You make possible
DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Olga Yakovenko, Customer Success Specialist

BRKSEC-2663
Agenda

- Introduction
- What do we Know About DoS/DDoS?
- Types of DoS/DDoS Attacks
- How to Identify a DoS/DDoS Attack in your Network?
- DoS/DDoS Mitigation with Radware vDP
- Radware vDP Next Generation DNS Protection
- Radware vDP Installation on Firepower Appliances
- Detailed Packet Flow with Radware vDP
- Conclusion
Questions?
Use Cisco Webex Teams to chat with the speaker after the session

How
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space
The Key Point to Remember

Firepower Appliances integrated with Radware vDP provide protection before, during and after DoS/DDoS attacks
Your Speaker For Today

Olga Yakovenko

olhayako@cisco.com

Customer Success Specialist
What do we Know About DoS/DDoS?
What do we Know About DoS/DDoS?

Denial-of-Service (DoS) attack
• A cyber-attack to make a website, a service or a complete infrastructure unavailable

Distributed Denial-of-Service (DDoS) attack
• More popular type of an attack
• The attack originates from multiple computers simultaneously
What do we Know About DoS/DDoS?

- The first DoS attack
  - 31 users were affected

1974

1999

- The first large-scale DDoS attack
- University's network outage for 2 days

Various businesses, financial institutions and government agencies were brought down

2000

2018

- 1.7 Tbps DDoS attack
- The target was US-based ISP
- No outage due to adequate measures
What do we Know About DoS/DDoS?

Scale of DDoS attacks

- March 2013: Spamhaus - 300 Gbps
- March 2018: GitHub - 1.35 Tbps, US-based ISP - 1.7 Tbps
- October 2016: Dyn - 1.2 Tbps
DDoS Attacks 2019

February  March/April  September
DDoS is Easy... and Cheap!

Our Pricing

<table>
<thead>
<tr>
<th></th>
<th>1 Month Basic</th>
<th>Bronze Lifetime</th>
<th>Gold Lifetime</th>
<th>Green Lifetime</th>
<th>Business Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Concurrent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>300 seconds boot time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>125Gbps total network capacity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resolvers &amp; Tools</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
</tr>
<tr>
<td>24/7 Dedicated Support</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
<td>Order Now</td>
</tr>
</tbody>
</table>

Price:
- 5.00€/month

Coffee & Espresso

- Piccolo Latte 4oz: 3.80€
- Latte, Cappuccino, Flat White: 3.80€ 4.40€ 4.90€ 5.40€
- Café Mocha: 4.60€ 5.60€ 6.20€
- White Chocolate Mocha: 4.60€ 5.60€ 6.20€
- Caramel Macchiato: 4.90€ 5.50€ 6.10€ 6.70€
- Long Black / Americano: 3.20€ 3.80€ 4.40€ 5.00€
- Short Black / Espresso: 3.20€ 3.80€ 4.40€ 5.00€
- Brewed Coffee: 2.80€ 3.10€ 3.40€ 3.70€

Make it your way. Soy is free in any beverage.
Top Daily DDoS Attacks Worldwide

Source: https://www.digitalattackmap.com/
Types of DoS/DDoS Attacks
## Types of DoS/DDoS Attacks

<table>
<thead>
<tr>
<th></th>
<th>Volumetric Attack</th>
<th>Protocol/Network Attack</th>
<th>Application Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is it?</strong></td>
<td>Uses massive amount of traffic saturating the bandwidth of the target</td>
<td>Exploits a weakness in the Layer 3 and Layer 4 protocol stack</td>
<td>Exploits a weakness in the Layer 7 protocol stack</td>
</tr>
<tr>
<td><strong>Effect on target</strong></td>
<td>Can completely block access to the target</td>
<td>Consumes the processing capacity of the target</td>
<td>Exhausts the server resources</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>ICMP Flood, NTP/DNS Amplification</td>
<td>SYN Flood, Ping of Death, Smurf Attack</td>
<td>HTTP/SMTP/SIP Flood</td>
</tr>
</tbody>
</table>
DNS Amplification Reflective Attack

Spoofed Source IP

Third-Party DNS Servers

Target DNS Servers

DNS query to get all records of example.com

Subdomain1.example.com IP
Subdomain2.example.com IP
Subdomain3.example.com IP
...
SubdomainX.example.com IP
Random Subdomains Attack

Random sub-domains

Recursive DNS

Authoritative DNS

rw56gj.paypal.com
gjk78j.paypal.com
kl9pvb.paypal.com
9486hjgj.paypal.com
h7n6mi.paypal.com

www.paypal.com
history.paypal.com
checkout.paypal.com
IoT is the Birthplace of Modern Day Bots

