cisco SECURE

DEVNET Demo Guide Cisco Secure DDoS Edge Protection with IOS XR







Contents

Goals of this document	3
Connecting to the Sandbox	4
Overview	4
Device credentials	5
Objectives	5
Gain familiarity with the Cisco Secure DDoS Edge Protection controller interface	5
Prerequisites	5
Terminology	5
From this point on, you will need to be connected to IOS XR and Edge Protection Sandbox	5
Step 1: Reviewing the controller	6
Step 2: Generating traffic	14
Step 3: Detecting an attack	21
Step 4: Stopping the attack	36
Resources	41





Goals of this document

The goal of this document is to demonstrate Cisco Secure DDoS Edge Protection[®] in service provider mobile and peering environments. After this lab, the user should be familiar with Cisco Secure DDoS Edge Protection, an industry-leading technology that blocks distributed-denial-of-service (DDoS) attacks at the network edge, enabling service providers to meet the sub-10-ms latency requirements of modern 5G networks and ensuring customer quality of experience (QoE).

This demo guide will provide an overview of the Edge Protection controller, which provides centralized management of one (1) or more Edge Protection detectors. The controller also provides the visualization of the status of each detector and any ongoing attacks in the network.

Upon completion of this lab, you should be able to demonstrate the value of deploying Cisco Secure DDoS Edge Protection in your customer's network to protect them and their customers from service interruptions due to DDoS attacks.

Scheduling the Sandbox

This lab is meant to be run on the DEVNET Sandbox environment. To schedule the Sandbox, you will need to reserve the Cisco IOS® XR and Edge Protection Sandbox.

For information about how to reserve a DEVNET Sandbox, go to: https://developer.cisco.com/docs/sandbox/#!getting-started/try-it-out.

To book a Sandbox, go to https://developer.cisco.com/site/sandbox/, click "Get Started with Sandbox," and search for the "DDoS Edge Protection" sandbox.





Q

Connecting to the Sandbox

Once the Sandbox has been scheduled, an automated email will be sent to the user with the VPN URL and the credentials to log in. The Cisco AnyConnect[®] client is required to be installed on the student's computer to connect to the DEVNET Sandbox environment. If you don't have AnyConnect installed, the email sent with the login information will also provide a link to download the AnyConnect client.

Overview

In this lab, we will be protecting a mobile edge network environment from malicious attacks that are hidden inside GTP packets.

We will review the Controller Dashboard and other menus. Once we have familiarized ourselves with the controller interface, we will launch traffic from a legitimate user and will review the relevant information and statistics. Then we will launch malicious traffic from another device and see how the Edge Protection solution almost immediately protects the network by identifying and mitigating this traffic.

The following describes the solution architecture:

In this lab, there are both legitimate and malicious (attacker) devices that connect to an application that's behind a Cisco[®] NCS 540 router. On this NCS 540, there is a Cisco Secure DDoS Edge Protection detector deployed that analyzes all the flows of data being received by the router. The Edge Protection detector is controlled and managed by the Edge Protection controller. Visibility into the traffic passing through the detector can be observed on the controller graphical user interface.









Device credentials:

Device	Username	Password	MGT access
Cisco NCS 540	client	cisco123	10.10.20.53
Controller HTTP	admin@example.com	12345	http://10.10.20.51.nip.io
Legit user	demo	cisco123	10.10.20.55
Attack user	demo	cisco123	10.10.20.65
Protect application	demo	cisco123	10.10.20.75

Objectives

- Gain familiarity with the Edge Protection controller interface
- · Launch legitimate traffic and see how it is viewed within the Edge Protection controller interface
- · Launch attack traffic and see how it is easily and quickly detected by the Edge Protection detector
- Block attack traffic

Prerequisites

No prerequisites are required, but having knowledge of the challenges that the DDoS poses for enterprise and service provider customers and networks will help the student appreciate the value that Edge Protection offers customers.

Applications needed:

- Cisco AnyConnect client (link provided in email)
- · Web browser
- SSH program, such as Putty

Terminology

This document uses the following terms with which you must be familiar:

- Controller A central management function and a user Interface that manages a fleet of one or more detectors. The controller includes a GUI dashboard that presents real-time attack information for detector visibility, forensics, and threat intelligence analysis.
- Detector DDoS detection and mitigation are functions implemented on a virtual Docker container as a microservice application. The function runs independently on the designated edge router.
- GTP GPRS Tunneling Protocol defined by the 3GPP standards to carry packets between mobile function zones in 3G/4G and 5G.

Note: From this point on, you will need to be connected to IOS XR and Edge Protection Sandbox.



cisco SECURE



Step 1: Reviewing the controller

Open Chrome (or other browser) and connect to the Edge Protection controller, <u>http://10.10.20.51.nip.io</u>. For the email, enter admin@example.com, and for the password, use: 12345. Then click "Login."

A Not secure	https://10.10.20.51.nip.io/login	
	alialia cisco	
	Email * admin@example.com	
	Password *	
	Login	
	Forgot password?	

Once logged in, you will be in the Controller Dashboard.

ahaha cisco	Dashboard		
	Detectors		Detectors Status Attack Severity
Dashboard	Geo Data	Dete	ectors by Status
D			
Detectors			\frown
ß			1us• -{ 1}
Attacks			
Ø			
Protected Objects			
	Ongoing Attacks	System	
	Number Of Attackers	Traffic Through Routers Bps 🌑 Pps	Last 5 minutes
			• Traffic
	0		through all routers
			Attack traffic



Along the left side of the page is the navigation bar, which allows access to different menus. The section being displayed has a light-blue background. As you can see, we are in the dashboard The dashboard provides an overview of your environment. It shows the number of detectors, whether any detectors are under attack, and the total amount of both legitimate and attack traffic.

Scroll down to see more information in the dashboard.

Protected Objects			
PO's By Type Total Number Of PO's	Туре	PO's Under Attack	# IP Ranges
⊙ 2 ©	DOT SRC Routers		1 Attack Motions to potent anomenous

In the top right-hand corner of the dashboard, we see the number of detectors, and, by default, we also visually see their overall status. We also have the option to view by attack severity. In the example below, there is one (1) detector, and the status is green, indicating that it is active. When we click on the attack severity, it is also green, indicating that the network is not under attack.



Looking at the "Traffic Through Routers" graph below under "System," we notice that no traffic is shown. The default time window is the last five minutes, but this can be changed by clicking on the dropdown menu on the top right of the graph.

