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。

- <u>要件</u>
- <u>このソリューションについて</u>
- <u>トポロジ</u>
- <u>はじめに</u>
- <u>シナリオ 1:BDoS 攻撃</u>
- シナリオ 2:SYN フラッド攻撃
- シナリオ 3:DNS 攻撃
- シナリオ 4: Low and Slow 攻撃
- シナリオ 5:マルチベクトル攻撃
- ・ 付録 A:シスコ次世代ファイアウォール アクセス

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2. 論理トポロジ

Cisco Firepower と vDP のトポロジ

vDP と Firepower POD

接続情報

13C47C119 FIX						
wkst1 IP		198.18.133	.36			
vDP管理I	P	198,18,133	.30			
vDP コンン	/-JUIP (Telne	t) 198,18,133	31:6401			
Alteon 管理	PIP (SSH/HTT	PS) 198 18 133	25	FMC		
Tuttoon E.	1. (00.11111		1	98.18.129.100/18		
			67	· · · · · · · · · · · · · · · · · · ·		
Firepower	r管理				正当たクライアントロ	
FMC	https://	198.18.129.100	wkett	APSolute Vision	27 1 31 11 / 24	10 10 10 10 10 10 10 10 10 10 10 10 10 1
FTD シリア	7ル 198.18	133 31 8401	100 10 100 20/10	198.18.133.15/18	27.1.31.117.24	
FTD SSH	198 18	133 20	190.10.133.30/10	······································	- 12	27.1.31.10724
110 0011	100.10					
攻撃側のマ	シン接続				MNG	Web 攻撃者
攻撃者のい	/NC	198 18 133 31 810	1	10 100 1 110	スイッチ	• 27.1.31.54/24
	F/ IP	27 1 31 10	198	.18.128.1 / 18		
正当たクラ	TTYLVNC	198 18 133 31-820		00	0000	
273	=/, ID	27 1 21 11			600	000 スイッチ
		27.1.31.11				•
サーバ側					VDP	101 m
DOS 2-1	Fin h (Turnkon	27 1 1 100		G-1	MNG-1: 198.18.133.30	/ 18
0037	/ / / / / / / / / / / / / / / /	// 2/.1.1.100				
ログイン情	t åg				1996 (1997)	
wket1.	administrator	C1cco12345		G-2		
Vicion:	aurimitsuator	2245				
VISIOII.	deleved/04eee	40045				
FMC:	acioua/C isco	12345				
その他	admin/C1sco	12345		1		
					ETD	
					IL-b	DOG & Hand
				5 本	- 27 1 31 100	DUSALFOR
				77司	- 27.1.31.100	27.1.1.100724
				内部	= 27.1.1.204	
				官坦	198.18.133.20/18	

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。 [<u>手順を見る</u>]

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 [<u>手順を見る</u>] 。 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。

PSolute Vision +					
🗲 🗊 🕰 https://198.18.133.15			C Q Search		*
🔊 Most Visited 📰 FMC 🛊 Absolute Vision					
	_	_	_		62.
				radware	
	APSolute Vi	sion Login		•	
	User Name:	cisco			
	Password:	•••••			
		~			
				Log To	
				Log In	

- 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。

DefensePro vDP-Team31	Vpdate Policies	Import Configuration File
	Global Parame	Export Configuration File
Status: Up Locked By: cisco Type: Virtual (VMware)	Device Name:	Export Configuration Log File
Agmt IP: 198.18.133.30 /ersion: 8.13.00	Device Description:	Update Software Version
A T	Base MAC Address:	Update Security Signatures
Configuration Monitoring Security Monitori	Location:	

Upload From:	C Client 🏾 Server		
File for Upload:	CiscoLab_vDP.txt	-	
Update			
Note: The devic	e will reboot immediately after i	mporting the configuration	file.
Note: The devic	e will reboot immediately after i	mporting the configuration	file.
Note: The devic	e will reboot immediately after i	mporting the configuration	file.