Mirai

Hajime

BrickerBot

Satori

Jen-X
IoT Mean Time Between Compromises

< 2 minutes

Aug 24th, 2017 - SANS Technology Institute: 2 minutes
Nov 30th, 2016 - Rob Graham @ErrataRob: 98 seconds
DDoS Attacks: Shift Towards Application Layer

- Application attacks become the preferred DDoS vector
- Network attacks declined significantly
- HTTP/S and TCP-SYN Floods are causing the most damage
DoS/DDoS Attacks Breaking all Layers of the DC

- Internet Pipe saturation attacks grew 50% since 2016
- Servers are the most common targets as they keep the profitable data
- 40% growth in complete outages over mere service degradation
# DoS/DDoS Mitigation

<table>
<thead>
<tr>
<th>Solution</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS on upstream device</td>
<td>Easy to implement</td>
<td>Good chance of dropping legitimate traffic</td>
</tr>
<tr>
<td>ISP engagement</td>
<td>Attack is mitigated before reaching organization’s resources</td>
<td>• Need to rely on ISP’s knowledge and maturity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Might produce high proportion of false positives</td>
</tr>
<tr>
<td>Firewall/IPS tuning</td>
<td>Effective for certain types of identified threats</td>
<td>Works with manual rules/signatures</td>
</tr>
<tr>
<td>DoS/DDoS dedicated device</td>
<td>• Quick analysis of the threat</td>
<td>Knowledge of a 3rd party product is needed</td>
</tr>
<tr>
<td></td>
<td>• Mitigate the attack without blocking legitimate user traffic</td>
<td></td>
</tr>
</tbody>
</table>
Firepower Threat Defense Introduction

ASA (L2-L4 functionality) → Firepower Threat Defense → Firepower Device Manager (On-box)

Firepower (L7 functionality) → Firepower Threat Defense → Firepower Management Center (On-premise)

Cisco Defense Orchestrator (Cloud-based)
FTD Software Architecture – The Big Picture

- LINA engine (multiple instances of Data Path) - Focused on L2-L4 functionality
- Snort engine (multiple instances of Snort) - Focused on L7 functionality

1. A packet enters the ingress interface and it is handled by the LINA engine.
2. If the policy dictates so the packet is inspected by the Snort engine.
3. Snort engine returns a verdict (whitelist or blacklist) for the packet.
4. The LINA engine drops or forwards the packet based on Snort’s verdict.
Option 1. Configure scanning threat-detection

Create a FlexConfig Object

Add the object to the FlexConfig Policy
Option 2. Set embryonic connections limitation

Create a FlexConfig Object

Add the object to the FlexConfig Policy

```
policy-map global_policy
class class-default
set connection embryonic-conn-max 50
```
Option 3. Enable rate-based attack prevention

**Enable Rate-Based Attack Prevention**

Specify parameters for SYN Attack Prevention
How to Identify a DoS/DDoS Attack in your Network?
How to Identify a DoS/DDoS Attack in your Network?

Firepower-module1# **show cpu**
CPU utilization for 5 seconds = 85%; 1 minute: 10%; 5 minutes: 6%

Firepower-module1# **show resource usage**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Current</th>
<th>Peak</th>
<th>Limit</th>
<th>Denied</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conns</td>
<td>8777473</td>
<td>8777473</td>
<td>250000000</td>
<td>0</td>
<td>System</td>
</tr>
<tr>
<td>Hosts</td>
<td>8658916</td>
<td>8658916</td>
<td>N/A</td>
<td>0</td>
<td>System</td>
</tr>
<tr>
<td>Conns [rate]</td>
<td>161131</td>
<td>273758</td>
<td>N/A</td>
<td>0</td>
<td>System</td>
</tr>
<tr>
<td>Inspects [rate]</td>
<td>161121</td>
<td>273751</td>
<td>N/A</td>
<td>0</td>
<td>System</td>
</tr>
<tr>
<td>Routes</td>
<td>10</td>
<td>10</td>
<td>unlimited</td>
<td>0</td>
<td>System</td>
</tr>
</tbody>
</table>

Firepower-module1# **show interface detail | include buffer| overrun**

9906871 packets input, 1816217751 bytes, 3295965 no buffer
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

Verify CPU utilization
Verify anomalies in resource usage
Verify the interface statistics
How to Identify a DoS/DDoS Attack in your Network?

