

## HOW TO – QUANTUM IOT PROTECT – ONBOARDING



Documento escrito por: Lisandro Weissheimer da Silva  
Security Engineering Brazil  
Dezembro/2023

## CONTEÚDO

Sobre a solução: Quantum IoT Protect	3
Cenário atual	3
Quantum IoT Protect	3
Proteção Autônoma para dispositivos IoT	3
Perfis de rede IoT autônoma de confiança zero	4
Gerenciamento simples de IoT em um único console	4
Onboarding do Quantum IoT Protect	5
Cenário utilizado	5
Gateway	5
Manager	5
Políticas	6
Regras de Acesso	6
Ativação do serviço IoT Protect no Portal Infinity	7

## Sobre a solução: Quantum IoT Protect

### Cenário atual

O uso de dispositivos da Internet das Coisas (IoT) em aplicações empresariais, de saúde e industriais oferece benefícios de produtividade, mas também expõe as redes à ameaças cibernéticas em constante evolução.

De câmeras IP e elevadores inteligentes a dispositivos médicos e controladores industriais, o Quantum IoT Protect protege suas redes IoT contra ataques cibernéticos.

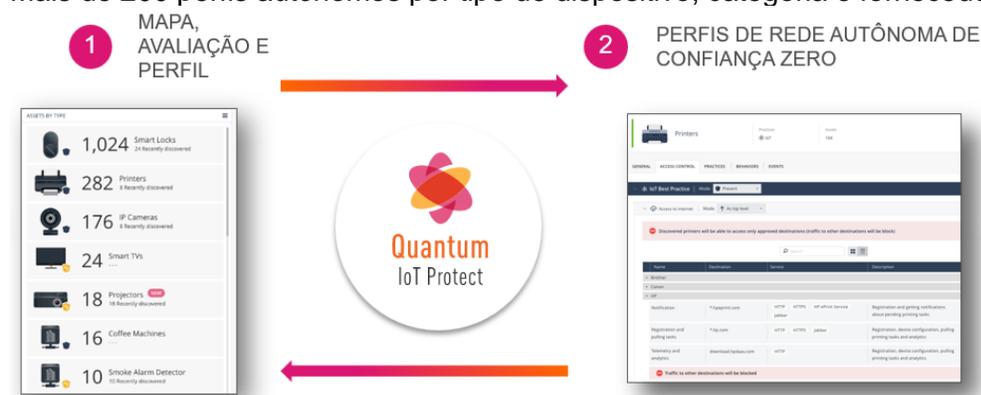
### Quantum IoT Protect

Prevenção autônoma de ameaças para proteção de rede e no dispositivo



### Proteção Autônoma para dispositivos IoT

Mais de 200 perfis autônomos por tipo de dispositivo, categoria e fornecedor



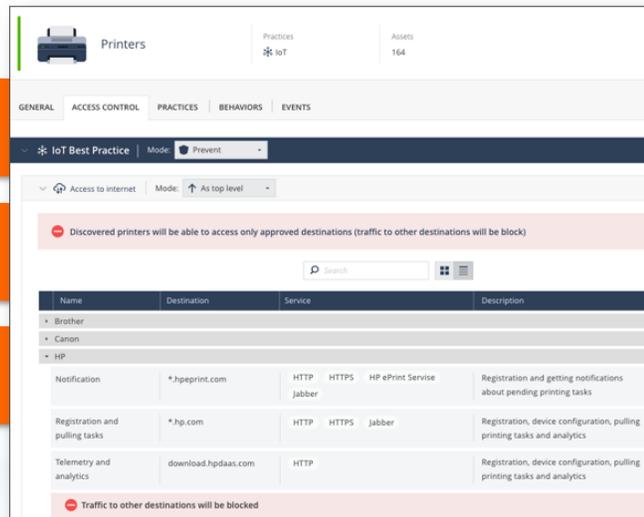
## Perfis de rede IoT autônoma de confiança zero

Com o Quantum IoT Protect, você também começa a entender como os dispositivos estão se comunicando e com o que estão se comunicando. Aproveitamos técnicas de IA e aprendizado de máquina para compreender completamente os padrões e criar automaticamente regras que permitem a comunicação adequada para o dispositivo e bloquear qualquer ação não autorizada que possa servir como uma ameaça potencial à rede. É aqui que você realmente percebe a peça de prevenção.