[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。

DefensePro vDP-Team31	Update Ne) Policies stwork Protec	Operations	s es						Diff	? •
Status: Up Locked By: Type: Virtual (VMware)	+ @ 6	I ≣ - Φ									
Mgmt IP: 198.18.133.30	Basic	Parameters			Class	ification			Profiles and	Action	
► More	Enabled	Policy Name	Priority	SRC Network	DST Network	Port Group	Direction	Context	Protection Profiles	Action	Packet F
	Search 🗸	Search	Search	Search 👻	Search 👻	Search 👻	Search 👻	Search 🔻		Search 👻	Search
Configuration Monitoring Security Monitori	Enabled	vDP-Policy	10	any	Protected		One Way			Block a	Disable
BDoS Profiles Connection Limit Profiles	•				m						
DNS Protection Profiles	14 4	Page 1	of 1								Displaying
Out of State Protection Profiles	•				III						E.
G Signature Protection	Alerts Tab	le Note: The fill	ter on the a	lert table can be	set in its maxim	= nized view.					5
G SYN Protection Profiles	Ack Seve	rity Time and	Date	Device Name	Device IP	Module	Product N	lame Us	er Name Mes:	age	
	true Info	09.10.20	17 22:29:	vDP-Team31	198.18.133	Device Genera	al Defensei	Pro cis	sco M_C	0938: vDP-	Team31, 1
	true Info	09.10.20	17 22:29:	vDP-Team31	198.18.133	Device Genera	al Defensel	Pro cis	sco M_C	1097: vDP-	Team31, 1
	4	00.10.00	17.00.00.	AL ALEW-III	100 10 100	Denies Orean	.1		м.	1007. 11 1.	
4											

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。 VMware vSphe... 🚾 New TightVNC Connection Connection Remote Host: 198.18.133.31:8101 Connect criter a name or an 1P address. To specify a port numb append it after two colons (for example, mypc::5902). putty.exe Options... Reverse Connections Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections. /NC Listening mode ight/N TightVNC Viewer TightVNC is cross-platform remote control software. Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions). VNC Version info... Licensing Configure... DP vm
- 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。

	Terminal	-	×
File B	d' View Search Terminal Help		
6 7	~ wg_dns_garbage_flood.sh - wg_dns_guery_flood.pv		
8	- wg dns recursive flood.py		
9	- wg HTTP bruteforce.sh		
10	- wg_HTTP_GetFlood_pass302.sh		
11	- wg_HTTP_GetFlood.sh		
12	- wg_HTTP_largePDF.sh		
13	- wg_HTTP_PostFlood.sh		
14	- wg_HTTP_Search.sh		
15	- wg_LOIC.sh		
10	- wg_NIP_reflective_flood.sh		
1/	- wg_pyloris.sn		
18	- wg_ruay.sn		
19	- wg_stowtoris.sn		
21	- wg_TCP-RST.sh		
22	wg_to_syntan		
23	- wa torshammer sh		
25	wg_torshammer.sh		
26	- wa UDP flood p80.sh		
27	- wa UDP flood p81.sh		
Number	: 21		10

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。

Defer	nsePro#13-1	0-2017 09:54:4	4 WARNING 12	5 Anomalies	"L4 Source or	Dest Port Zer	" TCP 24	9.95.93.31	0 27.1.1.10	0 80 1 Regu	lar "Packet	Anomalie	:s"
ample	d 1 54 N/A	O N/A low dro;	p FFFFFFFF-F	FFF-FFFF-OC	1A-000059E089B	В							
Defer	nsePro#13-1	0-2017 09:54:4	4 WARNING 12	5 Anomalies	"L4 Source or	Dest Port Zer	" IP 0.0	.0.0 0 0.0	.0.0 0 0 Reg	ular "Packet	t Anomalies	" occur	5 2
A O	N/A low dr	op FFFFFFFFF-FF	FF-FFFF-001J	-000059E085	BB								
Defer	nsePro#syst	em inf-stats											
Port	ifInPkts	ifInDiscards	ifInErrors	ifOutPkts	ifOutDiscards	ifOutErrors							
1	12897830	6	— 0	15									
2	15	0	- O	12897634									
MNG-1	1034			1922									
Defer	nsePro#												