Firepower-module1# show capture CAP

...  
84: 15:09:00.009032 192.168.1.55.32206 > 192.168.2.160.443: . ack 1771584612 win 29512
85: 15:09:00.009032 192.168.3.77.56027 > 192.168.2.160.443: . ack 1771584612 win 29512
86: 15:09:00.009032 192.168.5.18.17123 > 192.168.2.160.443: . ack 1771584612 win 29512
87: 15:09:00.009047 192.168.7.29.23741 > 192.168.2.160.443: . ack 1771584612 win 29512
88: 15:09:00.009047 192.168.4.66.35308 > 192.168.2.160.443: . ack 1771584612 win 29512
89: 15:09:00.009047 192.168.6.34.64247 > 192.168.2.160.443: . ack 1771584612 win 29512

Firepower-module1# show traffic outside:

received (in 94616.910 secs):
23728100885 packets 18588082482086 bytes
250009 pkts/sec 196456014 bytes/sec
transmitted (in 94616.910 secs):
16407809834 packets 6395127130755 bytes
173004 pkts/sec 67589003 bytes/sec

Verify traffic anomalies: 
Packet capture

Verify traffic anomalies: 
Traffic statistics
User Story #1

Firepower-module1# clear asp drop

Firepower-module1# show asp drop
Frame drop:
First TCP packet not SYN (tcp-not-syn) 8055649

Firepower-module1# show cpu
CPU utilization for 5 seconds = 100%; 1 minute: 100%; 5 minutes: 92%

Firepower-module1# show capture capi
... 
84: 15:09:00.009032 192.168.1.55.32206 > 192.168.2.160.80: . ack 1771584612
85: 15:09:00.009032 192.168.3.77.56027 > 192.168.2.160.80: . ack 1771584612
86: 15:09:00.009032 192.168.5.18.17123 > 192.168.2.160.80: . ack 1771584612
87: 15:09:00.009047 192.168.7.29.23741 > 192.168.2.160.80: . ack 1771584612

Verify the symptoms
Identify the attack
How to Identify a DoS/DDoS Attack in your Network?

Displaying hardware-switched flow entries in the PFC (Active) Module 5:

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP</th>
<th>DstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>VI204</td>
<td>192.168.1.55</td>
<td>VI204</td>
<td>192.168.2.160</td>
<td>06</td>
<td>E95B</td>
<td>0016</td>
<td>26</td>
</tr>
<tr>
<td>VI204</td>
<td>192.168.1.55</td>
<td>VI204</td>
<td>192.168.2.160</td>
<td>06</td>
<td>E96C</td>
<td>0016</td>
<td>23</td>
</tr>
<tr>
<td>VI204</td>
<td>192.168.1.55</td>
<td>VI204</td>
<td>192.168.2.160</td>
<td>06</td>
<td>E9DC</td>
<td>0016</td>
<td>30</td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VI204</td>
<td>192.168.7.17</td>
<td>VI204</td>
<td>192.168.2.160</td>
<td>06</td>
<td>083A</td>
<td>0016</td>
<td>17</td>
</tr>
<tr>
<td>VI204</td>
<td>192.168.5.35</td>
<td>VI204</td>
<td>192.168.2.160</td>
<td>06</td>
<td>0839</td>
<td>0016</td>
<td>13</td>
</tr>
<tr>
<td>VI204</td>
<td>192.168.3.88</td>
<td>VI204</td>
<td>192.168.2.160</td>
<td>06</td>
<td>0861</td>
<td>0016</td>
<td>19</td>
</tr>
</tbody>
</table>

Verify traffic anomalies:
- Netflow
- DoS Attack
- DDoS Attack

Verify the interface statistics:
- GigabitEthernet2/1 is up, line protocol is up (connected)
  - 5 minute input rate 187248000 bits/sec, 128626 packets/sec
User Story #2

Firepower-module1# show cpu
CPU utilization for 5 seconds = 95%; 1 minute: 94%; 5 minutes: 94%

Firepower-module1# show conn
TCP Inside 192.168.2.1:443 Outside 192.168.1.155:55231, bytes 0, flags aA N1
TCP Inside 192.168.2.3:443 Outside 192.168.1.155:55232, bytes 0, flags aA N1
TCP Inside 192.168.2.2:443 Outside 192.168.1.155:55231, bytes 0, flags aA N1

Firepower-module1# show capture capi
...31: 17:12:50.917 192.168.1.155.40060 > 192.168.2.3.20: S 1196265996:1196265996(0)
32: 17:12:50.917 192.168.1.155.55878 > 192.168.2.3.21: S 2947038085:2947038085(0)
33: 17:12:50.917 192.168.1.155.42864 > 192.168.2.3.22: S 3617959142:3617959142(0)
34: 17:12:50.917 192.168.1.155.49402 > 192.168.2.3.23: S 4217242163:4217242163(0)
DoS/DDoS Mitigation with Radware vDP
DoS/DDoS Mitigation with Radware vDP

Radware DefensePro virtual (vDP) platform:

• Is a real-time attack prevention device
• Is the first 3rd Party component of the new architecture
• Is a KVM-based platform
• Provides DoS/DDoS detection and mitigation capabilities
• Can be installed on Cisco ACI (APIC), Firepower NGFW, UCS
DoS/DDoS Mitigation with Radware vDP