System						
Traffic Through Routers	Bps 🔵 Pps					Last 5 minutes 🛛 🗸
						Last 5 minutes 🗸
						Last 10 minutes
1 kbps						Last 30 minutes
0 kbps						Last 1 hour
						Last 3 hours
0 kbps	05:19	05:20	05:21	05:22	05:23	Last 6 hours

To the left of the "System > Traffic Through Routers" graph, we see the ongoing attacks graph. As shown below, there are also no attacks.



Scrolling down in the dashboard page, we get an overview of the protected objects (POs). Starting on the left, we can see the POs by type.

There are two (2) POs defined. One PO is defined by destination IP, none by the source IP, and one by router. We will get more details about this PO on the Protected Objects page.

Protected Objects	
РО's Ву Туре	
Total Number Of PO's	Туре
	DST 1
2	SRC
۷	Routers

The "PO's Under Attack" widget provides information on how many of the POs are under attack. Presently there are none under attack.



Finally, on the dashboard under "Protected Objects," we can see the number of IP ranges in our POs. In this case, it is one.



IP Ranges 1 Activite Windows Gets Statuse Windows

We will now review the Detectors menu page. Click on the Detector Icon on the left-hand side of the screen.

← → C	A Not secure 10.1	0.20.51.nip.io/detectors?detectors Maps	Filter + %78"gerStatus"%3A%58%5D%7D							• Q @	🖈 🏝 i
-dhaha cisco	Secure DDos E	idge Protection								(4	. 📀
D8 Destioners	Search Satas Name		Description	Mudd	Weslan		Diployment	Cartainer	Configuration		۹
Detectors	• cas	ite Maesi	NC3 540	NC3540	dpro-clacor2222.564	61726460521ca65a2mbca06					•
sP											
Anada											
Protected Objects											

We see one detector with the status of green. Looking to the right, we can see the status for Deployment, Container, and Configuration. The green arrows indicate that all three are working correctly. See the enlargements below.



To add more detectors, one can click on the $\textcircled{\bullet}$ icon and fill in the required fields for the router in which we would want to deploy the Edge Protection detector. We can also edit/view the existing detector details

by clicking on the 🗓 icon to the right-hand side of the detector row and selecting "Edit."







In the Edit Detector menu, we have three (3) tabs: Info, Main Configuration, and Security Configuration. Only the Info and Main Configuration need to be configured. The Security Configuration can be left at the default settings and only needs to be tweaked as necessary.

Edit Detector
nfo > Main Configuration > Security Configuration
General Info
Detector Name:"
Sbox-1
NCS SandBox-1
Latitude 25.783874114385592
Longitude
-80.12784490574211
Hardware Template:
NCS540 default ~

	Edit Detect	or				
	Info > Main Configuratio	n > Security	Configuration			
	standard					
	Attack Detection Algorithms				Attack End Detection	
	Behavioral TEID:					
	Number Of buckets:	100	Avr active sessions per IP for learn		Attack End Grace:	60 Sec
	Min flows per sec threshold':	1000	Min BW per sec threshold:	0.01 Gbps		
	Swap flow key:	JE 🔿 FALSE	Inactivity before re-learning:			
	Bps attack threshold:		Pps attack threshold:		Attack Characterization	
	Bps attack end threshold:	1.5 %	Pps attack end threshold:	1.5 %	Characterization Intervals: <u>3</u>	Enabled: TRUE FALSE
	Bps attack start interval:		Pps attack start interval:			
	Bps attack detectable min load:	0.005 Gbps	Pps attack detectable min load:	1 Kpps		
(Dick on the "Cance	" button	Cancel Activ	ne bottom i	riaht.	
Γ	Now click on the gra	aph 📂	icon to the le	ft of the		

Here we get details specific to an individual detector. This page will be more interesting once we have both legitimate and attack traffic going through this particular router being monitored by the detector.



0

ashboard	Secure DDoS Edge Protection Sbox-1 The TRee Last Smirules					
etectors & Attacks	Telemetry Statistics Max Idous Telemetry Telem	first rev me 0	Detector CPU Detector uses 2 cores 200% maximum CPU	Detector Mem Usage 93MB	Traffic by Protocol	han han han udo cano adher
Dispects	Alerts		No alerts to display			
	Quantiles Traffic Percentage BPS A		No data			79] V(8)(5)7).
© [→	Total Traffic BPS	Total Traffic PPS	Traffic by Protocol			Activate Windows Or to Settings to actuese Windows,

Click on the Attacks icon . Here we see the active attacks. This page is empty at the current time.

$\leftarrow \ \ \rightarrow \ \ C$		Not secure 10102051nipio/attacks?attacksFitter=%78*attackSevenity %3A%58%5D%2C*status%3A%58*ONGOING%5D%2C*initigate %3A%58%5D%7D										07 6	2 🖈 😩		
Apps M	Gmail	🖸 YouTube 🙎	Maps												Reading li
alialia cisco		Secure DDoS	Edge Protection												
₽⊓		Alla													
02		Attack ID 🥃	Severity	Attack ID 🥃	Severity	PO Name	Status 🕎	BwBps	BwPps	#Attacked Routers	Attackers	#Mitigated Attackers	Start Time		Mitigation
Dashboard									No attacks to dis	play					
D															
Detectors															
Attacks															

Next, click on the Protected Objects icon . Here we can view the two POs, the default PO and one manually configured object called Protected-1. To create more POs, we would click on the flocated on the top right.





Click on the **i** at the end of the row for the Protected-1 object, and then click "Edit."



We can see the details for this PO. We see that the type is a destination IP (Dst). We can see that the value of the IP is 15.15.1.0/8 and, below that, the thresholds that classify an attack as medium or high severity. Click "Cancel."

	Update Protected Object X
Name:* Protected-1	Parameters: "
Type: Dst	15.15.10/8 X
Mode: User Confirmation	v
Attack Severity:	
Medium: [*] 0.3 Gbps	10 Kpps
High: 0.5 Gbps	100 Kops
	Cancel Update

At the bottom left, we see information regarding the Edge Protection controller itself. Click on the icon. Here we can see the details of the software that is installed on the various engines of the controller.

0

Ve	ersions X
controller:	2.4.0.1042
config:	2.4.1.218
controller-rest-api:	2.4.0.2229
deployer:	2.3.0.342
frontend:	2.4.0.1248
grpc-server:	2.4.0.251
health-monitor:	2.4.0.219
notifier:	1.0.0.75
warroom:	2.4.1.604
	Ok

Click on the 😟 icon. From the Settings page, you can access templates for the detectors, create users, and add the licensing.

Secure DDoS Edge Protection Settings Templates Integrations Users	□ Api Keys □ Licensing	
Hardware Configuration Security		
Name ^	Router Family	Description
emulator default	emulator	
NCS540 default	NCS540	

Finally, the last icon is the Exit Controller icon $\stackrel{\frown}{\vdash}$, which will log off the user from the controller.





