CISCO

You make **possible**

DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Olga Yakovenko, Customer Success Specialist

BRKSEC-2663

Barcelona | January 27-31, 2020

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

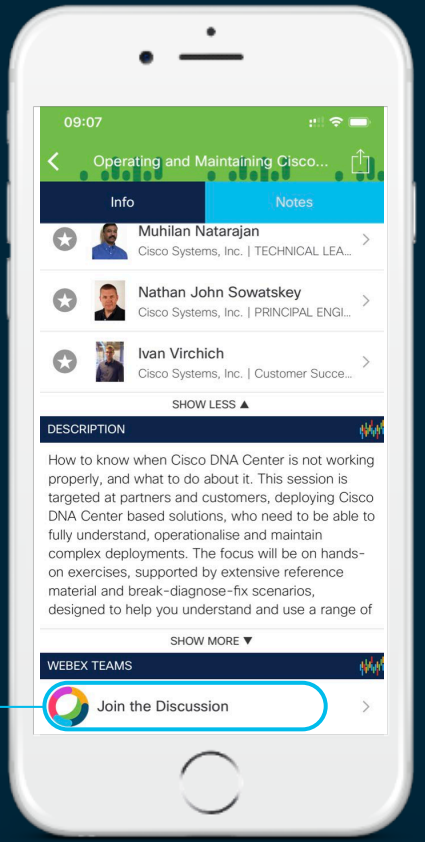
Cisco Webex Teams

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

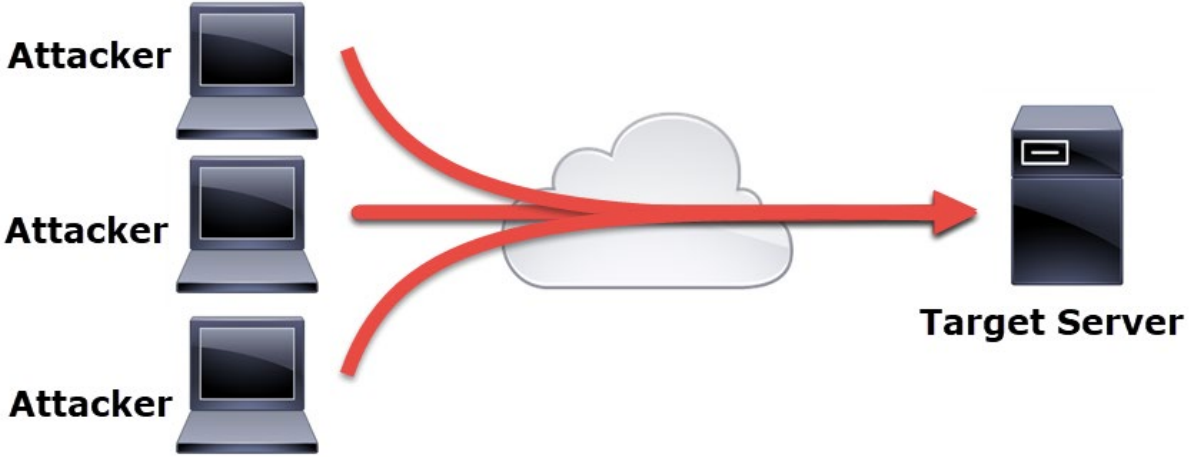
olhayako@cisco.com

Customer Success Specialist

CISCO CERTIFIED CCIE SECURITY

What do we Know About DoS/DDoS?

What do we Know About DoS/DDoS?



What do we Know About DoS/DDoS?

1974

- The first DoS attack
- 31 users were affected

1999

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

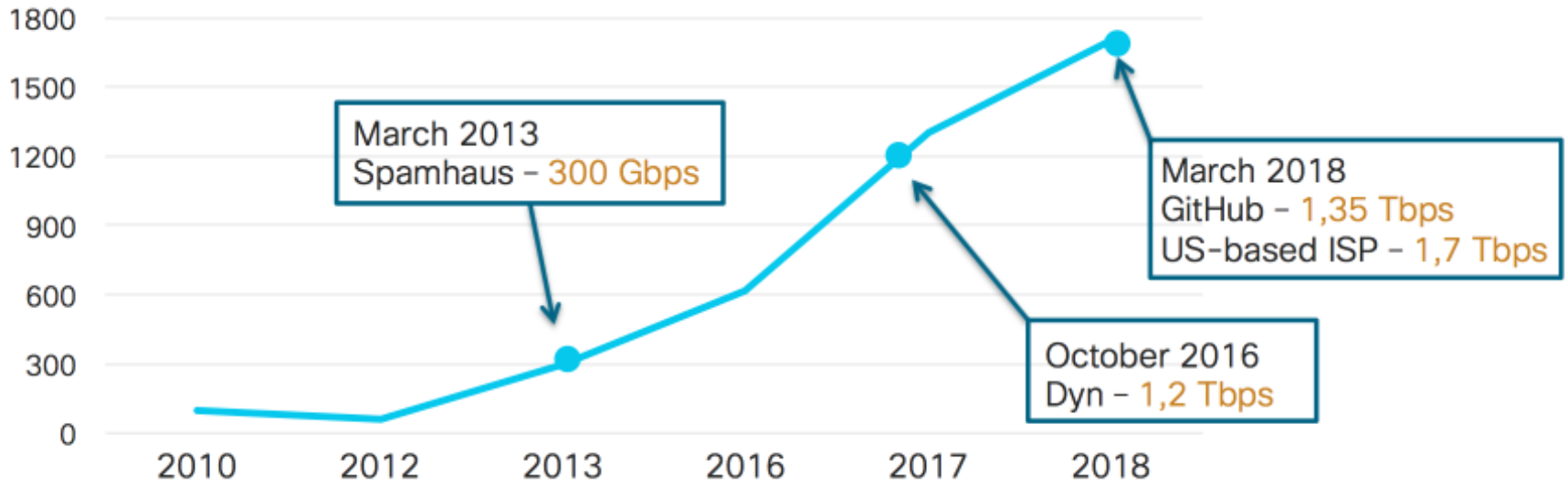
2000

Various businesses, financial institutions and government agencies were brought down

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

DDoS Attacks 2019

February | March/April | September

DDoS is Easy… and Cheap!

Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

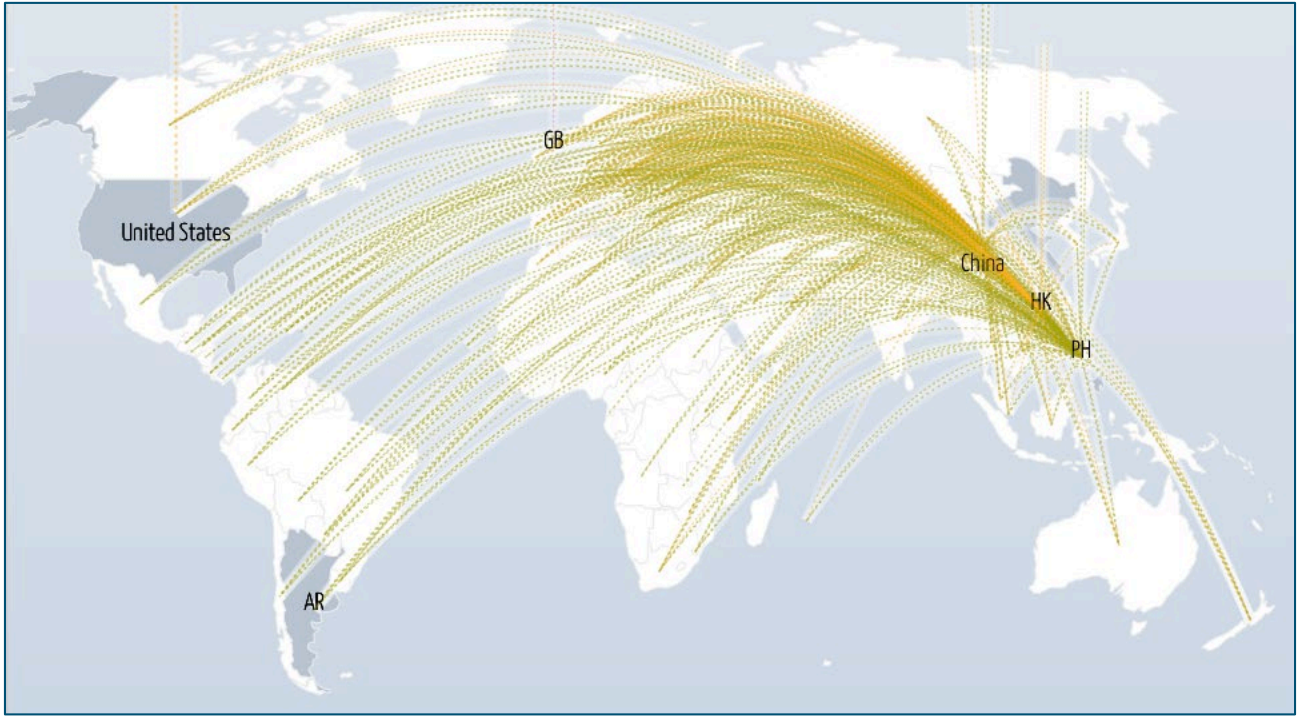
Coffee & Espresso

We're proud to use only 100% Fairtrade Espresso.

Enjoy hot or iced	short 237 ml	tall 354 ml	grande 473 ml	venti 591 ml
Piccolo Latte 4oz	3.80			
Latte, Cappuccino, Flat White	3.80	4.40	4.90	5.40
Café Mocha White Chocolate Mocha	[illegible]	5.00	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 solo		3.80 doppio	
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



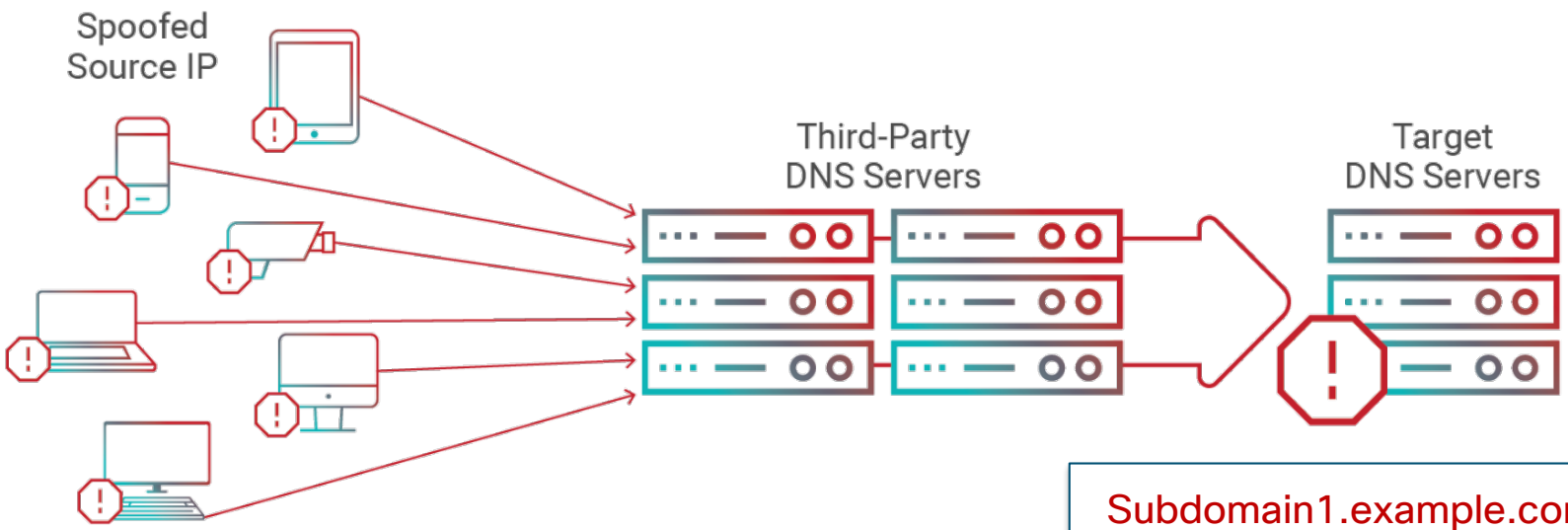
Source: https://www.digitalattackmap.com/