Rate-Based Detection
High false positives

Behavioral Detection
Low false positives
DoS/DDoS Mitigation with Radware vDP

Learning → Detection → Characterization → Mitigation

Good Traffic

Rate Analysis

Attack Traffic (RST Flood)

Rate Analysis

TCP Flag Distribution Analysis

Normal Traffic Distribution

TCP Flag Distribution Analysis

Attack Traffic
DoS/DDoS Mitigation with Radware vDP

Always-On Protection

Fast Detection and Mitigation

Adaptive behavioral DoS against IPv4/IPv6 TCP/UDP/ICMP/IGMP/DNS floods

Application signature protection

Anomaly protection against basic malformed packets

Bot detection with smart challenge
Safe-Reset Authentication with Radware vDP

Client → vDP → Protected Server

1. SYN
2. ACK (cookie, invalid ACK)
3. RST (invalid ACK)
4. SYN Retransmit
5. SYN-ACK / ACK / Data
6. SYN (forwarded)
Safe-Reset Authentication with Radware vDP

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Identification</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-01-14</td>
<td>09:40:45.036530</td>
<td>94.52.141.96</td>
<td>SSH</td>
<td>174</td>
<td>0xeb9f (60319)</td>
<td>Client: Encrypted packet (len=120)</td>
</tr>
<tr>
<td>2019-01-14</td>
<td>09:40:45.036872</td>
<td>192.168.2.160</td>
<td>TCP</td>
<td>60</td>
<td>0xeb9f (60319)</td>
<td>22 → 23007 [ACK] Seq=2080338225 Ack=2080338225</td>
</tr>
</tbody>
</table>

Frame 29385: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Cisco_Be:02:cc (2c:33:11:8e:02:cc), Dst: Vmware05:28:72 (00:50:56:05:28:72)
  Source Port: 22
  Destination Port: 23007
  [Stream index: 22750]
  [TCP Segment Len: 0]
  Sequence number: 2080338225 (relative sequence number)
  Acknowledgment number: 2080338225 (relative ack number)
  Header Length: 24 bytes
  Flags: 0x010 (ACK)
  Window size value: 1400
  [Calculated window size: 1400]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0xb308 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  Options: (4 bytes), Maximum segment size

ACK (cookie, invalid ACK)
Radware vDP Next Generation DNS Protection
Random Subdomains Attack – Query Rate Limiting

Random sub-domains

- rw56gj.paypal.com
- www.paypal.com
- gjk78j.paypal.com
- kl9p vb.paypal.com
- 9486hjgj.paypal.com
- history.paypal.com
- h7n6mi.paypal.com
- checkout.paypal.com
- www.paypal.com
- www.paypal.com

Non Radware DDoS Protector

Rate-Limit

Prone to False Positive
Random Subdomains Attack – vDP DNS Protection

Random sub-domains

- rw56gj.paypal.com
- www.paypal.com
- www.paypal.com
- gjk78j.paypal.com
- kl9pvb.paypal.com
- 9486hjgj.paypal.com
- history.paypal.com
- h7n6mi.paypal.com
- checkout.paypal.com
- www.paypal.com
- www.paypal.com

Allow: www.paypal.com, history.paypal.com, checkout.paypal.com

Block: *.paypal.com
Radware vDP DNS Protection

Rate Analysis per DNS Query Type

Query rate (QPS)

- A
- AAAA
- PRT
- MX

Time
Radware vDP DNS Protection

FQDN Analysis per Query Type

- Google.com
- Youtube.com
- Facebook.com
- Wikipedia.org
Radware vDP DNS Protection

DNS Query Distribution Analysis (Rate Invariant)

- A Records: 29%
- PTR Records: 14%
- AAAA Records: 14%
- TEXT Records: 9%
- SPV/NAPTR: 5%
- Other Records: 5%
- MX Records: 24%
Radware vDP DNS Protection

Suspicious Data Packet

- Packet checksums
- DNS Qname - domain name
- Source IP address
- Ports numbers
- Packet Identification number
- Identification number
- DNS query ID - query
- Packet size
- TTL (Time to Live)
- Destination IP address
- DNS Query count (Qcount)
- Fragment offset
- ...

Characterization

Automatic Real Time Signature Generation Module

Real Time Signature
Radware vDP DNS Protection

Behavioral Real-Time Signature Technology

Real-Time Signature Created

Real-Time Signature Challenge

Real-Time Signature Rate Limit

Collective Challenge

Collective Rate Limit

Mitigation
Radware vDP DNS Protection

1. **Real-Time Signature Challenge** – DefensePro challenges DNS queries that match the real-time signature. The purpose of the challenge is to distinguish between legitimate traffic created by legitimate users and DoS-traffic generated by botnets.

2. **Real-Time Signature Rate Limit** – If the attack continues, DefensePro limits the rate of DNS traffic that matches the real-time signature.

