The bridge to possible

DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Olga Yakovenko, Leader, Customer Delivery, ThousandEyes

Session Abstract

The distributed denial of service (DDoS) attack is one of the oldest criminal activities on the web. In today's world DDoS attacks continue to evolve and grow larger than ever. By integrating Radware Virtual Defense Pro (vDP) with the Cisco Firepower Appliances, users can achieve higher protection against application vulnerability exploitation, network anomalies and downtime. This session will provide an overview of Radware vDP and its capabilities, focusing on recently added and most used vDP features and include demonstrations on how to implement some of the Radware features to protect against DDoS threats. It is recommended for participants to have a working knowledge of Firepower platform architecture and to review previous BRKSEC-2663 session recordings.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- The Biggest DDoS Attacks 2022
- DoS/DDoS Mitigation with Radware vDP
- Radware vDP 8.22.2: What's New?
- Radware vDP HTTPS Flood Protection
- Radware vDP Next Generation DNS Protection
- Cloud DDoS Mitigation & SecureX Integration
- Conclusion

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

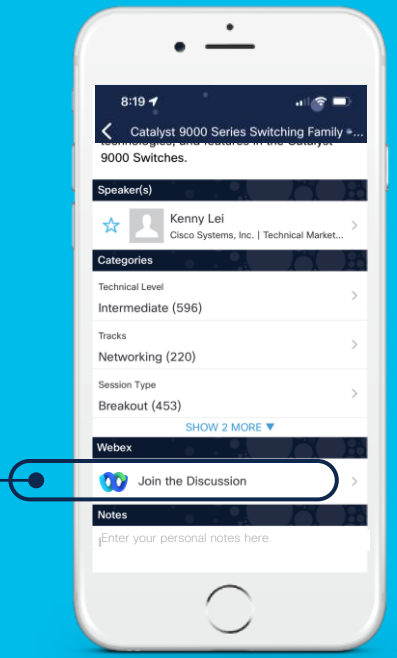
Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



Webex spaces will be moderated until February 24, 2023.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Key Point to Remember

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

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Your Speaker for Today

Olga Yakovenko

olhayako@cisco.com

Leader, Customer Delivery, ThousandEyes

CISCO CERTIFIED CCIE SECURITY

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Welcome Virg Santos!

Virg Santos

vidossan@cisco.com

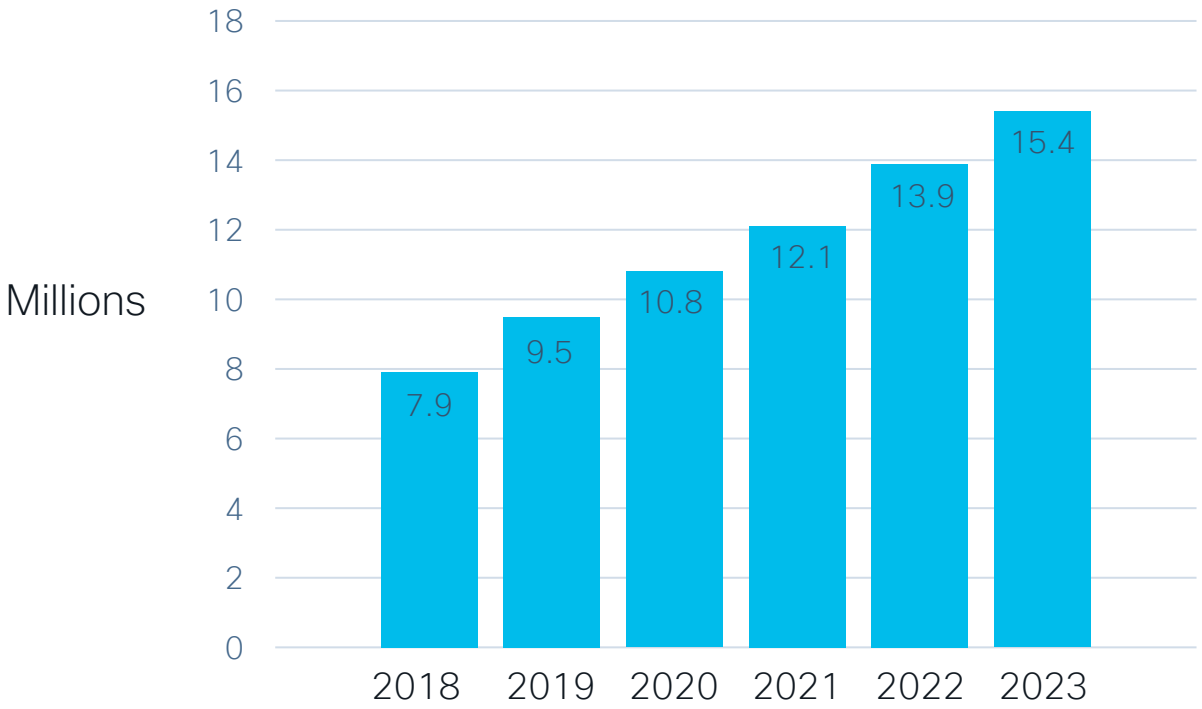
Virg.Santos@radware.com

Business Development Solutions Architect

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Biggest DDoS Attacks 2022

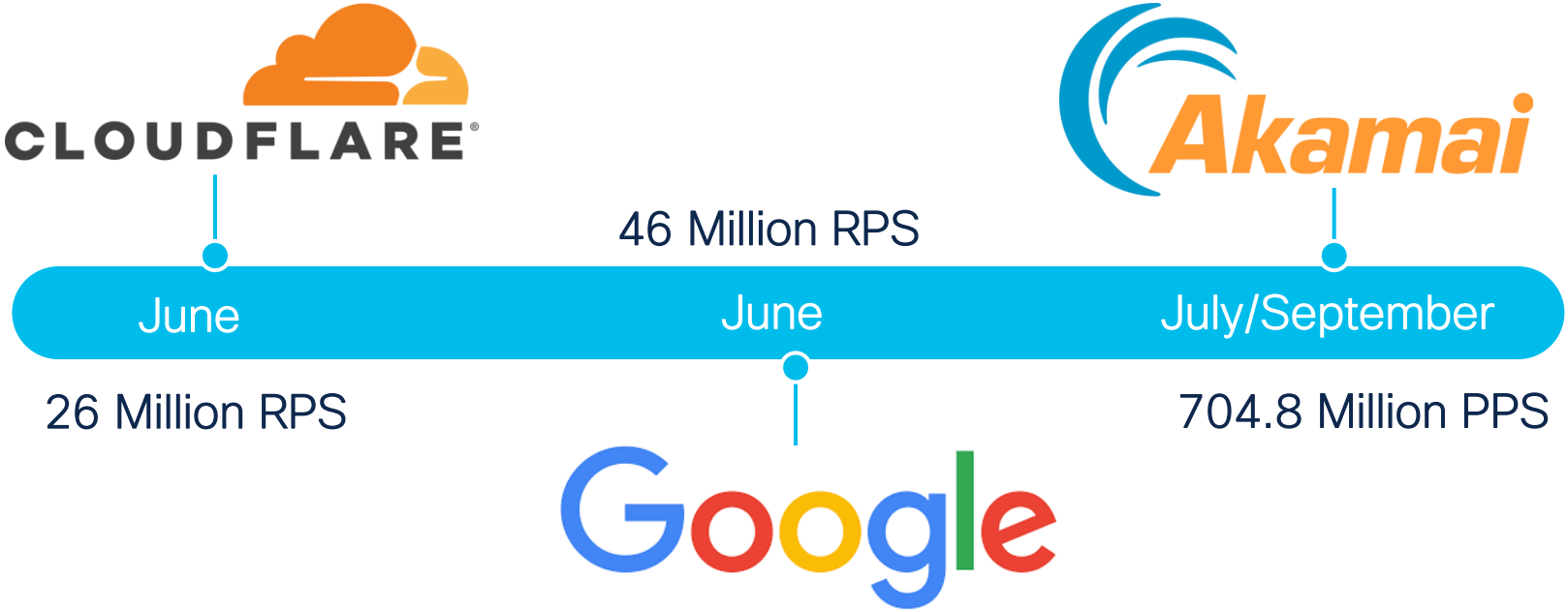
Number of DDoS Attacks Prediction



Source: Cisco Annual Internet Report, 2018–2023

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Biggest DDoS Attacks 2022



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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€	90.00€
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