Types of DoS/DDoS Attacks

Types of DoS/DDoS Attacks

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

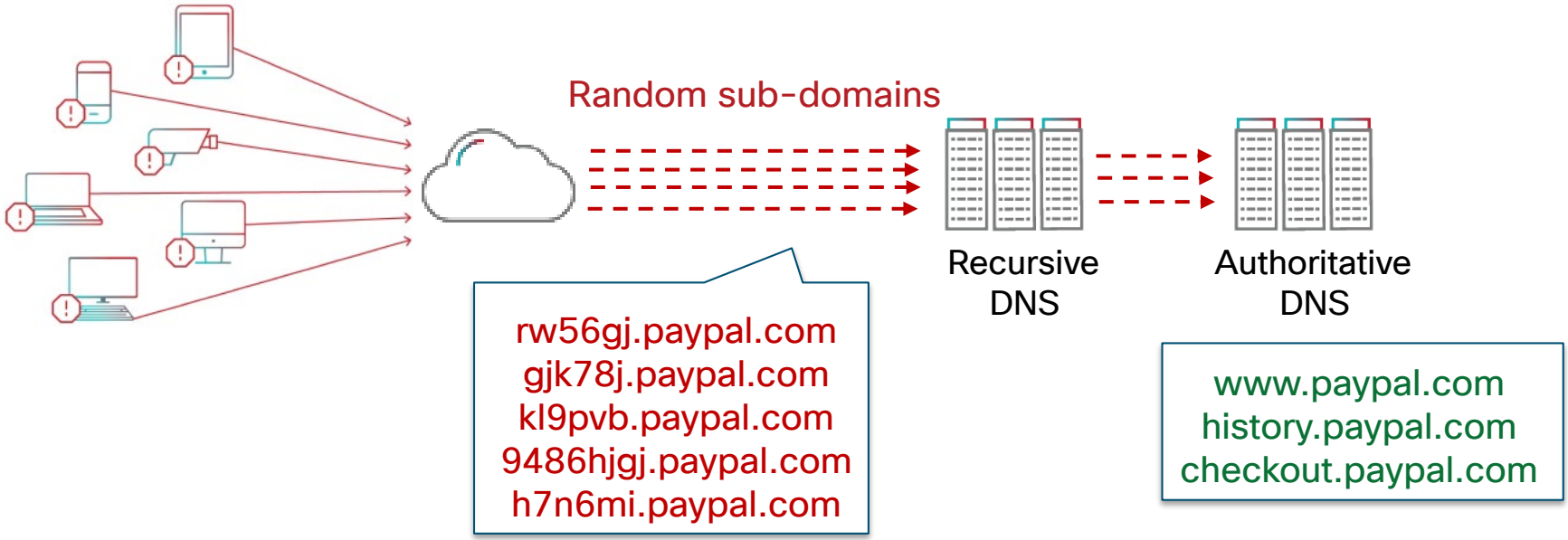
DNS Amplification Reflective Attack



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

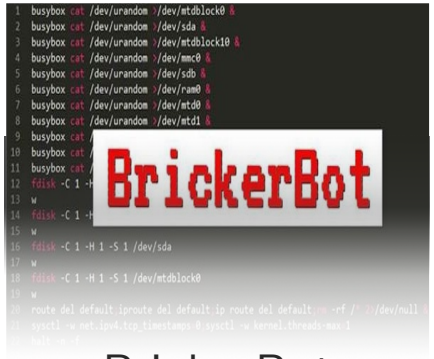
Random Subdomains Attack



IoT is the Birthplace of Modern Day Bots

Mirai

Hajime



BrickerBot

Satori

Jen-X

IoT Mean Time Between Compromises

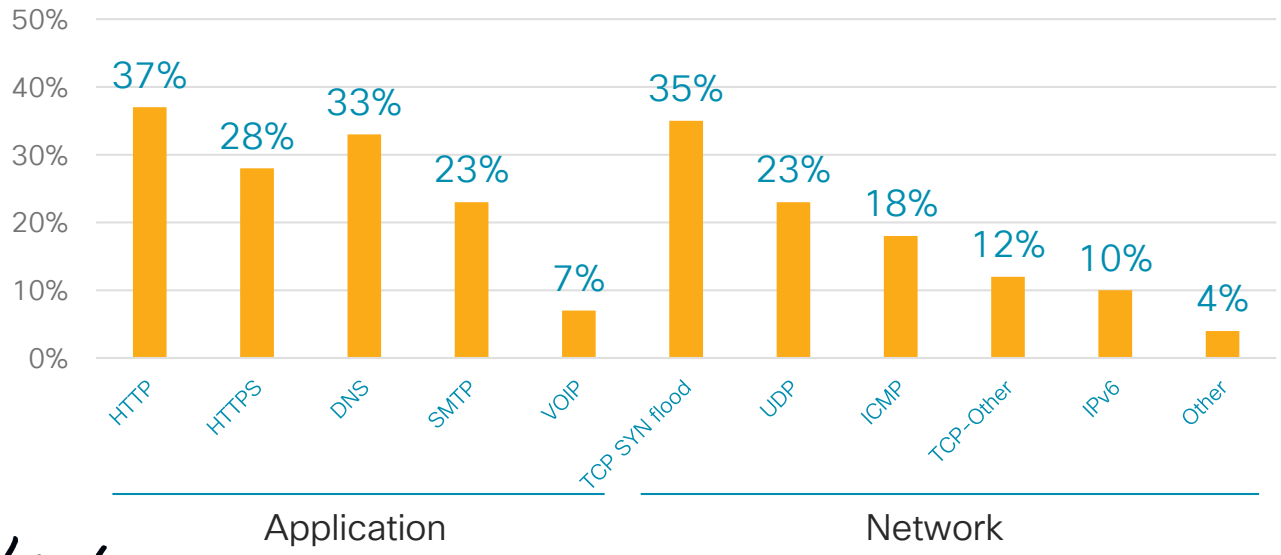
< 2 minutes

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



+ 10% DDoS Attacks

DoS/DDoS Attacks Breaking all Layers of the DC

Internet Pipe	Firewall	IPS/IDS	Load Balancer	Server	SQL Server
37%	17%	6%	4%	35%	1%

- 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

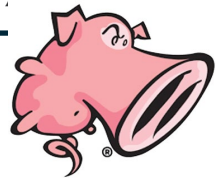
DoS/DDoS Mitigation

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

Firepower Threat Defense Introduction

ASA (L2-L4 functionality)

Firepower (L7 functionality)



Firepower Threat Defense

Firepower Management Center

On-premise

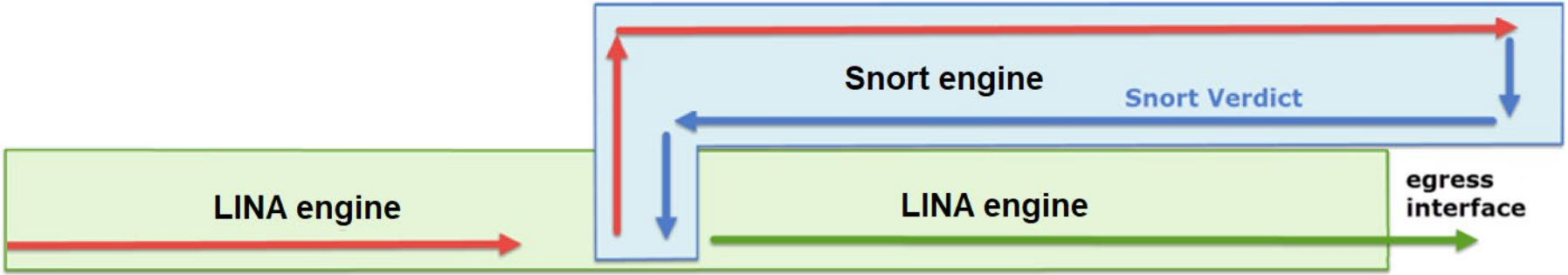
Cisco Defense Orchestrator

Cloud-based

Firepower Device Manager

On-box

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

DoS/DDoS Mitigation on Firepower Threat Defense

Option 1. Configure scanning threat-detection

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy

Object Management | Intrusion Rules

Add FlexConfig Object

Tunnel Zone
Application Filters
VLAN Tag
Security Group Tag
URL
Geolocation
Time Range
Variable Set
Security Intelligence
Sinkhole
File List
Cipher Suite List
Distinguished Name
PKI
SLA Monitor
Prefix List
Route Map
Access List
AS Path
Community List
Policy List
VPN
Address Pools
FlexConfig
Text Object
FlexConfig Object
RADIUS Server Group

Add FlexConfig Object

Name: threat-detection-shun

Description:

Insert | Deployment: Once | Type: Append

```
threat-detection scanning-threat shun duration 1800
```

Variables

Name	Dimension	Default Value	Property (Ty...	Override
No records to display				

Save

ISIS_Unconfigure_All — Unconfigures is-is.

Displaying 1

Create a FlexConfig Object

Add the object to the FlexConfig Policy

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management | NAT | VPN | QoS | Platform Settings | **FlexConfig** | Certificates

FlexConfig1

Preview Config | Save | Cancel

Policy Assignments (0)

Available FlexConfig | FlexConfig Object

User Defined
threat-detection-shun
System Defined
DHCPv6_Prefix_Delegation_UnConfigure
DNS_Configure
DNS_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	threat-detection-shun	

DoS/DDoS Mitigation on Firepower Threat Defense

Option 2. Set embryonic connections limitation

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy

Object Management | Intrusion Rules

Add FlexConfig Object

Tunnel Zone
Application Filters
VLAN Tag
Security Group Tag
URL
Geolocation
Time Range
Variable Set
Security Intelligence
Sinkhole
File List
Cipher Suite List
Distinguished Name
PKI
SLA Monitor
Prefix List
Route Map
Access List
AS Path
Community List
Policy List
VPN
Address Pools
FlexConfig
Text Object
FlexConfig Object
RADIUS Server Group

Add FlexConfig Object

Name: Embryonic_conn_limit

Description:

Insert | Deployment: Once | Type: Append

```
policy-map global_policy
class class-default
set connection embryonic-conn-max 50
```

Variables

Name	Dimension	Default Value	Property (Ty...	Override
No records to display				

Save

ISIS_Unconfigure_All — Unconfigures is-is.

Displaying 1

Create a FlexConfig Object

Add the object to the FlexConfig Policy

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management | NAT | VPN | QoS | Platform Settings | **FlexConfig** | Certificates

FlexConfig1

Preview Config | Save | Cancel

Policy Assignments (0)

Available FlexConfig | FlexConfig Object

User Defined
- Embryonic_conn_limit
- threat-detection-shun

System Defined
- Default_DNS_Configure
- Default_Inspection_Protocol_Disable

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	Embryonic_conn_limit	

DoS/DDoS Mitigation on Firepower Threat Defense

Option 3. Enable rate-based attack prevention

Enable **Rate-Based Attack Prevention**

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Edit Policy: NAP

Policy Information
- Settings
  - Back Orifice Detection
  - Checksum Verification
  - DCE/RPC Configuration
  - DNS Configuration
  - FTP and Telnet Configuration
  - GTP Command Channel Configuration
  - HTTP Configuration
  - IP Defragmentation
  - Packet Decoding
  - Rate-Based Attack Prevention
  - SMTP Configuration

Rate-Based Attack Prevention < Back

SYN Attack Prevention Add

Track By	Network	Rate		Drop	Timeout	
Destination	192.168.2.160	20 SYNs /	1 seconds	☑	60 seconds	Delete

Control Simultaneous Connections Add

Track By	Network	Count	Drop	Timeout

Revert to Defaults

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%
```

Verify CPU utilization

```
Firepower-module1# show resource usage
Resource          Current    Peak       Limit       Denied  Context
Conns             8777473    8777473    25000000         0  System
Hosts             8658916    8658916    N/A              0  System
Conns [rate]      161131     273758     N/A              0  System
Inspects [rate]   161121     273751     N/A              0  System
Routes            10         10         unlimited        0  System
```

Verify anomalies in resource usage

```
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 the interface statistics

How to Identify a DoS/DDoS Attack in your Network?

Verify traffic anomalies: Packet capture

```
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
```

Verify traffic anomalies: Traffic statistics

```
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
```

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%
```

Verify the symptoms

```
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
```

Identify the attack

How to Identify a DoS/DDoS Attack in your Network?

```
CAT-SWITCH# show ip cache flow
Displaying hardware-switched flow entries in the PFC (Active) Module 5:
 SrcIf     SrcIPaddress    DstIf     DstIPaddress    Pr  SrcP  DstP  Pkts
 Vl204     192.168.1.55    Vl204     192.168.2.160   06  E95B  0016  26
 Vl204     192.168.1.55    Vl204     192.168.2.160   06  E96C  0016  23
 Vl204     192.168.1.55    Vl204     192.168.2.160   06  E9DC  0016  30
....
 Vl204     192.168.7.17    Vl204     192.168.2.160   06  083A  0016  17
 Vl204     192.168.5.35    Vl204     192.168.2.160   06  0839  0016  13
 Vl204     192.168.3.88    Vl204     192.168.2.160   06  0861  0016  19
```

Verify traffic anomalies: Netflow

DoS Attack

DDoS Attack

```
CAT-SWITCH# show interface | include line| input rate
GigabitEthernet2/1 is up, line protocol is up (connected)
  5 minute input rate 187248000 bits/sec, 128626 packets/sec
```

Verify the interface statistics

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
```

Verify the symptoms

```
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)
```

Identify the attack

DoS/DDoS Mitigation with Radware vDP

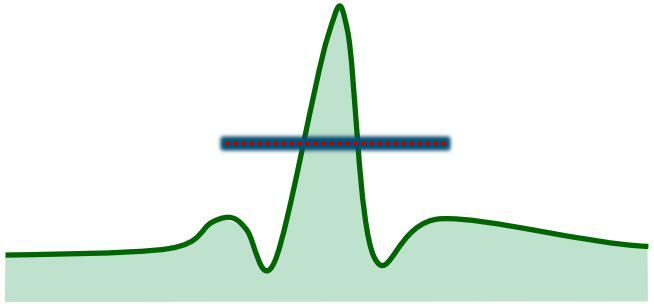
DoS/DDoS Mitigation with Radware vDP

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

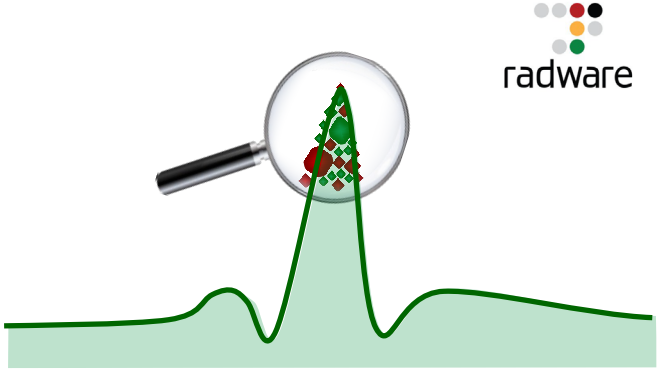
radware

DoS/DDoS Mitigation with Radware vDP



Rate-Based Detection

High false positives



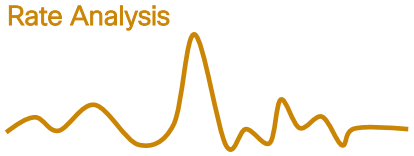
Behavioral Detection

Low false positives

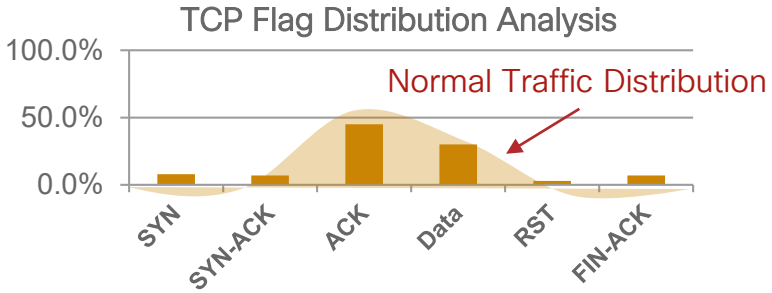
DoS/DDoS Mitigation with Radware vDP

Learning → Detection → Characterization → Mitigation

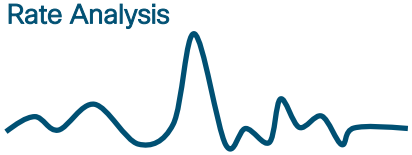
Good Traffic



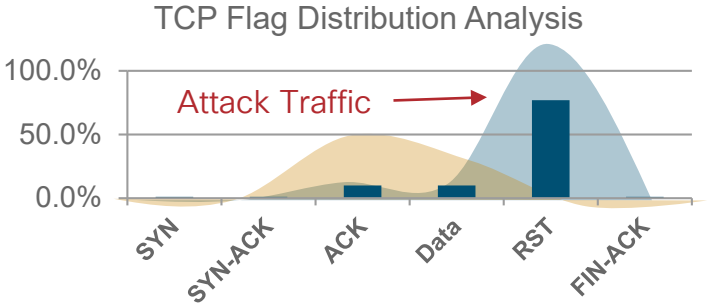
+



Attack Traffic
(RST Flood)