X

Cancel



Step 2: Generating traffic

Now that we are familiar with the Edge Protection controller interface, it is time to generate traffic from the legitimate user. We will be sending traffic to the protected application on the right of the diagram below.



SSH into the legit system with the IP address of 10.10.20.55 and the following credentials:

Username: demo Password: cisco123

If prompted with a security alert, click "Accept." This happens because it is your first time connecting to this device securely.

🗩 PuTTY Configuration		?	×			
Category:						
- Session	Basic options for your PuT	TY session				
Logging ─ Terminal - Keyboard	Specify the destination you want to co Host Name (or IP address)	onnect to Port		PuTTY S	ecurity Alert	
Bell Features	10.10.20.55 Connection type:	22				
Appearance Behaviour	SSH Serial Other:	Telnet	~	?	The server's host key is not cach guarantee that the server is the c	ed in the registry. You have no omputer you think it is.
 Translation € Selection 	Load, save or delete a stored session Saved Sessions	n			The server's ssh-ed25519 key fin ssh-ed25519 255 SHA256:G2uPj	gerprint is: UCHVmjkC+NEmQPQf8Dqj3klNjSY5nS/Sriv
Colours	Kali-1-Legit				If you trust this host, press "Accep cache and carry on connecting.	ot" to add the key to PuTTY's
- Data - Proxy	Default Settings EdgeProtect-Controller	Loa	1		If you want to carry on connecting to the cache, press "Connect One	just once, without adding the key e".
SSH Serial	Kali-1-Legit Kali-2-Attacker	Sav	•		If you do not trust this host, press	"Cancel" to abandon the connection.
- Telnet - Rlogin - SUPDUP	NCS-540	Dele	te	Не	More info	Accept Connect Once
	Close window on exit: Always Never Only	y on clean exit				
About Hel	p Open	Canc	el			

Move into the ddos-work directory with the following command:

cd ddos-work

Now execute the script called run-legit-traffic.sh:

./run-legit-traffic.sh

The Kali Linux box will now generate traffic and send it to the protected object.



Note: Wait about 30 seconds to ensure that the traffic is being seen by the router and the detector.

🧬 demo@kali-1-Legit: ~/ddos-work	_		×
<pre>demo@kali-1-Legit: ~/ddos-work\$ demo@kali-1-Legit: ~/ddos-work\$ demo@kali-1-Legit: ~/ddos-work\$ demo@kali-1-Legit: ~/ddos-work\$ demo@kali-1-Legit: ~/ddos-work\$ demo@kali-1-Legit: ~/ddos-work\$./run-legit-traffic.sh HPING 15.15.1.1 (eth0 15.15.1.1): NO TCP FLAGS are set (GTP Tunne rs + 1400 data bytes hping in flood mode, no replies will be shown</pre>	_ ≥ling),	48	heade
			-

Notice in the above image, the HPING command shows a destination IP address of 15.15.1.1. This is the final destination of the packet that has been encapsulated in the GPRS tunnel protocol (GTP). The GTP tunnel endpoint is 10.10.22.76, which can be clearly seen in the packet capture below.

>	Frame 1: 1490 bytes on wire (11920 bits), 1490 bytes captured (11920 bits)
>	Internet Protocol Version 4. Src: 10.10.21.66. Dst: 10.10.22.76
>	User Datagram Protocol, Src Port: 2152, Dst Port: 2152
>	GPRS Tunneling Protocol
~	Internet Protocol Version 4, Src: 10.10.21.55, Dst: 15.15.1.1
	0100 = Version: 4
	0101 = Header Length: 20 bytes (5)
	> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
	Total Length: 1440
	Identification: 0xbfce (49102)
	> Flags: 0x00
	0 0000 0000 = Fragment Offset: 0
	Time to Live: 64
	Protocol: TCP (6)
	Header Checksum: 0x8639 [validation disabled]
	[Header checksum status: Unverified]
	Source Address: 10.10.21.55
	Destination Address: 15.15.1.1
>	Tangentic Control Destacol Sec Dest: 20022 Det Dest: 20 Sec. 1 Long 1400

Now let's go back to the controller graphical user interface (GUI) portal and review some of the widgets. Open Chrome (or other browser) and connect to the Edge Protection controller: http://10.10.20.51.nip.io. For the email, enter admin@example.com, and for the password, use: 12345. Then click "Login."





▲ Not secure	https://10.10.20	.51.nip.io/login		
		alada		
		cisco		
	Email *			
	admin@exam	ple.com		
	Password *			
	•••••			
		Login		
			Forgot password?	

After logging in, we can see traffic. See the blue line in the "System > Traffic Through Routers" pane two screenshots below.

← → C ▲	Not secure 10.10.20.51.nip.io/dashboard?detectors	/iewType=status&trafficThroughRoutersTimeFilter=5&	trafficThroughRoutersUnit=bps		야 ☆ 😩
🔛 Apps M Gmail	💶 YouTube 🔣 Maps				Reading
ultuultu ctsco Dashboard Dashboard Detectors	Geo Data			Detectors by Status)
Attacks	Ongoing Attacks	System			
Protected Objects	Number Of Attackers	Traffic Through Routers	Вря ෩ Рря		Last 5 minutes Y
	0				Traffic through all routers Attack traffic

We can change the time from "Last 5 minutes" to "1 hour" (top right of the widget) to see the traffic going from 0 to over 2 Gbps.



Ó



Click on the Detector icon the left-hand side of the screen. Then click on the graph icon on the right-hand side of the detector row.



We can obtain a lot of information about what is being seen by the detector.



Starting from the top left, we can see telemetry statistics, which show the number of frames per second (fps), packets per second (pps), and the bandwidth that is used to collect statistics (telemetry) from the router.

Click on the time filter to notice that these statistics are for the last five minutes. We can change this range from one minute up to seven days.

Sbox-1		Secure DDoS Edge Protection Sbox-1
Time Filter: Last 5 minutes		Time Filter: Last 5 minutes ~
Telemetry Statistics		Last 3 hours Telemet Last 6 hours
Max 10 sec:	44,950 fps	Max 10 se Last 12 hours
lelemetry:	1,683 pps	Telemetry Last 24 hours Last 2 days
	2.38 Mbps	Telemetry Last 7 days

We can also see the amount of CPU and memory being consumed by the detector. Note that the CPU can be over 100%. Since there are two (2) CPUs, the range is up to 200% ($2 \times 100\%$).



On the top right, the traffic is broken down by type. We can see that all the traffic is TCP.