7. 攻撃用マシンで、Ctrl+Cを押して攻撃を停止します。

Defense Pro

- 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。

DefensePro vDP-Team31	Update Policies	Operations			
	Network Prote	ction Policies Edit Network Protect	ction Policy ×		
Status: Up Locked By: DP-Team31 Type: Virtual (KVM) Mgmt IP: 10.10.244.31 Version: 8.12.00 More *	Enabled Policy Name: VDP	P-Policy			
		Action			
Configuration Monitoring Security Monitoring	Classification	BDoS Profile:	vDP-BDOS	•	1 +
Setup	Profiles and Action	DNS Profile:	6	•	1 +
Classes	Packet Reporting				
Network Protection		Signature Protection Profile:	ĺ.	•	/ +
Network Protection Policies		Connection Limit Profile:	1	•	1 +
BDoS Profiles					
Connection Limit Profiles		Out of State Profile:		•	/ +
G Signature Protection					
SYN Protection Profiles		SYN Flood Profile:		•	/ +
DNS Protection Profiles			For a set of the set of the set of the set		
Out of State Protection Profiles		Action:	Block and Report		

- 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。

	it, category, perspeterate	un sale: Methyle Dist; 2	7.8.1.199.96			network flood IPv4 TCP-R	T, Category: Behavioral DoS SRC: Multiple DST: 27.1.1.100:00
6.9.10						a = di	
	Charlasteriatics					S 1 Martin California	Fostprint
Characteristics	Baurus b4 Port	Hulfole	770.	64	of Originals		
de .	Prohestal	704	10P Departor Notified		37 35 Novibur	Characteristics	[AND packet-site=54, AND destination-port=80, AND destination-sp=17.1.1.100, AND fil=
and the second	Hysical Fort	3	Pragnantation Officed		Praymentation Ring	Jofo	
teck thereis table	Tetal Policy! Court	1910-199	Pice Label		705	(12)(5)(2)(5)	
tech Shatistics Grand	VC-MS	5/4	Packet Dor	ы	tars P	Footprint	
	HPLS 4D	2/4	Qentratian 24	25.8.8.860	Taria Fata	Attack Statistics Table	
COLUMN T	Derice IP	19030-130-30	Destruction Ports		Part Come Point	Attack Statistics Graph	
	Valuese (PB (s))	0013944	085 0140		THE VERY CASE		
						Attack Description	
16 e 16							
		Footprint					
		LAND packy	et-size=54. AND de	stination-nort	te80. AND destination-ine27.1	1.1.100. AND #1=64.1	
Characteristics	e e e e e e e e e e e e e e e e e e e	[AND packs	st-size=54, AND de	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND ttl=64,]	
Characteristics Info		[AND packs	:t-size=54, AND de	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND ttl=64,]	
Characteristics Info Footprint		[AND packs	st-size=54, AND de	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND ttl=64,]	
Characteristics Info Footprint Attack Statistic	s ts Table	[AND packs	:t-size=54, AND de	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND tt=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic	s Table cs Graph	[AND packs	it-size=54, AND de	stination-port	t=80, AND deștination-ip=27.1	1.1.100, AND ₩=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Attack Descrip	s Table cs Graph tion	[AND packs	it-size=54, AND de	stination-port	t=80, AND deștination-ip=27.1	1.1.100, AND ₩=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Attack Descrip	s Sable Sable Sable Sable Sable Sable Sable Sable Sable Sable Sable Sable Sable	[AND packs	it-size⇔S4, AND de	stination-port	t=80, AND destination-ip=27.	1.1.100, AND tt=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Attack Descrip	s Table cs Graph tion	[AND packs	it-size=S4, AND de	stination-port	t=80, AND destination-ip=27.	