+



DoS/DDoS Mitigation with Radware vDP

Always-On Protection

Fast Detection and Mitigation

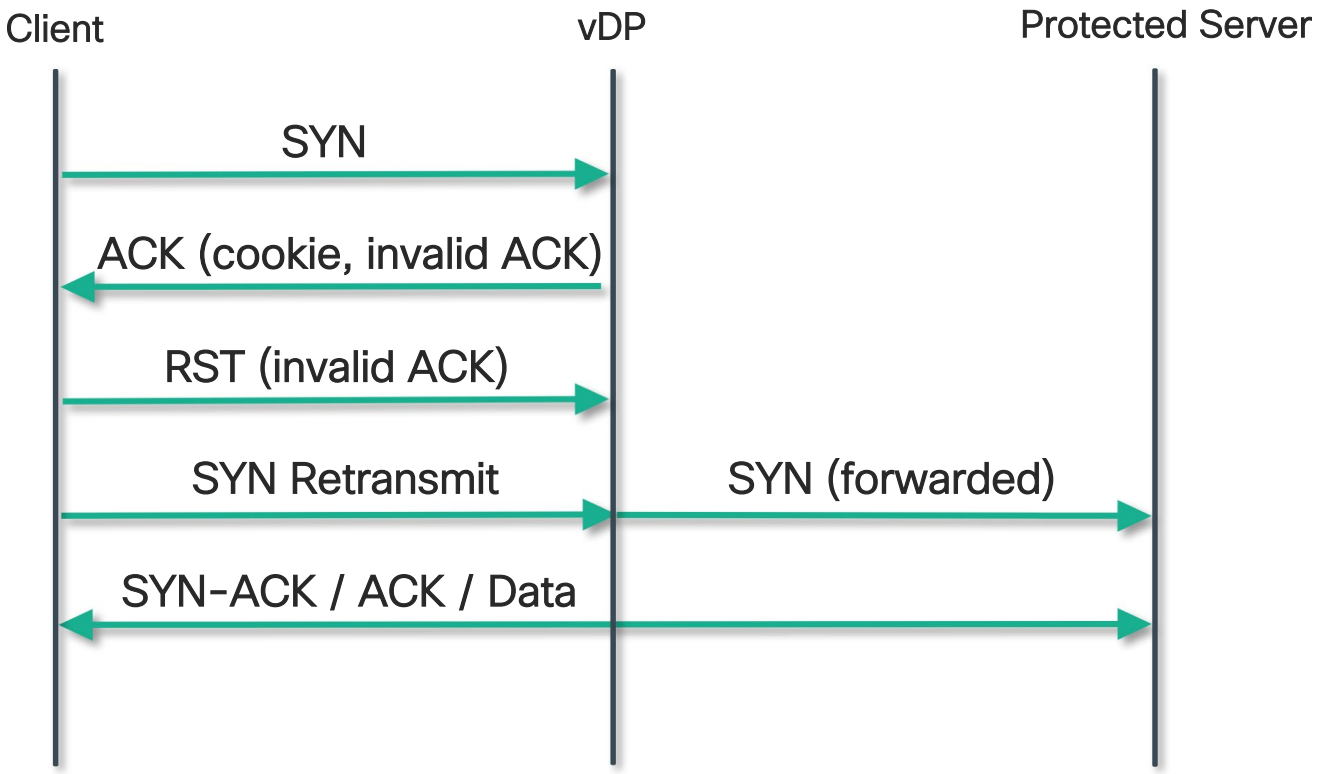
Adaptive behavioral DoS against IPv4/IPv6 TCP/UDP/ICMP/IGMP/DNS floods

Application signature protection

Anomaly protection against basic malformed packets

Bot detection with smart challenge

Safe-Reset Authentication with Radware vDP



Safe-Reset Authentication with Radware vDP

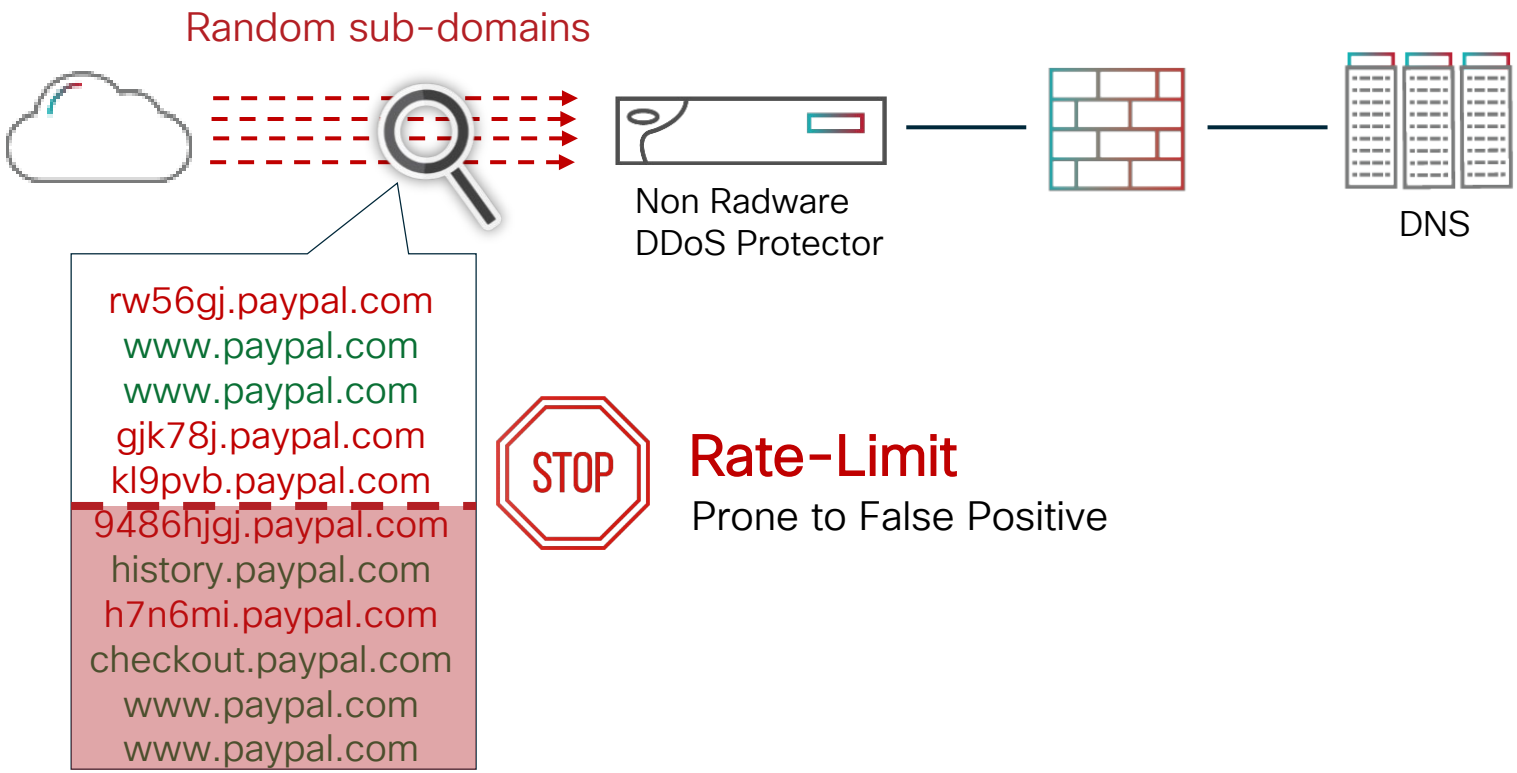
Time	Source	Destination	Protocol	Length	Identification	Info
2019-01-14 09:40:45.036530	94.52.141.96	192.168.2.160	SSH	174	0xeb9f (60319)	Client: Encrypted packet (len=120)
2019-01-14 09:40:45.036872	192.168.2.160	94.52.141.96	TCP	60	0xeb9f (60319)	22 → 23007 [ACK] Seq=2080338225 Ack=2080338225

```
▶ Frame 29385: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: Cisco_8e:02:ce (2c:33:11:8e:02:ce), Dst: Vmware_85:28:72 (00:50:56:85:28:72)
▶ Internet Protocol Version 4, Src: 192.168.2.160, Dst: 94.52.141.96
▼ Transmission Control Protocol, Src Port: 22, Dst Port: 23007, Seq: 2080338225, Ack: 2080338225, Len: 0
    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
```

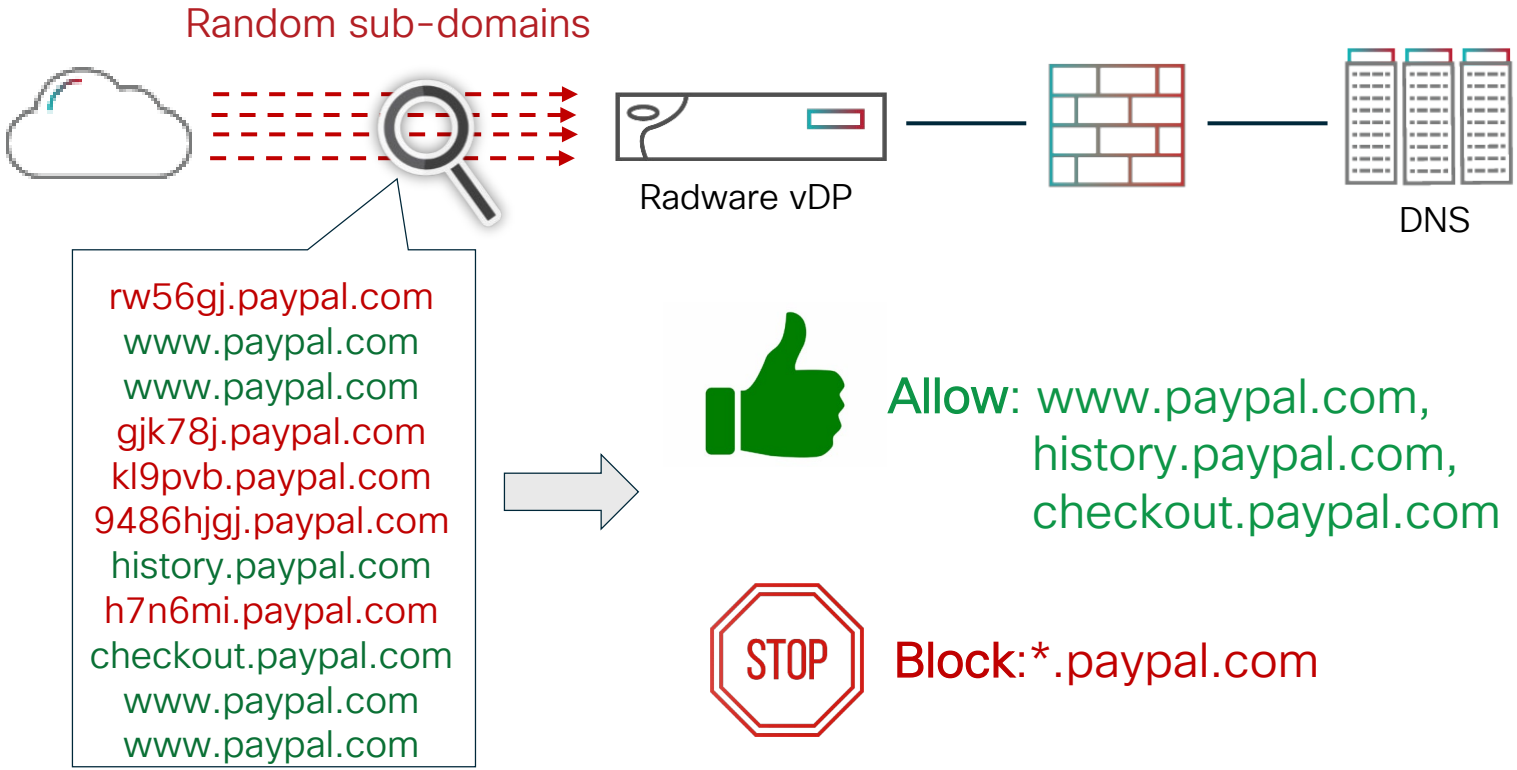
ACK (cookie, invalid ACK)