3. **Collective Challenge** – If the attack continues, DefensePro challenges all DNS-query traffic, not only from the suspicious sources, but from all users. Again, the purpose of this challenge is to distinguish between legitimate traffic created by legitimate users and DoS-traffic generated by botnets.

4. **Collective Rate Limit** – If the attack continues, the last resort, and the last escalation step, is to impose a rate limit on all DNS traffic according to the specified maximal query rate.
Radware vDP on Firepower NGFW Appliances
Radware vDP on Firepower NGFW Appliances

Cisco Firepower 9300 Appliance

Cisco Firepower 4100 Series Appliance

Cisco Firepower 4100/9300 Appliances have its own:

- Operating system - Firepower eXtensible Operating System (FXOS)
- Management tool - Firepower Chassis Manager (FCM)

* BRKSEC-3035: Firepower Platform Deep Dive
Radware vDP on Firepower NGFW Appliances

- Supported with ASA and FTD on Firepower 4100 and 9300 appliances
- Mitigation capacity/throughput from 14Gbps to 42Gbps
- DDoS flood attack prevention rate from 1,800,000 to 5,400,000 Packets Per Second (PPS)

**Note:** On Firepower 4110 and 4120 you must deploy the decorator at the same time as the logical device
Firepower Threat Defense Performance with vDP

<table>
<thead>
<tr>
<th>Firepower</th>
<th>Throughput FW + AVC + IPS</th>
<th>Throughput FW + AVC + IPS + vDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>9300 – SM 44</td>
<td>53 Gbps</td>
<td>49.4 Gbps (93.2%)</td>
</tr>
<tr>
<td>9300 – SM 36</td>
<td>34 Gbps</td>
<td>31.2 Gbps (91.7%)</td>
</tr>
<tr>
<td>9300 – SM 24</td>
<td>24 Gbps</td>
<td>21 Gbps (87.5%)</td>
</tr>
<tr>
<td>4150</td>
<td>24 Gbps</td>
<td>22.4 Gbps (93.2%)</td>
</tr>
<tr>
<td>4140</td>
<td>20 Gbps</td>
<td>18.3 Gbps (91.7%)</td>
</tr>
<tr>
<td>4120</td>
<td>15 Gbps</td>
<td>13.1 Gbps (87.5%)</td>
</tr>
<tr>
<td>4110</td>
<td>10 Gbps</td>
<td>7.5 Gbps (75.0%)</td>
</tr>
</tbody>
</table>

Performance Criteria
• vDP defaults to 6 cores
• Subtract vDP cores from total cores
• Percentage of remaining cores = \( \frac{48 - 6}{48} \times 100 = 87.5\% \)

Variable Cores
• You may change the default number of cores assigned to vDP
• Min = 2 cores, Max = 10 cores
Radware vDP Capacity & Licensing

Licensing is based on maximum peace time traffic:

- Peace time traffic is a known value, attack size is unknown
- If peak traffic is 2Gb (inbound + outbound), purchase a 2Gb clean traffic license
- 14Gb – 2Gb = 12Gb of DDoS Scrubbing on Box

Reference: DefensePro Throughput-License Calculation
Radware APSolute Vision Manager

Supported platforms:

- Physical Appliance (On-Demand Switch VL/VL2)
- Virtual environment
  - Vmware vSphere ESXi
  - KVM
  - Microsoft Hyper-V
  - OpenStack/CloudBand
Radware vDP Installation on Firepower Appliances
Radware vDP Installation Prerequisites

**FP4120-6-A# show version**
FPRM:
- Running-Vers: 4.3(1.107)
- Package-Vers: 2.3(1.99)
- Activate-Status: Ready

**FP4120-A(fxos)# show run ntp**
- version 5.0(3)N2(4.31)
- logging level ntp 7
- ntp server 144.254.15.78

**FP4120-A# show ntp**
- NTP Overall Time-Sync Status: Time Synchronized

**FP4120-A# show clock detail**
- Sun Nov 11 16:09:07 UTC 2018

- Confirm the FXOS and vDP compatibility
- Configure the NTP server on Firepower Chassis
- Specify Etc/UTC timezone on Firepower Chassis

CSCvp95275
Radware vDP Installation Prerequisites

If the NTP server/timezone settings are not configured:

- Configure the NTP server
- Specify the Time Zone
Radware vDP Installation Using FCM

Step 1. Upload the vDP image (.csp) to FCM.
Radware vDP Installation Using FCM

Step 2. On FCM configure FTD/vDP Management and Data Interfaces (Interfaces tab).
Radware vDP Installation Using FCM

Step 3. On FCM Create an FTD Logical Device (Logical Devices > Add Device).
Radware vDP Installation Using FCM

Step 4. On FCM provision the FTD Management interface.
Radware vDP Installation Using FCM

Step 5. On FCM provision the FTD settings and FMC info.
Radware vDP Installation Using FCM

Step 6. On FCM provision the FTD Data interface(s).
Radware vDP Installation Using FCM

Step 7. On FCM provision the Radware vDP general information (version, resource profile management interface, data port(s) allocated.)
Radware vDP Installation Using FCM

Step 7. Save to start the installation.
Radware vDP Installation Using FCM

Step 8. Login to vDP and change the password to finish the installation.