DDoS-as-a-Service Pricing Example

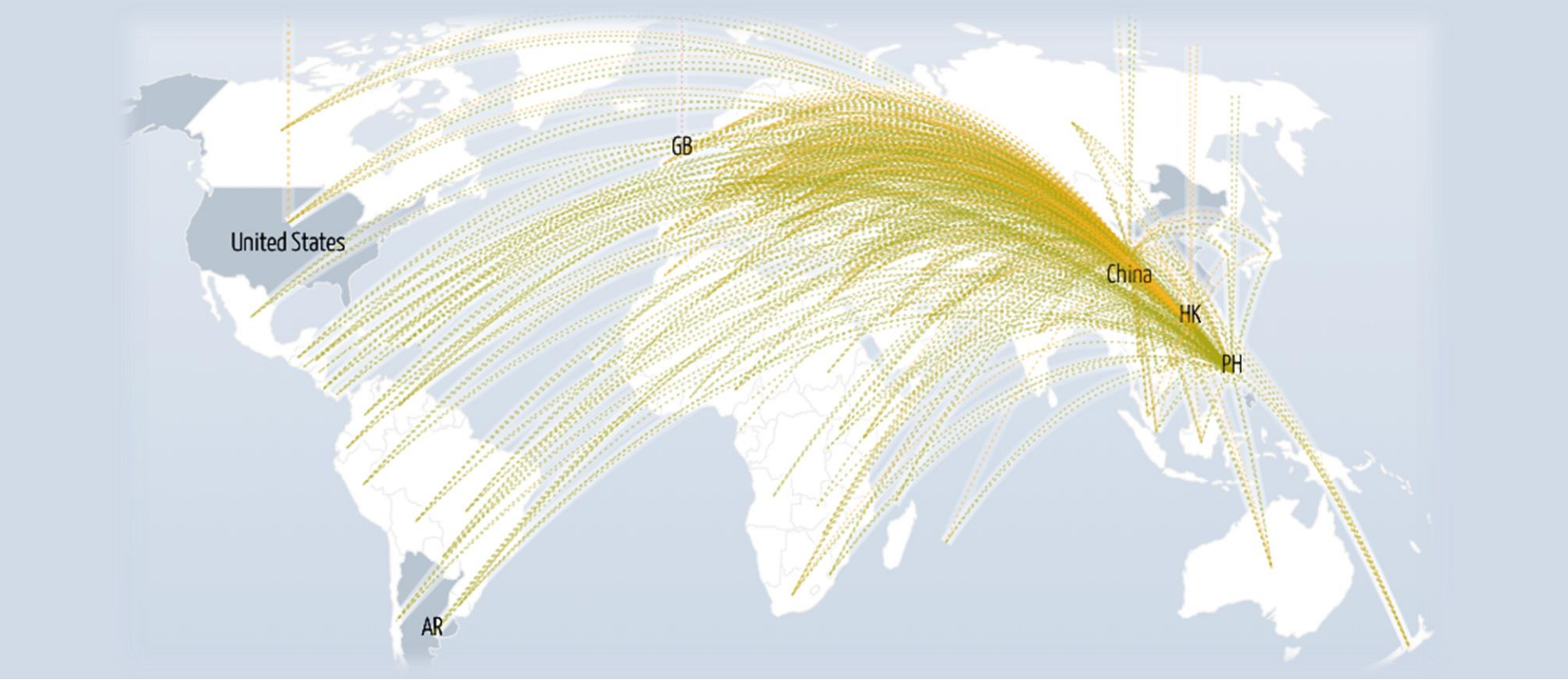
Coffee & Espresso

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
Cafe 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.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



Top Daily DDoS Attacks Worldwide

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

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Business Impact of Denial of Service

Business Impact

Inability to access the network and applications results in loss of online revenues

100ms of Latency = 7% Drop in Conversion Rate

Brand Damage

Data breaches destroy trust, impacting business and financial performance

30% average churn after a breach

$100K average investment to win back customers

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

DoS/DDoS Mitigation with Radware vDP

DoS/DDoS Mitigation with Radware vDP

Real-time attack prevention device

First 3rd Party component of the new architecture

KVM-based platform

Provides DoS/DDoS detection and mitigation

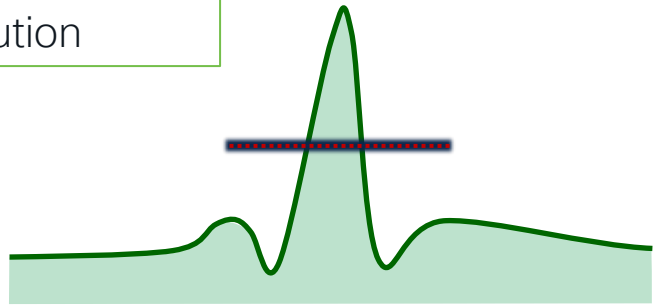
Install on Cisco ACI (APIC), Secure Firewall, UCS

radware

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

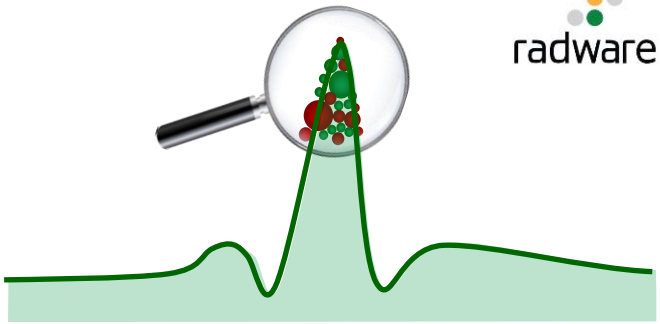
DoS/DDoS Mitigation with Radware vDP

Non-Radware Solution



Rate-Based Detection

High false positives



Behavioral Detection

Low false positives

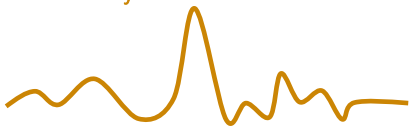
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

DoS/DDoS Mitigation with Radware vDP

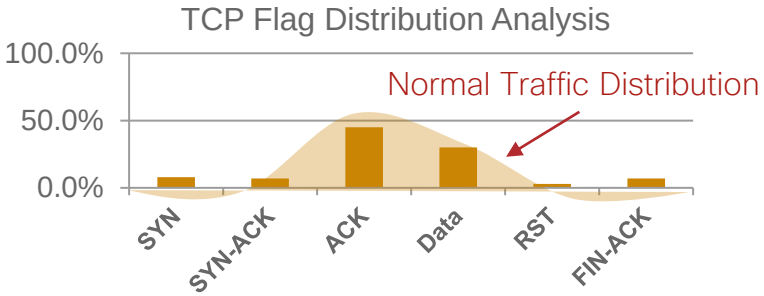
Learning → Detection → Characterization → Mitigation

Good Traffic

Rate Analysis

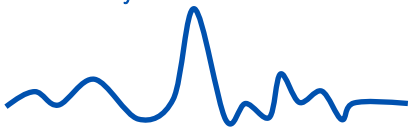


+

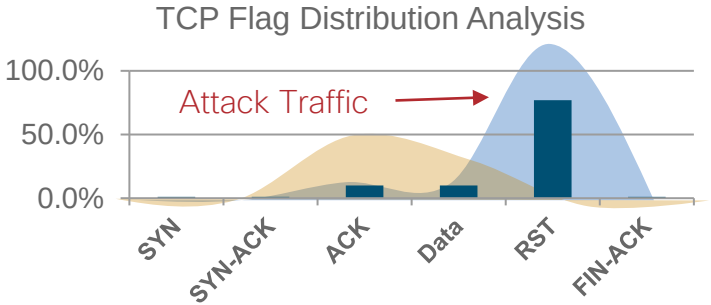


Attack Traffic
(RST Flood)

Rate Analysis



+



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware vDP 8.22: What's New?

cisco Live!

What is vDP 8.22 for Cisco Secure Firewall?

- vDP version 8.22.2.0 replaces version 8.13.01
- Existing customers can download vDP 8.22 for free from Cisco
- vDP 8.22.2.0 requires FXOS version 2.8.1+ and FTD – 6.6.0+

radware

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enhanced DDoS Capabilities in vDP 8.22

A few of the new features now available to Cisco Secure Firewall customers:

- Anti-Scanning Protection
- Burst-Attack Protection
- Carpet-Bombing Protection
- Connection PPS Protection
- HTTPS Flood Protection
- Subscription Services:
  - Geolocation Protection
  - ERT Active Attackers
  - SUS
- Traffic Filters
- And many more…

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enhanced DDoS Capabilities in vDP 8.22

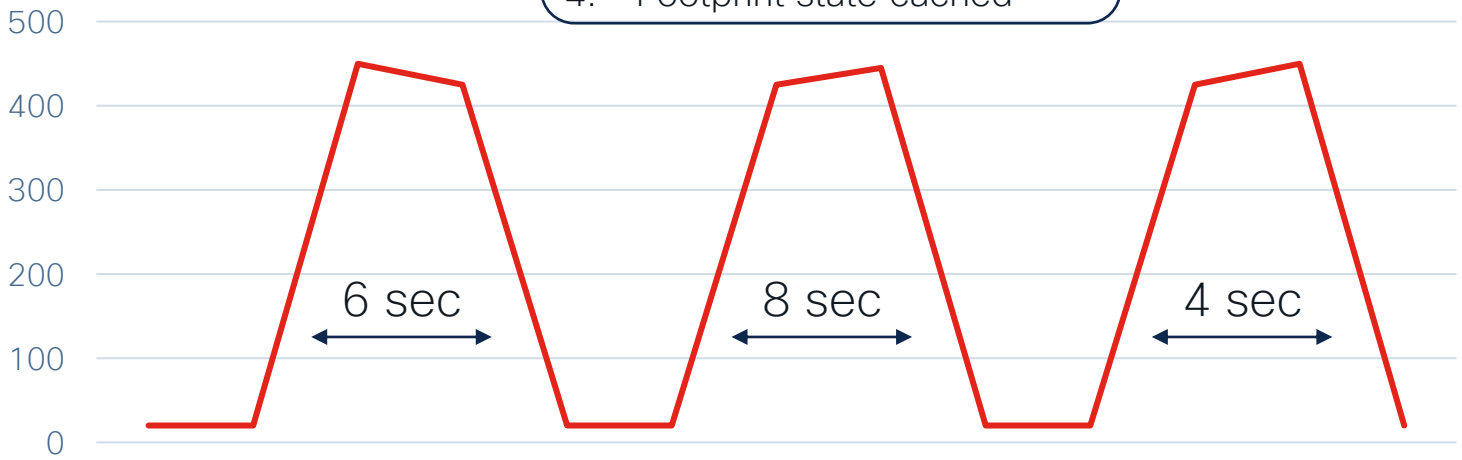
A few of the new features now available to Cisco Secure Firewall customers:

- Anti-Scanning Protection
- Burst-Attack Protection
- Carpet-Bombing Protection
- Connection PPS Protection
- HTTPS Flood Protection
- Subscription Services:
  - Geolocation Protection
  - ERT Active Attackers
  - SUS
- Traffic Filters
- And many more…

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Burst-Attack Protection

1. DoA High
2. Footprint creation continues
3. DoA Low
4. Footprint state cached

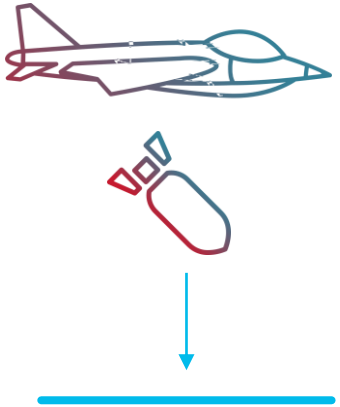


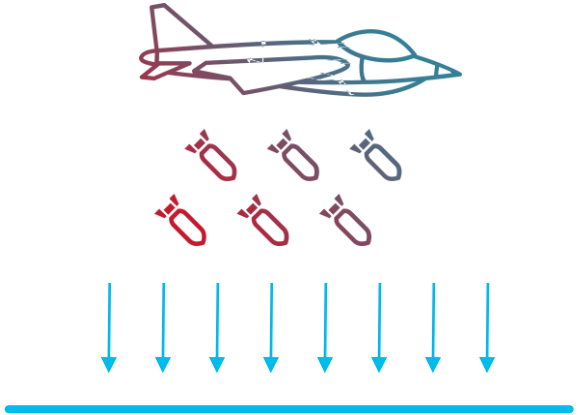
1. DoA High
2. Footprint creation starts
3. DoA Low
4. Footprint state cached

