティ モニタリング（Security Monitoring）] > [現在の攻撃テーブル（Current Attack Table）] を選択すると、攻撃が表示されます。

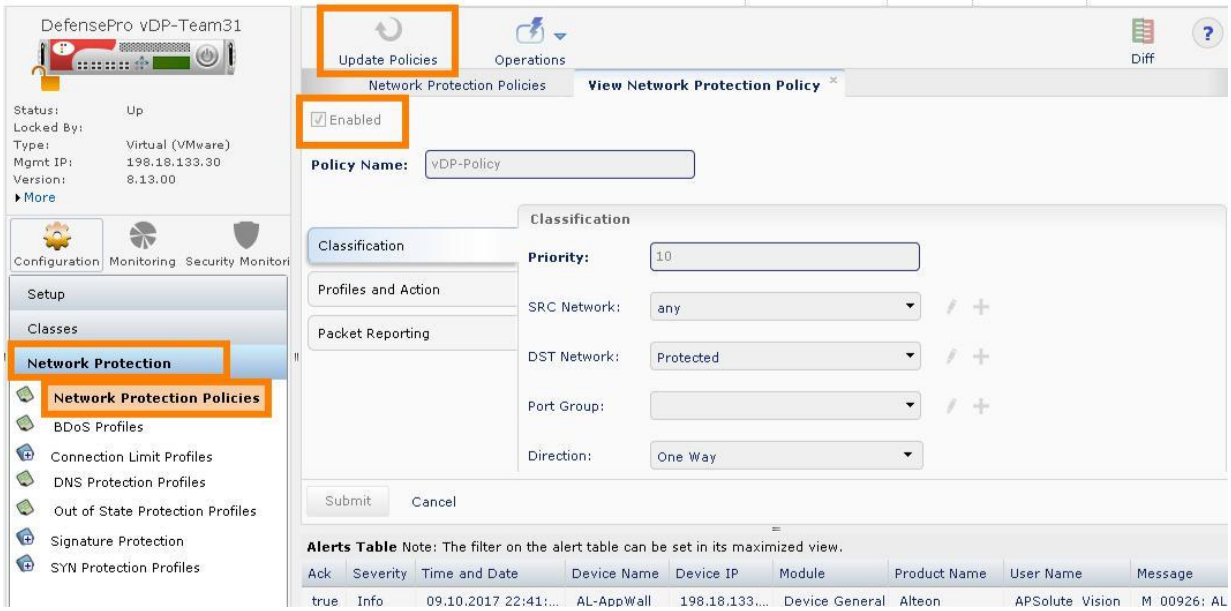
7. 攻撃をダブルクリックすると、詳細が表示されます。



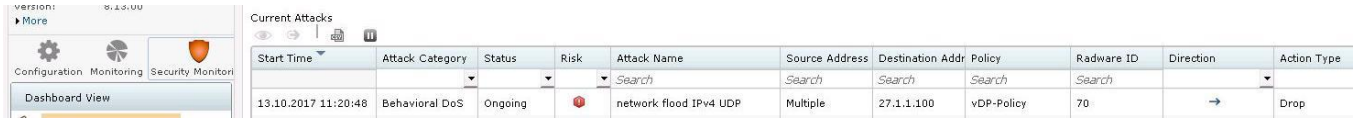
8. Ctrl+C を押して、攻撃用マシンの攻撃を停止します。

UDP フラッド

1. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択して、現在のポリシーを無効にします。ポリシーをダブルクリックします。
2. [有効（Enabled）] ボックスをオフにして、[送信（Submit）] をクリックします。
3. [ポリシーの更新（Update Policies）] をクリックします。



4. 攻撃用マシンの端末で **./start.sh** を実行します。オプションの [26 wg_UDP_flood_p80.sh] を選択します。



5. **`system inf-stats`** を実行して、vDP の統計情報を確認します（最初に `system inf-stats reset` を実行してリセットします）。