Radware vDP Next Generation DNS Protection

Random Subdomains Attack – Query Rate Limiting



Random Subdomains Attack – vDP DNS Protection



Radware vDP DNS Protection

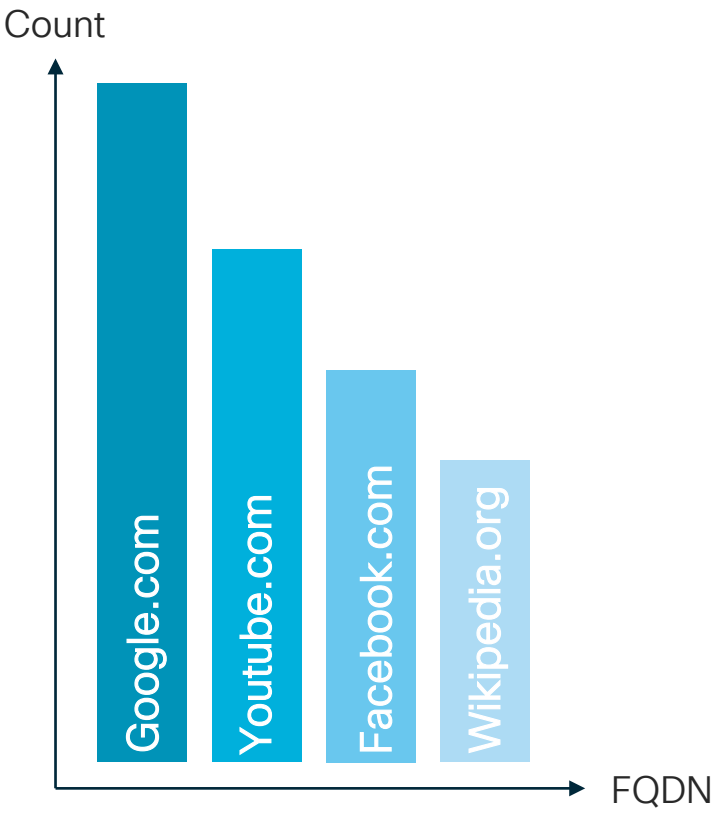
Detection

Rate Analysis
per DNS Query Type

Radware vDP DNS Protection

Detection

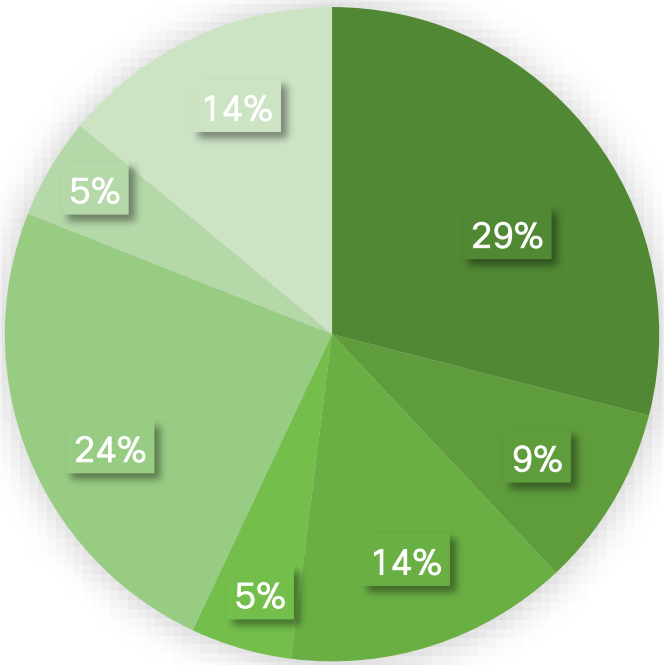
FQDN Analysis per Query Type



Radware vDP DNS Protection

Detection

DNS Query Distribution Analysis (Rate Invariant)



- A Records
- PTR Records
- AAAA Records
- TEXT Records
- SPV/NAPTR
- Other Records
- MX Records

Radware vDP DNS Protection

Characterization

Suspicious Data Packet

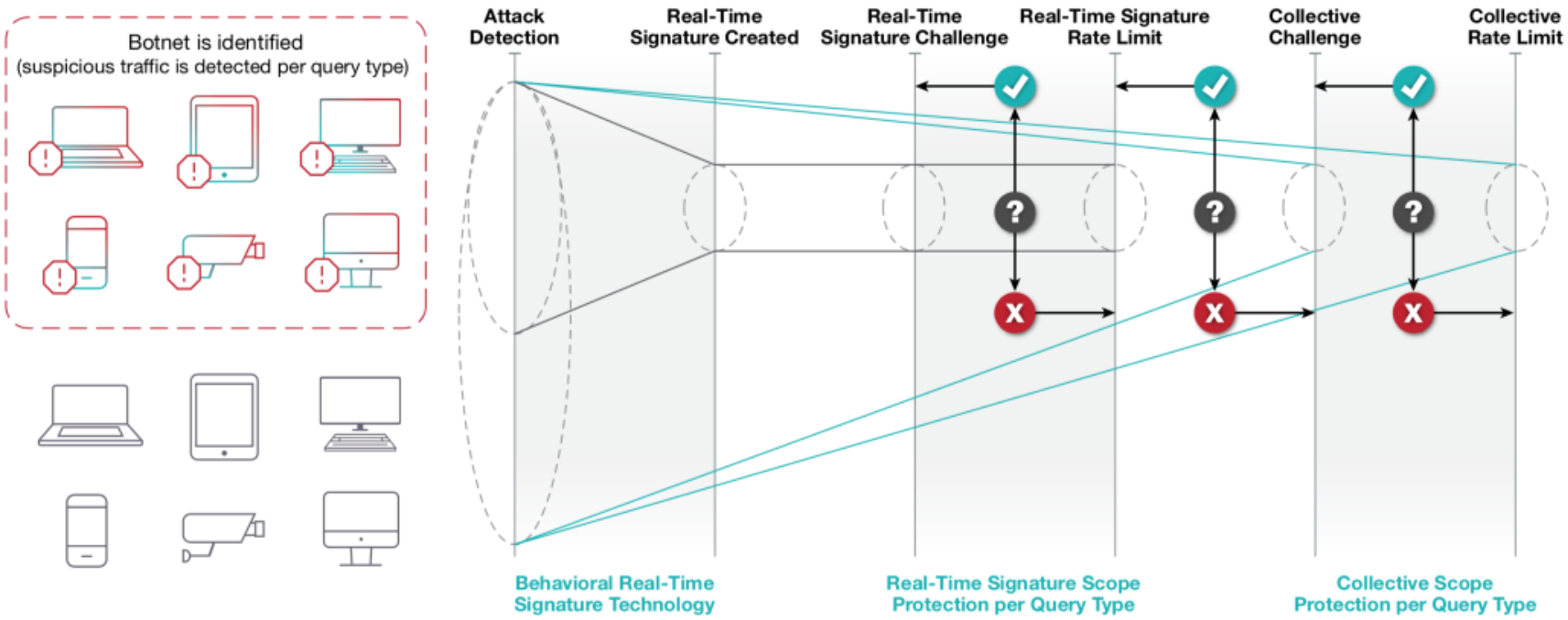
- Packet checksums
- DNS Qname – domain name
- Source IP address
- Ports numbers
- Packet Identification numer
- Identification numer
- DNS query ID - query
- Packet size
- TTL (Time to Live)
- Destination IP address
- DNS Query count (Qcount)
- Fragment offset
- …

Automatic Real Time Signature Generation Module

Real Time Signature

Radware vDP DNS Protection

Mitigation



Radware vDP DNS Protection

Mitigation

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 it's 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

Firepower	Throughput FW + AVC + IPS	Throughput FW + AVC + IPS + vDP
9300 – SM 44	53 Gbps	49,4 Gbps (93.2%)
9300 – SM 36	34 Gbps	31,2 Gbps (91.7%)
9300 – SM 24	24 Gbps	21 Gbps (87.5%)
4150	24 Gbps	22,4 Gbps (93.2%)
4140	20 Gbps	18,3 Gbps (91.7%)
4120	15 Gbps	13,1 Gbps (87.5%)
4110	10 Gbps	7,5 Gbps (75.0%)

$$\frac{48-6}{48} \times 100 = 87{,}5\%$$

Performance Criteria

- vDP defaults to 6 cores
- Subtract vDP cores from total cores
- Percentage of remaining cores = Expected Performance

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:

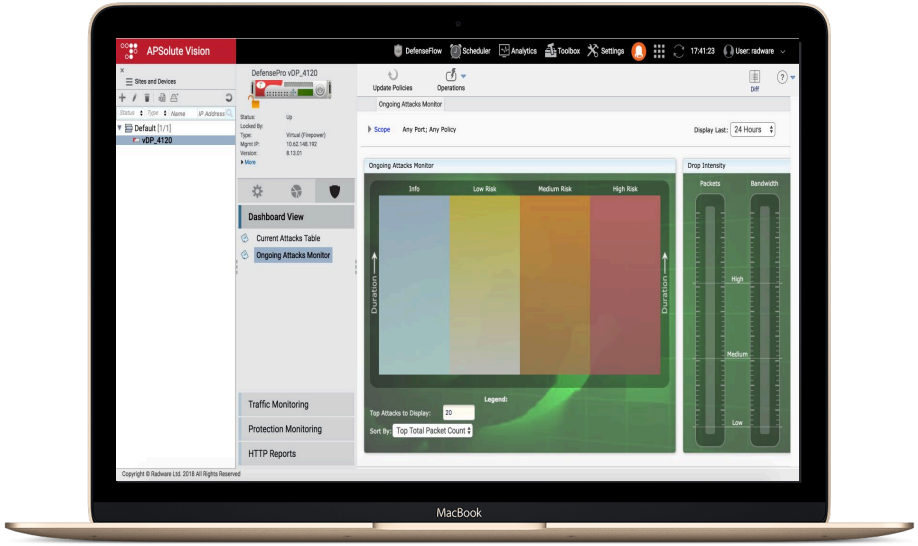
- Peace time traffic is a known value, attack size is unknown
- If peak traffic is 2Gb (inbound + outbound), purchase a 2Gb clean traffic license
- 14Gb – 2Gb = 12Gb of DDoS Scrubbing on Box