 \bigcirc

Scrolling further down in the page, notice a bar graph with quantiles. This shows the traffic being broken down into blocks. These blocks are known as quantiles. The quantiles are then analyzed by the detector for anomalies and attacks.



Just below the quantile traffic graph we have the "Total Traffic BPS," "Total Traffic PPS," and "Traffic by Protocol" graphs.

Total Traffic BPS	Total Traffic PPS	Traffic by Protocol
2.5 Gbos	200 kone	
2 Gbps	150 kone	2.5 Gbps • other bps
1.5 Gbps		Is Glops e udp bps
1 Gbps		
S00 Mbps		
0kbps 09:17 09:18 09:19 09:20 09:21 09:22		

Scrolling right to the end of the page we get a list of top talkers.

Top Talkers					
TIME 🧹	KEY	UDP BPS	OTHER BPS	TCP BPS	
10/30/21 09:23:32	10.10.20.55			2,266,041,600	
10/30/21 09:23:29	10.10.20.55			2,543,616,000	
10/30/21 09:23:26	10.10.20.55			2,569,939,200	
10/30/21 09:23:23	10.10.20.55	0		2,553,408,000	

Next log in to the Cisco NCS 540 router and take a look at the flows being forwarded to the detector. SSH into Cisco NCS 540 with the IP address of 10.10.20.53 and use the following credentials:

Username: demo Password: cisco123

If prompted with a security alert, click "Accept." This happens because it is your first time connecting to this device securely.

Demo Guide Cisco public

cisco SECURE

Section 2017 Putty Configuration		? >	
Category:			
Session	Basic options for your Pu	TTY session	
- Logging	Specify the destination you want to	connect to	
Keyboard	Host Name (or IP address)	Port	
Bell	10.10.20.53	22	
- Features	Connection type:		
-Appearance -Behaviour	SSH Oserial Other:	Telnet ~	
Translation	Load, save or delete a stored sessi	ion	
Selection	Saved Sessions		
Colours	NCS-540		
Data	Default Settings		
Proxy	EdgeProtect-Controller	Load	
	Kali-1-Legit	Save	
Serial	Kali-2-Attacker Kali-3-Protected-App		
Place	NCS-540	Delete	
SUPDUP	NCS-540-2		
	Close window on exit: Always Never O O	nly on clean exit	
About Heli	Open	Carrel	

Run the following command on the router to view the GTP access-list: show flow monitor DetectPro_NFv9 cache brief location 0/0/CPU0 The output shows details of the flows being sent from the router to the detector.

RP/0/RP0/CPU):NCS1#sl	how flow	monit	or Detect	Pro	NFv9 c	cache	brief	location	0/0/C\$
Wed Nov 24 14	4:58:48.0	029 UTC								
Cache summary	for Flo	ow Monit	or Det	ectPro NE	fv9:					
Cache size:				1000000						
Current entri	les:			2349						
Flows added:			64	61486834						
Flows not add	ded:			0						
Ager Polls:				2357805						
- Active ti	imeout		64	61484485						
- Inactive	timeout			0						
- Immediate	e			0						
- TCP FIN 1	Elag			0						
- Emergency	7 aged			0						
- Counter w	vrap ageo	d		0						
- Total			64	61484485						
Periodic expo	ort:									
- Counter w	vrap			0						
- TCP FIN 1	Elag			0						
Flows exporte	ed		64	61484485						
RecordType II	V4SrcAd	dr	IPV4Ds	tAddr	L 4	SrcPor	rt L4	DestPo	ort IPV4Pr	ot IPV4
TOS InputInt	terface	ByteCou	int	PacketCoi	int	Dir				
GTP Tunneled	Record 1	10.10.21	.55	15.15	.1.1		5040	1	80	tcp
0	Te0/0/0	0/4	1440		1		In	q		
GTP Tunneled	Record	10.10.21	.55	15.15	.1.1		3783		80	tcp
0	Te0/0/0	0/4	1440		1		In	g		
GTP Tunneled	Record	10.10.21		15.15	.1.1		1616	6	80	tcp
										-

Let's launch an attack. Please go to the next step.





Step 3: Detecting an attack

We are now going to launch an attack. We want to keep the legitimate traffic going, so make sure you have not stopped the script from the legitimate server. If required, return to the previous section to see how to launch the legitimate traffic.



Log back into the Cisco NCS 540 Router and take a look at the access-list policy that has been preconfigured.

SSH into Cisco NCS 540 with the IP address of 10.10.20.53 and use the following credentials:

Username: client

Password: cisco123

PuTTY Configuration		? ×						
Category:								
- Session	Basic options for your PuTTY session							
Logging Terminal Keyboard Bell Peatures Window Appearance Behaviour Translation Colours Colours Connection Colours Connection Proxy SSH Serial Telnet Riggin SUPDUP	Specify the destination you want to contr Host Name (or IP address) 10.10.20.53 Connection type: SSH SsH Other: Tel Load, save or delete a stored session Saved Sessions NCS-540 Default Settings EdgeProtect-Controller Kall-3-Protected-App NCS-5400 NCS-540-2	Port 22 net V Load Save Delete						
	Close window on exit: Always Never Only or	n clean exit						
About Hal	Open	Canaal						



Run the following command on the router to view the GTP access-list:

show access-list gtp

The output shows details of the flows being sent from the router to the detector.

Presently there are three entries in the GTP access-list.

RP/0/RP0/CPU0:NCS1#	
RP/0/RP0/CPU0:NCS1#show access-lists gtp	
Mon Nov 1 18:51:13.106 UTC	
ipv4 access-list gtp	
1000 permit udp any any eq 2152 capture ((1175 matches)
2000 permit ipv4 any any (4 matches)	
2001 permit icmp any any	
RP/0/RP0/CPU0:NCS1#	

Now SSH into the attacker system with the IP address of 10.10.20.65 and the following credentials:

Username: demo

Password: cisco123

If prompted with a security alert, click "Accept." This happens because it is your first time connecting to this device securely.