Defense Pro

1. ポリシーに戻り、[設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択して再度有効にします。ポリシーをダブルクリックします。
2. [有効（Enabled）] ボックスをオンにして、[送信（Submit）] をクリックします。
3. [ポリシーの更新（Update Policies）] をクリックします。
4. これで、vDP によって攻撃が軽減されるようになり、正当なマシンから http://27.1.1.100 のデモンストレーション マシンにアクセスできます。
5. 攻撃用マシンで、Ctrl+C を押して攻撃を停止します。

6. 次のシナリオに進む前に、BDoS 保護を解除します。ポリシーに移動し、[設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択して **bdos プロファイル**を削除します。ポリシーをダブルクリックします。
7. [プロファイルとアクション（Profiles and Action）] を選択します。
8. [BDoS プロファイル（BDoS Profile）] でドロップダウンをクリックし、空白のプロファイルを選択します。
9. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。

シナリオ 2.　SYN フラッド攻撃

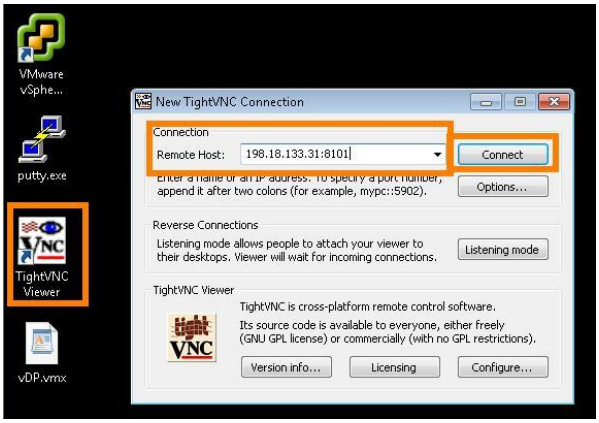
このシナリオでは、2 つの攻撃を行います。1 つはポート 80 に対するシンプルな SYN フラッドです。この攻撃は、大量の SYN パケットによってファイアウォール状態テーブルを過負荷にすることを意図したものであり、BDOS エンジンと SYN フラッド保護によって軽減できます。

2 番目の攻撃は HTTP GET フラッドです。この攻撃は正当な TCP トラフィックとしてファイアウォールをバイパスし、サーバを過負荷にします。SYN フラッド保護を使用して攻撃を軽減します。