Os perfis são baseados em IA e análise comportamental

Zero-Trust: permite apenas a comunicação necessária do dispositivo

Prevenção contra ameaças aplicada automaticamente em novos ativos

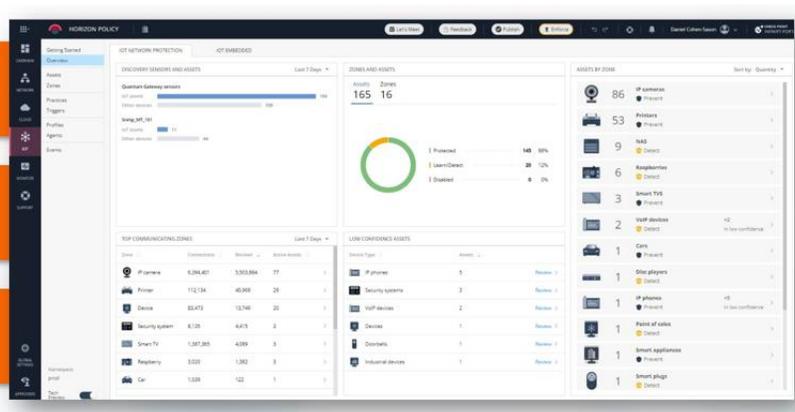


## Gerenciamento simples de IoT em um único console

Visibilidade para todos os ativos conectados em poucos minutos!

Perfis autônomos de confiança zero aplicados imediatamente depois.

Ataques conhecidos e desconhecidos de dia zero são bloqueados em tempo real.



Uma solução abrangente de segurança de IoT é necessária para proteger sua empresa contra esses riscos e é um componente vital da estratégia de segurança cibernética de cada empresa.

## Onboarding do Quantum IoT Protect

### Cenário utilizado

Os próximos passos descrevem o processo de onboarding do Quantum IoT Protect bem como as características do ambiente utilizado. Neste cenário presumimos que o gateway de segurança já está operacional e sua manager devidamente conectada e ativada. Este exemplo utiliza a manager SaaS Smart-1 Cloud e o procedimento leva isto em conta.

### Gateway

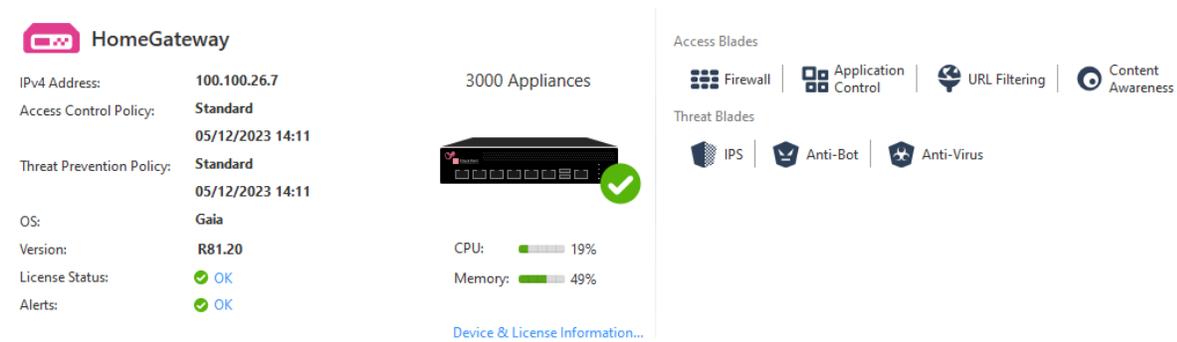
**Modelo:** 3600

**Versão Gaia:** R81.20 Jumbo Hotfix Take 41

**Kernel:** 3.10.0-1160.15.2cpx86\_64

**Edition:** 64-bit

**Build:** 631



**HomeGateway**

IPv4 Address: 100.100.26.7

Access Control Policy: Standard

Threat Prevention Policy: Standard

OS: Gaia

Version: R81.20

License Status: ✔ OK

Alerts: ✔ OK

3000 Appliances

CPU:  19%

Memory:  49%

[Device & License Information...](#)

**Access Blades**

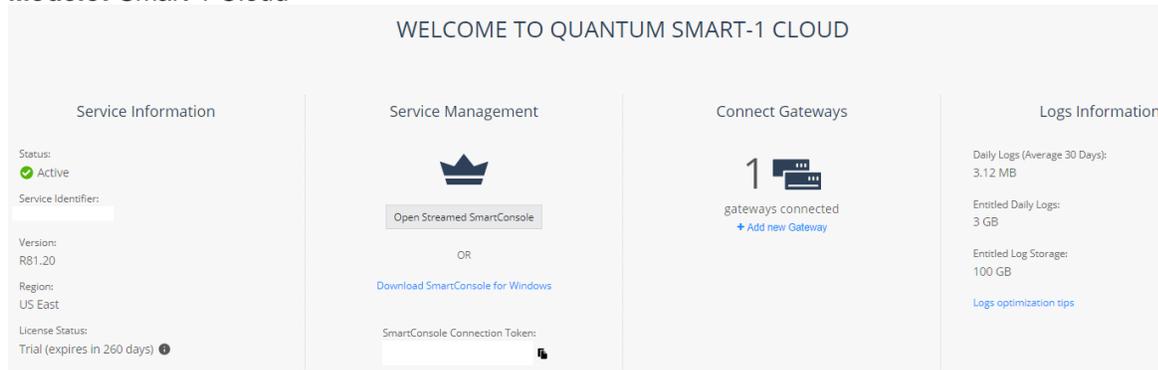
- Firewall
- Application Control
- URL Filtering
- Content Awareness