			A TOOLWARD TELEGIL TANGOS WORK	
PuTTY Configuration		? ×	₽ 10.10.20.65 - PuTTY	
Category:				
- Session Logging	Basic options for your PuTTY Specify the destination you want to com	session nect to		
Keyboard	Host Name (or IP address)	Port		
Bell	10.10.20.65	22		
-Features	Connection type:		t PuTTY Security Alert	<
- Appearance Behaviour - Translation - Colours ■ Connection - Data - Proxy ♥ SSH - Serial - Telnet - Riogin	SSH Serial Other: Tel Load, save or delete a stored session Saved Sessions Kali-2-Attacker Default Settings EdgeProtect-Controller Kali-1-Legit Kali-2-tegit Kali-2-Protected-App NCS-540	Load Save Delete	The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's ssh-ed25519 key fingerprint is: ssh-ed25519 J255 SH2452 CaUPJIOH/my/ko-NEm0P048DqJ3kINj3Y5nS/Srix3ro If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".	
SUPDUP	Close window on exit: Always Never Only or	n clean exit	If you do not trust this host, press "Cancel" to abandon the connection.	
About Help	Open	Cancel		_

Move into the ddos-work directory with the following command:

cd ddos-work

Now execute the script called ddos-udp-target.sh:

./ddos-udp-target.sh

The Kali Linux box will now generate traffic and send it to the protected object. Notice that the IP of traffic being sent is 15.15.1.1. This is the IP of the protected application server itself.





demo@kali-2-Attacker:~/ddos-work\$
demo@kali-2-Attacker:~/ddos-work\$ ls
ddos-top-Attack.sh ddos-udp-attack.sh
demo@kali-2-Attacker:~/ddos-work\$./ddos-udp-attack.sh
HPING 15.15.1.1 (eth0 15.15.1.1): udp mode set (GTP Tunneling), 36 headers + 400
data bytes
hping in flood mode, no replies will be shown

Now let's go back to the controller GUI portal and review some of the widgets.

Open Chrome (or other browser) and connect to the Edge Protection Controller: http://10.10.20.51.nip.io. For the email, enter admin@example.com, and for the password, use: 12345. Then click "Login."



Click "Attack Severity."

"Detectors by Attack Severity" is now red (if yellow, wait another minute), indicating that an attack has been detected.



Ó



Click on the "1" and you will be redirected to the Detectors page. Notice that the graph is now red.

← → C H Apps M Gr	A Not secure 10.102.051/niploj/detecton/Adetecto									
alialia cisco	Secure	e DDoS Edge Protection								
80	De	Detectors (a) 🕒								
Deshtowed										٩
	Saba	Name ^	Description	Model	Version		Dipkyment	Container	Configuration	
Detectors	•	Cell Ste Marri	NCS 540	NCS540	dpro-cisco:2.2.2.564	61726460521ca65s210a06				
Ø										
Attacks										
O										
Protected Objects										

Click on the graph. Notice that, in the bar graph for "Quantiles Traffic Percentage," we see some red quantiles. These are the quantiles where the attack has been detected.





Total Traffic BPS		Total Traffic PPS		Traffic by Protocol				
2 Gbps								
					m	mynn	······································	
500 Miler		50 knos						
0 K0ps	09:37 09:38 09:39	0 kpps 09:34 09:35 09:36	09:37 09:38 09:39	0 kbps 09:34	09:36	09:37	09:39	
Logs							L Expo	t Log File
TIME 🗸		DEBUGLEVEL	MODULE	MESSAGE				
10/30/21 09:38:09	WARN		detMSD2	All attacks were o	leared because the traffic is less than	10 MB		C .
10/30/21 09:37:58	WARN		detMSD2	All attacks were o	leared because the traffic is less than	10 MB		
10/30/21 09:35:27	INFO		cntrGRPC	Sending the Cont	roller a Forensics report: [["name":"S	RC_ADDR","total_pps":158990,"total_bps":1053	149760,"signature":[["value":"10.10.	
10/30/21 09:35:26	INFO		cntrGRPC	Sending the Cont	roller a Forensics report: [["name":"S	RC_ADDR","total_pps":19810,"total_bps":13122	1440,"signature":[["value":"10.10.20	
Top Talkers								
TIME 🗸			UDP BPS		OTHER BPS	TCP BPS		
10/30/21 09:39:41	10.10	0.20.65	1,016,817,120					
10/30/21 09:39:41	10.10	0.20.55				1,383,206,400		
10/30/21 09:39:38	10.10	0.20.65	392,472,000					
10/30/21 09:39:38	10.10	0.20.55				680,716,800		

Scroll down on your screen to see additional widgets that provide information about the network traffic.

In the "Traffic by Protocol" graph, we now see TCP and UDP traffic.



Below we now see logs indicating warning.

Logs					1 Export Log File
TIME 🗸	TYPE	DEBUGLEVEL	MODULE	MESSAGE	
10/30/21 09:40:22	WARN		detMSD2	All attacks were cleared because the traffic is less than 10 MB	
10/30/21 09:39:48	WARN		detMSD2	All attacks were cleared because the traffic is less than 10 MB	
10/30/21 09:38:09	WARN		detMSD2	All attacks were cleared because the traffic is less than 10 MB	
10/30/21 09:37:58	WARN		detMSD2	All attacks were cleared because the traffic is less than 10 MB	

We now see the attacker machine as a top talker.

Top Talkers					
TIME 🗸	KEY	UDP BPS	OTHER BPS	TCP BPS	
10/30/21 09:41:02	10.10.20.65	888,775,200			
10/30/21 09:41:02	10.10.20.55			1,125,964,800	
10/30/21 09:40:59	10.10.20.65	987,009,120			
10/30/21 09:40:59	10.10.20.55			1,421,798,400	

Click on the Attacks icon *L*. We now see an active attack.





	Secure DDoS E	dge Protection ks											
08	Attack ID 🤟	Severity	PO Name	Status 🟹	BwBps	BwPps	#Attacked Routers	Attackers	#Mitigated Attackers	Start Time	End Time	Mitigation	
(D)			Protected-1	Ongoing	848 Mbps	131 Kpps		10	0	30/10/21 09:35:12			
Detectors													
Attacke													
Ø													
Protected Objects													

Note that the green shield in the upper right is flashing, indicating that an attack has been detected, but that the mitigation needs to be activated manually. This can also be set to automatic; however, mitigation would occur so quickly that the user would most likely miss viewing the attack. Therefore, for this lab, the mitigation has been set to user manual activation.