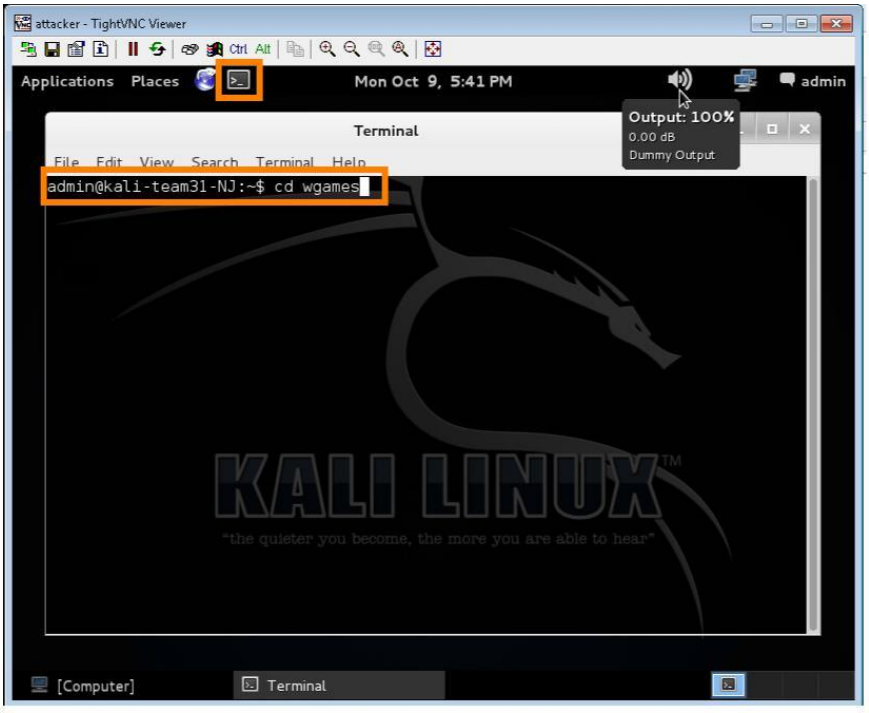
手順

SYN フラッド

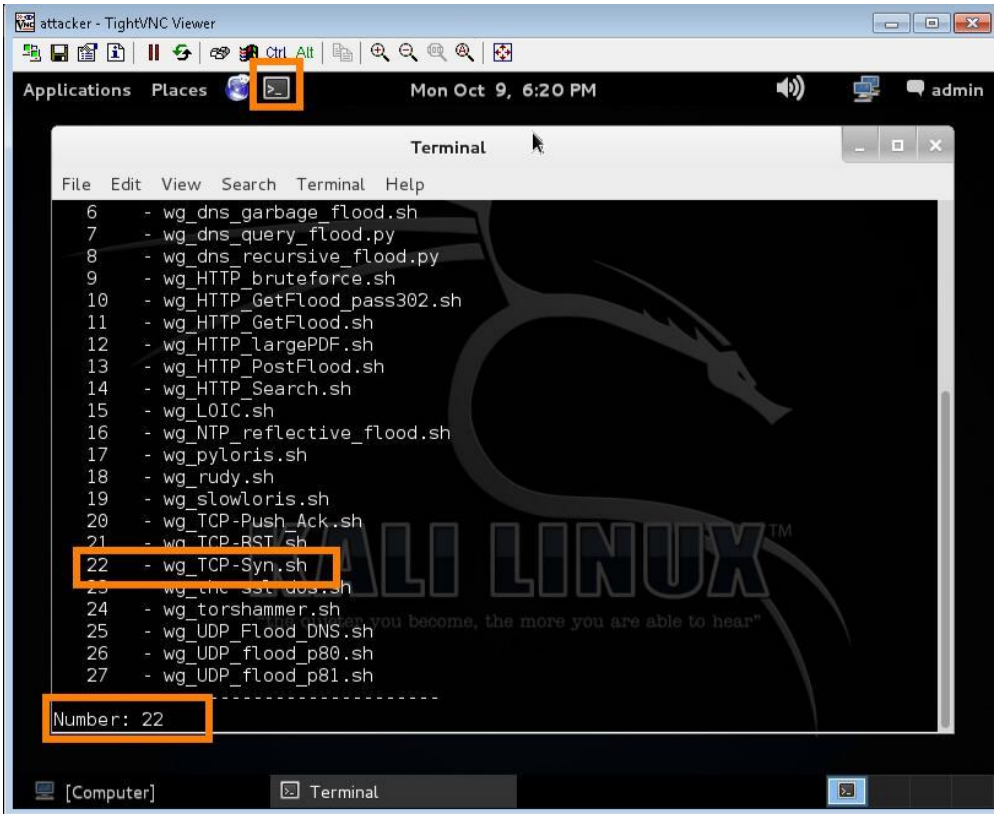
1. デスクトップで TightVNC Viewer を開きます。Kali マシンに `198.18.133.31:8101` で VNC 接続します。ユーザ ID admin とパスワード `C1sco12345` でログインします。



2. 左上部の**端末**アイコンをクリックし、プロンプトに「**`cd wgames`**」と入力します。



3. 端末で「`sudo ./start.sh`」と入力し、オプションの [option 22 wg_TCP-Syn.sh] を選択して、基本的な SYN 攻撃を開始します。