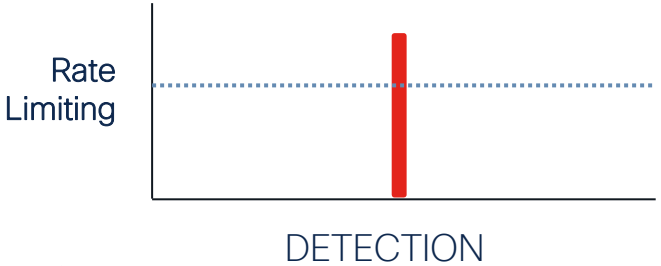
1. DoA High
2. Footprint creation completed
3. Attack blocked

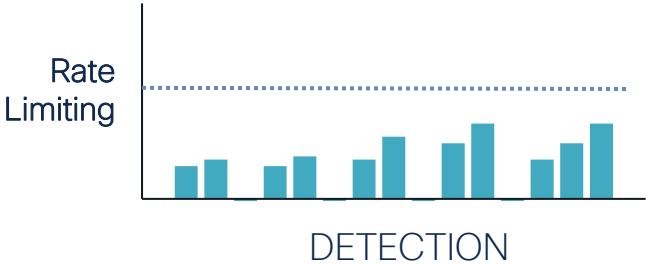
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Carpet-Bombing Attacks





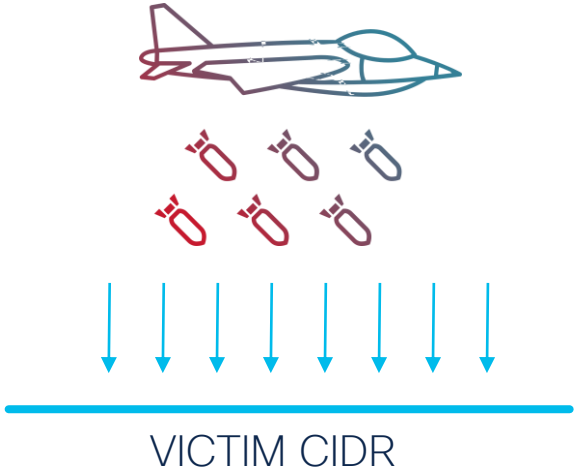


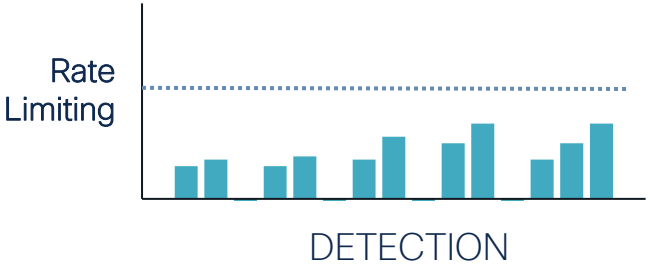


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Spoofed SYN Attack Protection

- Spoofed SYN Attack Protection handles carpet-bombing attacks.
- SYN packets are tracked for all the protected subnet
- Includes 2 methods for tracking SYN packets:
  - Tracking per Destination IP Address
  - Spoofed SYN Attack Protection





© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware ERT Active Attackers Feed

Preemptive Protection
against known DDoS attackers

Data Correlation
across multiple Radware sources

Active Attackers
blocked in real time

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware ERT Active Attackers Feed

Draws intelligence data from three main sources:

- Radware's Cloud Security Services
- Radware's Global Deception Network
- Emergency Response Team (ERT)

Generates a validated list of IPs involved in active DDoS attacks

In real-time, that list is downloaded to Radware's Attack Mitigation Solution, enabling it to block attacks before they target the network.

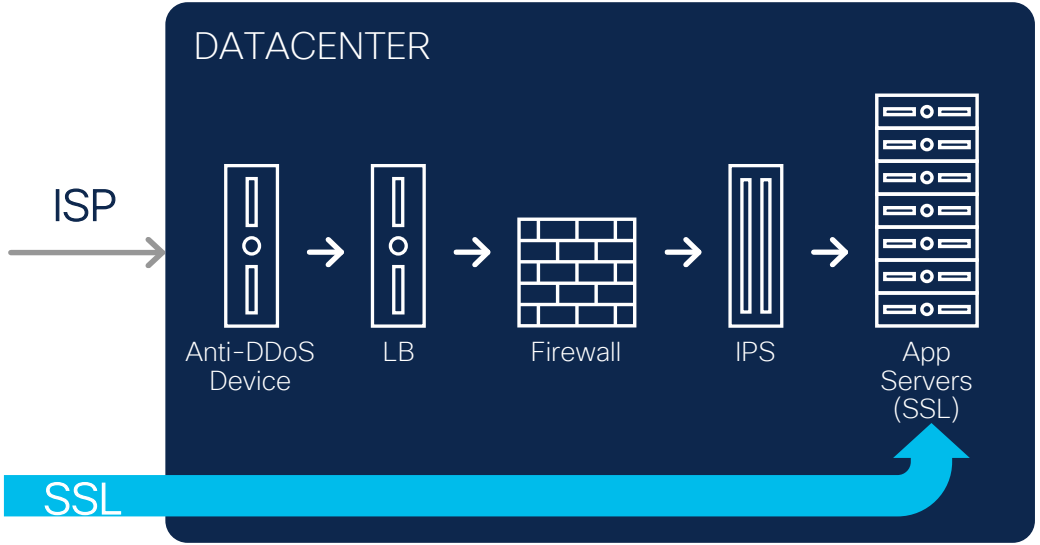
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware vDP HTTPS Flood Protection

Encrypted DDoS Attacks

Application-layer DDoS attacks using encrypted **HTTPS floods** are increasing all the time

SSL floods can overwhelm the stateful SSL encryption/decryption appliances in the network



ENCRYPTED DDoS ATTACK FLOWS ARE HARD TO DETECT AND MITIGATE

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Challenges of Protecting Against SSL DDoS Attacks

1. Accurate SSL attack detection

2. Accurate SSL attack mitigation

3. Price of full SSL inspection

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware SSL Protection Solution

Keyless SSL Protection

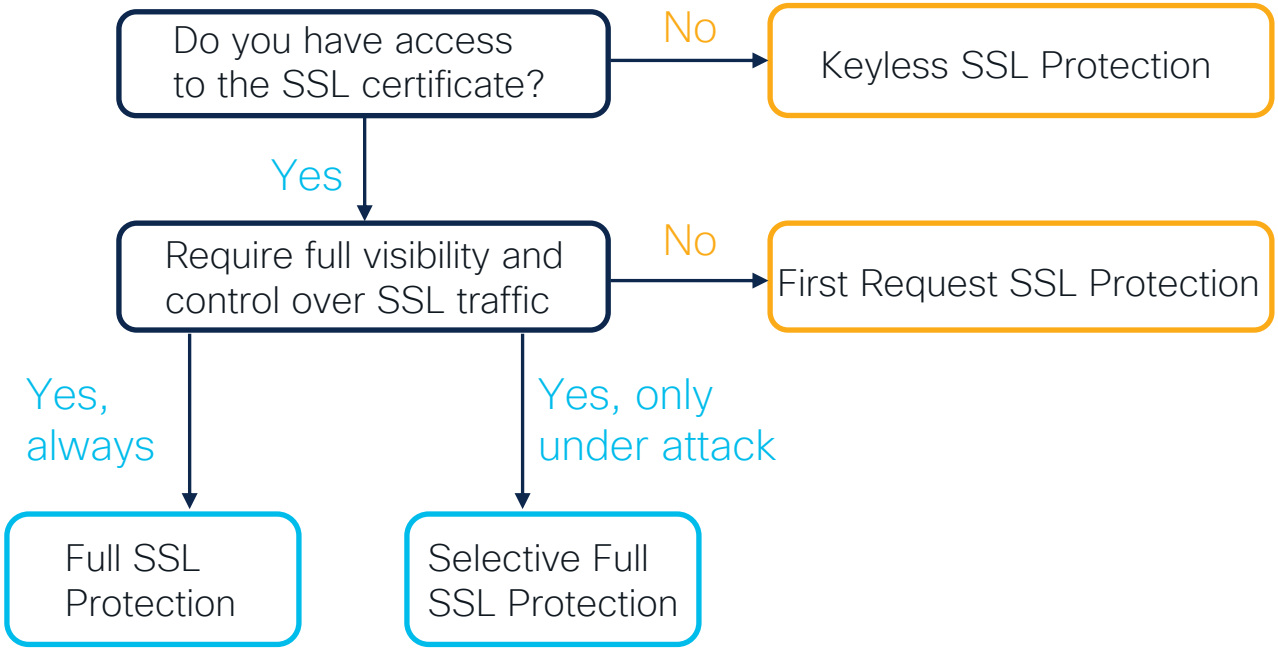
First Request SSL Protection

Selective Full SSL Protection

Full SSL Protection

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

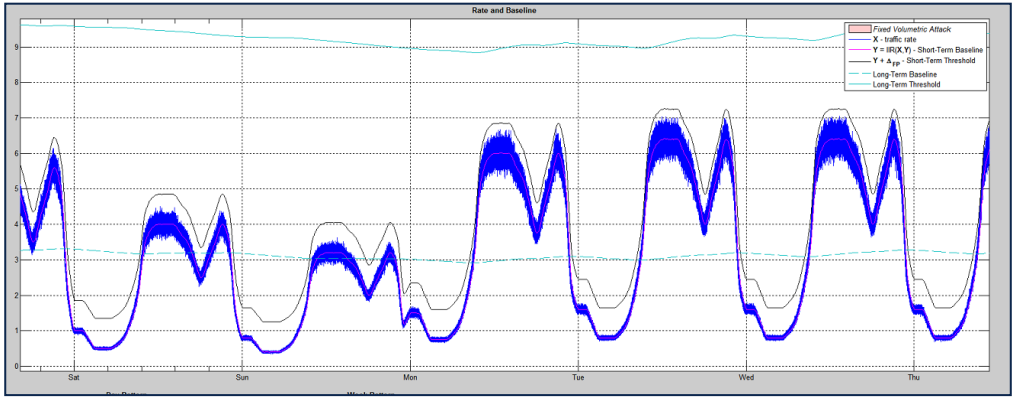
SSL DDoS Attack Protection



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Learning Phase – Establish Baselines