Click on the shield to view more details of the attack that has been detected. Analyzing this interface, we can see that there are ten (10) attackers and zero (0) have been mitigated. To the right of "Attackers and Mitigated Attackers," we have the option of manually starting a mitigation on a particular attacker.

uludu cisco	Secure DDoS Edge Protection Attacks										
08		Attack Details									×
Dashboard	6 HIGH Protected-1	Вивря	BwPps		#Attacked Routers	Attackers	#Mitigated Attackers			Mitigation	
۲		848 Mbps	131 Kops	Ongoing		10	0	30/10/21 09:35:12			
Detectors											
s de la companya de l		Attack Vectors Attack T	type: UDPFlood Attack Pr	otocol: UDP Attacked IF		RC_ADDR:10.10.20.6	5;DST_ADDR:15.15.1.1;L	LDST_PORT:53; PROTOCOL:			
Attacks		Total Attack Traffic	Bps 🔵 Pps		Last 1 minute	- R	outer Contribution	Bps 🌑 Pps			
\bigcirc							Sbox-1				
Protected Objects											
		Attackers and Mitigate	ed Attackers								
		ATTACKERS ^	10	TALBPS	TOTAL PPS		ROUTER		MITIGATION		
		0x0000002	**	210.000	15,310		Sbox-1				
		0x00000003		280,000			Sbox-1				
		0x00000004		940,000	11,890		Show-1				
		0x00000005		610,000	11,530		Sbox-1				
		0x00000005		000,088	15,410		Show-1				



If you hover your mouse over the graph labeled "Total Attack Traffic," you will see the amount of total attack traffic and how much of that traffic has be mitigated. As you can see, no traffic has been mitigated yet.

Attack Vecto	Drs Attack	Type: UDPFlood	Attack Protocol: UDP	Attacked IP: 15.15.1.1	Attack Analysis: SR(C_ADDR:10
Total Attac	ck Traffic	Bps 🔵 Pps			Last 1 minute	~
600 Mbps						
500 Mbps				• Total Traffic 5	00 5 50 Mbps	
400 Mbps				Mitigated Tra	offic 0 kbps	
300 Mbps						
200 Mbps						
100 Mbps						
O kbps —						12:09

Click on the icon in the upper right of the screen and click "Start Mitigation."

	X
Mitigation	
Start Mitigation	
Stop Mitigation	
End Attack	
Copy To Clipboard	

Click the "Start" button. Now all attackers will be mitigated.



0

					Mitigation
	Start Mitig	ate			
		itigation for this attack?			
	"Protected	-1"			
	Cancel	Start			

The green shield has stopped flashing, and we see that "# Mitigated Attackers" shows "10," matching the number of attackers. This confirms that all attackers are now being mitigated. We can also stop a particular attacker from being mitigated by clicking the "Release Mitigation" button to the right of a particular attacker under the heading "Attackers and Mitigated Attackers" section.



Attackers and Mitigated Attackers							
Attackers and Miti							
ATTACKERS ^	TOTAL BPS	TOTAL PPS	ROUTER	MITIGATION			
0x0000001	99,050,000	15,310	Sbox-1	$\overline{\bigcirc}$	Release Mitigation		
0x0000002	99,210,000	15,340	Sbox-1	$\overline{\bigcirc}$	Release Mitigation		
0x0000003	76,280,000	11,790	Sbox-1	$\overline{\bigcirc}$	Release Mitigation		
0x0000004	76,940,000	11,890	Sbox-1	$\overline{\bigcirc}$	Release Mitigation		
0x0000005	74,610,000	11,530	Sbox-1	$\overline{\bigcirc}$			
0x0000006	99,680,000	15,410	Sbox-1	\bigcirc	Activate Windows		

Changing the view from "Last 1 Minute" to "Last 5 Minutes," we can get a better view of the total attack traffic ramp-up.



cisco SECURE



We can also view the attack signature that was created based on the attack traffic. The attack analysis shows a source address of 10.10.20.65, destination address of 15.15.1.1, protocol UDP port 53, and time to live (TTL) of 64.

Attack Analysis: SRC_ADDR:10.10.20.65; DST_ADDR:15.15.1.1; L4_DST_PORT:53; PROTOCOL:UDP; TTL:64

Clicking on the box with the arrow pointing out (see image above) provides a cleaner view of the attack signature detected.

Total Attack Attack Analysis Image: Contribution Bps Pps 1.5 Cbps SRC_ADDR:10.10.20.65; DST_ADDR:15.15.1.1; L4_DST_PORT:53; PROTOCOL:UDP; TTL:64 Image: Contribution Bps Pps 500 Mtps Close Copy to Clipboard Image: Copy to Clipboard Image: Copy to Clipboard Image: Copy to Clipboard				
1.5 Chps 1.5 Chps 1 Chps 500 Mtps 01kps 0741	Total Attack	Attack Analysis	er Contribution	
500 Mtps Okbps 07:41		SRC_ADDR:10.10.20.65 ; DST_ADDR:15.15.1.1 ; L4_DST_PORT:53 ; PROTOCOL:UDP ; TTL:64		
		Close Copy to Clipboard		

Now go back to your SSH session to the NCS 540 router (if closed, open it again) and look at the GTP access-list:

show access-list gtp

The GTP access-list has been updated with ten (10) new deny policies blocking the malicious traffic. Looking at each of the new lines in the ACL (below), each malicious GTP tunnel endpoint ID has been blocked (example: 0x8 GTP tunnel endpoint ID).

0

№ 10.10.20.53 - PuTTY	-	×
RP/0/RP0/CPU0:NCS1#		
RP/0/RP0/CPU0:NCS1#		
RP/0/RP0/CPU0:NCS1#		- 7
RP/0/RP0/CPU0:NCS1#		
RP/0/RP0/CPU0:NCS1#show access-lists gtp		
Mon Nov 1 19:16:42.141 UTC		
ipv4 access-list gtp		
l deny ipv4 any any udf udf-gtp 0x8 0xffffffff		
2 deny ipv4 any any udf udf-gtp 0x9 0xffffffff		
3 deny ipv4 any any udf udf-gtp 0xa 0xffffffff		
4 deny ipv4 any any udf udf-gtp 0x1 0xffffffff		
5 deny ipv4 any any udf udf-gtp 0x2 0xffffffff		
6 deny ipv4 any any udf udf-gtp 0x3 0xffffffff		
7 deny 1pv4 any any udf udf-gtp 0x4 0xffffffff		
8 deny 1pv4 any any udf udf-gtp 0x5 0xfffffff		
9 deny 1pv4 any any udf udf-gtp 0x6 0xfffffff		
10 deny 1pv4 any any udf udf-gtp 0x7 0xfffffff		
1000 permit udp any any eq 2152 capture (1175 matches)		
2000 permit ipv4 any any (4 matches)		
2001 permit 1cmp any any		
KP/0/KP0/CP00:NCS1#		

Going back to the Controller Dashboard we can see that a device is still under attack. Note that in a real attack, multiple devices would most likely be under attack. Although we are protecting the network by mitigating the attack, the network is still under attack.



Scroll down on the Dashboard page to the Protected Objects section.

Protected Objects			
PO's By Type		PO's Under Attack	# IP Ranges
Total Number Of PO's	Туре		
2	55T 1 SRC 0 Roders 1		1

DevNet Demo Guide: Cisco Secure DDoS Edge Protection with IOS XR $~\mid~$ 30



Click on the "1" in the "PO's Under Attack" screen.