4. `system inf-stats` テーブルで攻撃を確認してください。

BDOS 保護の有効化

1. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択し、ポリシーをダブルクリックして、BDoS プロファイルを再度有効にします。[ポリシーの更新（Update Policies）] を押して変更を有効化します。
2. `dp rtm-stats` テーブルで、着信したパケットと破棄されているパケットを確認します。
3. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択して、ポリシーの BDOS 保護をオフにします。ポリシーをダブルクリックします。
4. [プロファイルとアクション（Profiles and Action）] を選択します。
5. [BDoS プロファイル（BDoS Profile）] でドロップダウンをクリックし、空白のプロファイルを選択します。
6. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。
7. 攻撃を続行します。

SYN 保護プロファイルの有効化

1. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択し、ポリシーをダブルクリックします。
2. [プロファイルとアクション（Profiles and Action）] を選択します。
3. [SYN フラッド プロファイル（SYN Flood Profile）] オプションで、[Lab-SYN-nocookie] を選択します。
4. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。
5. vDP によって攻撃が軽減されますが、今度は攻撃に次のラベルが付けられます。

```
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. `system inf-stats` を確認します。

```
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. 着信したインターフェイスと同じインターフェイスで、パケットがバウンスされています。vDP は、BDOS のようにパケットをドロップするのではなく、検出されたこの SYN フラッドに対して SYN チャレンジを送信します。
8. Ctrl+C を押して、攻撃用マシンの攻撃を停止します。

HTTP GET フラッド

1. 攻撃用マシンで「**`sudo ./start.sh`**」と入力し、オプションの [11 wg_HTTPGetFlood.sh] を選択して、新しい攻撃を開始します。
2. それによって **HTTP GET** フラッドが開始されます。

注：HTTP GET は基本的な SYN 保護による SYN チャレンジの通過には支障がなく、ファイアウォールや vDP によっては検出されません。

Defense Pro

1. 攻撃を軽減するには、[設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択し、ポリシーをダブルクリックします。
2. [プロファイルとアクション（Profiles and Action）] を選択します。
3. [SYN フラッド プロファイル（SYN Flood Profile）] オプションで [Lab-SYN-cookie] を選択します。
4. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。

5. 攻撃用マシンで保護をアクティブにすると、速度が大幅に低下することがわかります。また、[セキュリティ モニタリング（Security Monitoring）] での SYN フラッド保護も確認できます。
6. vDP が攻撃を検出していることを確認できない場合は、標準の **HTTP 保護**ではなく **HTTP_Low protection** を使用するように [SYN フラッド（SYN flood）] プロファイルを変更するか、標準の HTTP 保護を変更してアクティベーションしきい値を下げます。