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
```

Confirm the FXOS and vDP compatibility

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

Configure the NTP server on Firepower Chassis

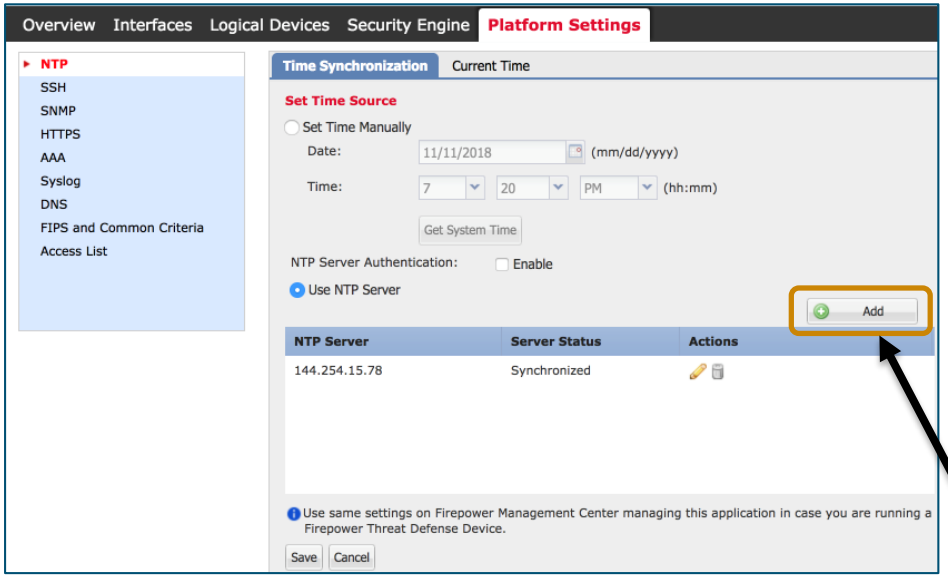
```
FP4120-A# show ntp
    NTP Overall Time-Sync Status: Time Synchronized
FP4120-A# show clock detail
Sun Nov 11 16:09:07 UTC 2018
```

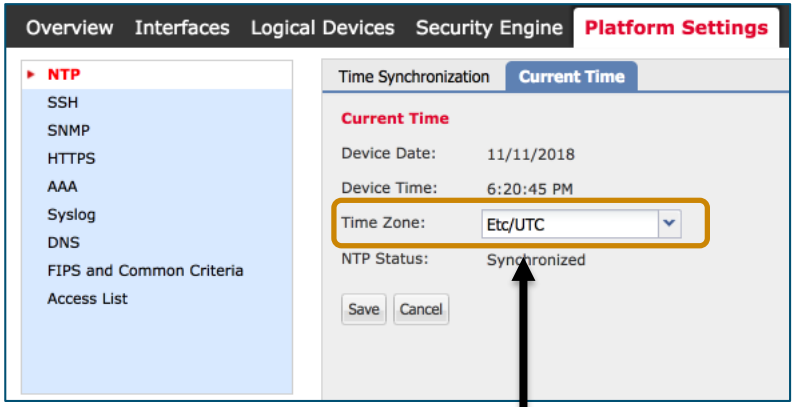
Specify Etc/UTC timezone on Firepower Chassis

CSCvp95275

Radware vDP Installation Prerequisites

If the NTP server/timezone settings are not configured:





Specify the Time Zone

Configure the NTP server

Radware vDP Installation Using FCM

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

Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin

Configuration Licensing Updates User Management

Available Updates

Refresh Upload Image Filter..

Image Name	Type	Version	Status	Build Date	Image Integrity
fxos-k9.2.4.1.101.SPA	platform-bundle	2.4(1.101)	Installed	10/20/2018	Verified - Sun 1 Jan 2012, 01:41 AM
radware-vdp.8.13.01.09-2.csp	vdp	8.13.01.09-2	Installed	11/2/2017	Verified - Mon 12 Nov 2018, 12:08 AM
cisco-ftd.6.2.3.83.csp	ftd	6.2.3.83	Installed	04/01/2018	Verified - Sun 1 Jan 2012, 04:37 AM

Radware vDP Installation Using FCM

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

Overview | Interfaces | Logical Devices | Security Engine | Platform Settings | System | Tools | Help | admin

Network Module 1: 1, 3, 5, 7, 2, 4, 6, 8 — CONSOLE, MGMT, USB
Network Module 2 : Empty
Network Module 3 : Empty

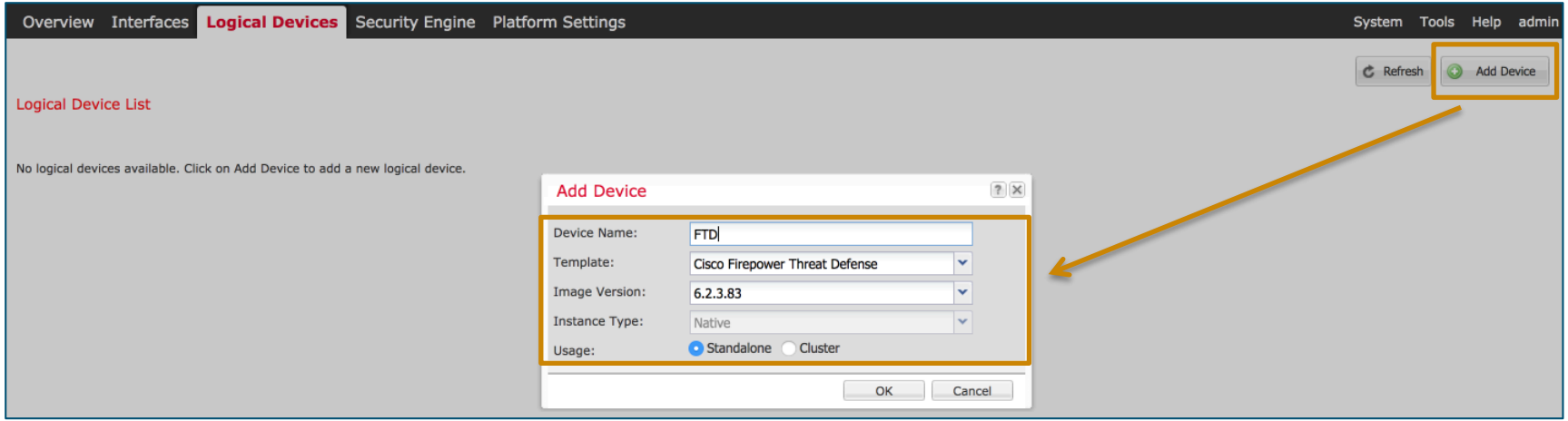
All Interfaces | Hardware Bypass

Add New

Interface	Type	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management								
Port-channel10	data	10gbps	10gbps			Full Duplex	no	failed	
Port-channel20	data	10gbps	10gbps			Full Duplex	no	failed	
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	failed	
Ethernet1/1	mgmt	1gbps	1gbps			Full Duplex	no	up	
Ethernet1/2	data	10gbps	10gbps			Full Duplex	no	admin-down	
Ethernet1/3	data	10gbps	10gbps			Full Duplex	no	admin-down	
Ethernet1/4	data	10gbps	10gbps			Full Duplex	no	sfp-not-present	

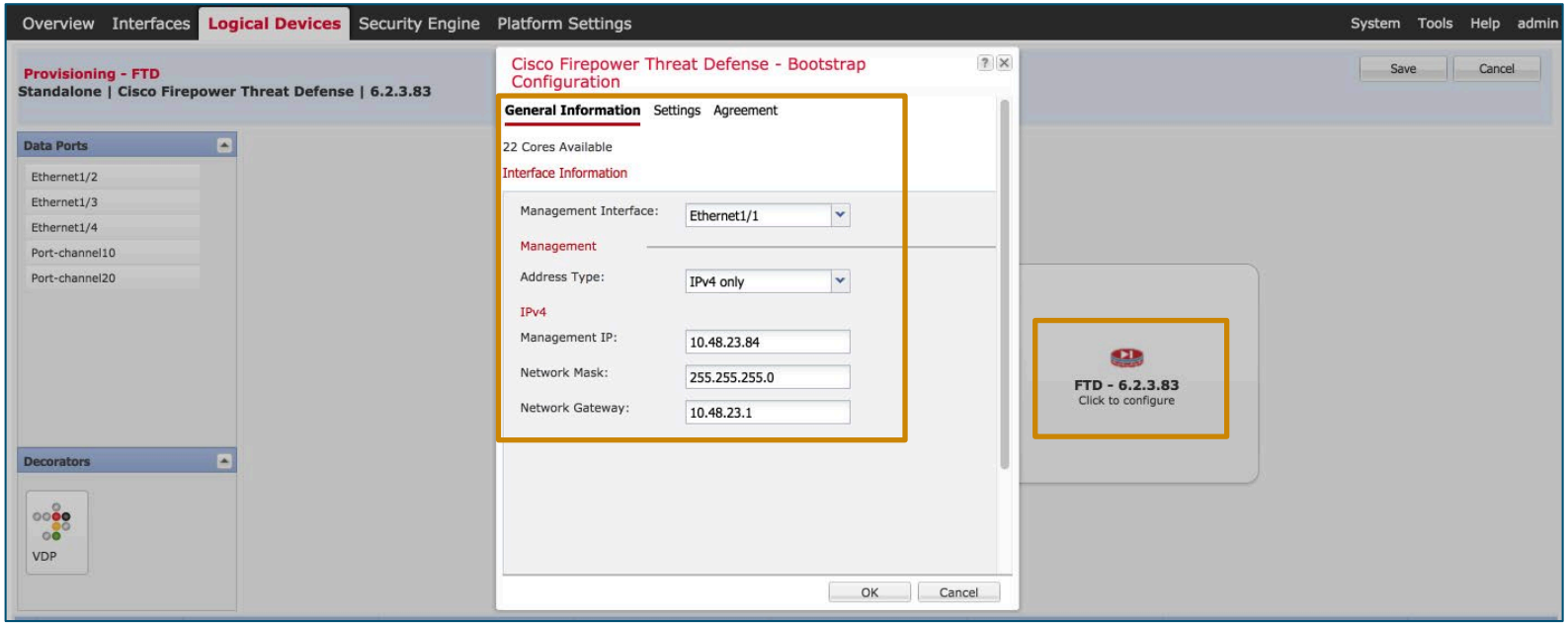
Radware vDP Installation Using FCM

Step 3. On FCM Create an FTD Logical Device (Logical Devices > Add Device).



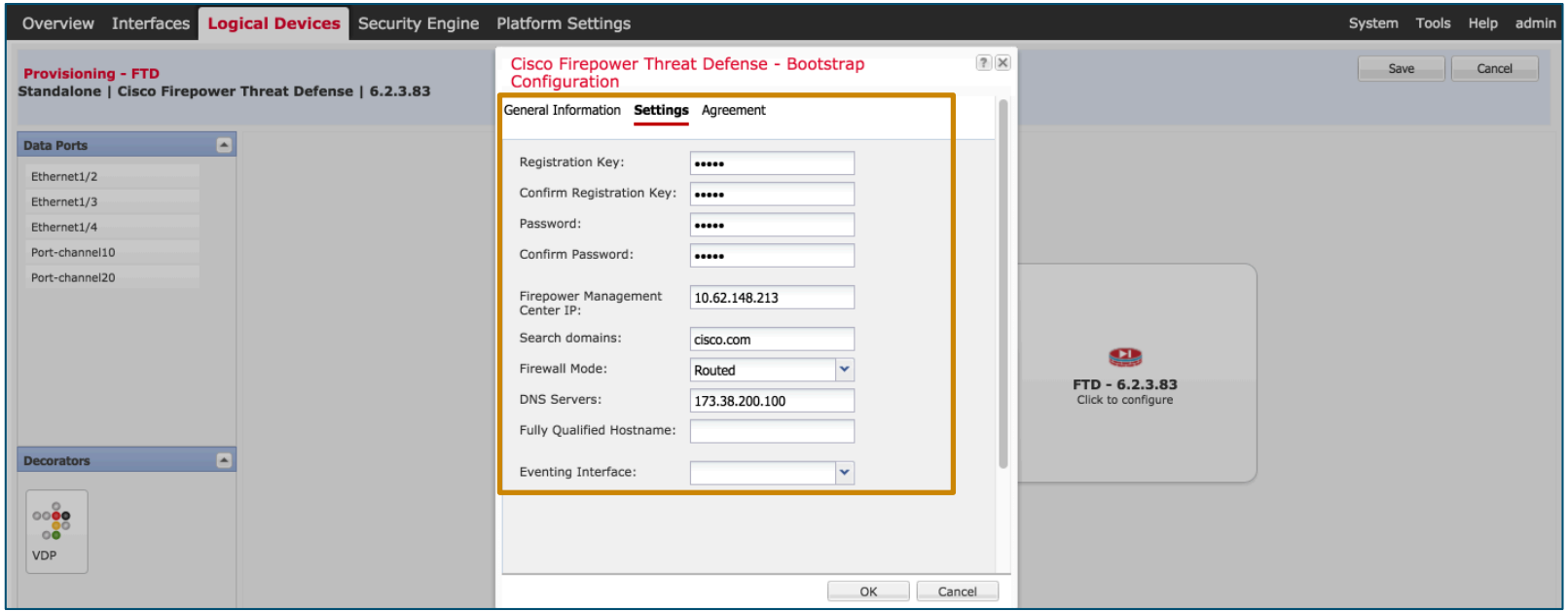
Radware vDP Installation Using FCM

Step 4. On FCM provision the FTD Management interface.



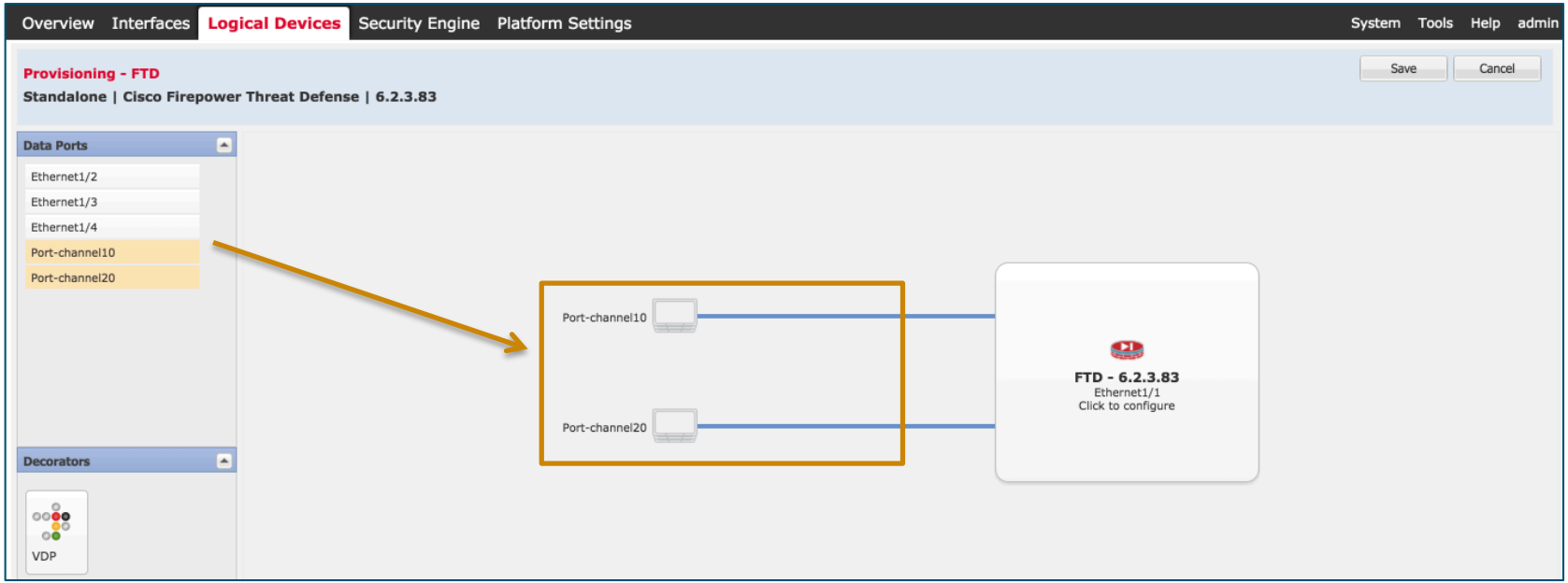
Radware vDP Installation Using FCM

Step 5. On FCM provision the FTD settings and FMC info.



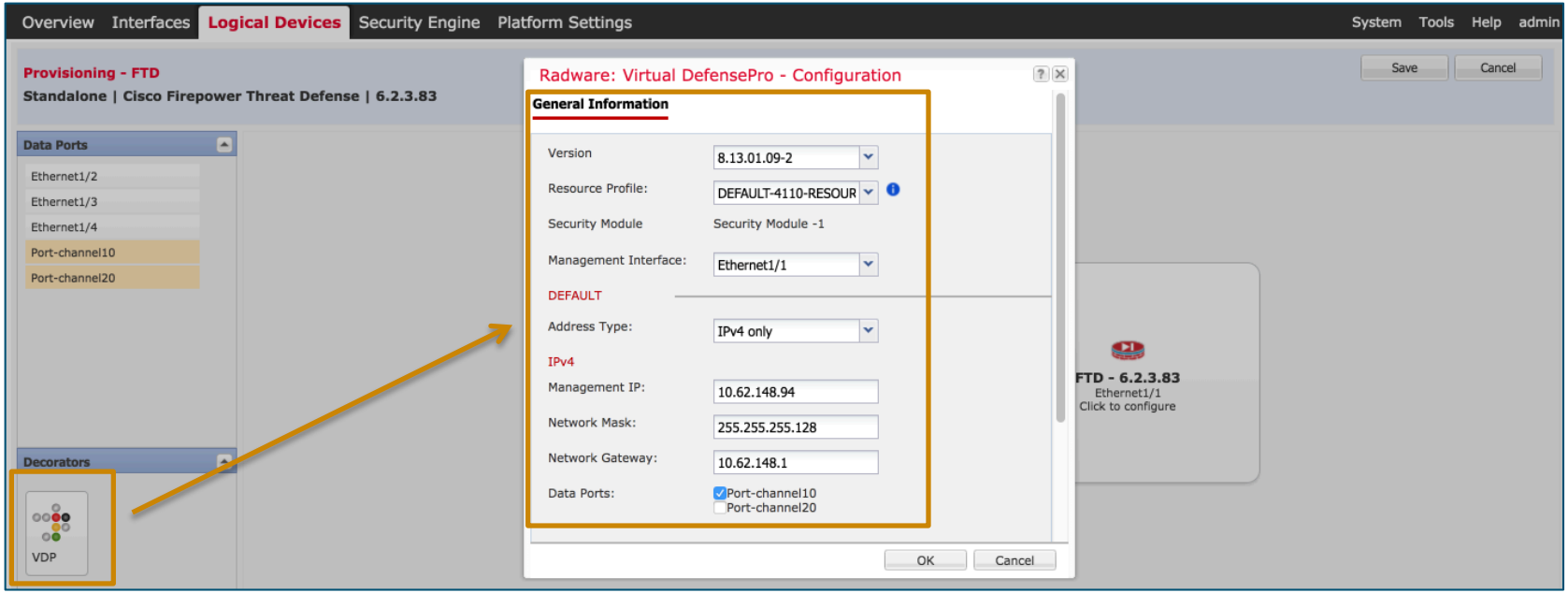
Radware vDP Installation Using FCM

Step 6. On FCM provision the FTD Data interface(s).



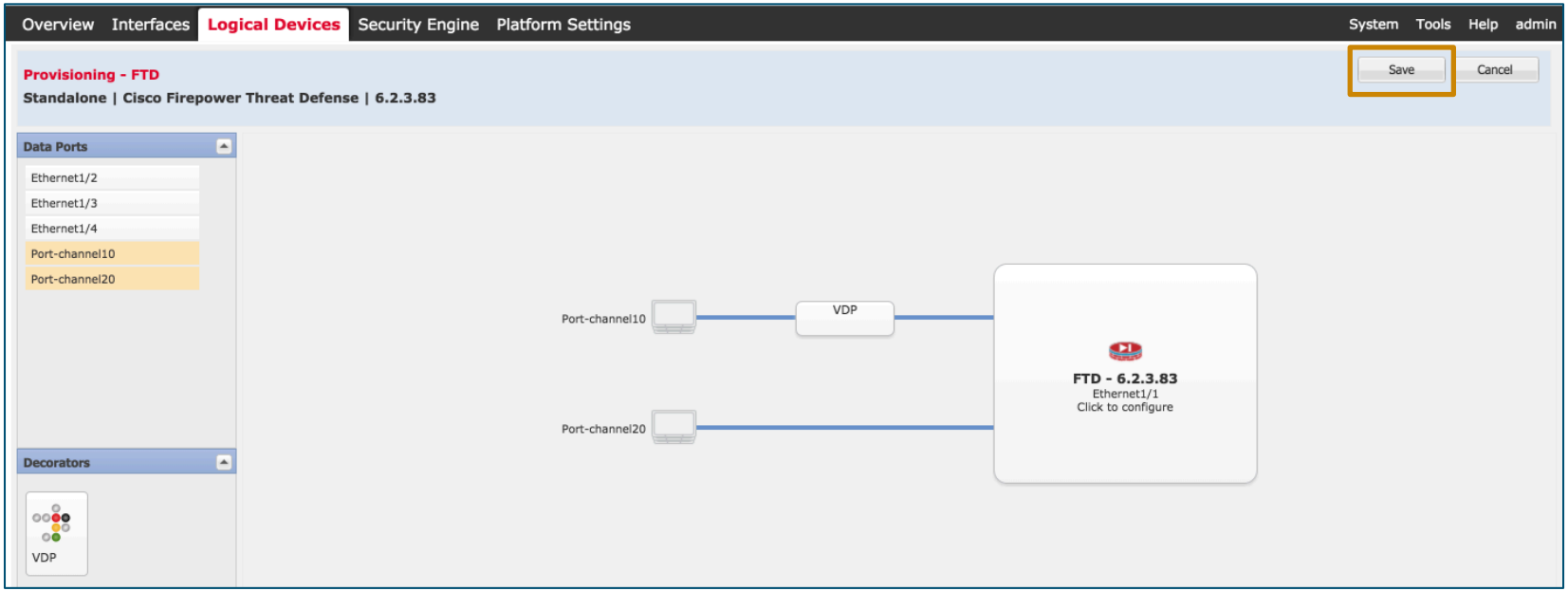
Radware vDP Installation Using FCM

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.
DefensePro>12-11-2018 13:57:13 INFO Port 1 Down
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
```