- Two baselines are continuously calculated:
  - **Long-term** baseline – Requires approx. 1 week of learning
  - **Short-term** baseline – Requires approx. 1 hour of learning
- **Attack is triggered** based on one of the two baselines



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detection Phase – Accurate Behavioral Detection

Internet

Protected Organization

SSL Attack

Firepower 9300 / 4100
with vDP

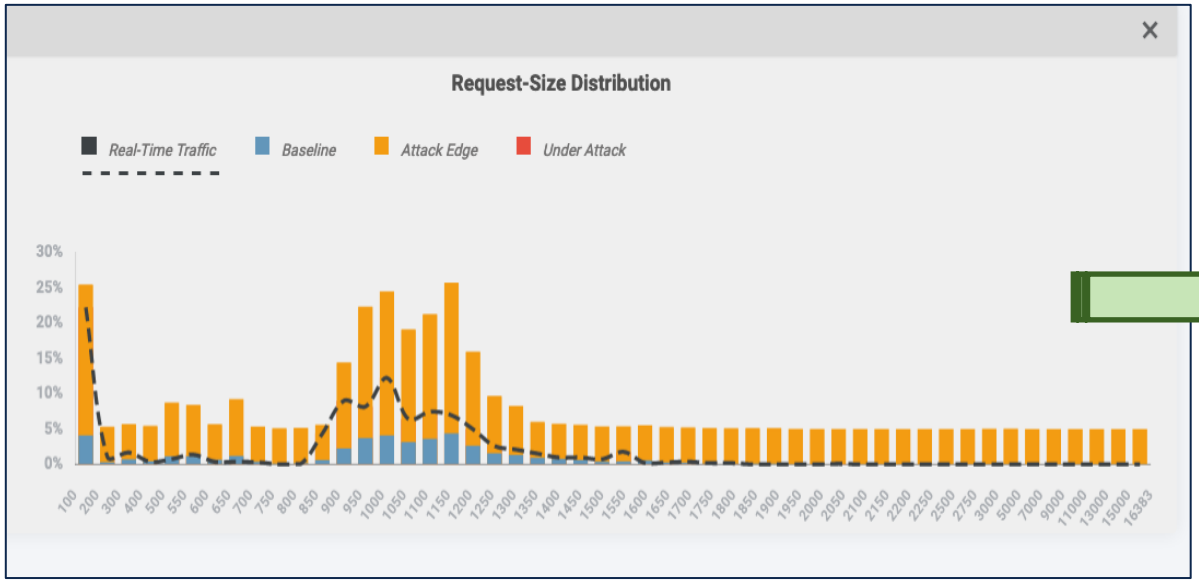
Protected Online
Services

Detection Mechanisms

- L4 – SYN/sec to a protected object
- L5 – SSL TPS, Request Size Distribution

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Characterization Phase – Isolate the Attack



After detection DefensePro automatically creates a list of **Suspicious Source IPs**

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mitigation Phase – Blocking Attack Traffic

Internet

Protected Organization

SSL Attack

Firepower 9300 / 4100
with vDP

Clean Traffic

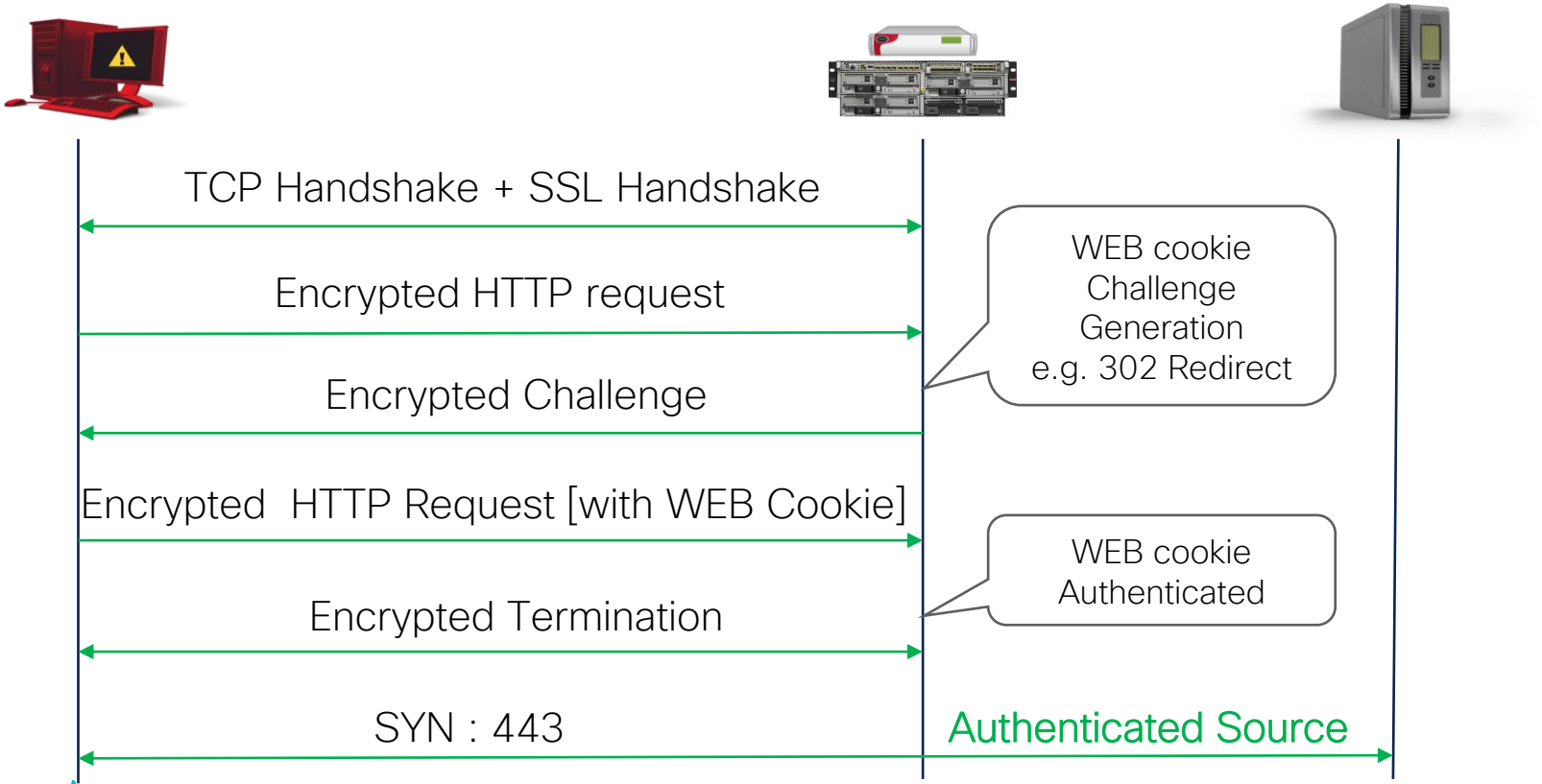
Protected Online
Services

Mitigation Mechanisms

- Rate Limit Traffic from Suspect Sources
- HTTPS Authentication on All Sources
- Full Session Decryption and Inspection

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Decryption Escalation – HTTPS Authentication



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

HTTPS Flood Protection Building Blocks

Detection

No Decryption!

Learn peacetime traffic characteristics

Establish baselines **per Protected SSL Object**

Characterization

No Decryption!

Track Sources and Isolate misbehaving ones (by **Source IP**)

Create **Suspect list**

Mitigation

Decrypt only if/when needed!

Apply mitigation actions:
- To Suspect list
- To All clients

Escalate Mitigation Action

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo 1

Protection Against DDoS attacks with HTTPS Engine

In this Demo we will...

- Configure the vDP HTTPS Flood Protection Profile and Protection Policy
- Initiate legitimate traffic to establish baseline
- Initiate the DDoS HTTPS Flood attack
- Verify the DDoS attack mitigation results

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware vDP Verification Commands

```
DefensePro#system internal security https source-table 100

Policy ID  | Source Ip          | Server IP          | Server Port  | State     | Rate  | Age     | SR
0            ::ffff:10.1.101.13   ::ffff:10.1.102.4      443          Legit       28      11.135    No SR
0            ::ffff:10.1.101.15   ::ffff:10.1.102.4      443          Attacker    28      11.135    80 rate
0            ::ffff:10.1.101.16   ::ffff:10.1.102.4      443          Suspect     28      11.135    Ex. Max
```