7. Ctrl+C を押して、攻撃用マシンの攻撃を停止します。

シナリオ 3.　DNS 攻撃

手順

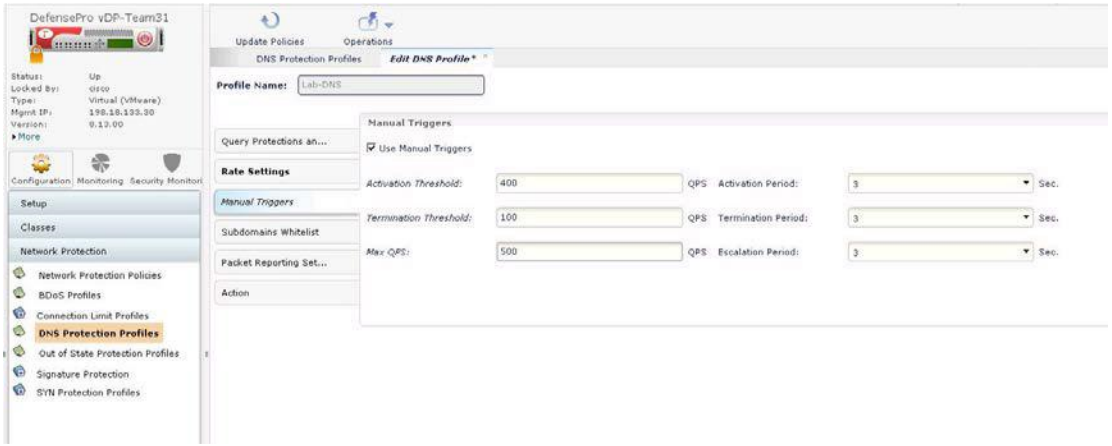
攻撃の軽減

DNS 攻撃も 2 つの方法で軽減できます。BDOS では、DNS サーバがないネットワークをターゲットとした DNS フラッド攻撃をブロックできます。ただしフラッドが DNS サーバをターゲットとしている場合は、署名が作成され、正当な DNS 要求がブロックされます。

1. 攻撃用マシンで「`sudo ./start.sh`」と入力し、オプションの [7] を選択して、**DNS クエリ** フラッドを開始します。
2. `system inf -stats reset` コマンドを実行します。
3. 攻撃が開始されたら、vDP コンソールで `system inf-stats` テーブルを確認します。

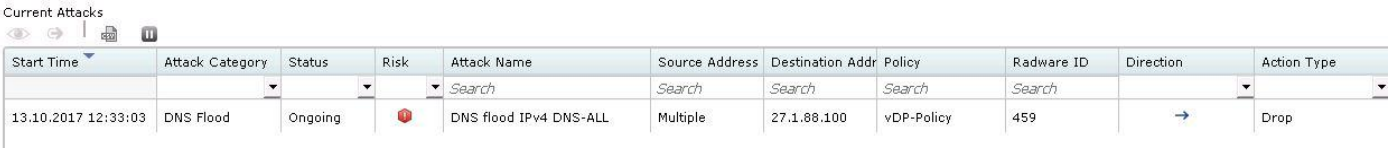
Defense Pro

1. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択します。
2. ポリシーをダブルクリックして、[アクション（Action）] をクリックします。
3. [DNS プロファイル（DNS Profile）] を選択して、ドロップダウンから [Lab-DNS] を選択します。
4. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。
5. DNS が検出されない場合は、攻撃ツールによって 1 秒あたりに生成されるクエリ数が不足している可能性があります。
6. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [DNS 保護プロファイル（DNS Protection Profiles）] に移動し、既存のプロファイルをダブルクリックします。
    a. [手動トリガー（Manual Triggers）] タブを選択し、しきい値を次のように低い値に変更します。
    b. [アクティベーションしきい値（Activation threshold）] = 40 QPS、[終了しきい値（Termination threshold）] = 10 QPS、[最大 QPS（Max QPS）] = 50
    c. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。



7. [セキュリティ モニタリング（Security Monitoring）] ウィンドウで、攻撃が軽減されていることを確認できます。

8. 確認したら、Ctrl+C を押して攻撃を停止します。


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

シナリオ 4.　Low and Slow 攻撃

手順

攻撃の開始

Low and Slow 攻撃は HTTP GET フラッドに似ていますが、低速の接続から開始し、最初に少数の接続を送信し、そこから不完全な GET 要求による接続を重ねていきます。

1. 攻撃用マシンで「`./start.sh`」と入力し、オプション [19 wg_slowloris,sh] を選択して、Low and Slow 攻撃を開始します。
2. 攻撃が開始されたら、`system inf-stats table` コマンドを実行して vDP コンソールを確認します。
3. VNC を使用して正当なクライアントに接続します。しばらくすると、攻撃によって http://27.1.1.100 のサーバが応答を停止するか、大幅に低速になります。

Defense Pro

1. [設定（Configuration）] > [ネットワーク保護（Network Protection）] > [ネットワーク保護ポリシー（Network Protection Policies）] を選択します。
2. ポリシーをダブルクリックして、[アクション（Action）] をクリックします。
3. [署名保護プロファイル（Signature Protection Profile）] を選択し、ドロップダウンから [DOS-All] を選択します。
4. [送信（Submit）] をクリックして、[ポリシーの更新（Update Policies）] をクリックします。
5. [セキュリティ モニタリング（Security Monitoring）] ウィンドウで、攻撃が軽減されていることを確認できます。
6. 正当なクライアントを確認します。サーバが応答を再開します。
7. 確認したら、Ctrl+C を押して攻撃用マシンによる攻撃を停止します。