PO's Under Attack		
	1	

This will take you into a filter view of the Protected Objects page, showing only the PO that is under attack.

altalta cisco	Secure DDoS Edge Protection Protected Obj	ects			<u>ب</u>
Dashboard	Name 🔿	Туре	Mode	Ongoing Attack 🛛 🏹	
D	> Protected-1	Dst	User Confirmation		
Detectors					
ß					
Attacks					
\bigcirc					
Protected Objects					

Click on the ">" symbol to view details of the PO.







 \bigcirc

Creating a New Protected Object (PO)



From the Protected Objects menu click on the icon in the right of Protected-1

Secure DDoS Edge Protection			
Protected C	Objects		ب 🕂
Search			۹
Name 1	Туре	Mode	Ongoing Attack
> default	Routers	User Confirmation	
> Protected-1	Dst	User Confirmation	 ∠ Edit i Delete
			C Duplicate



Click on Duplicate

Fill-in the form. For Name use DemoPO-2, click on the x next 15.15.1.0/8 under parameters heading to delete the entry and type 16.16.1.0/24 and press enter. Then click the Create button at the bottom.





	New Protected Object	×
Name: DemoPO-2 Type: Dst Mode: User Confirmation	Parameters: Enter lp Address / Range 16.16.1.0/24 x	
Medium: 0.3 Gbps	10 кррз	
High: 0.5 Gbps	<u>100</u> Кррз	
	Cancel	

You should now see 3 PO: default, Protected-1 and the newly created DemoPO-2

altalta cisco	Secure DDoS Edge Protection Protected O	biects		ر ب ب
	Search			٩
Dashboard	Name ^	Туре	Mode	Ongoing Attack
D Detectors	> default	Routers	User Confirmation	
R	> DemoPO-2	Dat	User Confirmation	
Attacks	> Protected-1	Dst	User Confirmation	
Protected Objects				

Now that we have the new PO created let's launch a second attack.

Open a second SSH session into the attacker system with the IP address of 10.10.20.65 and the following credentials:

Username: demo

Password: cisco123



 \bigcirc

🗩 PuTTY Configuration		? >
Category:		
- Session	Basic options for your P	uTTY session
- Logging - Terminal - Keyboard - Bell	Specify the destination you want to Host Name (or IP address) 10.10.20.65	Port 22
- Features - Window - Appearance - Behaviour	Connection type: SSH Serial Other:	Telnet ~
Translation Selection Colours	Load, save or delete a stored sess Saved Sessions Kali-2-Attacker	ion
-Data -Proxy	Default Settings EdgeProtect-Controller	Load
SSH Serial	Kali-1-Legit Kali-2-Attacker	Save
-Telnet -Rlogin	Kali-3-Protected-App NCS-540	Delete
	Close window on exit: Always Never	inly on clean exit
		Orrest

Move into the ddos-work directory with the following command:

```
cd ddos-work
```

Now execute the script called ddos-tcp-target.sh:

./ddos-tcp-Attack.sh

The Kali Linux box will now generate a second attack.

```
demo@kali-2-Attacker:~$
demo@kali-2-Attacker:~$
demo@kali-2-Attacker:~$
cd ddos-work/
demo@kali-2-Attacker:~/ddos-work$
demo@kali-2-Attacker:~/ddos-work$
demo@kali-2-Attacker:~/ddos-work$
demo@kali-2-Attacker:~/ddos-work$ ./ddos-tcp-Attack.sh
HPING 16.16.1.2 (eth0 16.16.1.2): S set (GTP Tunneling), 48 headers + 800 data b
ytes
hping in flood mode, no replies will be shown
```

Wait for about 15 seconds and then go back to the controller GUI portal and review some of the widgets.

Review the Attack menu, we now see 2 attacks. The first attack shows 10 attackers and 10 mitigated attacks and a new attack, with a PO Name of DemoPO-2, shows 10 attackers and 0 mitigated.

alialia cisco	Secure DDoS	Edge Prote	ction										
88		CKS Severity	PO Name	Status 🟹	BwBps	BwPps	#Attacked Routers	Attackers	#Mitigated Attackers	Start Time	EndTime	Mitigation	
Dashboard (D)	78		DemoPO-2	Ongoing	2 Gbps	247 Kops	1	10	0	24/11/21 12:08:40			
Detectors	76		Protected-1	Ongoing	968 Mbps	290 Koos	1	10	10	24/11/21 12:00:51		$\overline{\bigcirc}$	
Attacks													

Click on the DemoPO-2 attack to go into the Attack Dashboard





We can see that the attack is about 1.6Gbps(+ or -) in size and that the attack type is TCPSYNFlood

Attack Vectors Attack Type: TCPSYNFlood Attack Protocol: TCP Attacked IP: 16.16.1.2 Attack Analysis: SRC_ADDR:10.10.20.65; DST_ADDR:16.16.1.2; L4_DST_PORT:443; ... [7]

If you like, you can mitigate the attack as you did in the previous section and review how the ACL has been updated to protect against both attacks. Once mitigated the router ACL will be updated blocking the new attack

On the router command line type:

show access-list gtp

சு 10.10.20.53 - PuTTY
RP/0/RP0/CPU0:NCS1#show access-lists
Tue Nov 30 19:33:30.897 UTC
ipv4 access-list gtp
1 deny ipv4 any any udf udf-gtp 0x8 0xffffffff
2 deny ipv4 any any udf udf-gtp 0x9 0xffffffff
3 deny ipv4 any any udf udf-gtp 0xa 0xffffffff
4 deny ipv4 any any udf udf-gtp 0x1 0xffffffff
5 deny ipv4 any any udf udf-gtp 0x2 0xffffffff
6 deny 1pv4 any any udf udf-gtp 0x3 0xfffffff
/ deny 1pv4 any any udr udr-gtp 0x4 0xfffffff
8 deny ipv4 any any udf udf-gtp 0x5 0xffffffff
10 deny ipy4 any any udf udf-gtp 0x8 0x1111111
11 deny ipv4 any any udf udf-gtp 0x7 0x1111111
12 deny ipv4 any any udf udf-gtp 0x20021b5 0xffffffff
13 deny ipv4 any any udf udf-gtp 0x20021b8 0xffffffff
14 deny ipv4 any any udf udf-gtp 0x20021af 0xffffffff
15 deny ipv4 any any udf udf-gtp 0x20021b7 0xffffffff
16 deny ipv4 any any udf udf-gtp 0x20021b2 0xffffffff
17 deny ipv4 any any udf udf-gtp 0x20021b1 0xffffffff
18 deny ipv4 any any udf udf-gtp 0x20021b4 0xffffffff
19 deny ipv4 any any udf udf-gtp 0x20021b3 0xffffffff
20 deny ipv4 any any udf udf-gtp 0x20021b0 0xffffffff
21 deny ipv4 any any udf udf-gtp 0x10009f 0xffffffff
1000 permit udp any any eq 2152 capture (1251 matches)
2000 permit ipv4 any any (7 matches)
2001 permit icmp any any
RP/0/RP0/CPU0:NCS1#

We can see that the ACL has been updated to protect the networks both attacks.