FPR-4110-4# connect module 1 console
Firepower-module1>connect vdp
Connected to domain vDP
Escape character is ^A
The password of user "radware" must be changed. Please enter the new password: ********
Confirm password: ********
Password change OK.
Init completed successfully.
12-11-2018 13:57:13 INFO Port 2 Down
12-11-2018 13:57:13 INFO Port MNG-1 Down
12-11-2018 13:57:17 INFO Port 1 Up
12-11-2018 13:57:17 INFO Port 2 Up
12-11-2018 13:57:17 INFO Port MNG-1 Up
12-11-2018 13:57:50 INFO Cold Start
Demo 1

Radware vDP Installation Using FCM
In this Demo we will...

• Confirm the prerequisites for the vDP installation
• Perform initial vDP and FTD installation from the FCM
• Verify the FTD and vDP status from the FCM and FXOS CLI
• Register vDP to the APSolute Vision Manager
Radware vDP Capacity & Licensing

DefensePro# `system license throughput get`
License Key : **500Mbps-XXxxXXxx**
MAC Address  : 5897bdb9369e
License ID   : e19-d18-e0c

Default vDP license

DefensePro# `system license throughput set 2Gbps-YYyyYYyy`

Apply a license key

DefensePro# `system license throughput get`
License Key : **2Gbps-YYyyYYyy**
MAC Address  : 5897bdb9369e
License ID   : e19-d18-e0c

Applied vDP license
### Apply throughput license key

- **Throughput License ID**: `e19-d18-e0c`
- **Throughput License Key**: `2Gbps-YYyyYYYY`

### Apply vCPU license key

- **vCPU License ID**: `e19-d18-e0c`
- **vCPU License Key**: `10vCPU-ZzzZZzz`

---

**Cisco Live!**

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public 71
Radware vDP Installation Using Command Line

Step 1. Navigate to **Logical Devices** tab and confirm that the application is installed.
Radware vDP Installation Using Command Line

Step 2. Connect to the Firepower Command Line Interface (CLI) and install the vDP image on the same slot that the application is installed on.

```
FPR4100-1# scope ssa
FPR4100-1 /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version Deploy Type Profile
Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- --------------- ----- 
------ ------------ --------------- ------------
ftd       FTD4140-1 1          Enabled     Online           6.3.0.45        6.3.0.45        Native                   Not
Applicable  None
FPR4100-1 /ssa # scope slot 1
FPR4100-1 /ssa/slot # create app-instance vdp FTD4140-1
FPR4100-1 /ssa/slot/app-instance* # commit-buffer
FPR4100-1 /ssa/slot/app-instance # exit
```
Radware vDP Installation Using Command Line

Step 3. The vDP application starts the installation.

```
FPR4100-1# scope ssa
FPR4100-1 /ssa/slot # show app-instance

Application Instance:
<table>
<thead>
<tr>
<th>App Name</th>
<th>Identifier</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Running Version</th>
<th>Startup Version</th>
<th>Deploy Type</th>
<th>Profile Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd</td>
<td>FTD4140-1</td>
<td>Enabled</td>
<td>Online</td>
<td>6.3.0.45</td>
<td>6.3.0.45</td>
<td>Native</td>
<td></td>
</tr>
<tr>
<td>vdp</td>
<td>FTD4140-1</td>
<td>Disabled</td>
<td>Installing</td>
<td>8.13.01.09-2</td>
<td>Vm</td>
<td>DEFAULT-RESOURCE</td>
<td></td>
</tr>
</tbody>
</table>
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Radware vDP Installation Using Command Line

Step 4. Configure the Management interface settings for the vDP.

FPR4100-1 /ssa # scope logical-device FTD4140-1
FPR4100-1 /ssa/logical-device # create mgmt-bootstrap vdp
FPR4100-1 /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
FPR4100-1 /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.62.148.1
FPR4100-1 /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.62.148.97 mask 255.255.255.128
FPR4100-1 /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
FPR4100-1 /ssa/logical-device/mgmt-bootstrap* # exit
Radware vDP Installation Using Command Line

Step 5. Specify the vDP interface used for management. The interface must be created as a Management type on the FCM.

```
FPR4100-1 /ssa/logical-device* # create external-port-link mgmt_vdp Ethernet1/1 vdp
FPR4100-1 /ssa/logical-device/external-port-link* # exit
```
Step 6. Add the vDP application to the logical device.