**Threat Blades**

- IPS
- Anti-Bot
- Anti-Virus

### Manager

**Modelo:** Smart-1 Cloud



WELCOME TO QUANTUM SMART-1 CLOUD

**Service Information**

Status: ✔ Active

Service Identifier:

Version: R81.20

Region: US East

License Status: Trial (expires in 260 days) 🔔

**Service Management**



[Open Streamed SmartConsole](#)

OR

[Download SmartConsole for Windows](#)

SmartConsole Connection Token:

**Connect Gateways**

1 

gateways connected

[+ Add new Gateway](#)

**Logs Information**

Daily Logs (Average 30 Days): 3.12 MB

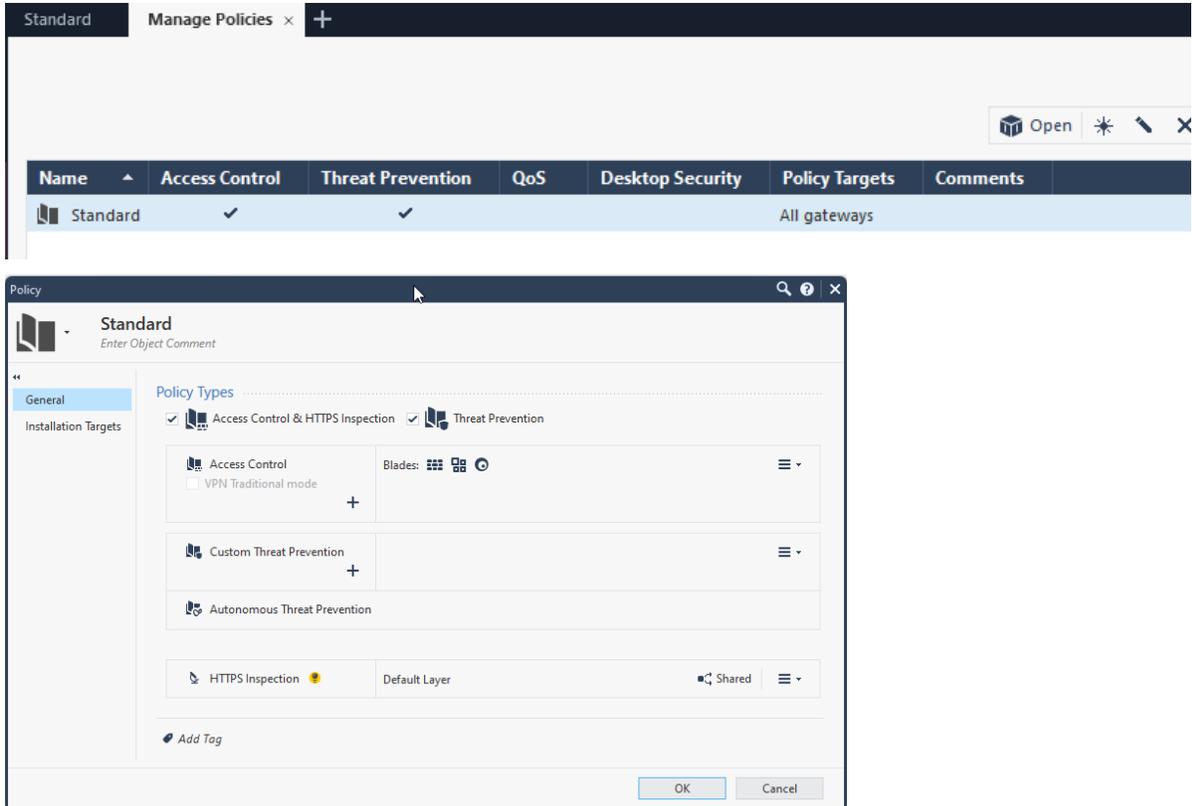
Entitled Daily Logs: 3 GB

Entitled Log Storage: 100 GB

[Logs optimization tips](#)

## Políticas

Abaixo temos as políticas criadas, onde podemos notar que há apenas a layer de Controle de Acesso, no pacote de políticas Standard.