注：DOS-All 署名の他に、SYN 保護によって軽減することもできます。必要に応じて [LAB-SYN-Cookie] オプションを選択すると、ツールが HTTP チャレンジを通過できなくなります。

シナリオ 5.　マルチベクトル攻撃

このセクションではあなたがハッカーになります。以下に、Kali マシン上のスクリプトとその説明のリストを示します。既存のすべての vDP ポリシーを有効にして、もう少し多くのスクリプトを実行してみてください。また、別個の cmd ウィンドウでいくつかのスクリプトを同時に実行し、結果を Vision でモニタしてください。

スクリプト名	攻撃/攻撃ツール	説明
wg_apache_Killer.sh	Apache Killer	https://security.radware.com/ddos-knowledge-center/ddospedia/apache-killer/
wg_botnet.sh	BoNeSi	DDoS ボットネット シミュレータ https://github.com/Markus-Go/bonesi
wg_dnsflood_STAS.py	DNS フラッド	DNS サーバにランダム パケットを送信
wg_dns_flood.py	DNS クエリ フラッド	www.radware.com に対する DNS 要求をサーバに送信
wg_dns_garbage_flood.sh	DNS ガーベッジ フラッド	ポート 53 の DNS サーバにガーベッジ（HTML ページ）を送信
wg_dns_query_flood.py	DNS フラッド	wg_dns_flood.py と同様。重複するため削除する必要あり
wg_dns_recursive_flood.py	DNS 再帰フラッド	再帰 DNS 要求をサーバに送信
wg_HTTP_bruteforce.sh	HTTP フラッド/包囲攻撃	認証が必要なページ（/accounts.aspx）に HTTP フラッドを送信
wg_HTTP_GetFlood.sh	HTTP フラッド	多数の HTTP GET 要求をサーバのスタート ページに送信
wg_HTTP_GetFlood_pass302.sh	HTTP フラッド	GetFlood.sh に似ているが HTTP-302 チャレンジに対応する機能を追加
wg_HTTP_largePDF.sh	HTTP フラッド	サーバ上のサイズの大きいファイルに多数の HTTP 要求を送信し、すべてのアップストリーム帯域幅を使用することで、正当なクライアントでサーバからの応答が低速になる
wg_HTTP_PostFlood.sh	HTTP フラッド	多数の HTTP POST 要求をサーバのスタート ページに送信
wg_HTTP_Search.sh	HTTP フラッド	多数の HTTP GET 要求をサーバの検索ページに送信し、CPU 使用率を過大にする
wg_LOIC.sh	LOIC	Low Orbit Ion Cannon（LOIC）は Praetox Technologies が開発した、オープン ソースのネットワーク ストレス テスト ツール。これにより開発者は、診断目的でサーバに大きなネットワーク トラフィック負荷をかけることが可能になりましたが、その後パブリック ドメインで各種の更新によって修正が加えられ、Anonymous により DDoS ツールとして広範に利用されるようになりました。 https://security.radware.com/ddos-knowledge-center/ddospedia/loic-low-orbit-ion-cannon/
wg_NTP_reflective_flood.sh	NTP リフレクション フラッド	https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/ntp-reflected-flood/
wg_pyloris.sh	Pyloris	Pyloris は Slow HTTP DoS ツール。 https://security.radware.com/ddos-knowledge-center/ddospedia/pyloris/
wg_rudy.sh	R.U.D.Y	R.U.D.Y.Attack（R-U-Dead-Yet?）は、Slow Rate HTTP POST（レイヤ 7）によるサービス妨害ツール。 https://security.radware.com/ddos-knowledge-center/ddospedia/rudy-r-u-dead-yet/
wg_slowloris.sh	Slowloris	Slowloris はグレーハット ハッカー「RSnake」が開発したサービス妨害（DoS）ツールであり、非常に低速な HTTP 要求によって DoS を発生させます。 https://security.radware.com/ddos-knowledge-center/ddospedia/slowloris/
wg_TCP-Ack_flood.sh	TCP フラッド	TCP-ACK アウトオブステート パケットによってサーバのフラッディングを発生させる
wg_TCP-Push_Ack.sh	TCP フラッド	TCP-Push-ACK アウトオブステート パケットによってサーバのフラッディングを発生させる
wg_TCP-RST.sh	TCP フラッド	TCP-RST アウトオブステート パケットによってサーバのフラッディングを発生させる
wg_TCP-Syn.sh	TCP フラッド	新しいセッションを開始する TCP-SYN パケットによってサーバのフラッディングを発生させる
wg_thc-ssl-dos.sh	THC-SSL-DOS	The Hacker's Choice（THC）というハッキング グループが開発した THC-SSL DOS は、SSL の重大な脆弱性にベンダーがパッチを適用するうえでの、概念実証となることを目的としたもの。 https://security.radware.com/ddos-knowledge-center/ddospedia/thc-ssl-dos/
wg_torshammer.sh	TORSHAMMER	Torshammer は、phiral.net が開発した Slow Rate HTTP POST（レイヤ 7）DoS ツールです。 https://security.radware.com/ddos-knowledge-center/ddospedia/tors-hammer/
wg_UDP_Flood_DNS.sh	DNS フラッド	ランダム DNS パケットによってサーバのフラッディングを発生させる
wg_UDP_flood_p80.sh	UDP フラッド	ファイアウォールでの設定ミスによってポート 80 がオープンになっていることを前提に、ポート 80 に対するランダム パケットによってサーバのフラッディングを発生させる。それによってサーバの IP スタックの負荷を高めます。
wg_UDP_flood_p81.sh	UDP フラッド	UDP パケットによってポート 81 でサーバのフラッディングを発生させる。