```
KSEC-FPR4100-1 /ssa/logical-device* # show external-port-link

External-Port Link:
Name                  Port or Port Channel Name       Port Type          App Name           Description
------------------------------------------------------------------------------------
Ethernet11_ftd        Ethernet1/1                              Mgmt ftd          ftd
PC1_ftd               Port-channel1                          Data              ftd
PC2_ftd               Port-channel2                          Data              ftd

FPR4100-1 /ssa/logical-device* # scope external-port-link PC1_ftd
FPR4100-1 /ssa/logical-device/external-port-link* # set decorator vdp
FPR4100-1 /ssa/logical-device/external-port-link* # exit
FPR4100-1 /ssa/logical-device* # commit-buffer
```

Note: the vDP and the application will reboot.
Radware vDP Installation Using Command Line

Step 7. Connect to the vDP application CLI and finish the installation. You are prompted to change the password for the default radware user.

```
FPR4100-1# connect module 1 console
Firepower-module1> connect vdp
Connected to domain vDP
Escape character is ^A
The password of user "radware" must be changed. Please enter the new password: *********
Confirm password: ********
Password change OK.
Generic Version: 01.00-00.00
Init completed successfully.
DefensePro>12-11-2018 17:39:58 INFO Port 1 Down
12-11-2018 17:39:58 INFO Port 2 Down
12-11-2018 17:39:58 INFO Port MNG-1 Down
12-11-2018 17:40:02 INFO Port 1 Up
12-11-2018 17:40:02 INFO Port 2 Up
12-11-2018 17:40:02 INFO Port MNG-1 Up
12-11-2018 17:40:35 INFO Cold Start
```
### Radware vDP Installation Verification

**FPR4100-1# scope ssa**

**FPR4100-1 /ssa # show app-instance**

<table>
<thead>
<tr>
<th>App Name</th>
<th>Identifier</th>
<th>Slot ID</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Running Version</th>
<th>Startup Version</th>
<th>Deploy Type</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd</td>
<td>FTD4140-1</td>
<td>1</td>
<td>Enabled</td>
<td>Online</td>
<td>6.3.0.45</td>
<td>6.3.0.45</td>
<td>Native</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>vdp</td>
<td>FTD4140-1</td>
<td>1</td>
<td>Enabled</td>
<td>Online</td>
<td>8.13.01.09-2</td>
<td>8.13.01.09-2</td>
<td>Vm</td>
<td>DEFAULT-RESOURCE</td>
</tr>
</tbody>
</table>

**FPR4100-1# connect module 1 console**

Firepower-module1> show services status all

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Identifier</th>
<th>Oper State</th>
<th>Up Since</th>
<th>Instance ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd (native)</td>
<td>FTD4140-1</td>
<td>RUNNING</td>
<td>02:59:51</td>
<td>ftd_001_JMX2215L02BPXFTYE20</td>
</tr>
<tr>
<td>vdp (vm)</td>
<td>FTD4140-1</td>
<td>RUNNING</td>
<td>03:02:15</td>
<td>vdp_001_JMX2215L02BEK2YYC26</td>
</tr>
</tbody>
</table>
Register vDP to APSolute Vision Manager

Step 1. Enable vDP web interface on vDP application.

DefensePro#manage secure-web status set enable
Updated successfully
Web Server SSL Status: enable

DefensePro#manage web-services status set enable
Updated successfully
Web Services Status: enable
Register vDP to APSolute Vision Manager

Step 2. Log in to Radware APSolute Vision Manager and add the device.
Register vDP to APSolute Vision Manager

Step 3. In Device Properties select Type DefensePro, specify the name and configure the SNMP settings.
Register vDP to APSolute Vision Manager

Step 4. Navigate to the HTTP/S Access tab and specify the User Name and the Password.
Register vDP to APSolute Vision Manager

Step 5 (Optional). Navigate to the SSH access tab and specify the User Name and the Password.
Register vDP to APSolute Vision Manager

Step 6. Specify whether the APSolute Vision server configures itself as a target of the device events.
Detailed Packet Flow with Radware vDP
Detailed Packet Flow with Radware vDP

1. MIO (Management Input/Output) receives the packet on the physical port
2. MIO sends the packet to the Decorator (vDP Radware)
3. MIO receives the packet from the Decorator (vDP Radware)
4. MIO sends the packet to the Security Module (FTD/ASA)
5. FTD/ASA sends the packet back to the MIO
6. MIO sends the packet to the egress physical port
Detailed Packet Flow with Radware vDP

1. MIO – Capture Point 1 – The packet does not have any VN-Tag
2. MIO – Capture Point 2 – The packet has a VN-Tag