The top screenshot shows the 'Manage Policies' window with a table of policies:

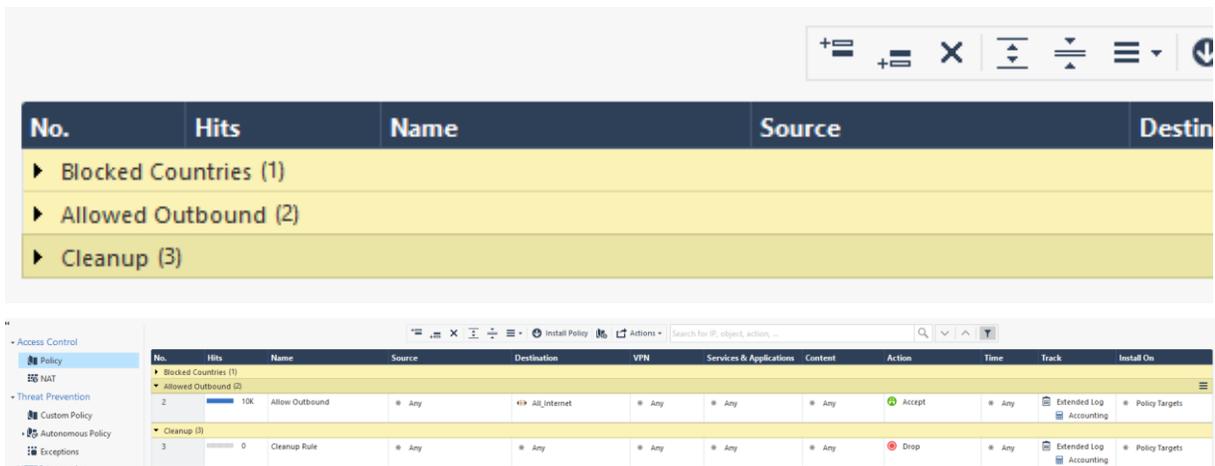
Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets	Comments
Standard	✓	✓			All gateways	

The bottom screenshot shows the configuration for the 'Standard' policy:

- Policy Types:**
  - Access Control & HTTPS Inspection
  - Threat Prevention
- Access Control:**
  - VPN Traditional mode
  - Blades: [Grid Icon] [Shield Icon]
- Custom Threat Prevention:** [Add] (+)
- Autonomous Threat Prevention:** [Add] (+)
- HTTPS Inspection:**
  - Default Layer
  - Shared

## Regras de Acesso

As regras de acesso criadas bloqueiam acesso inbound de determinados países. Esta regra não é mandatória, mas recomenda-se como boa prática. Possui ainda uma regra que permite qualquer tráfego de saída para a Internet e uma regra de Cleanup.



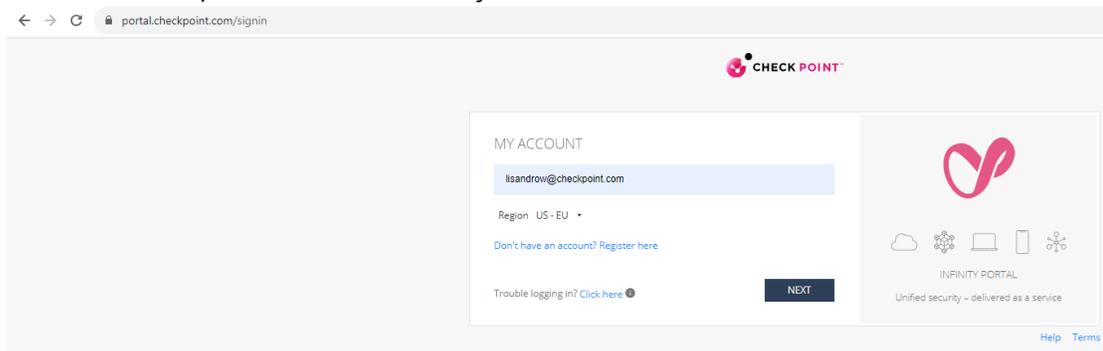
The screenshot shows the 'Access Control' rule base with the following rules:

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Content	Action	Time	Track	Install On
▶ Blocked Countries (1)											
▶ Allowed Outbound (2)											
▶ Cleanup (3)											
2	10K	Allow Outbound	Any	All Internet	Any	Any	Any	Accept	Any	Extended Log Accounting	Policy Targets
3	0	Cleanup Rule	Any	Any	Any	Any	Any	Drop	Any	Extended Log Accounting	Policy Targets

## Ativação do serviço IoT Protect no Portal Infinity

Para este exemplo iremos considerar que você já tem uma conta criada no Portal Infinity e sua instância de gerência, Smart-1 Cloud, está ativa e funcional, como mostrado nas imagens anteriores.