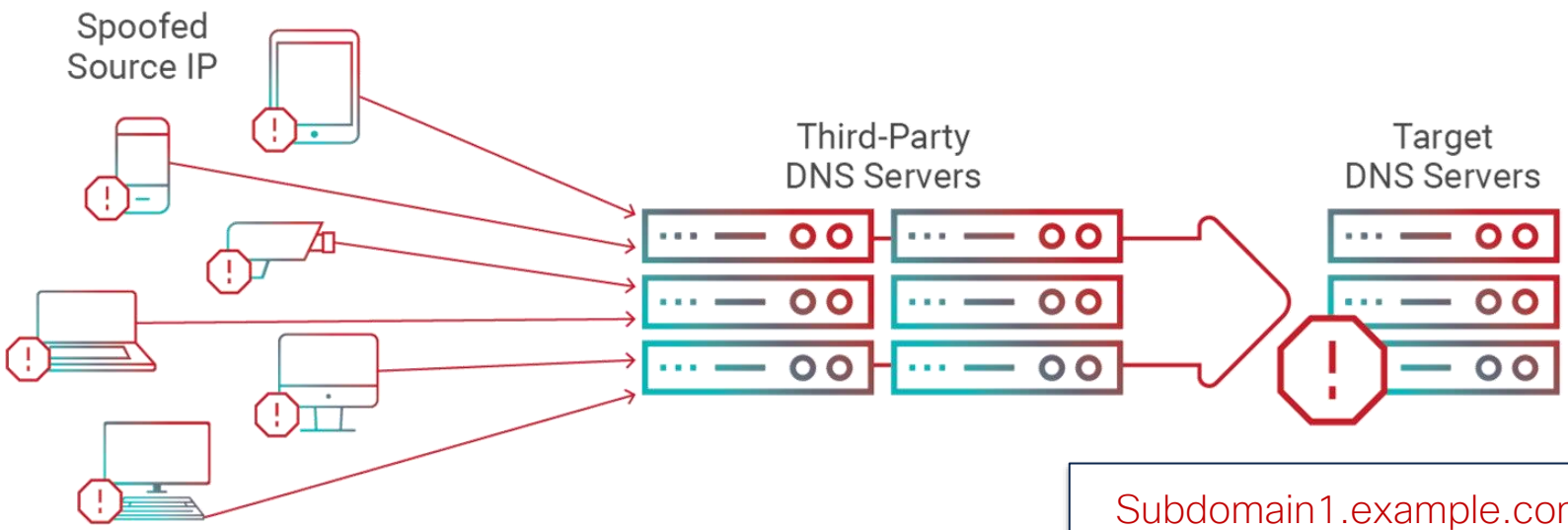
```
DefensePro#system internal security https baseline print 10.1.102.4 443 0

HTTPS baseline for server IP ::ffff:10.1.102.4 | port 443 | policy ID 0 | Server Name server | Server
State Learn & Detect
```

```
DefensePro#system internal security policyID

Policy VDP_Demo_Lab ID is 0
Policy VDP_Demo_Lab_Advanced ID is 1
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radware vDP Next Generation DNS Protection

DNS Amplification Reflective Attack

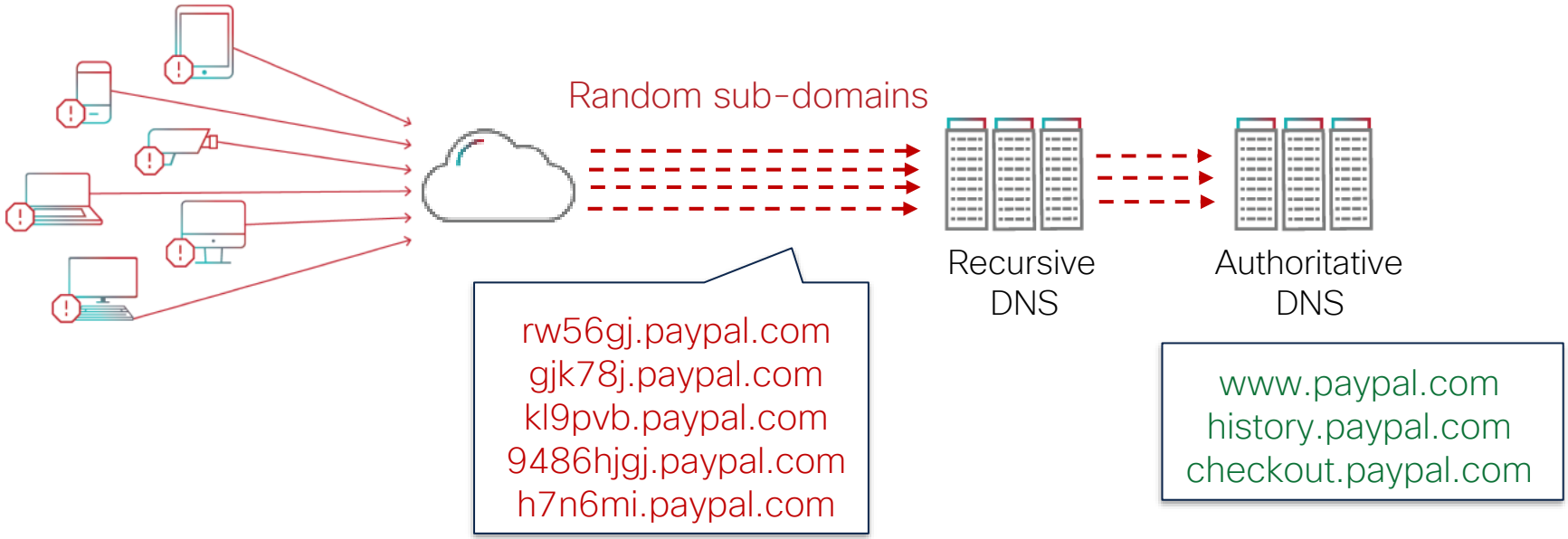


DNS query to get all records of example.com

Subdomain1.example.com IP
Subdomain2.example.com IP
Subdomain3.example.com IP
...
SubdomainX.example.com IP

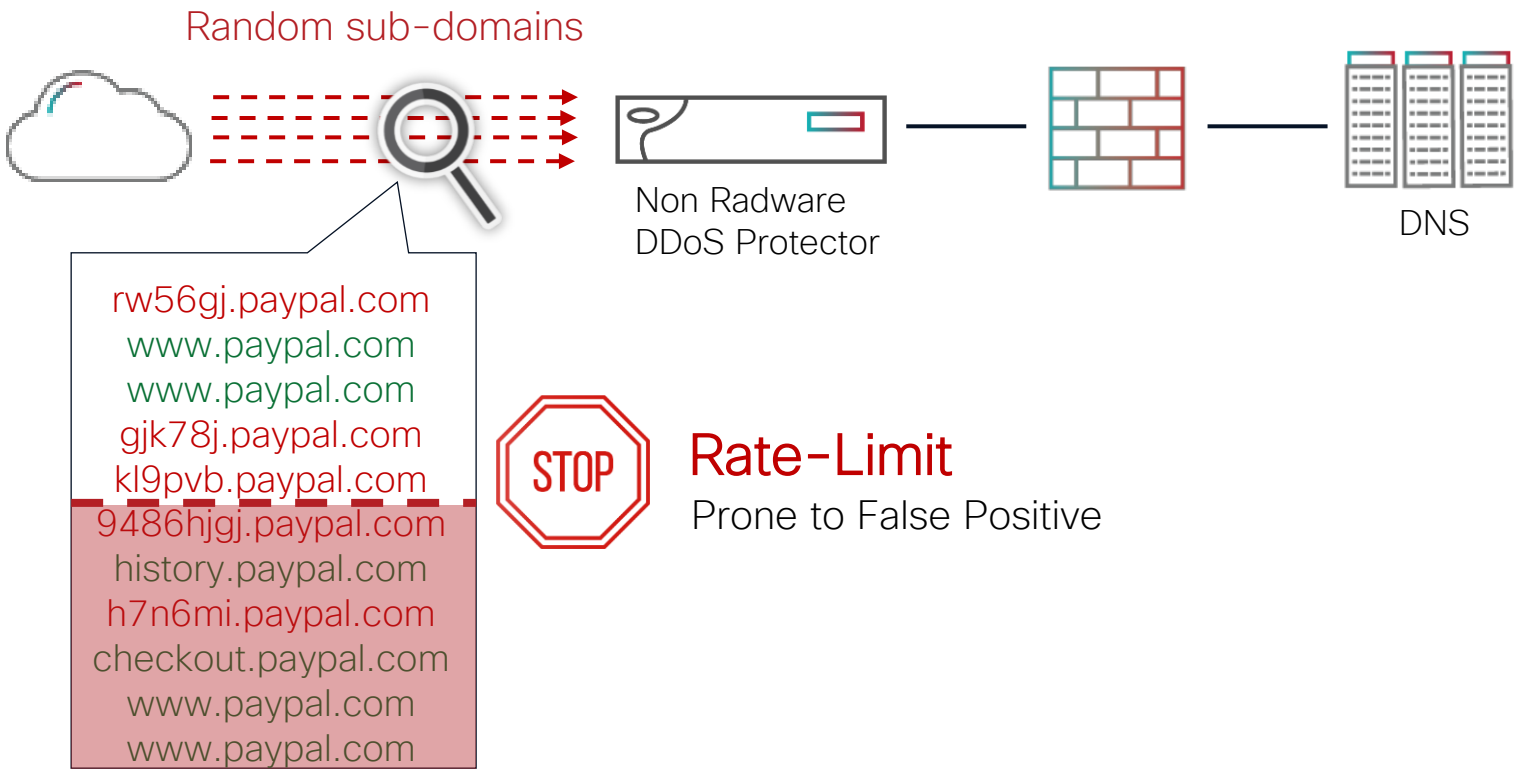
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Random Subdomains Attack



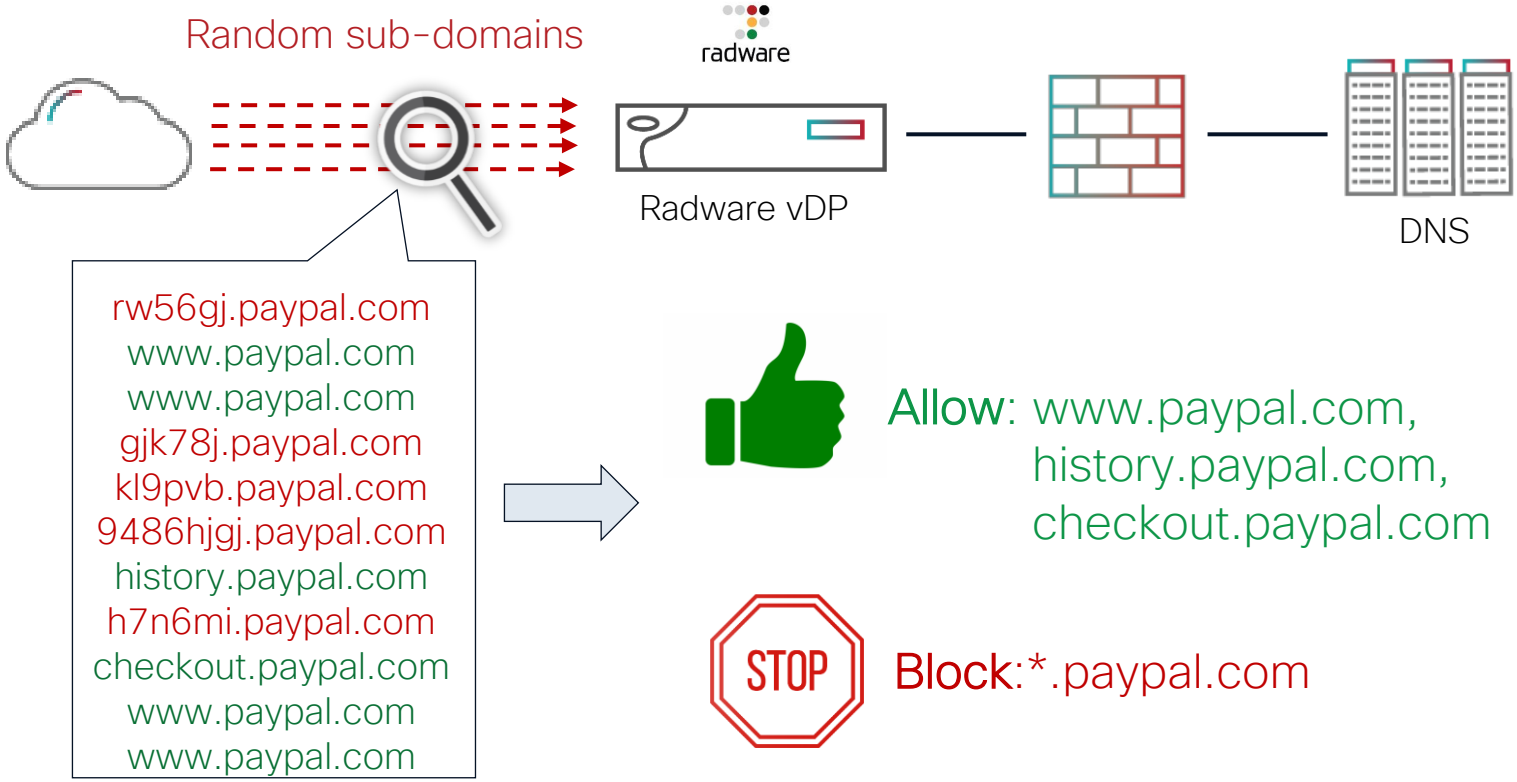
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Random Subdomains Attack – Query Rate Limiting



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Random Subdomains Attack – vDP DNS Protection



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detection

Radware vDP DNS Protection

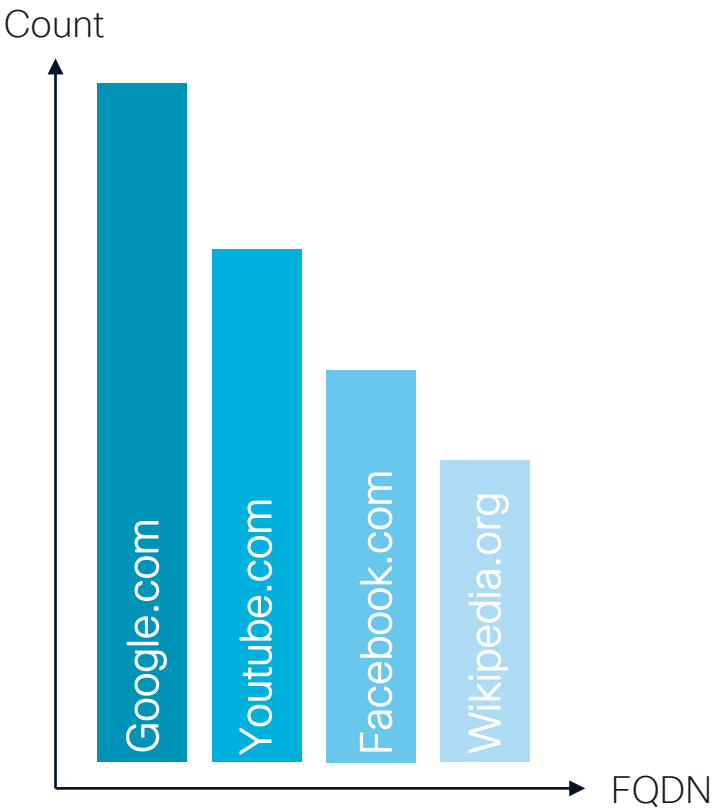