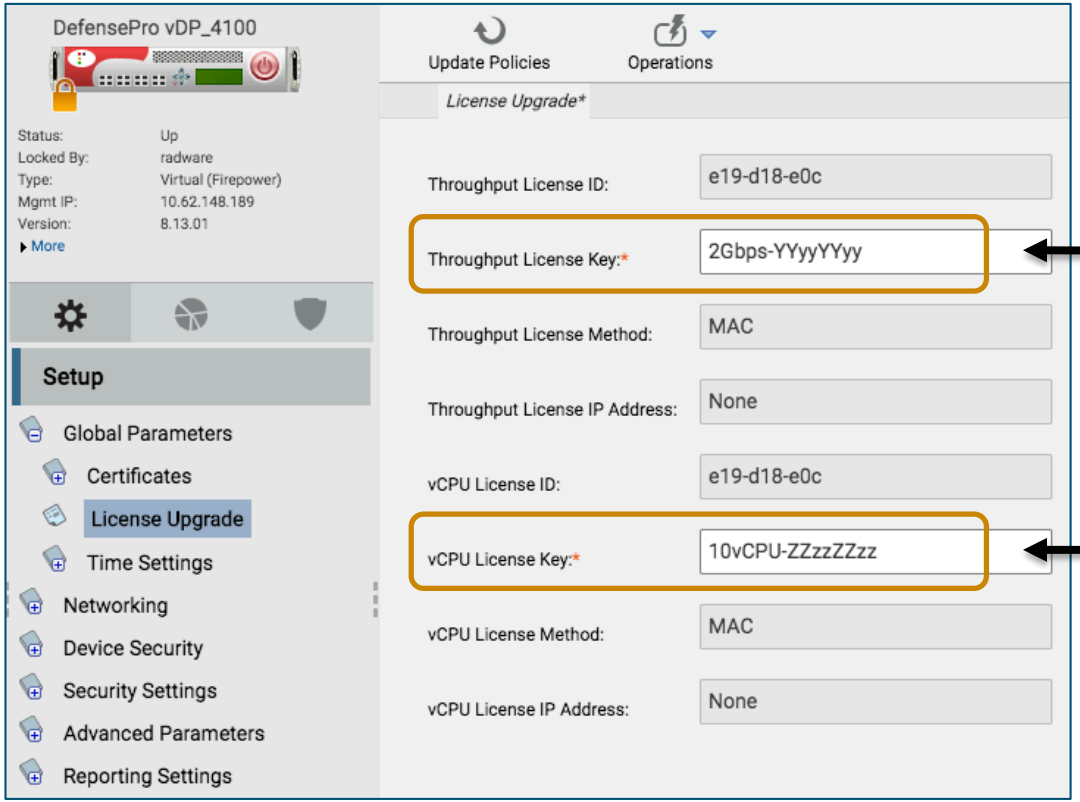
Apply a license key

```
DefensePro#system license throughput get

License Key : 2Gbps-YYyyYYyy
MAC Address  : 5897bdb9369e
License ID   : e19-d18-e0c
```

Applied vDP license

Radware vDP Capacity & Licensing



Apply throughput license key

Apply vCPU license key

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:
   App Name   Identifier Admin State Oper State  Running Version Startup Version Deploy Type Profile Name
Cluster State   Cluster Role
   ---------- ---------- ----------- ---------------- --------------- --------------- ----------- --
---------- --------------- ------------
   ftd        FTD4140-1        Enabled     Online       6.3.0.45          6.3.0.45          Native
Not Applicable  None
   vdp        FTD4140-1        Disabled    Installing                 8.13.01.09-2       Vm        DEFAULT-RESOURCE
Not Applicable  None
```


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
```


Radware vDP Installation Using Command Line

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
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
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
vdp        FTD4140-1 1         Enabled     Online       8.13.01.09-2     8.13.01.09-2    Vm     DEFAULT-RESOURCE
Not Applicable  None
```

```
FPR4100-1# connect module 1 console
Firepower-module1>show services status all
Services currently running:
Application Type | Identifier        | Oper State | Up Since | Instance ID
-------------- | ------------| ---------- | --------| -----------
ftd (native)     | FTD4140-1     | RUNNING    | 02:59:51 | ftd_001_JMX2215L02BPXFTYE20
vdp (vm)         | FTD4140-1     | RUNNING    | 03:02:15 | vdp_001_JMX2215L02BEK2YYC26
```


Register vDP to APSolute Vision Manager

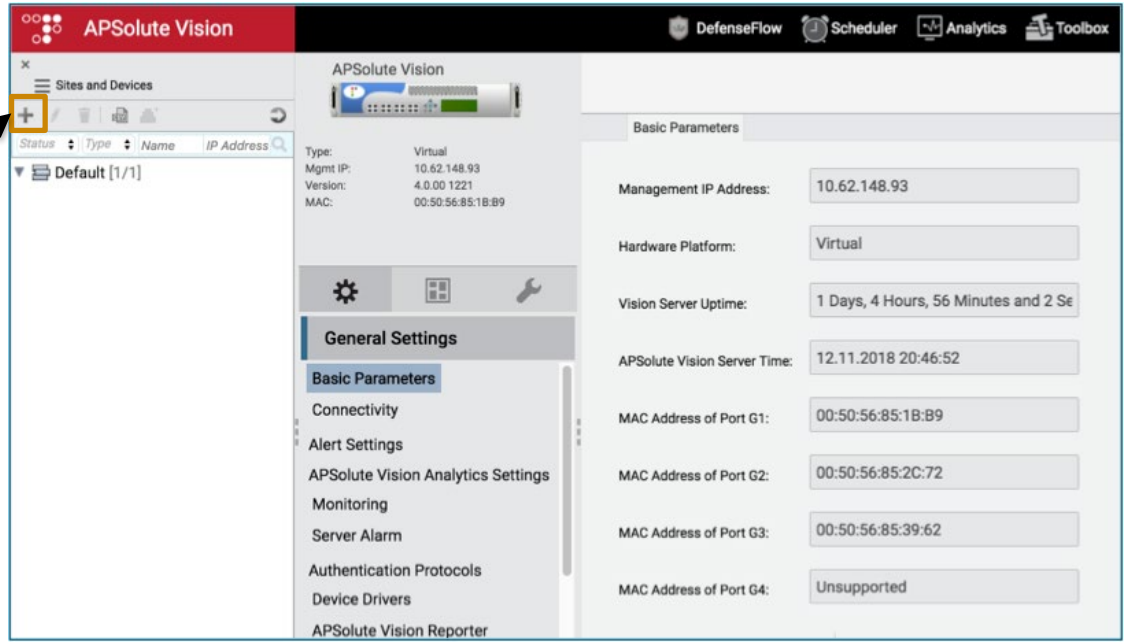
Step 1. Enable vDP web interface on vDP application.

```
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

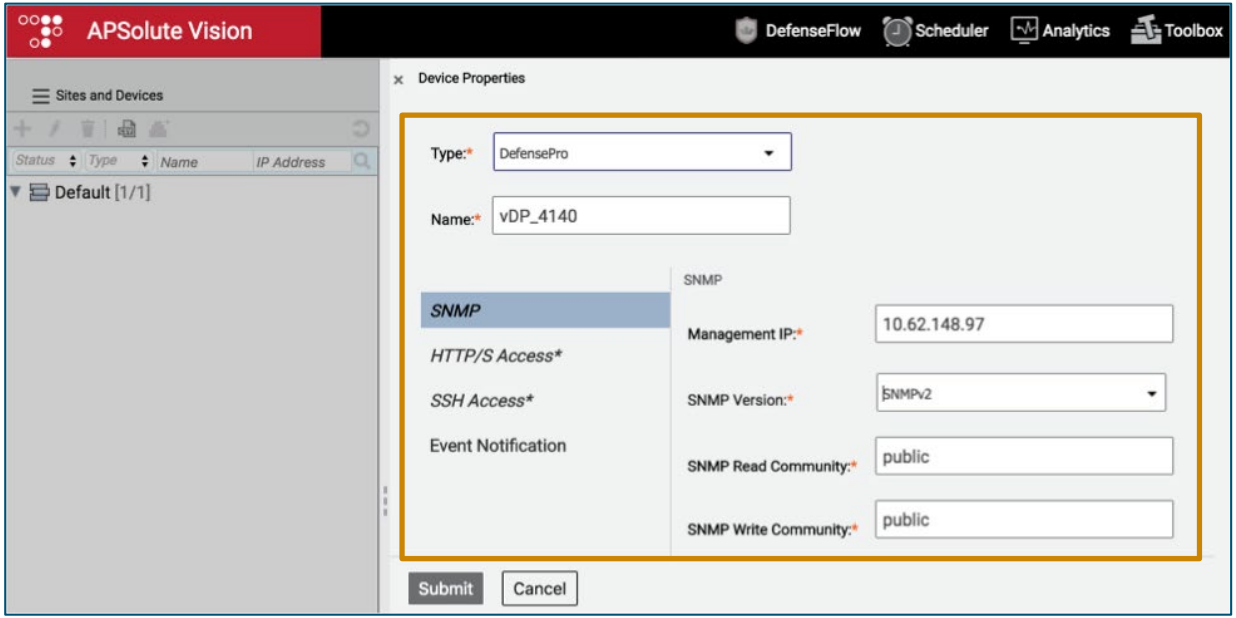
Step 2. Log in to Radware APSolute Vision Manager and add the device.