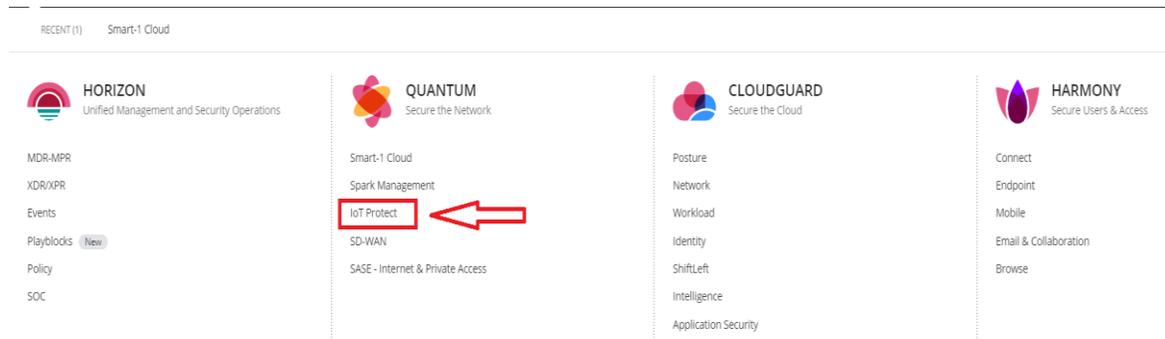
- 1- Faça login no Portal Infinity (<https://portal.checkpoint.com>) com uma conta que possua direitos administrativos e pode ativar novos serviços:



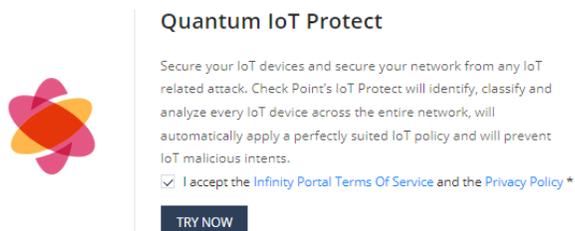
- 2- Após o login, vá até o canto superior esquerdo e clique no ícone do menu:



- 3- Selecione IoT Protect, como mostra a imagem abaixo:



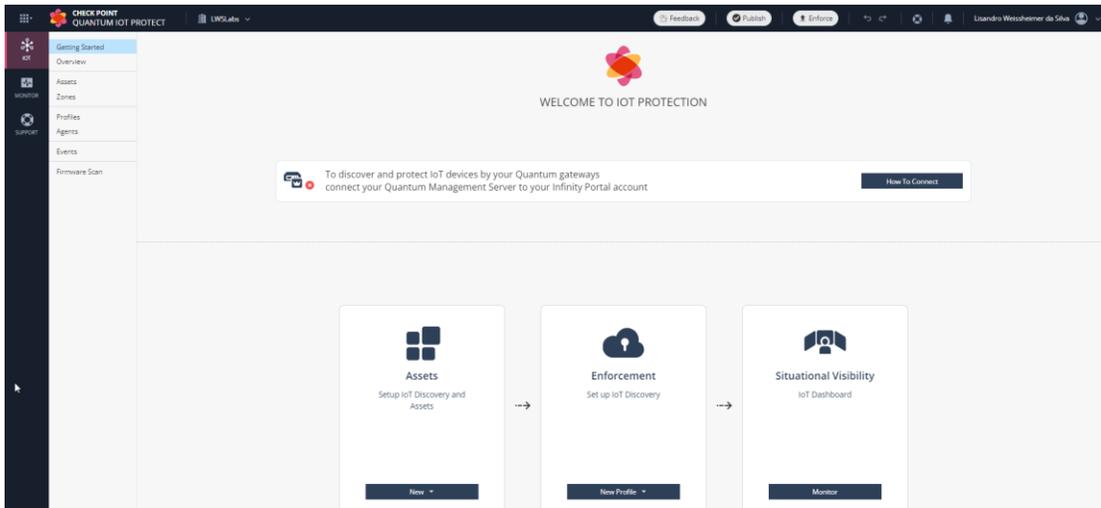
- 4- Aceite os termos e clique em TRY NOW:



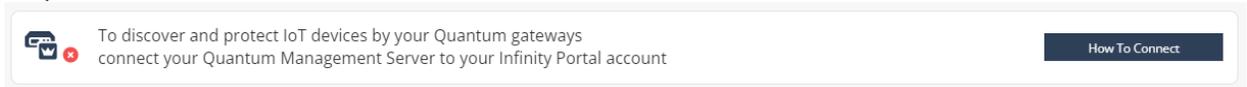
- 5- Aguarde a ativação dos serviços:



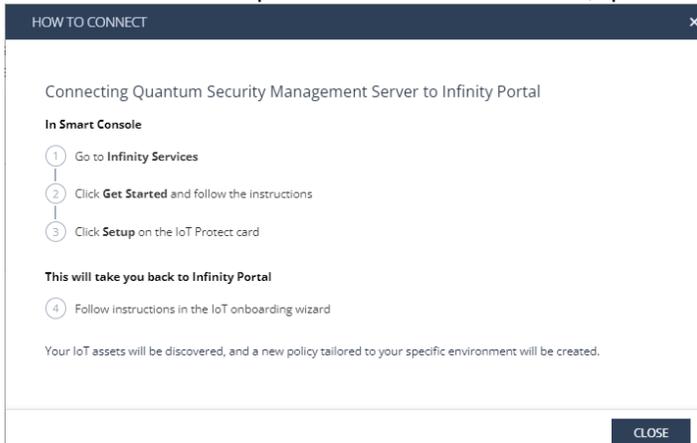
- 6- Após a ativação dos serviços, é necessário realizar algumas configurações na Smart-1 Cloud. A tela abaixo indica que os serviços foram ativados mas ainda dependem de configurações para funcionarem corretamente:



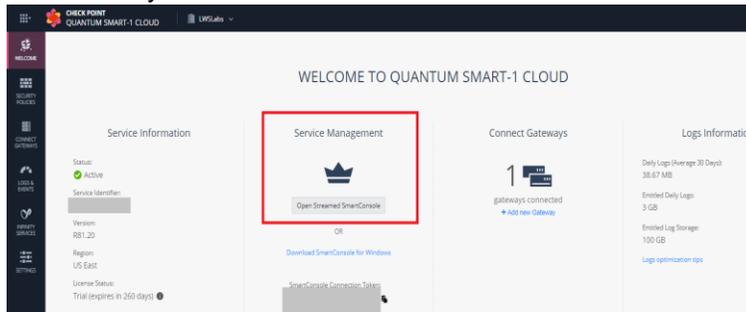
- 7- Clique em How To Connect:



- 8- A tela exibida traz os passos a serem executados, que faremos na sequencia:



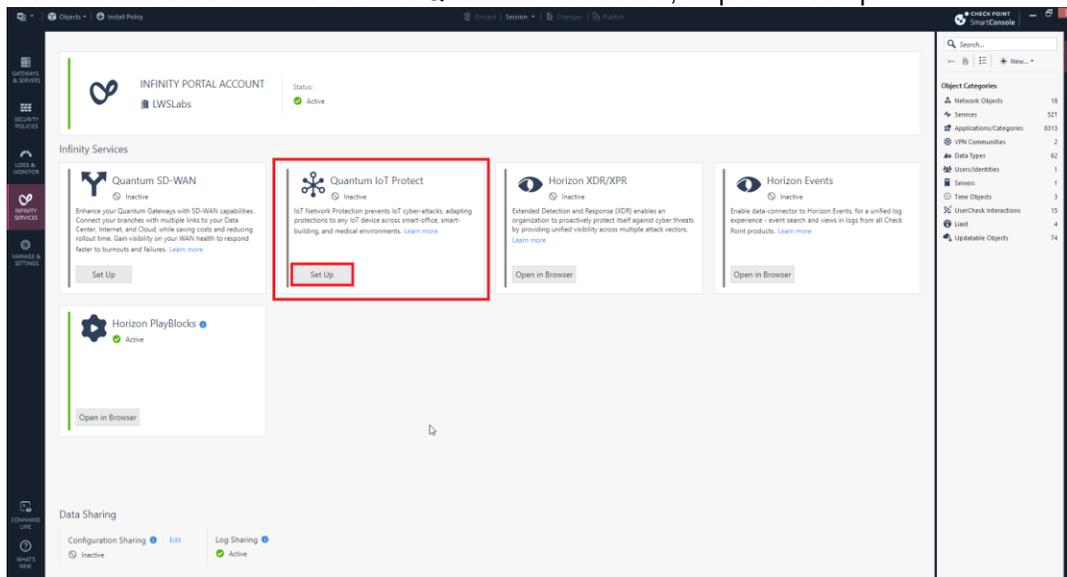
- 9- Acesse a SmartConsole instalada em seu computador ou através da Streamed SmartConsole no Portal Infinity:



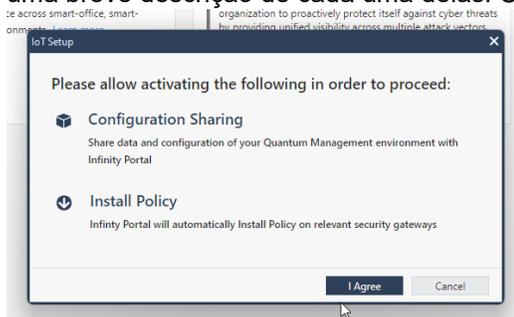
- 10- Neste exemplo usaremos a SmartConsole instalada localmente. Clique no botão Infinity Services:



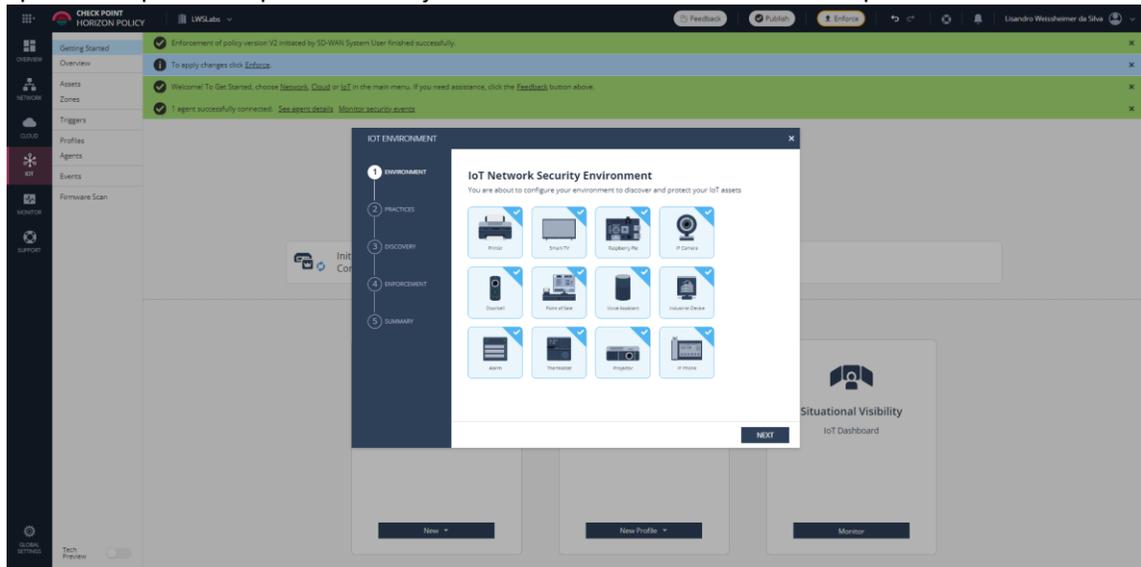
- 11- A tela abaixo será exibida. No card Quantum IoT Protect, clique em Setup:



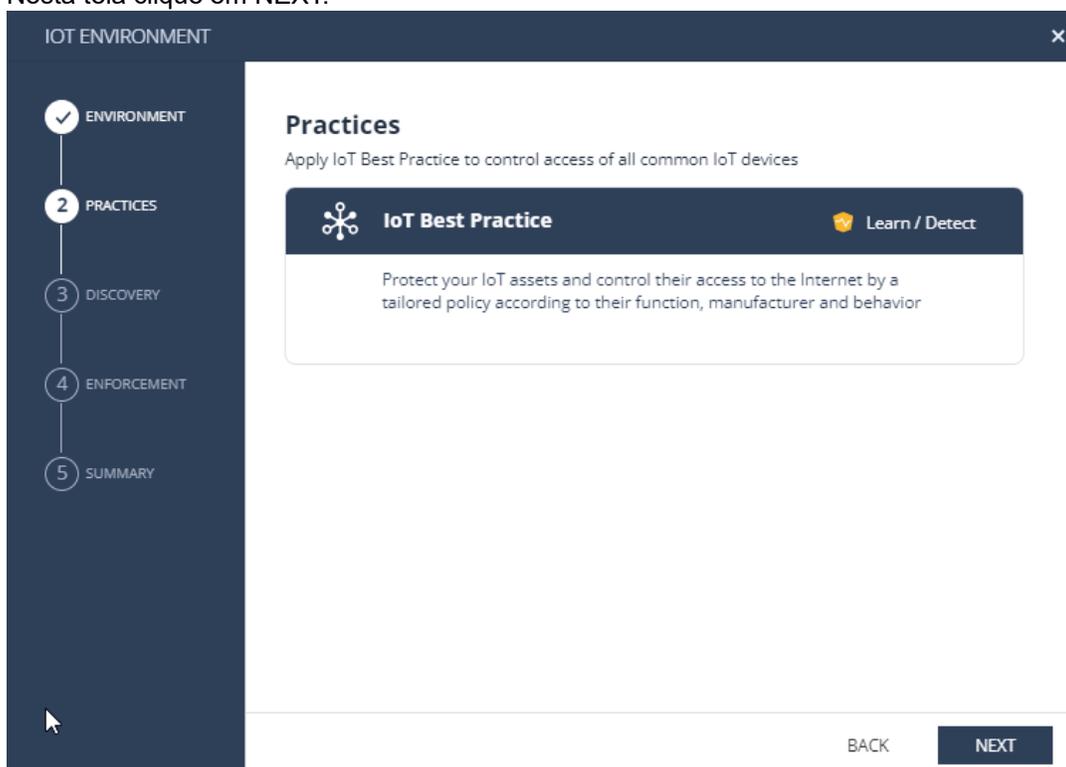
- 12- A tela abaixo traz as duas ações a serem executadas, Configuration Sharing e Install Policy, e uma breve descrição de cada uma delas. Clique em I Agree