3. vDP – Capture Point 3 – Decorator level capture
4. MIO – Capture Point 3 – The MIO Backplane receives the packet
5. MIO – Capture Point 4 – The MIO processes the packet
6. FTD/ASA – Capture Point 5 – Application level capture(s)
7. MIO – Capture Point 6 – The MIO Backplane receives the packet
8. MIO – Capture Point 7 – The MIO processes the packet
Detailed Packet Flow with Radware vDP

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2019-01-11 13:57:29...</td>
<td>192.168.1.155</td>
<td>192.168.2.155</td>
<td>ICMP</td>
<td>106</td>
<td>Echo (ping) request id=0x467c, seq=1/256, ttl=64</td>
</tr>
<tr>
<td>2</td>
<td>2019-01-11 13:57:29...</td>
<td>192.168.1.155</td>
<td>192.168.2.155</td>
<td>ICMP</td>
<td>112</td>
<td>Echo (ping) request id=0x467c, seq=1/256, ttl=64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2019-01-11 13:57:29...</td>
<td>192.168.1.155</td>
<td>192.168.2.155</td>
<td>ICMP</td>
<td>112</td>
<td>Echo (ping) request id=0x467c, seq=1/256, ttl=64</td>
</tr>
<tr>
<td>2</td>
<td>2019-01-11 13:57:29...</td>
<td>192.168.1.155</td>
<td>192.168.2.155</td>
<td>ICMP</td>
<td>112</td>
<td>Echo (ping) request id=0x467c, seq=1/256, ttl=64</td>
</tr>
<tr>
<td>3</td>
<td>2019-01-11 13:57:29...</td>
<td>192.168.1.155</td>
<td>192.168.2.155</td>
<td>ICMP</td>
<td>112</td>
<td>Echo (ping) request id=0x467c, seq=1/256, ttl=64</td>
</tr>
<tr>
<td>4</td>
<td>2019-01-11 13:57:29...</td>
<td>192.168.1.155</td>
<td>192.168.2.155</td>
<td>ICMP</td>
<td>112</td>
<td>Echo (ping) request id=0x467c, seq=1/256, ttl=64</td>
</tr>
</tbody>
</table>
Hybrid Inline & Cloud DDoS Mitigation Use Case

ERT and the customer decide to divert the traffic

Protected Organization

Radware Cloud DDoS Protection Service

Large volumetric DDoS attack that saturates the pipe

Sharing essential information for attack mitigation

Firepower 9300 / 4100 with vDP

Protected Online Services

Internet

Defense Pros

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Hybrid Inline & Cloud DDoS Mitigation Use Case

ERT and the customer decide to divert the traffic

Radware Cloud DDoS Protection Service

Neutral traffic

Protected Organization

Sharing essential information for attack mitigation

Protected Online Services

Firepower 9300 / 4100 with vDP

Defense Pros

Clean traffic
Demo 2

Protection Against DDoS with Radware vDP
In this Demo we will...

- Configure the vDP BDoS Profile and Network Protection Policy
- Initiate the DDoS TCP RST Flood attack
- Verify the DDoS attack mitigation results
Conclusion
Conclusion

- DDoS attacks keep evolving and growing every year
- Radware vDP is a virtual platform that provides DoS/DDoS detection and mitigation capabilities
- Radware vDP can be installed on Firepower 9300/4100 on top of ASA or FTD applications
- When the interface is decorated with the vDP, ingress traffic from the network first passes through the vDP before reaching the FTD/ASA application
Firepower Diagonal Learning Map

Monday
TECSEC-2600 – for beginners
Next Generation Firewall Platforms and Integrations
TECSEC-3004 – for existing customers
Troubleshooting Firepower Threat Defense like a TAC Engineer

Tuesday
BRKSEC-3328
Making Firepower Management Center (FMC) Do More

BRKSEC 2020
Deploying FP Tips and Tricks

BRKSEC 3036
Decrypting the Internet with Firepower!

Wednesday
BRKSEC-3093
ARM yourself using NGFWv in AZUR

BRKSEC 2494
Maximizing Threat Efficacy & Perf

Thursday
BRKSEC 3035
Firepower Platforms Deep Dive

BRKSEC-2056
Threat Centric Network Security

BRKSEC-3629
Designing IPSec VPNs with Firepower Threat Defense integration for Scale and High Availability

BRKSEC-3030
Advanced IPS Deployment with Firepower NGFW

Friday
BRKSEC-2140
2 birds with 1 stone: DUO integration with Cisco ISE and Firewall solutions

BRKSEC-3032
Firepower NGFW Clustering Deep Dive

BRKSEC-2034
Cloud Management of Firepower and ASA with Cisco Defense Orchestrator

Security Track Overview
The Key Point to Remember

Firepower Appliances integrated with Radware vDP provide protection before, during and after DoS/DDoS attacks
Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.

- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.
Continue your education

Demos in the Cisco Showcase

Meet the Engineer 1:1 meetings

Walk-In Labs

Related sessions
Thank you
You make possible