1.1.100, AND tt=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Attack Descrip Current Attack Take are flood For Re-	s s Table ss Graph tion #ttech betady " #t. colegares, behavioral	[AND packs	177.1.1.100.00	stination-port	t=80, AND destination-ip=27.	1.1.100, AND tt=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Attack Descrip Connect Attack Tains on these filter STP-STP attack Statistic	s s Table ss Graph tion Much brinks " Micels Hanstore	[AND packs	127.1.3.100.00	stination-port	t=80, AND destination-ip=27.	1.1.100, AND tt=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Attack Statistic Attack Descrip curred Attack Testin arithmed Event	s ss Table ss Graph tion #Keck Detady * #K.ck Detadyses	[AND packet	127.5.100.00	stination-port	t=80, AND destination-ip=27.	1.1.100, AND tt=64,]	
Characteristics Info Footprint Attack Statistic Attack Statistic Count Assas Tale artificial Attack Descrip Count Assas Tale artificial Attack Descrip artificial Attack Descrip Attack Descrip Attack Descrip Attack Descrip artificial Attack Descrip Attack Desc	s cs Table cs Graph tion 81. Colegares Reheaters 20.000	[AND packet	177.13.100400	stination-port	t=80, AND destination-ip=27.	L.1.100, AND tt=64,]	
Characteristics Info Pootprint Attack Statistic Attack Statistic Attack Descrip Correct Attack Tale exhibits a different tite at a different tite	s cs Table cs Graph tion attack betaty " attack betaty " attack transmiss attack transmiss attack	[AND packer	1.27.1.3.100400	stination-port	t=80, AND destination-ip=27.1	2.1.3.00, AND ttl=64,] 	
Characteristics Info Pootprint Attack Statistic Attack Statistic Attack Descrip Council Attack Descrip Council Attack Descrip Council Attack Descrip artisticiona attack Internet attack Inter	s Table cs Graph tion #Resk Details * #R Cologony, Behavioral	[AND packe	127.4.1.199499	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND tt=64,]	
Characteristics Info Pootprint Attack Statistic Attack Statistic Attack Descrip Curver Attack Descrip Curver Attack Descrip attack Descrip at	s s Table ss Graph tion #Kodspers, Schenierd #K. Crispers, Schenierd #K. Crispers, Schenierd #K. Crispers, Schenierd #K. Crispers, Schenierd	[AND packet	127.1.1 100-00	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND tt=64,] 	
Characteristics Info Pootprint Attack Statistic Attack Statistic Attack Descrip Covered Attack Taire each Ineed Hys Harr St ar all heralderins Attack Descrip and Hys Harr St ar all heralderins Attack Descrip	s Table ss Graph tion #Kask breaks " #K.celegares Scherology #K.celegares Scherology #K.celegares Scherology	[AND packed bot SEC. Nullquie 691	1274.3.10040	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND tt=64,] 	
Characteristics Info Pootprint Attack Statistic Attack Statistic Attack Descrip Cover Attack Descrip Cover Attack Descrip Cover Attack Descrip and Head Descrip Statistics Attack Description Statistics Attack Statistics Attack Description Statistics Stat	s cs Table cs Graph tion #teck Details	[AND packet	127.1.1.100400	stination-port	t=80, AND destination-ip=27.1	2.1.100, AND tti=64,] 	
Characteristics Info Pootprint Attack Statistic Attack Statistic Attack Descrip Current Attack Descrip Current Attack Descrip Current Attack Descrip Attack Description Attack Description Attack Description	s s Table s Graph tion Attack braneral Attack Statemers attack Statemers atta	[AND packs	127.1.1.18040	stination-port	t=80, AND destination-ip=27.1	1.1.100, AND tt=64,]	