Add the device

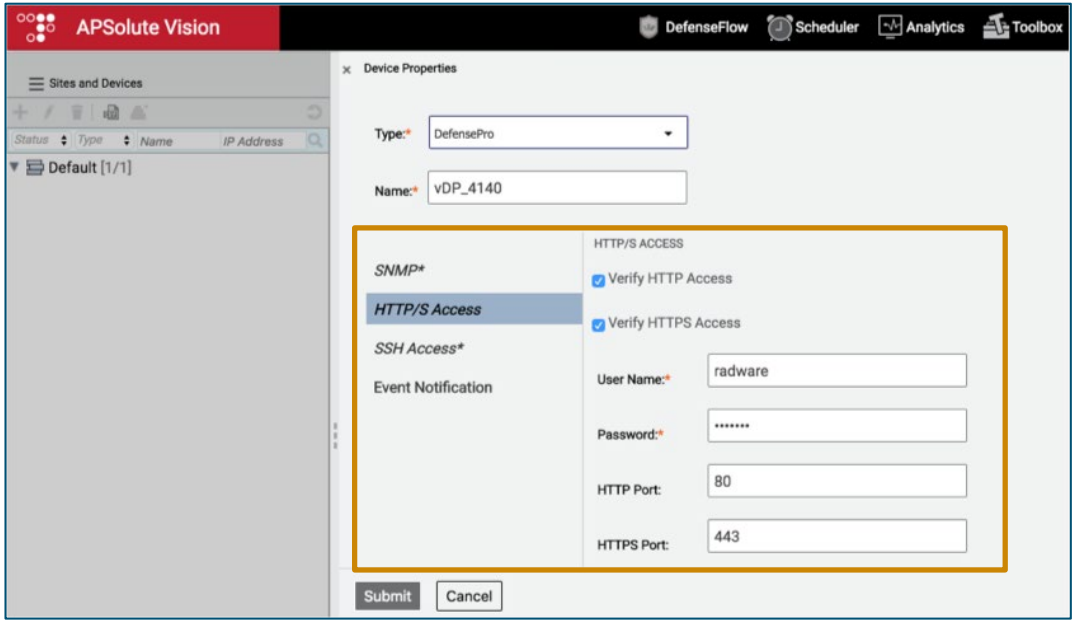
Register vDP to APSolute Vision Manager

Step 3. In Device Properties select Type DefensePro, specify the name and configure the SNMP settings.



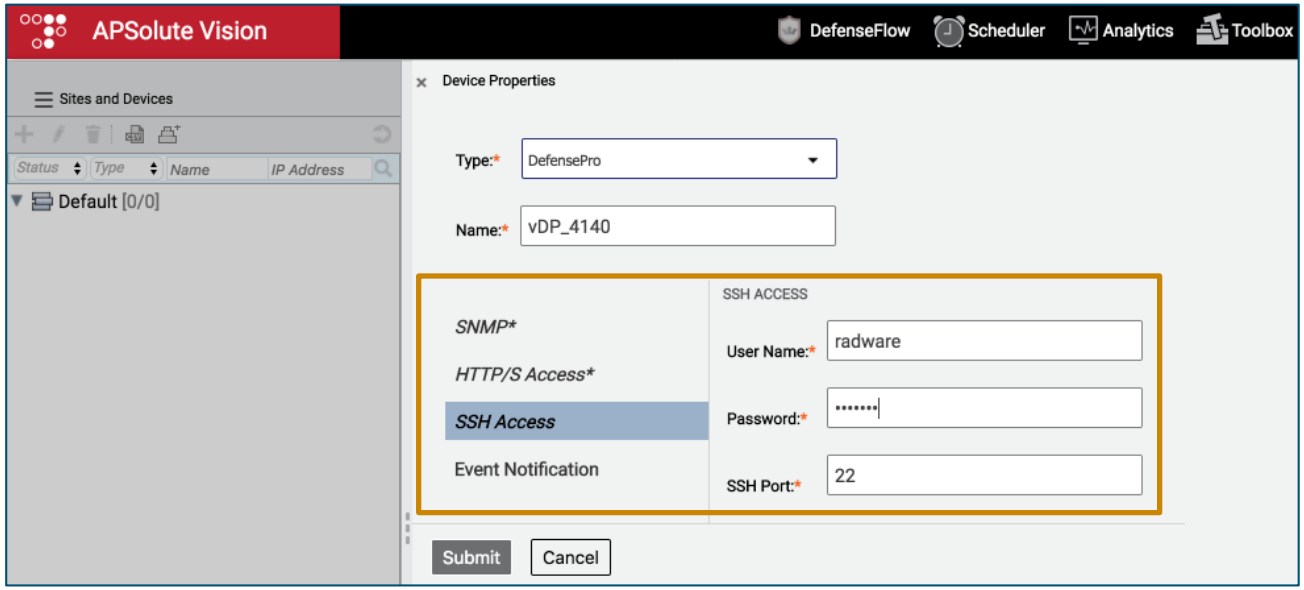
Register vDP to APSolute Vision Manager

Step 4. Navigate to the HTTP/S Access tab and specify the User Name and the Password.



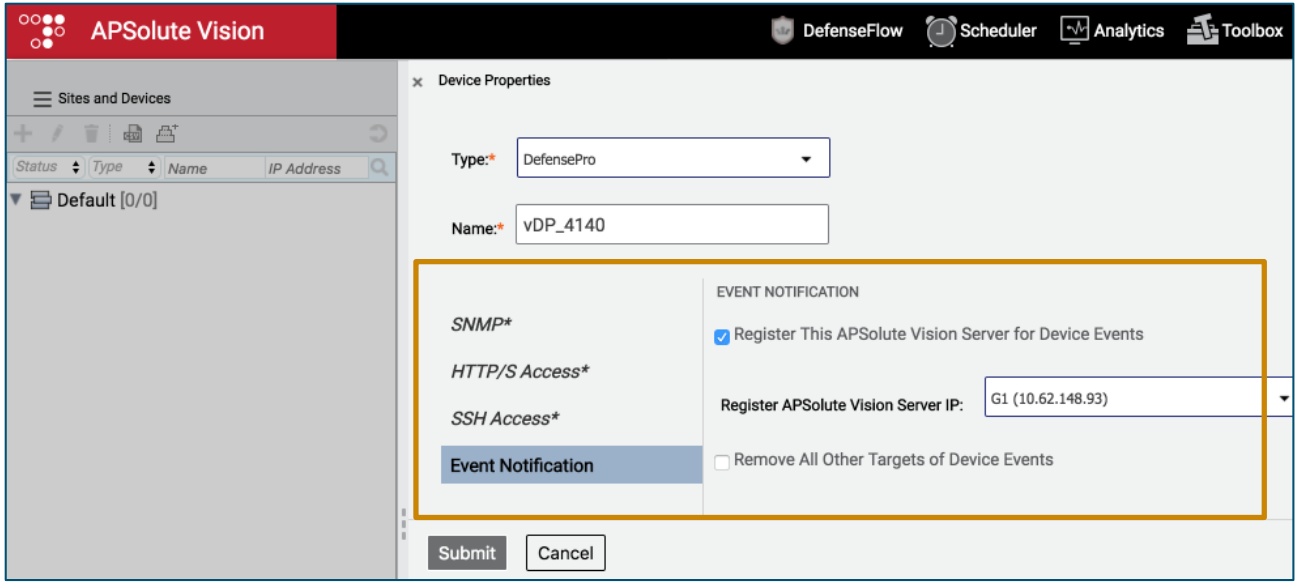
Register vDP to APSolute Vision Manager

Step 5 (Optional). Navigate to the SSH access tab and specify the User Name and the Password.



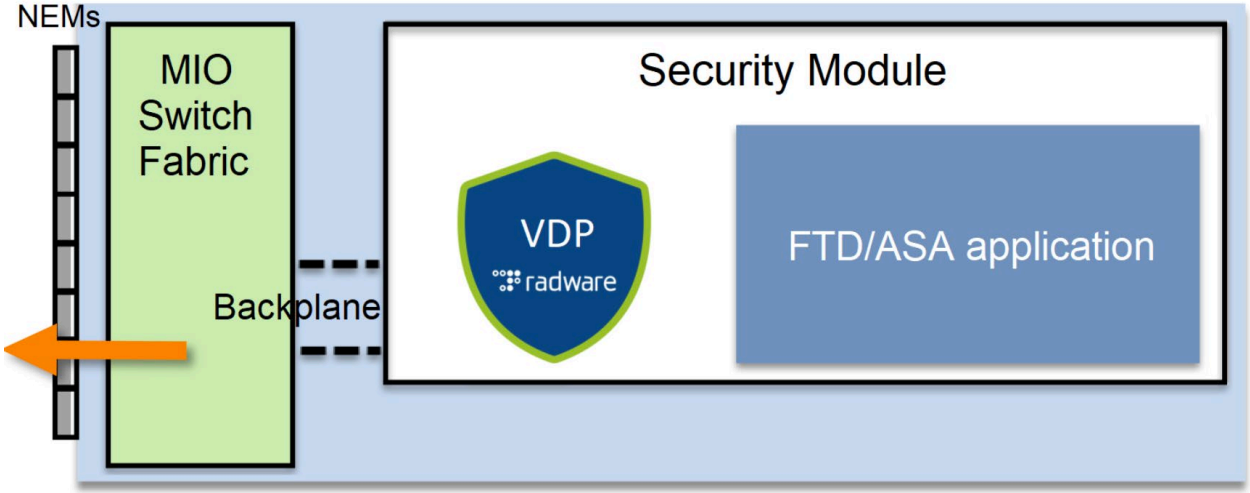
Register vDP to APSolute Vision Manager

Step 6. Specify whether the APSolute Vision server configures itself as a target of the device events.



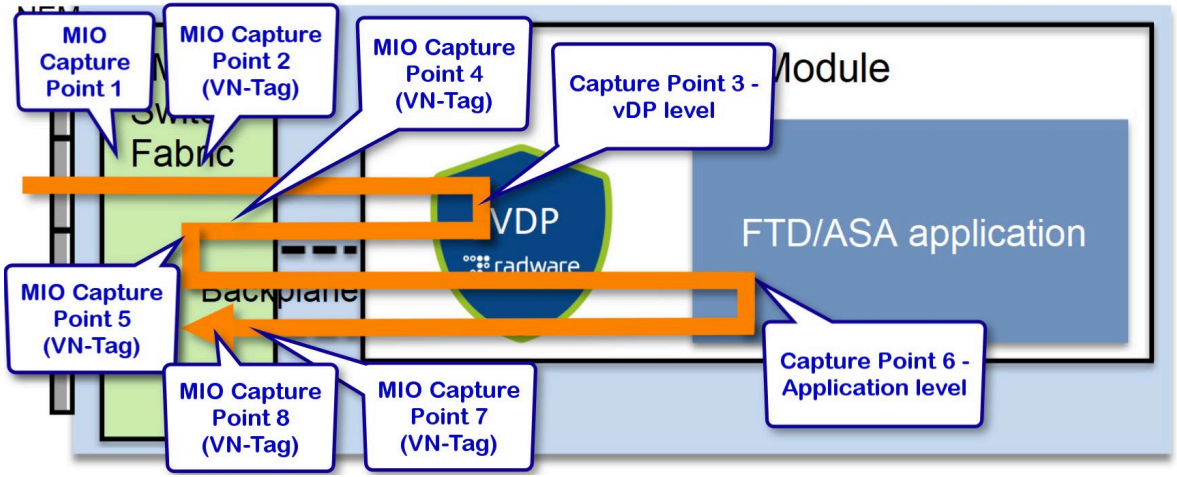
Detailed Packet Flow with Radware vDP

Detailed Packet Flow with Radware vDP



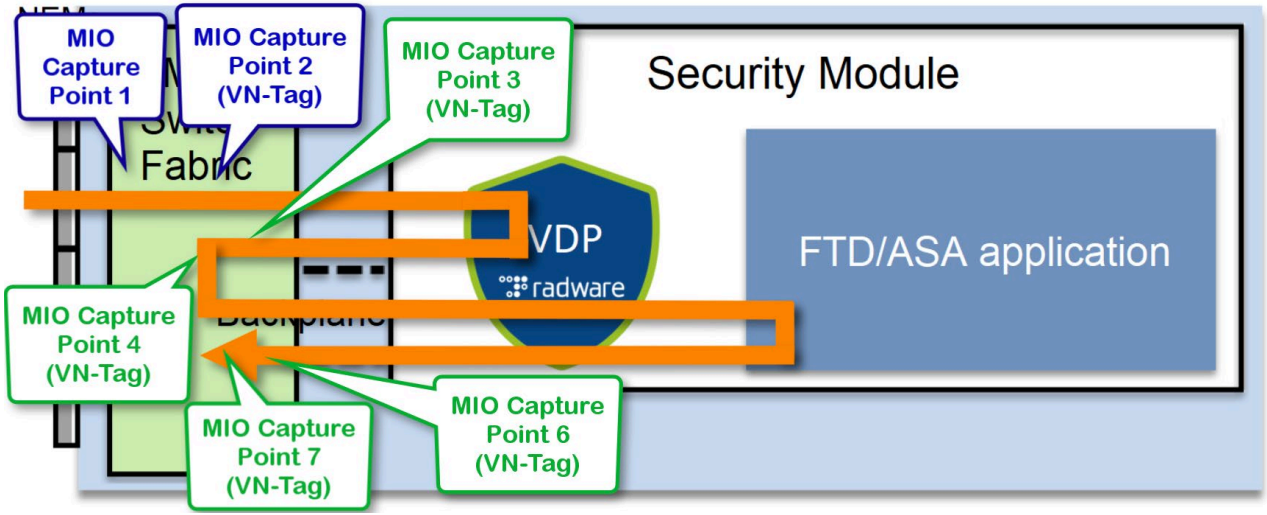
1. MIO (Management Input/Output) receives the packet on the physical port
2. MIO sends the packet to the Decorator (vDP Radware)
3. MIO receives the packet from the Decorator (vDP Radware)
4. MIO sends the packet to the Security Module (FTD/ASA)
5. FTD/ASA sends the packet back to the MIO
6. MIO sends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