Rate Analysis
per DNS Query Type

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detection

Radware vDP DNS Protection

FQDN Analysis per Query Type

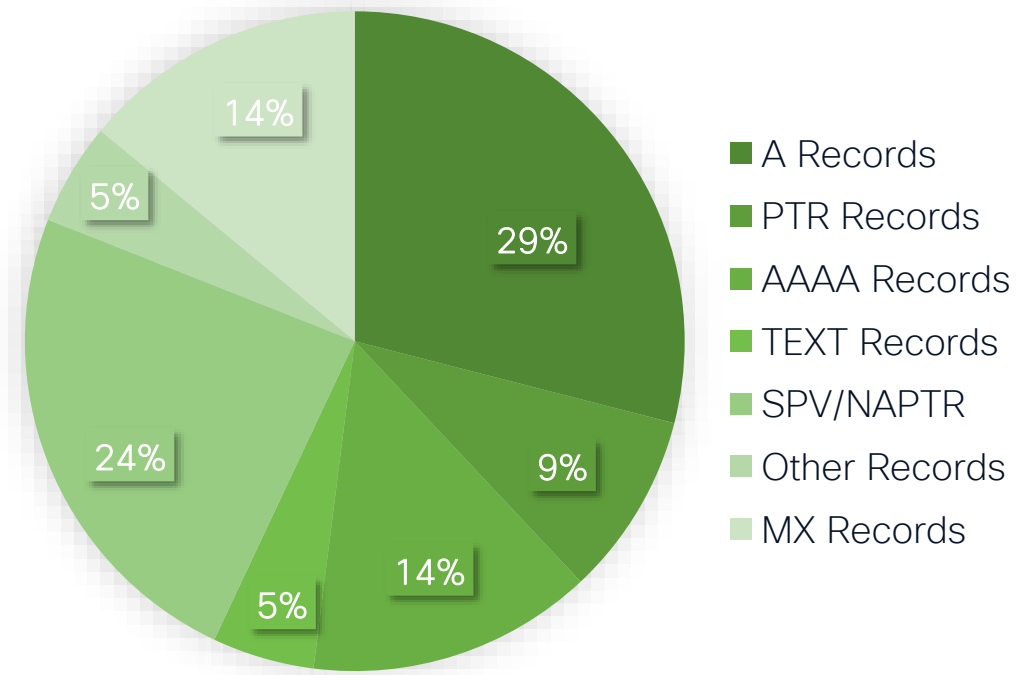


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detection

Radware vDP DNS Protection

DNS Query Distribution Analysis (Rate Invariant)



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Characterization

Radware vDP DNS Protection

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
- …

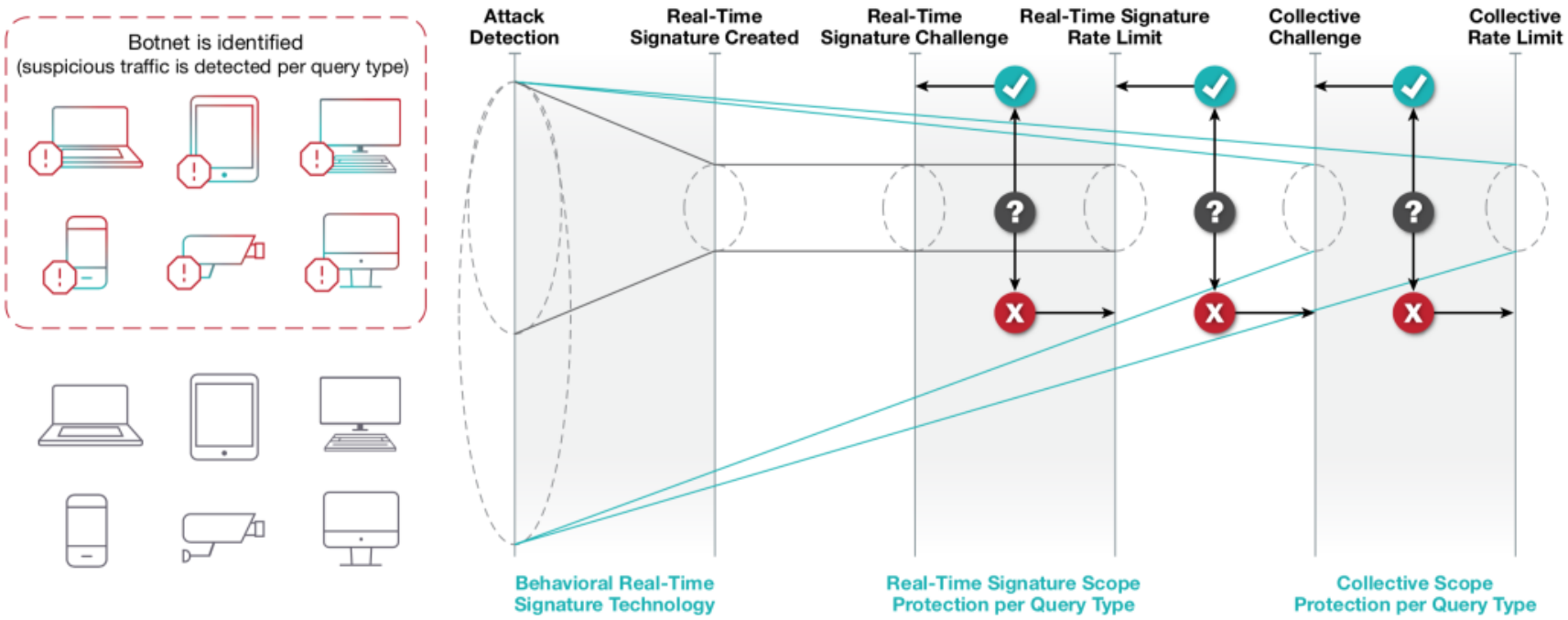
Automatic Real Time Signature Generation Module

Real Time Signature

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mitigation

Radware vDP DNS Protection



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo 2

Protection Against DDoS attacks with DNS Engine

In this Demo we will...

- Configure Subdomains whitelist as a part of DNS Flood Protection Profile
- Initiate legitimate traffic to establish baseline
- Initiate DNS Random Subdomains attack
- Verify the DDoS attack mitigation results

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

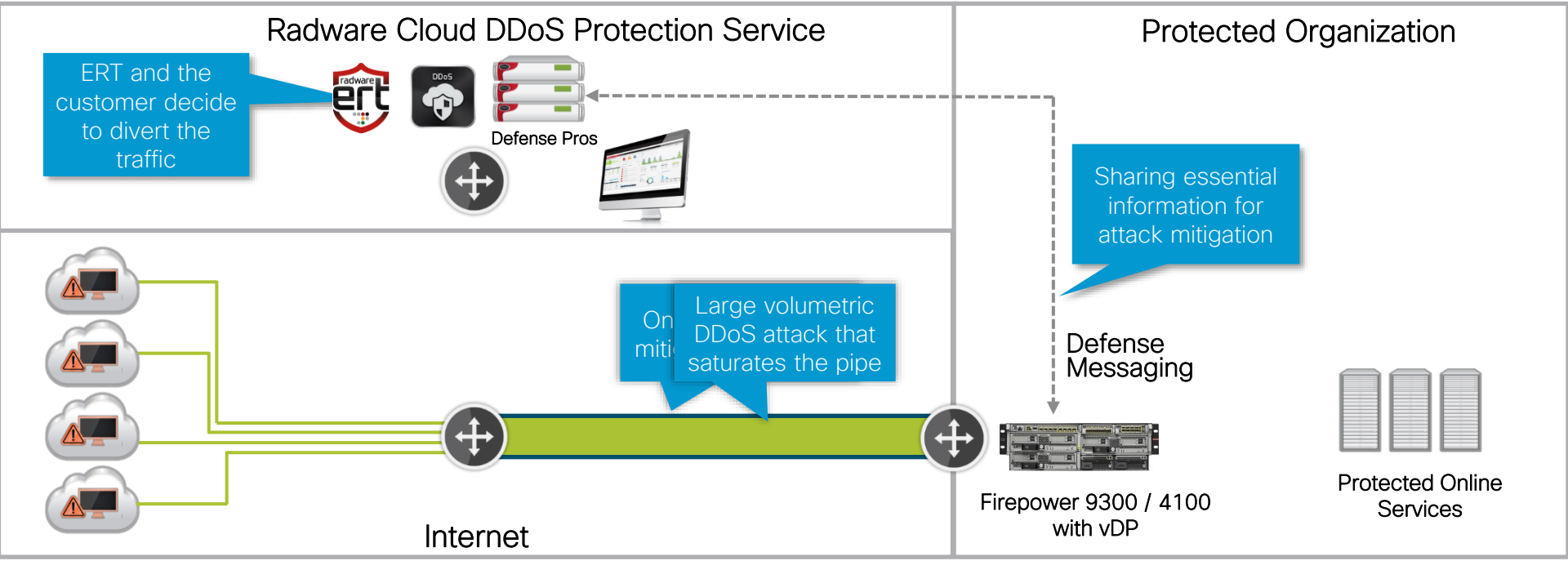
Radware vDP Verification Commands