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

- [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。

DefensePro vDP-Team31	Update Policie: Network P	s Operations	/iew Network Protection Poli	с у ×	Diff
Status: up Locked By: Type: Virtual (VMware) Mgmt IP: 198.18.133.30 Version: 8.13.00 ►More	Policy Name:	vDP-Policy			
Configuration Monitoring Security Monitori	Classification	Priority:	10		
Setup	Profiles and Action	n SRC Netw	ork: any	- / +	
Classes	Packet Reporting				
Network Protection	1	DST Netw	ork: Protected	• / +	
 Network Protection Policies BDoS Profiles 		Port Grou	p:	• / +	
Connection Limit Profiles		Direction:	One Way	•	
DNS Protection Profiles Out of State Protection Profiles Signature Protection SVN Protection SVN Protection	Submit Car	ncel : The filter on the alert t	able can be set in its maximized	view.	
STN Protection Profiles	Ack Severity Ti true Info 0	me and Date Dev 19.10.2017 22:41: AL	vice Name Device IP Mod -AppWall 198.18.133 De	vice General Alteon	User Name Message APSolute Vision M 00926: AL

4. 攻撃用マシンの端末で Jstart.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。

version: 8.13.00 ►More		Current Attacks										
Configuration Monitoring Security M		Start Time 🍸	Attack Category	Status	Risk	Attack Name	Source Address	Destination Add	r Policy	Radware ID	Direction	Action Type
	ecurity Monitori				-	 Search 	Search	Search	Search	Search		-
Dashboard View		13.10.2017 11:20:48	Behavioral DoS	Ongoing	0	network flood IPv4 UDP	Multiple	27.1.1.100	vDP-Policy	70	\rightarrow	Drop

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

- 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。

- 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。



 $\ensuremath{\mathbb{C}}$ 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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

- [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。
- [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 FFFFFFFFFFFFFFFFFFFFFF0023-000058F7DC9D

6. system inf-stats を確認します。

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

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

- 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。
- 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。

100	8135	0	8135	0	Θ	114k 0:: 116k
%	Total	%	Received	%	Xferd	Average Speed Time Time Time Current
						Dload Upload Total Spent Left Speed
100	8134	Θ	8134	0	Θ	133k 0::: 134k
90	Total	96	Received	90	Xferd	Average Speed Time Time Time Current
						Dload Upload Total Spent Left Speed
100	8130	Θ	8130	0	Θ	119k 0:: 120k
%	Total	96	Received	do,o	Xferd	Average Speed Time Time Time Current
						Dload Upload Total Spent Left Speed
100	144	100	144	0	Θ	14814 0:::: 48000
%	Total	ŝ	Received	00	Xferd	Average Speed Time Time Time Current
						Dload Upload Total Spent Left Speed
100	144	100	144	Θ	0	28788 0:::: 36000/
90	Total	8	Received	80	Xferd	Average Speed Time Time Time Current
						Dload Upload Total Spent Left Speed

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。
- [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。

DefensePro vDP-Team31	Update Policies C DNS Protection Prof	operations les Edit DAS Profile*				
atusi Up icked Byi Cisco pei Virtual (VMvare) gmt IPi 198-18-133-30	Profile Name: Lab-DNS					
sioni 0.10.00	Query Protections an	Vanual Triggers				
Guration Monitoring Security Monitori	Rate Settings	Activation Threshold:	400	QPS Activation Period:	3	• Sec.
Hup	Manual Triggers		124		12	
asses	Subdomains Whitelist	Termination Threshold;	100	QPS Termination Period:	3	· Sec.
twork Protection	Packet Reporting Set Max QPS:	Max QPS:	500	QPS Escalation Period:	3	• Sec.
BDoS Profiles	Action					
ONS Protection Profiles Out of State Protection Profiles Signature Protection SYN Protection Profiles						

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	0	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	<u>R.U.D.Y</u>	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	<u>Slowloris</u>	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。 <u>https://security.radware.com/ddos-knowledge-center/ddospedia/thc-ssl-dos/</u>
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。

 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。

©2017 Cisco Systems, Inc. All rights reserved. Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。 「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は 2017 年 12 月現在のものです。 この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

お問い合せ先

〒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