Step 4: Stopping the attack

Now we would like to stop the attack. Use CTRL+ A to stop the attack for both attacks launched.

```
demo@kali-2-Attacker:~/ddos-work$ ./ddos-udp-attack.sh
HPING 15.15.1.1 (eth0 15.15.1.1): udp mode set (GTP Tunneling), 36 headers + 400
data bytes
hping in flood mode, no replies will be shown
^C
---- 15.15.1.1 hping statistic ---
276760956 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
demo@kali-2-Attacker:~/ddos-work$
```



Please make sure that the attack script has stopped. Sometimes the script continues to run even though the terminal shows stopped. If you don't see the attack traffic stop in the Controller Dashboard, it is possible that the script is continuing to run and the process needs to be manually stopped (killed). The first step is to find the process ID.

To find the process ID of the hping4 attack script, use the following command:

command: ps -a

Look for the PID that says hping4. In the example below, it is 1127. Then kill that process by running the kill command:

kill -9 <PID>

In the example below:

kill -9 1127





Once the attack has stopped, the controller will still report the router as under attack for a few minutes until it is certain that the attack has been terminated.

Going back to the Detectors page and clicking on the detector, we can now see that there no longer is any UDP traffic. The quantile bar graph is no longer showing any red bars, indicating that none of the quantiles are malicious.





0///

Scrolling further down on the Detectors page, we also see that we no longer have any logs and that the top talkers are now all coming from our legitimate user.

80											
	Total Traffic BPS	Total Traffic PPS	Traffic by Protocol								
Dashboard Detectors Detectors Attacks	1 Clops 2 Clops 2 Clops 1 Clops 1 Clops 1 Clops 1 Clops 0 C	255hpps 705hpps 155hpps 100hpps 55hpps 90 0kpp 9785 0959 1000 100	1 1002 1003	0937 1000							
Protected											
Ubjects	دمین میں										
	Top Talkers										
	TIME		UDPBPS	OTHERBPS	TCP BPS						
	10/30/21 10:03:17	10.10.20.55			2,880,288,000						
	10/30/21 10:03:11	10.10.20.55			1.331.596.800						
	10/30/21 10:03:08	10.10.20.55			2,881,209,600 Activ						



Secure DDoS Edge Protection Protected Objects									
Sea					Q				
	Name ^	Туре	Mode	Ongoing Attack					
	default	Routers	User Confirmation						
	Destasted 1	Det	Heer Confirmation						
	Protected-1	Dst	Oser Commation		:				

Notice that "Mode" is set to "User Confirmation."

Mode	
User Confirmation	
User Confirmation	



In a live environment, this would be changed to automatic, as we want to minimize the time between when the attack is detected and when it is stopped, or mitigated. When set to automatic, the attack is stopped within seconds.

New Protected Object										
Name:*		Parameters: *								
Туре:										
Src										
Mode:										
Automatic										
User Confirmation Manual										
Automatic	· · · · ·									
Ignore										
High: [*] 50 Gbps	500 Kpps									
	Cancel	Create								

Let's go back to the dashboard. Be sure to wait at least five minutes after the attack is stopped. We now see that the router is longer under attack, and looking at "System > Traffic Through Routers," we see the red line (attack traffic) going down to zero (0).





If we go back to the Detectors screen, we see the graph on the right-hand side has changed from red to blue, indicating that there is no attack on this detector.

cisco	Secure DDoS Edge Protection Detectors									
OS										
Dashboard	Status	Name 🔿	Description	Model	Version		Deployment	Container	Configuration	
Detectors	•	Sbox-1	NCS SandBox-1	NC\$540	dpro-cisco:2.2.2.564	61726460521ca65a2ffbca06				
sl										
Attacks										
\heartsuit										
Protected Objects										

Going to the Attacks screen, we also see no attacks listed on this screen.

← → C	C 🔺 Not secure 10.102.051.nipie/attacks?attacks?ittacks										01	a 🖈 😩		
Apps M Gm	Apps M Gmail 🗖 YouTube 😻 Maps											Reading lin		
alialia cisco	Secure DDoS	Edge Protection												
90	Alla	-13												
Ua	Attack ID 🗸	Severity	Attack ID 🧹	Severity	POName	Status 🖓	BwBps	BwPps	#Attacked Routers	Attackers	#Mitigated Attackers	Start Time	End Time	Mitigation
Dashboard								No attacks to dis	splay					
D														
Detectors														
Attacks														

Finally, checking the Cisco NCS 540 GTP access-list, we see that the deny statements have been removed since there no longer is an attack on the network:

show access-list gtp

🛃 10.10.20.53 - PuTTY	_	×
$\mathbf{J}^{\mathbb{R}}$ login as: client		
F Keyboard-interactive authentication prompts from server:		
Password:		
$\mathbf{J}^{\mathbf{R}}$ End of keyboard-interactive prompts from server		
RP/0/RP0/CPU0:NCS1#show access-lists gtp		
Mon Nov 1 19:41:06.835 UTC		
ipv4 access-list gtp		
1000 permit udp any any eq 2152 capture (1175 matches)		
2000 permit ipv4 any any (4 matches)		
2001 permit icmp any any		
RP/0/RP0/CPU0:NCS1#		



You have now completed the Cisco Secure DDoS Edge Protection Lab. Feel free to explore more of the user interface.





Resources

For more information about Cisco Secure DDoS Edge Protection, see:

- Cisco Secure DDoS Edge Protection on DEVNET: https://developer.cisco.com/docs/secure-ddos-edge-protection
- Cisco Secure DDoS Edge Protection AAG: www.cisco.com/c/en/us/products/collateral/security/secure-ddos-edge-protection-aag.pdf
- Cisco Secure DDoS webpage: <u>www.cisco.com/go/secure-ddos</u>
- Edge Protection Support email alias: secure-ddos-edge-protection@external.cisco.com

For information about Cisco security solutions that enable Any Device, go to: www.cisco.com/go/security

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 11/21