```
DefensePro#system internal security dns attacks
DNS Protection Active Attacks:
[0] policy VDP_Demo_Lab, IPv4, protection DNS A, mitigation Signature Rate Limit
footprint for DNS A:
        DNS Sub Domain:
            vdplab.com
        AND

        DNS Flags:
            256
        AND

        Packet Size:
            77, 76, 80, 78, 75, 79
        AND
        Destination IP:
            155.1.102.4
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

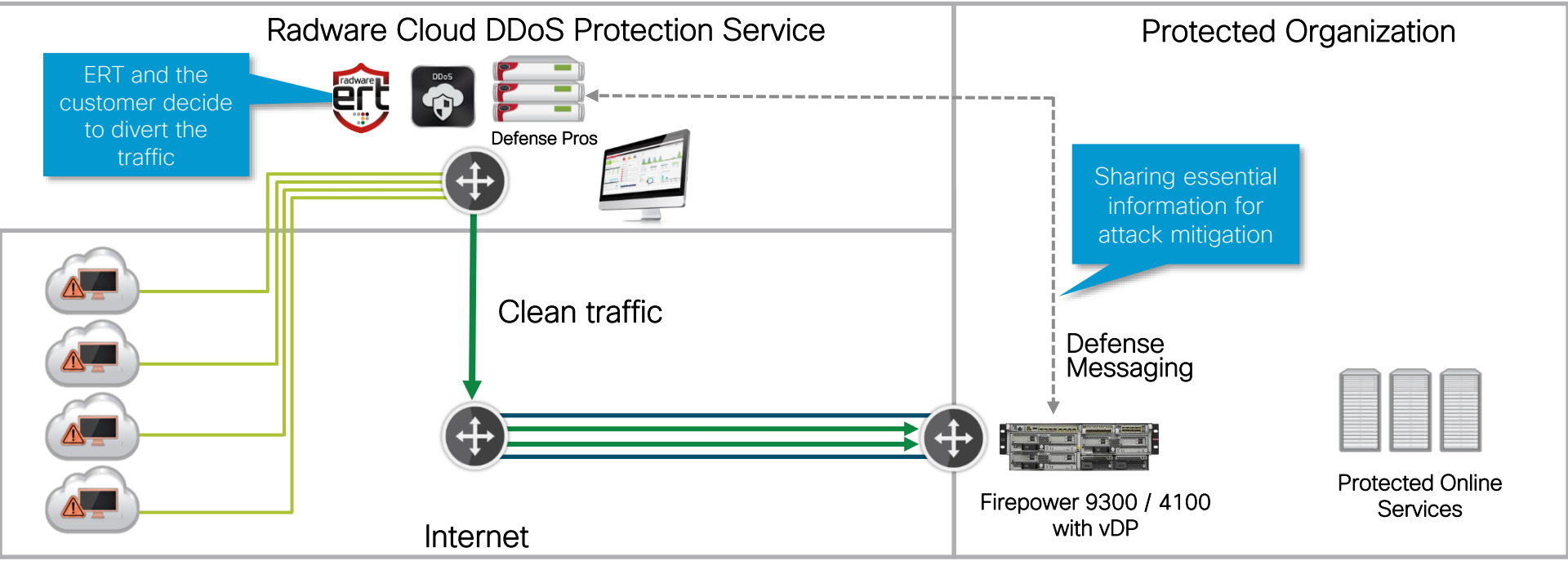
Cloud DDoS Mitigation & SecureX Integration

Hybrid Inline & Cloud DDoS Mitigation Use Case



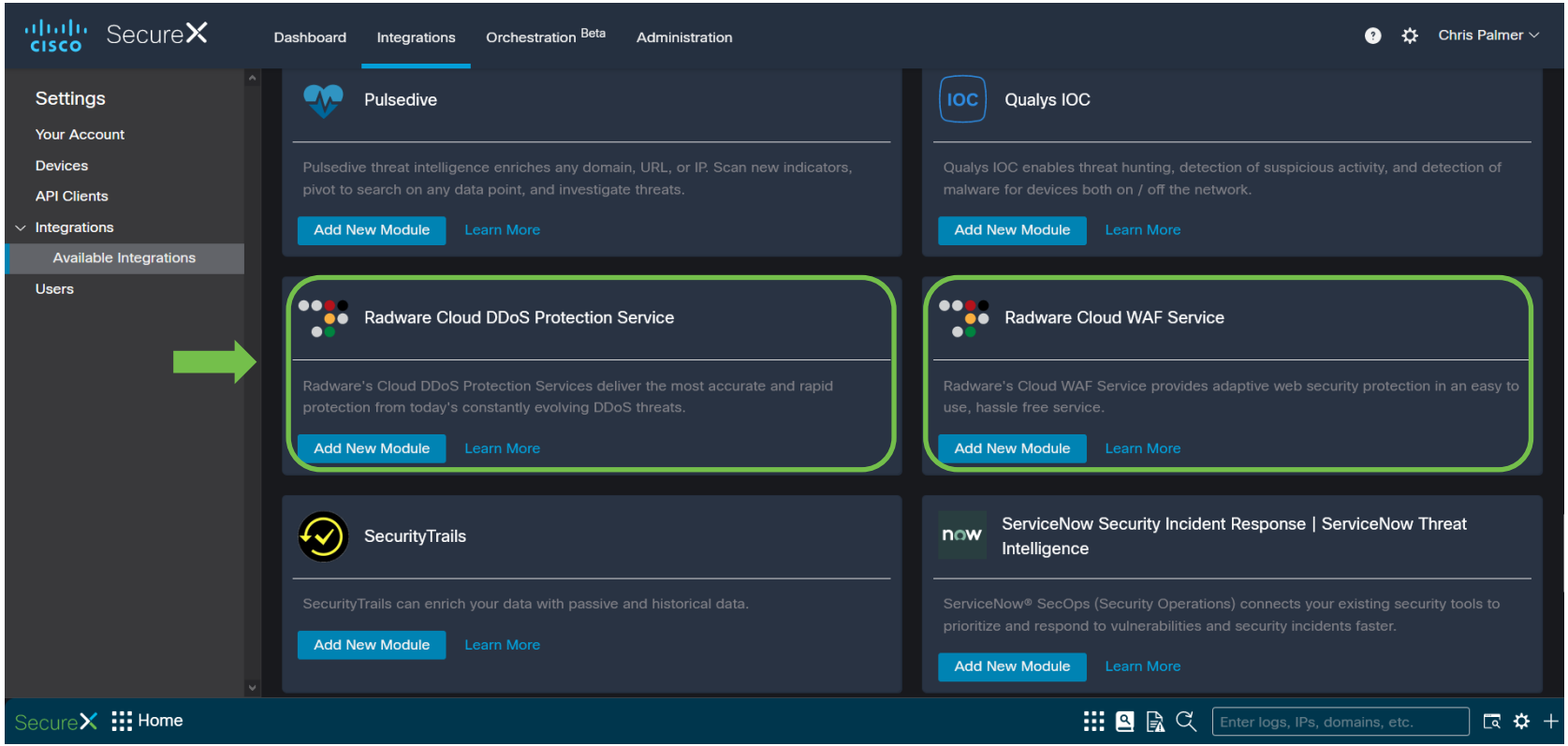
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hybrid Inline & Cloud DDoS Mitigation Use Case