付録 A.　シスコ次世代ファイアウォールへのアクセス

シスコ次世代ファイアウォールは、この環境の追加機能として配置されたもので、Radware の機能を示すうえで必須ではありません。現在はルーテッド インライン モードになっていますが、すべてのポリシーがアラート限定に設定されています。発生した攻撃の一部が表示されるように、いくつかの特別な設定が有効になっていますが、すべての攻撃を確認することはできません。ただし必要に応じて、Radware と連動する Cisco Firepower ソリューションのフル機能にアクセスすることが可能です。

1. Firepower 管理コンソールを開くには、wkst1 から Google Chrome ブラウザを開き、ツールバーの **FMC** ショートカットをクリックします。Firepower のログイン クレデンシャルは、ユーザ名：**dcloud**、パスワード：**C1sco12345** を使用します。

注：FTD インターフェイスにトラフィックがないことを示すヘルス警告が表示されても、手動で開始された攻撃によってのみトラフィックが発生することから、これは通常の動作と見なすことができます。攻撃シナリオを開始すると、警告はクリアされます。ライセンスが付与されている数よりもホスト数が多いことを示すライセンス アラートが表示される場合もあります。これは、Radware ソリューションでブロックされるように設定されていない場合に、大量の DDoS 攻撃ホストが NGFW にアクセスすることによります。

現実には、Kali マシンをブラック ホール化するだけで済ます場合があります。ただし現実はそれほど単純ではありません。DDoS 攻撃は、数千から数百万のデバイスのボットネットによる場合も、1 つの IP アドレスによる場合もあるため、アプリケーションを実行する AWS を、または大学の場合は学生寮だけを、単純に停止するようなことはできません。Radware vDP は、こうしたタイプの攻撃を自動的に検出して軽減するように設計されています。Cisco FTD と vDP の連携によって大きな効果が得られます。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp