The bridge to possible

At a glance Cisco public

# Installation and Quick Start Guide

**Cisco Secure DDoS Edge Protection** 

## Contents

1. Introduction	3
2. System requirements	3
3. Solution architecture	3
4. Downloading Cisco Secure DDoS Edge Protection software	4
5. OVA installation and setup	4
6. Adding a detector	21
7. Resources	26

## 1. Introduction

Cisco Secure DDoS Edge Protection<sup>®</sup> is a software solution that stops cyberattacks at the service provider network edge. The Cisco Secure DDoS Edge Protection solution consists of two (2) components, a controller and one (1) or more detectors. A Cisco Secure DDoS Edge Protection detector can be deployed on Cisco IOS<sup>®</sup> XR. When a detector is deployed on the Cisco<sup>®</sup> NCS 540 routers, Cisco Secure DDoS Edge Protection detects and mitigates distributed-denial-of-service (DDoS) attacks at the cell site router. By moving DDoS protection to the network edge, service providers are able to meet the sub-10-ms latency requirements of 5G applications and ensure customer quality of experience (QoE).

This quick start guide (QSG) is intended to help customers download, install, and start using Cisco Secure DDoS Edge Protection.

## 2. System requirements

Minimum virtual machine (VM) requirements for installing the Cisco Secure DDoS Edge Protection controller:

- CPU: 4vCPU
- Memory: 8 GB
- Storage: 50 GB
- 1 network interface

The VM can be deployed on VMware or KVM hypervisors.

The VM is based on a Linux Ubuntu 20.4 LTS distribution with Docker and SSH server installed. There is an OVA image that can be shared. Please reach out to your Cisco systems engineer for the file.

Minimum VM requirements for installing the Cisco Secure DDoS Edge Protection detector:

- CPU: 2vCPU
- Memory: 8 GB
- Storage: 50 GB

The detector VM will be installed on Cisco IOS XR such as the NCS 540.

## 3. Solution architecture

The Edge Protection solution has two main parts. The detector runs on the edge router running IOS XR and collects traffic flow information from specific interface on the router. The controller is a remote management system that controls the operation, monitors, and analyzes the information provided by the detector.

#### **Detector:**

DDoS detection and mitigation functions are implemented on a virtual Docker container as a microservice application. The function runs independently on the designated edge router.

#### **Controller:**

The controller provides a central management function and a user Interface to manage a collection of detectors. The controller includes a GUI dashboard that presents information for real-time attacks for detector visibility, forensics, and threat intelligence analysis.

The following is an illustration of the current Edge Protection topology integrated with a Cisco NCS 540 router:

**Demo setup - Cisco Secure DDoS Edge Protection** 



## 4. Downloading Cisco Secure DDoS Edge Protection software

There are two (2) software components, the OVA image, which is the Linux virtual machine, and the tar file that contains the controller software to be installed.

Download the OVA file with the link provided by your Cisco sales engineer.

## 5. OVA installation and setup

## **5A. Deploy the OVA on hypervisor**

Please note the steps provided are for VMware.

From your hypervisor, click on "Create/Register VM," select "Deploy a Virtual Machine" from an OVF or OVA file, and then click "Next."

🔁 New virtual machine		
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> </ul>	Select creation type How would you like to create a Virtual Machine?	
4 License agreements 5 Deployment options	Create a new virtual machine	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
6 Additional settings 7 Ready to complete	Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	
<b>vm</b> ware <sup>®</sup>		
		Back Next Finish Cancel

Enter a name for the new VM such as "EdgeProtect-Controller," and then click inside the light blue box to bring up the File Explorer and select the OVA file.

🔁 New virtual machine - EdgeProtect-	Controller				
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Additional settings</li> <li>7 Ready to complete</li> </ul>	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to dep Enter a name for the virtual machine. EdgeProtect-Controller Virtual machine names can contain up to 80 characters and they must b	ploy De unique with	nin each ESXi i	nstance.	
	Click to select files o	or drag	ı/drop		
<b>vm</b> ware*					
		Back	Next	Finish	Cancel

## Select the file and click Open

• •		~			-			
Drganize • New folder					<b>⊪</b> • <b>∎</b>	Security	Certificates 📙 Cisco	Cloud
J This PC	Name		Date modified	Туре	Size			
3D Objects	backup		10/22/2021 8:12 AM	File folder				
Desktop	Backup2		10/22/2021 2:58 PM	File folder				
Documents -	📕 test		10/22/2021 4:13 PM	File folder				
Downloads	🥡 controller-1633594795-export-i-0	dae94a24fd3fe319.ova	10/14/2021 8:44 AM	Open Virtualization F	1,323,070 KB			
Music						est OS		Host name
Pictures								
Videos						untu Linux (64-	DIT)	AlteonUS-32-6-4
🔓 Local Disk (C:)								
Seagate Expansion Drive (D:)								
Radware-BakUpDrive (E:)						deploy		
→ vim (\\192 168 11 12) (7·)								
File name: controlle	r-1633594795-export-i-0dae94a24fd3fe31	9.ova		<ul> <li>All Files</li> </ul>	(*.*)	~		
				Op	en Cancel	ust be unique wi	thin each ESXi instanc	э.
	Quick filters							
				Cl	ck to select f	ïles or drag	g/drop	
		<b>vm</b> wa	are					
	😨 Recent tasks					Ro-li	Next	aich Carsel
						Back	INext Fi	Cancel

## Then click next

🔁 New virtual machine - EdgeProtect-	Controller
<ul> <li>New virtual machine - EdgeProtect-</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Additional settings</li> <li>7 Ready to complete</li> </ul>	Controller         Select OVF and VMDK files         Select the OVF and VMDK files or OVA for the VM you would like to deploy         Enter a name for the virtual machine.         EdgeProtect-Controller         Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.         Image: Controller-1633594795-export-i-0dae94a24fd3fe319.ova
<b>vm</b> ware <sup>*</sup>	
	Back Next Finish Cancel

Click Next on the following screen.

To New virtual machine - EdgeProtect-Controller											
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Additional settings</li> <li>7 Ready to complete</li> </ul>	Select storage Select the storage type and datastore Standard Persistent Memory Select a datastore for the virtual machin	ne's c	onfiguration	files	and all of i	its' vi	rtual disks				
	Name	~	Capacity	~	Free	$\sim$	Туре	~	Thin pro $\vee$	Access	$\sim$
	datastore1		1.86 TB		158.58 GE	З	VMFS6		Supported	Single	
										1 ii	tems
<b>vm</b> ware <sup>*</sup>											
						Ва	ck	Ne	kt Finis	h C	Cancel

Select the appropriate VM network that you want your controller to connect to. In our lab, we used VLAN-2-Native. Disk provisioning should be thick to ensure that enough disk space is reserved for the VM. Uncheck the "Power on Automatically" option and then click "Next."

1 New virtual machine - EdgeProtect-Controller						
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> </ul>	Deployment options Select deployment options					
4 Deployment options     5 Ready to complete	Network mappings	VM Network	VLAN-2-Native			
	Disk provisioning	O Thin  Thick				
	Power on automatically					
<b>vm</b> ware*						
			Back Next Finish Cancel			

Then click "Finish."

1 New virtual machine - EdgeProtect	Controller						
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	Review your settings selection before finishing the wizard						
	Product VM Name	export-i-0dae94a24fd3fe319 EdgeProtect-Controller					
	Files	export-i-0dae94a24fd3fe319-disk-1.vmdk					
	Provisioning type	Thick					
	Network mappings Guest OS Name	VM Network: ALT-2-INT Linux -Ubuntu 20.04.2 LTS					
	Do not refresh your brows	ser while this VM is being deployed.					
VIIIware							
		Back Next Finish Cancel					

Wait until OVA deployment is complete.

E Recent tasks								
I	Task ~	Target ~	Initiator ~	Queued ~	Started ~	Result 🛦 🗸 🗸	Completed <b>v</b>	~
I	Upload disk - export-i-0dae94a24fd3fe319-disk-1.vmdk (1 of 1)	BugeProtect-Controller	root	10/22/2021 16:19:14	10/22/2021 16:19:14	S 3	Running 25 %	
Ĩ								

E Recent tasks									
Task	Target V	Initiator ~	Queued	Started ~	Result 🔺 🗸 🗸	Completed v			
Upload disk - export-i-0dae94a24fd3fe319-disk-1.vmdk (1 of 1)	B EdgeProtect-Controller	root	10/22/2021 16:19:14	10/22/2021 16:19:14	Completed successfully	10/22/2021 16:21:12			

Once complete, right click on the VM and click on "Edit Settings."

O. B EdgePro	otect-Controller	
Quick filters	Power	•
	Guest OS	•
	Snapshots	•
	Provide Console	-
	🙀 Autostart	
	🙀 Upgrade VM Compatibility	
	🙀 Export	
	😝 Export With Images	
	Bdit settings	
	Permissions	

Change the CPU to 4 and Memory to 8 GB, and then click "Save."

ß	Edit settings - EdgeProtect-Controller	(ESX/ESXi 4.x virtual machine)	
	Virtual Hardware VM Options		
	🔜 Add hard disk 🛛 🎫 Add network ada	apter 🗧 Add other device	L
	CPU	4 ~ (1)	L
	- Memory		L
	RAM	8 GB ~	L
	Reservation	None ~ MB ~	L
		Reserve all guest memory (All locked)	l
	Limit	Unlimited ~ MB ~	
	Shares	Normal ~ 1000 ~	
	Memory Hot Plug	Enabled	
	▶ 🔜 Hard disk 1	100 GB ~	
		Save Cancel	

Power on the VM.

Once the controller is powered on, connect to the console. The username and password will be provided by your Cisco sales engineer.

EdgeProtect-Controller

🗔 🖬 🗖 🧾 💮 Actions 🛞

Ubuntu 20.04.2 LTS controller tty1 controller login: \_\_

Log on using the credentials provided by your Cisco sales engineer.

```
, Lugo, 101001 00111 0110
 EdgeProtect-Controller
                                                                  🗔 🖬 🗖 🌉 🏠 Actior
  System information as of Fri Oct 22 20:16:11 UTC 2021
  System load: 0.04
                                   Processes:
                                                              171
  Usage of /: 2.9% of 96.88GB
                                   Users logged in:
                                                              Û
  Memory usage: 3%
                                   IPv4 address for docker0: 172.17.0.1
  Swap usage:
              0%
123 updates can be applied immediately.
67 of these updates are standard security updates.
To see these additional updates run: apt list ––upgradable
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
ast login: Thu Oct 7 08:40:44 UTC 2021 from 87.239.255.105 on pts/0_
Context "default" modified.
rdadmin@controller:~$
rdadmin@controller:~$
 rdadmin@controller:~$
 rdadmin@controller:~$
 rdadmin@controller:~$
rdadmin@controller:~$
```

Discover the name of the controller interfaces by running the command ip add, as this may vary per installation.



Look for the interface that begins with "ens." In this example, we see "ens32." This information will be needed to configure the network settings.

Change directories to the /etc/netplan:

#### cd /etc/netplan

Find the yaml file by running the ls command.



Edit the yaml file to reflect the static IP address for the controller with the default gateway and your DNS servers. In this example, we will set the IP address to 192.168.2.118/24 with a default gateway of 192.168.2.1 and the Cisco Umbrella<sup>®</sup> DNS server of 208.67.222.222.

#### sudo nano 50-cloud-init.yaml

This is what it looks like before you edit it.



Below is the newly configured yaml file, with the correct interface name (ens32) and network settings.



Press "Control + X" to exit, and then press "Enter" to confirm the save.

Apply the new network setting using the following command:

sudo netplan apply

## rdadmin@controller:/etc/netplan\$ sudo netplan apply rdadmin@controller:/etc/netplan\$

Validate that the configuration took effect by running the command ip addr | head again and validating that the interface is configured correctly. Also make sure that your network is reachable by pinging a known valid and pingable address such as your default gateway.

rdadmin@controller:~\$ ip add   head	
1: lo: <loopback,up,lower_up> mtu 65536 qdisc noqueue state UNKNOWN group defa</loopback,up,lower_up>	ul
t glen 1000	
link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00	
inet 127.0.0.1/8 scope host lo	
valid_lft forever preferred_lft forever	
inet6 ::1/128 scope host	
valid_lft forever preferred_lft forever	
2: ens32: <broadcast,multicast,up,lower_up> mtu 1500 qdisc fq_codel state UP g</broadcast,multicast,up,lower_up>	ro
up default qlen 1000	
link/ether 00:0c:29:3e:8b:71 brd ff:ff:ff:ff:ff	
inet 192.168.2.118/24 brd 192.168.2.255 scope global ens32	
valid_lft forever preferred_lft forever	
rdadmin@controller:~\$ ping 192.168.2.1	
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.	
64 bytes from 192.168.2.1: icmp_seq=1 ttl=255 time=0.462 ms	
64 bytes from 192.168.2.1: icmp_seq=2 ttl=255 time=0.195 ms ^C	
192.168.2.1 ping statistics	
2 packets transmitted, 2 received, 0% packet loss, time 1029ms	
rtt min/avg/max/mdev = 0.195/0.328/0.462/0.133 ms	
rdadmin@controller:~\$	2

#### Installing the controller software on the VM.

Download the controller .tar file using the provided wget command. A link to the .tar file will be provided in a separate email:

\$ wget -O "controller-<version x\_y\_z>.tar.gz" "https://<DOWNLOAD LINK>"

File can also be copied using SCP onto the VM if direct internet access is not available.

1. Copy the .tar file to /tmp/ with \$ cp controller-<version x\_y\_z>.tar.gz /tmp/.

```
$ cd /tmp
$ tar -xvf controller<version x_y_z>.tar.gz
```

```
2021-10-23 01:47:47 (6.38 MB/s) - `/tmp/controller-2.4.0.998.tar.gz' saved [2125
305304/2125305304]
rdadmin@controller:~$ ls
rdadmin@controller:~$
rdadmin@controller:~$
rdadmin@controller:~$ cd /tmp
rdadmin@controller:/tmp$ ls
controller-2.4.0.998.tar.gz
snap.1xd
systemd-private-91b70d0b5aa94190be93d38557723777-fwupd.service-nfuTaf
systemd-private-91b70d0b5aa94190be93d38557723777-systemd-logind.service-CioSlg
systemd-private-91b70d0b5aa94190be93d38557723777-systemd-resolved.service-eEMvxi
systemd-private-91b70d0b5aa94190be93d38557723777-systemd-timesyncd.service-quBdl
i
vmware-root_391-1823935079
rdadmin@controller:/tmp$ tar -xvf controller-2.4.0.998.tar.gz
controllerctl
defaults.yml
images/
images/confluentinc_cp-kafka@5.5.0
images/confluentinc_cp-zookeeper@5.5.0
```

Run the deployment script:

#### \$ ./scripts/deploy.sh

Note

The deployment process will run a set of validation tests to confirm that the minimum requirements are met and that no errors were encountered.

#### **Controller configuration**

Follow the steps below to configure the controller. At the end of this process, you will be able to connect to the controller management system with your web browser: http://<controller\_hostname> or http://<controller\_ip>.nip.io

To access the controller, a valid hostname is required that is resolvable via DNS. If you do not have access to create a resolvable hostname, the nip.io service can be used, but you must manually add the client IP to hostname mapping in the client machine's hosts file that is by default located in C:\Windows\System32\ drivers\etc. Administrator access to the client machine is required to modify the hosts file.

1. Verify that the controller directory exists:

```
$ cd /opt/app/controller
$ ls -lah
```

2. Create a file named config.yml in the /opt/app/controller directory and modify the hostname to an applicable URL.

\$ nano config.yml

Use the configuration below as a reference for the config.yml. Copy the example file to config.yml and modify it based on your setup.

Note: Be sure to use the right yaml format and two spaces for indentation.

#### **IMPORTANT**

The hostname **MUST be a valid DNS hostname** that can be reached from your browser. It is possible to use the nip.io services and set the internal IP or add the URL to your local hostname file with a matching IP. More information on the nip.io service can be found at https://nip.io.

Reference example for config.yml file using the nip.io:

```
---
global: authentication:
user: admin@example.com
password: 12345
kubernetes:
ingress:
hostname: 192.168.2.118.nip.io
```

Reference example for config.yml file using the hostname:



3. Start the controller service.

#### \$ ./controllerctl start

4. Verify that the controller services are running with the command:

#### \$ cd /opt/app/controller

\$ kubectl get pods

		-									
🞤 rdadmin@controller: /opt/app/controller			_		×						
secret/warroom-secrets unchanged											
deployment.apps/warroom unchanged											
rdadmin@controller:/opt/app/controlle	r\$ kubect	tl get pods									
NAME	READY	STATUS	RESTARTS	AGE							
broker-0	1/1	Running	0	7m5s							
zookeeper-0	1/1	Running	0	7m5s							
grafana-bdfd449f8-zrwgs	1/1	Running	0	7m5s							
ca-0	1/1	Running	0	7m5s							
mongodb-0	1/1	Running	0	7m5s							
influxdb-0	1/1	Running	0	7m5s							
redis-0	1/1	Running	0	7m5s							
broker-init-7dfzn	0/1	Completed	0	7m1s							
config-6d8dcd78b-t4kcf	1/1	Running	0	6m38s							
rpm-registry-0	1/1	Running	0	6m38s							
controller-rest-api-5484997486-mpkvb	1/1	Running	0	6m38s							
notifier-5dbd6db744-xwqhs	1/1	Running	0	6m38s							
config-6d8dcd78b-h52hm	1/1	Running	0	6m38s							
warroom-f448d6bf5-vlxtk	1/1	Running	0	6m38s							
frontend-7974b96b85-flshw	1/1	Running	0	6m38s							
grpc-server-5855c844cb-6q9kl	1/1	Running	0	6m38s							
deployer-644774779-rkg8n	1/1	Running	0	6m38s							
deployer-644774779-wmkl6	1/1	Running	0	6m38s							
health-monitor-bf76b8d49-krdrm	1/1	Running	0	6m38s							
rdadmin@controller:/opt/app/controlle:	r\$ 🗧										

Make sure you are in the correct namespace. If not, run:

sudo kubectl config set-context --current --namespace controller

5. Open your browser and use the URL set in hostname: http://<controller-hostname> or http://<controller\_ip>.nip.io

🟥 Release N 🗙 📑 XR toolb X 👬 👬	oplicatic 🗙 🛛 G cisco um 🗙 📔 Domains 🗙 💿 Dpro Con	× +	• -		× I
$\leftarrow$ $\rightarrow$ C ( A Not secure   edgecon	.santossec.com/login	\$	e 🛯 🦕	* 🔍	i din
🗰 Apps   S Direct download 📙 3d Printi	g 📙 5G 📙 A10 📙 Admin 📙 Andrew 📙 Ansible	» 📙 Othe	r bookmarks	🛅 Readin	g list
	cisco				
					F
	Email <sup>*</sup>				a
	admin@example.com				
	Decessory *				
	•••••				tr
	Login				
	Forgot password?				.c
			0,		n

6. Log in with the default user admin@example.com and password 12345 or with the user and password configured in the config.yml file.



#### Controller installation is now complete.

#### **5B. Licensing**

By default, the controller is provided with a 30-day evaluation license.

To add or view the license, go to Settings (bottom left) and then click on the licensing tab.

To obtain a new license, reach out to your Cisco sales engineer and provide them with the controller MAC address:



## 6. Adding a detector

To add an emulator detector or a real detector, follow the same steps. Differences include using either the controller's IP address and SSH credentials or using the router's IP addresses and credentials.

Prior to adding an emulator detector, the emulator JSON file may need to be edited with the correct emulator filename.

To find an available emulator file, go to the following directory on your controller CLI.

\$ cd /opt/app/controller/rpm
\$ ls

rdadmin@controller:/opt/app/controller\$ cd rpm rdadmin@controller:/opt/app/controller/rpm\$ ls dpro-210529.rpm dpro-emulator@2.1.0.529 rdadmin@controller:/opt/app/controller/rpm\$

Copy the name of the "dpro-emulator..." In this case, it is dpro-emulator@2.1.0.529.

Go to Settings (bottom left) and then click on the "Templates" tab. Then click on the in the righthand side of the emulator default.

alialia cisco	Secure DDoS Edge Protection			
88	Templates   Integrations   Us	ers   Api Keys   Licensing		
Dashboard	Hardware Configuration Security			
D	Name ^	Router Family	Description	
Detectors	emulator default	emulator		
کی Attacks	NCS540 default	NC5540		
$\bigcirc$				
Protected Objects				

Select "Edit JSON."



Scroll down through the file until you reach the line that starts with "rpmSrc."

Edit Template JSON	×
<pre>"memoryInMB": 8096, "allocatedCores": 2, "allocatedMemoryInMB": 1024, "warningMemoryPercentage": 50, "criticalMemoryPercentage": 80, "warningCpuPercentage": 80, "roriticalCpuPercentage": 80, "maxCpuGauge": 200, "detectorMaxFPS": 120000, "maxTelemtryPPS": 5000, "maxTelemtryPPS": 5000, "maxTelemtryMBs": 10, "deploySupport": true, "appStartSupport": true, "appStartSupport": true, "configSupport": true, "configSupport": true, "rpmSrc": "dpro-emulator@2.0.0.493", "interfaces":[ "TenGigE0/0/0/0", "TenGigE0/0/0/2",</pre>	

Edit the line with the correct file name capture in the rpm directory. Then click "Update."



nta Release Note:	s for Cisco NCS 540 🗙 📔 🛅 XR toolbox, Part	6: Running Dock 🗙   🏥 Application Hostin	g Configuratio 🗙 📔 Ġ cisco umbrella d	ns servers - Goo; 🗙 📔 Domains	& SSL   IONOS ×	<ul> <li>Dpro Controller</li> </ul>	× +		o – ø ×
⊢ → C (	A Not secure   edgecont.santossec.com	n/detectors?detectorsFilter=%7B"genSta	tus"%3A%5B%5D%7D					\$ 0	🕼 😋 🛪 🕥 i
🚦 Apps  🚱 Di	irect download 🔜 3d Printing 📑 5G	📕 A10 📃 Admin 📃 Andrew 📃 Ar	sible 🔜 API 🔜 App IOS course	AWS 🔜 Azure 🔜 BGP	CCIE Security 🧧 Certifice	ates 🔜 Cisco 🔜 Cloud 📃	Coursera 🔜 CURL	📙 DataCentre 🛛 » 📔 Other br	ookmarks 🕴 🔠 Reading list
alialia cisco	Secure DDoS Edge Protect	tion							
		5							
Dashboard	Status Name ^	Description	Model	Version		Deploymen	t Container	Configuration	Import Detectors
				No Detect	ors				
Detectors									

On the Info page, fill in the fields with the appropriate information. In this example, we use the following:

- Detector Name: Detector-Example
- Description: My Emulator Detector
- Latitude: 40.748817
- Longitude: -73.985428
- Hardware Template: emulator default

uludu cisco	Secure DDoS Edge Protection Add Detector
Dashboard	into / Main Conngulation / Security Conngulation
Detectors	General Info Detector Name: * Detector-Example
S.	Description:
Attacks	My Emulator Detector
Protected	Latitude 40.748817
Objects	Longitude
	-73.985428
	Hardware Template: emulator default ~

Click on the "Main Configuration" tab.

Use the IP address of the controller for the IP Address, NETCONF Server IP, and the Exporter IP. Also use the SSH username and password of your controller, as this is an emulator.

Uncheck the TenGigE0/0/0/2 rx box and then click "Create."

allulu cisco	Secure DDoS Edge Protection Add Detector Info > Main Configuration > Security Configuration	
	standard v	
Detectors	Management Access Info (gRPC)	Telemetry Info
<del>S</del>	Ip Address: *	Protocol:
Attacks	1721002110	
$\bigcirc$	NETCONF Access Info	192.168.2.118
Protected Objects	NETCONF Server 1p: * 192.168.2.118	Interfaces Interface Name: Mode:
	NETCONF User Name:*	Ten:GigEΩ/0/0/1 -
	_rdiadmini	TenGigE0/0/0/2 V Irx Itx X
	NETCONF Server Password:	TenGigE0/0/0/3 - nx tx X
		Cancel

ahaha cisco	Secure	DDoS Edge Protection								
	De	lectors								
Dashboard										
	Status	Name 🔿	Description	Model	Version		Deployment	Container	Configuration	
Detectors	•	Detector-Example	My Emulator Detector	emulator	dpro-emulator@2.1.0.	529 6173951829026dde7e098173				

Secure De	DDoS Edge Protection tectors								<u>ب</u>
Searc									
Status	Name ^	Description	Model	Version		Deployment	Container	Configuration	
۰	Detector-Example	My Emulator Detector	emulator	dpro-emulator:2.1.0.529	6173963629026dde7e0985f6				

After one to two minutes, you should see the emulator detector up.

The process is now complete to add the emulator detector.

### 7. Resources

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

Americas Headquarters

Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

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: https://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. (1110R)

Printed in USA