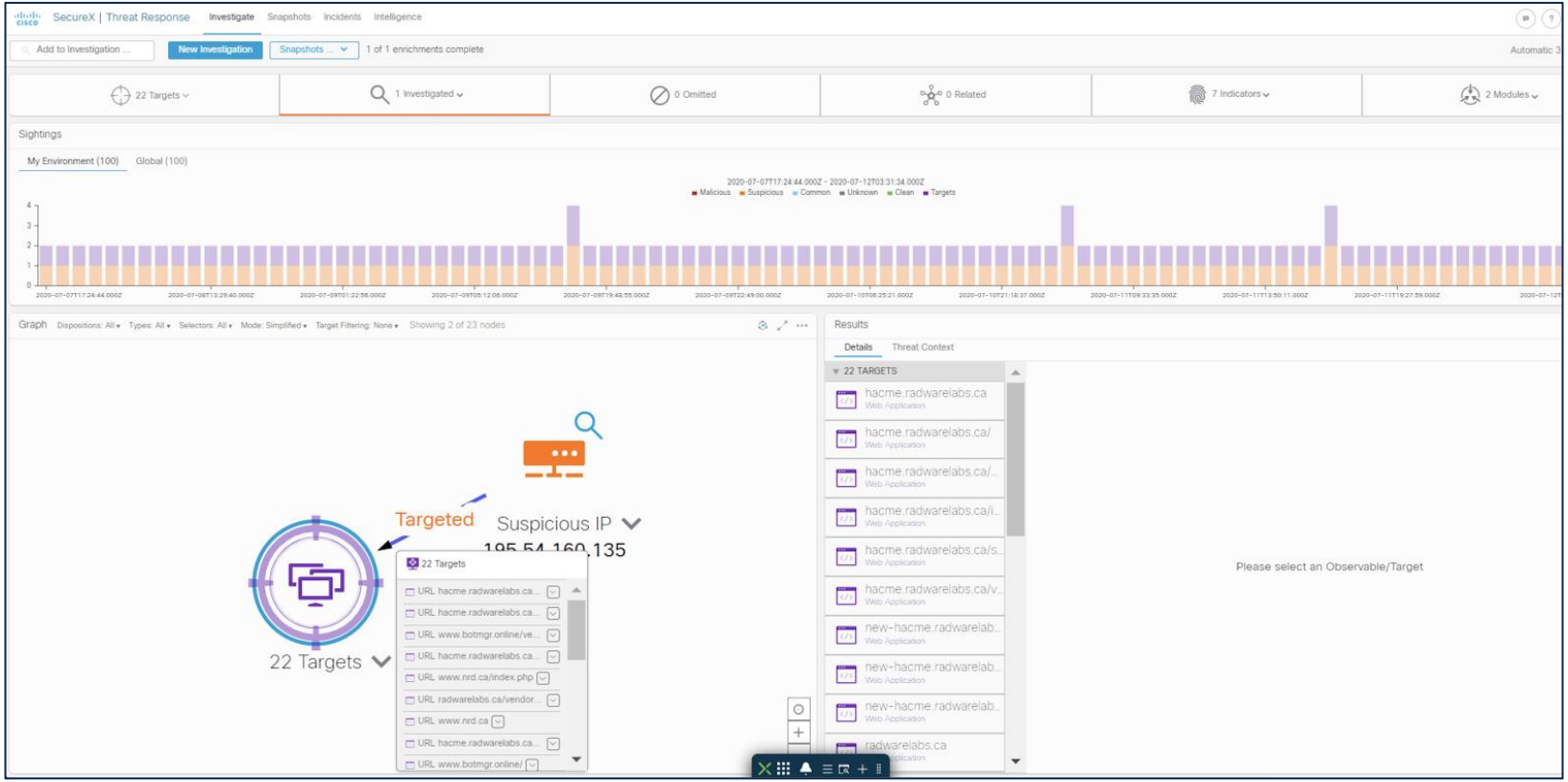
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud DDoS and WAF Integrations with SecureX



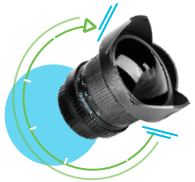
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud DDoS and WAF Integrations with SecureX



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud Security Services with SecureX



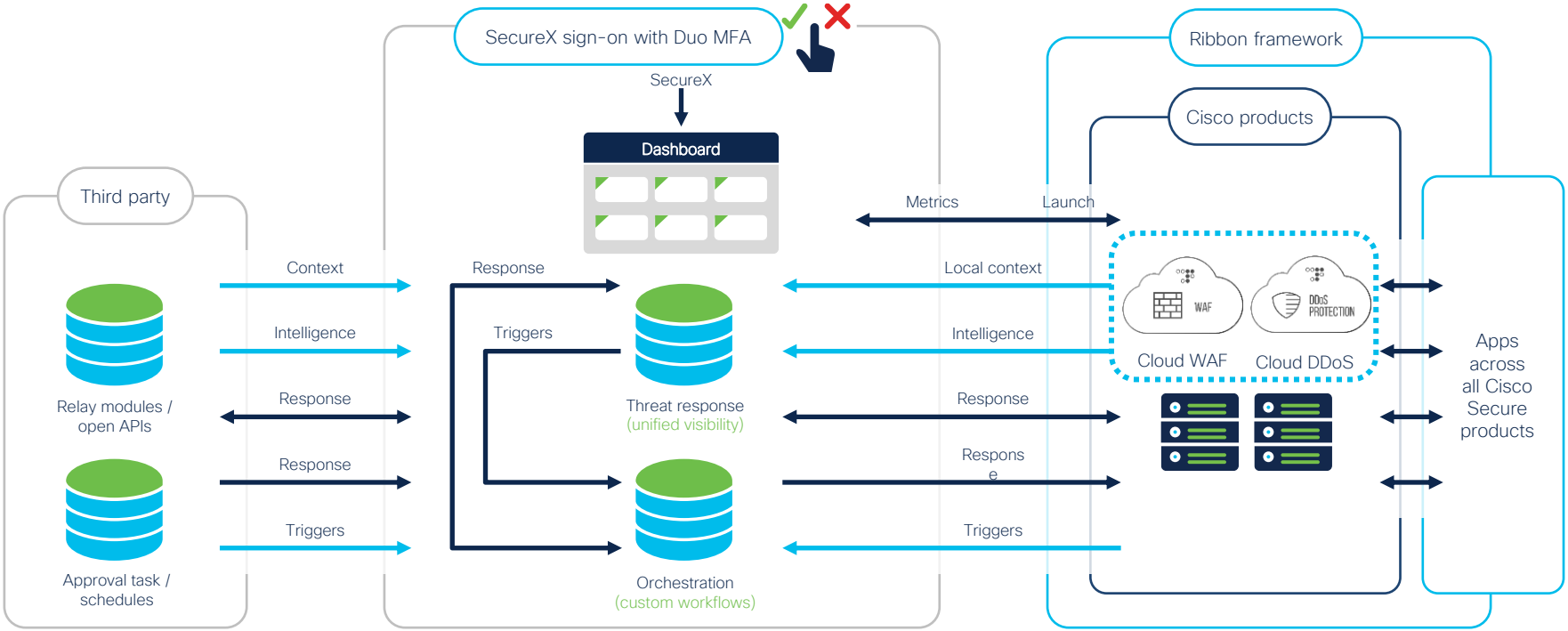
SecureX integration with Cloud DDoS and Cloud WAF provides:

- Visibility into Cisco Cloud DDoS and Cloud WAF platforms within SecureX Threat Response
- A single interface to perform threat hunting and research across an install base
- Security events presented side-by-side with intelligence data generated by Cisco (and other third party) security infrastructures
- Information to correlate threat data to get a bigger picture and gain insight through TALOS threat intelligence

No additional software needed!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX Architecture with Cloud Security Services



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Technology Partnership - Radware

Cisco SecureX
Simplify your security with the broadest, most integrated platform

Network Security

User And Endpoint Protection

Application Security

Cisco Secure Firewall with vDP
Cisco Secure Network Analytics with integration to Defense Flow and Vision
Cisco Secure Web Appliance with WAF/KWAF to protect “Web Apps”
AnyConnect with Cisco Secure DDoS to protect the VPN concentrator
Cisco Cyber Vision with Cisco Secure ADC with Bot Management
Identity Services Engine
Meraki MX with Cisco Secure DDoS to protect the Enterprise (Meraki Network)
Cisco Secure DDoS
Cisco Secure ADC
    Cisco Advanced WAF/KWAF
    Cisco Advanced Bot
Cisco Secure SSLi

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion

Conclusion

- DDoS attacks keep getting more powerful and more disruptive 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
- HTTPS Flood Protection module provides different protection modes, allowing you to mitigate SSL attacks even without SSL decryption
- DNS Protection mitigates DNS attacks without impact to user experience
- Radware provides Cloud solution to mitigate massive volumetric attacks

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Technologies

Network Security

Learn about a broad range of solution and technologies which will help you better understand how to secure your network. You will find topics such as VPN, ISE, IPv6, DDoS, IoT....

START

Feb 5 | 19:00
LABSEC-2333
ISE integrations via pxGrid with FTD, WSA, StealthWatch

Feb 6 | 08:45
TECSEC-3781
Walking on solid ISE - Advanced Use Cases and Deployment Best Practices

Feb 7 | 08:45
BRKSEC-2445
The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 11:30
BRKSEC-2037
Securing Starlink Internet Services

Feb 8 | 10:45
BRKSEC-2096
Securing Industrial Networks: Where do I start?

Feb 8 | 13:30
BRKSEC-2678
DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Feb 9 | 08:30
BRKSEC-2660
ISE Deployment Staging and Planning

Feb 9 | 10:30
BRKSEC-2101
Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Feb 9 | 15:45
BRKSEC-3058
Route based VPNs with Cisco Secure Firewall

Feb 9 | 15:45
BRKSEC-2044
Secure Operations for an IPv6 Network

Feb 10 | 09:00
BRKSEC-3019
Visibility, Detection and Response with Cisco Secure Network Analytics

If you are unable to attend a live session, you can watch it On Demand after the event

CISCO Live!

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from 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 Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you

cisco Live!

CISCO Live!

ALL IN