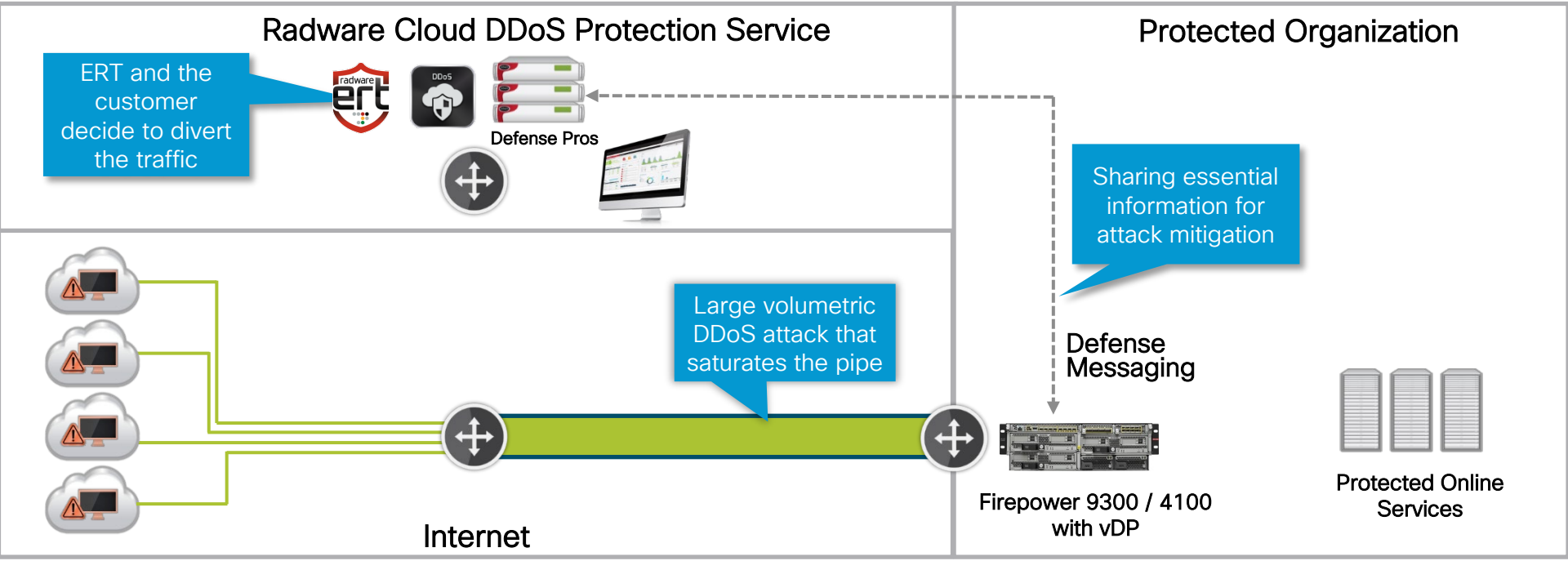
Detailed Packet Flow with Radware vDP



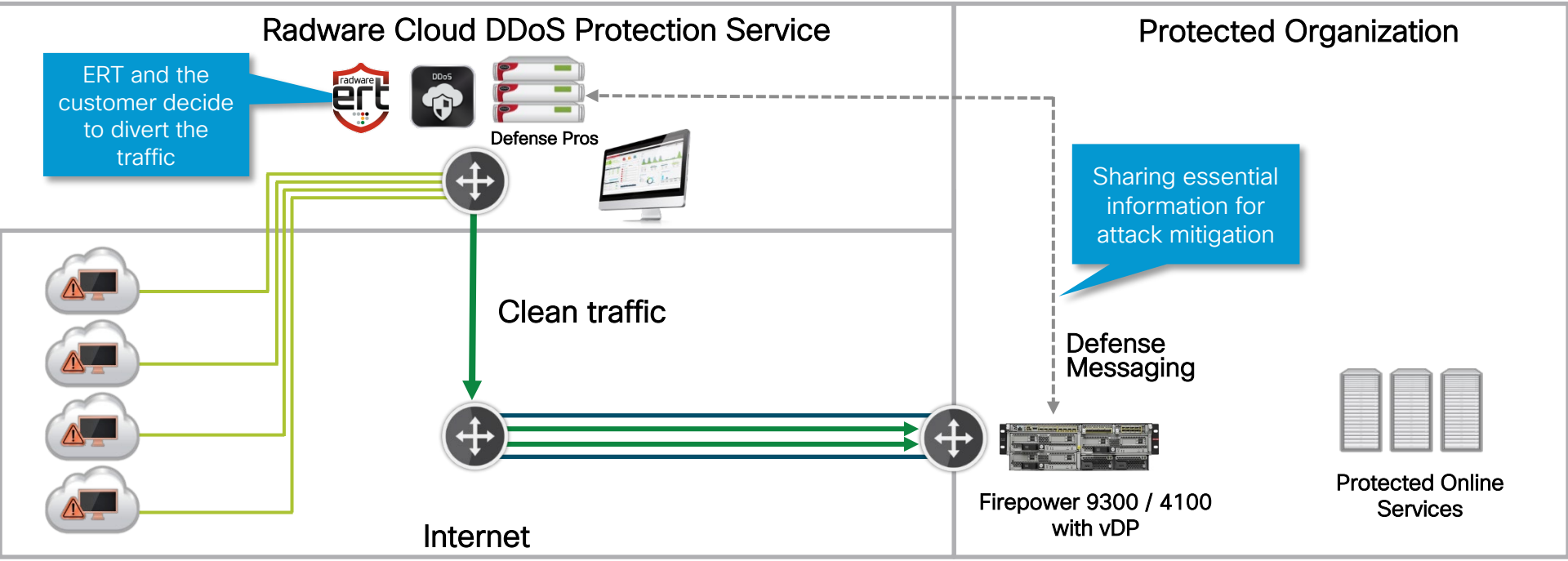
No.	Time	Source	Destination	Protocol	Length	Info
1	2019-01-11 13:57:29…	192.168.1.155	192.168.2.155	ICMP	106	Echo (ping) request id=0x467c, seq=1/256, ttl=64
2	2019-01-11 13:57:29…	192.168.1.155	192.168.2.155	ICMP	112	Echo (ping) request id=0x467c, seq=1/256, ttl=64

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-01-11 13:57:29…	192.168.1.155	192.168.2.155	ICMP	112	Echo (ping) request id=0x467c, seq=1/256, ttl=64
2	2019-01-11 13:57:29…	192.168.1.155	192.168.2.155	ICMP	112	Echo (ping) request id=0x467c, seq=1/256, ttl=64
3	2019-01-11 13:57:29…	192.168.1.155	192.168.2.155	ICMP	112	Echo (ping) request id=0x467c, seq=1/256, ttl=64
4	2019-01-11 13:57:29…	192.168.1.155	192.168.2.155	ICMP	112	Echo (ping) request id=0x467c, seq=1/256, ttl=64

Hybrid Inline & Cloud DDoS Mitigation Use Case



Hybrid Inline & Cloud DDoS Mitigation Use Case



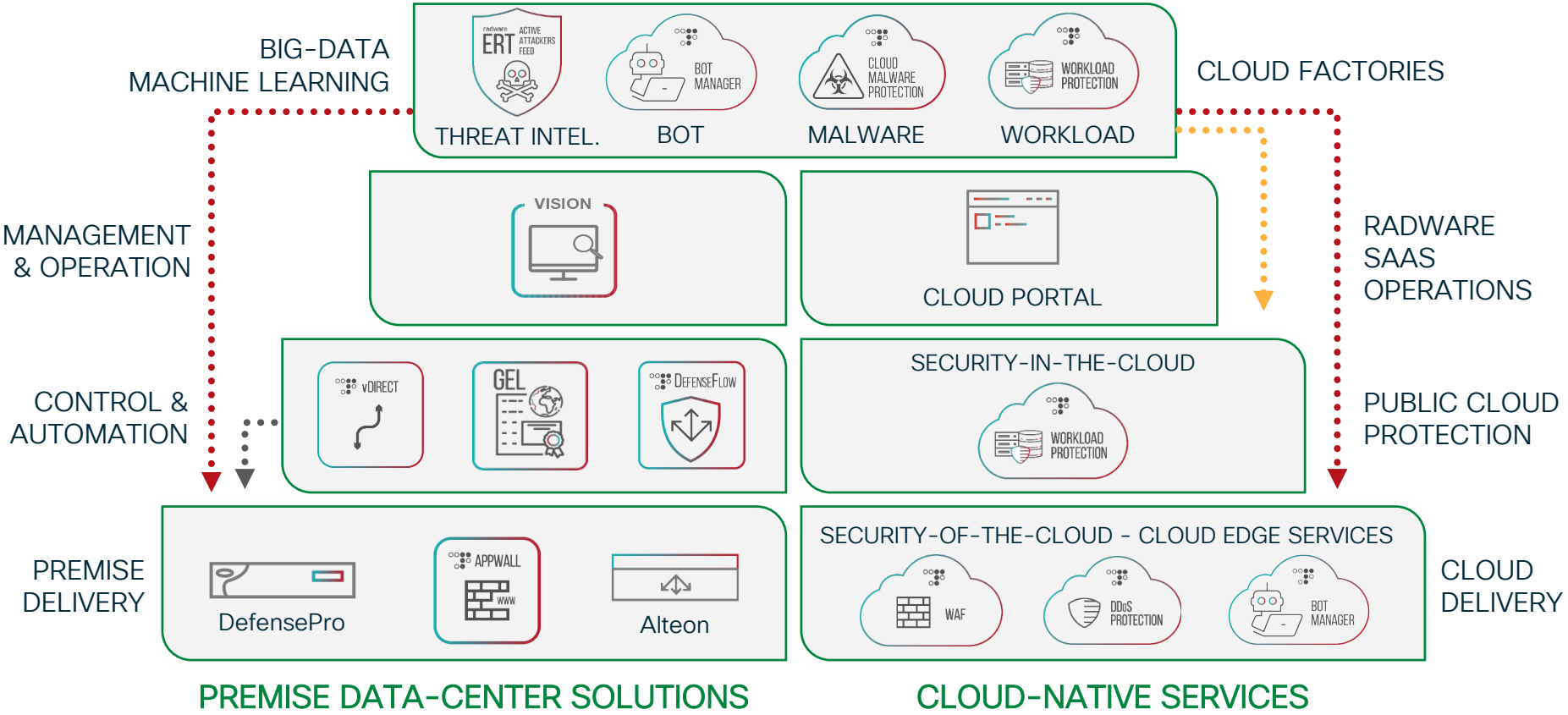
Demo 2

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

Radware Portfolio



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

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

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

BRKSEC-3035
Firepower Platforms Deep Dive

BRKSEC-2056
Threat Centric Network Security

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

BRKSEC-3093
ARM yourself using NGFWv in AZUR

BRKSEC 2348
Deploying AC with FP

BRKSEC-3300
Advanced IPS Deployment with Firepower NGFW

BRKSEC 2020
Deploying FP Tips and Tricks

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

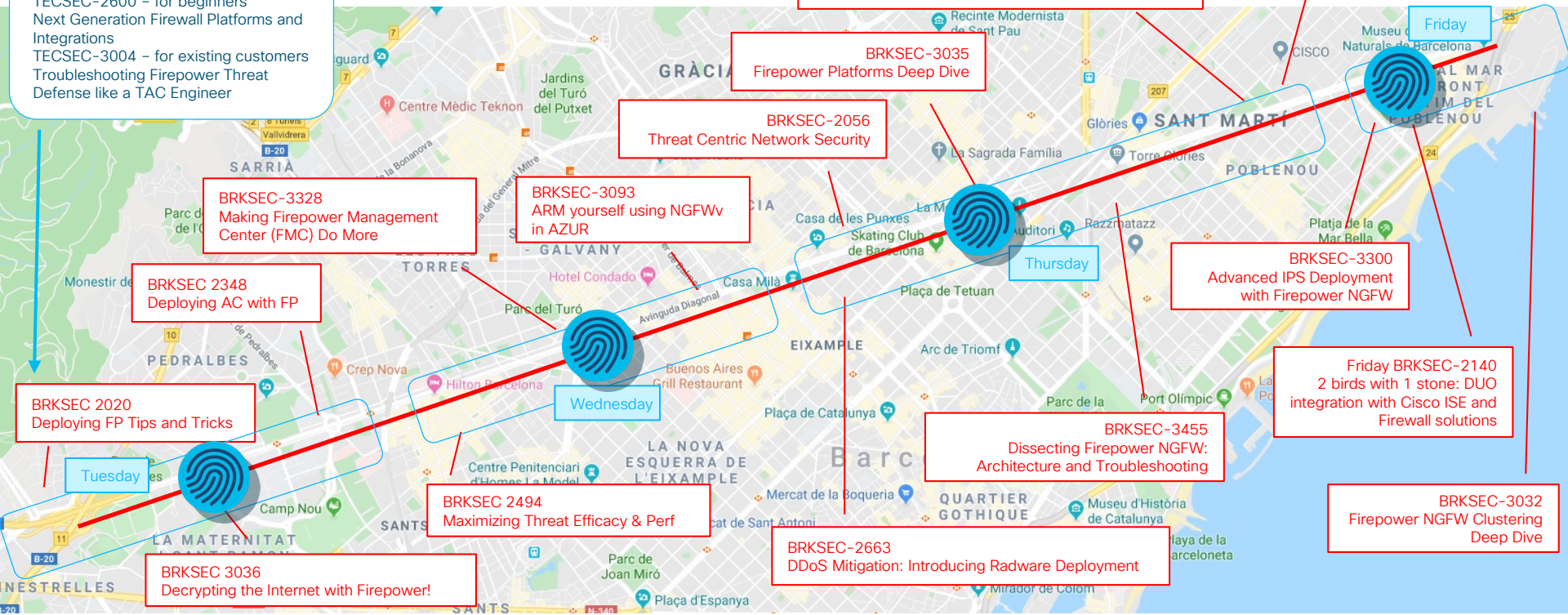
BRKSEC-3455
Dissecting Firepower NGFW: Architecture and Troubleshooting

BRKSEC 2494
Maximizing Threat Efficacy & Perf

BRKSEC-3032
Firepower NGFW Clustering Deep Dive

BRKSEC-2663
DDoS Mitigation: Introducing Radware Deployment

BRKSEC 3036
Decrypting the Internet with Firepower!



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

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**