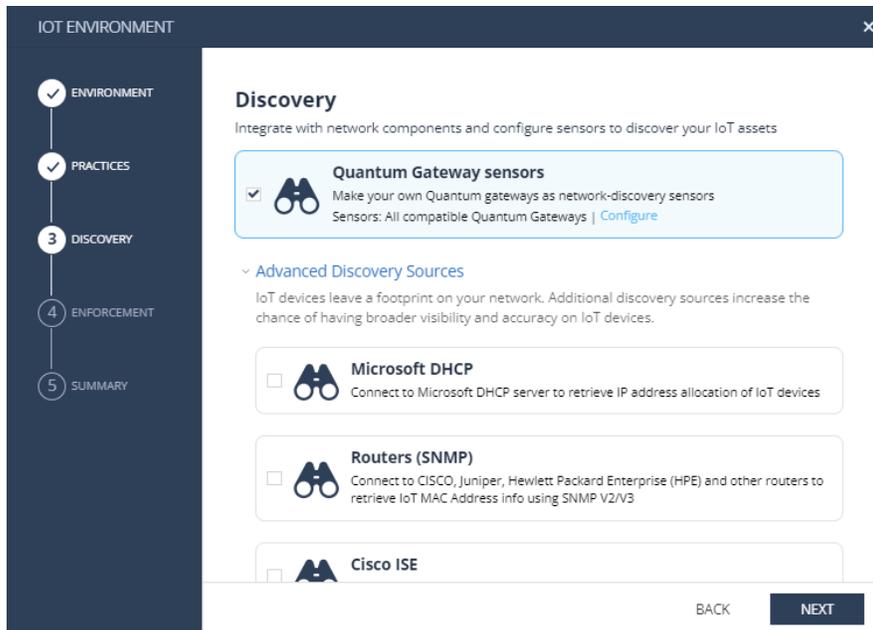
13- Você será direcionado ao Portal Infinity para finalizar a configuração. Certifique-se que todos os tipos de dispositivos que você deseja identificar estão selecionados e clique em NEXT:



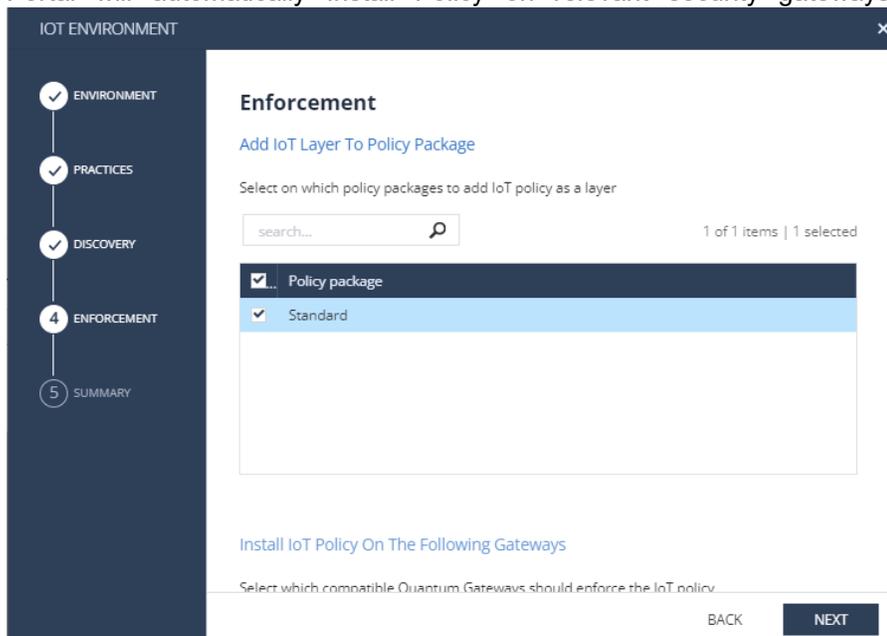
14- Nesta tela clique em NEXT:

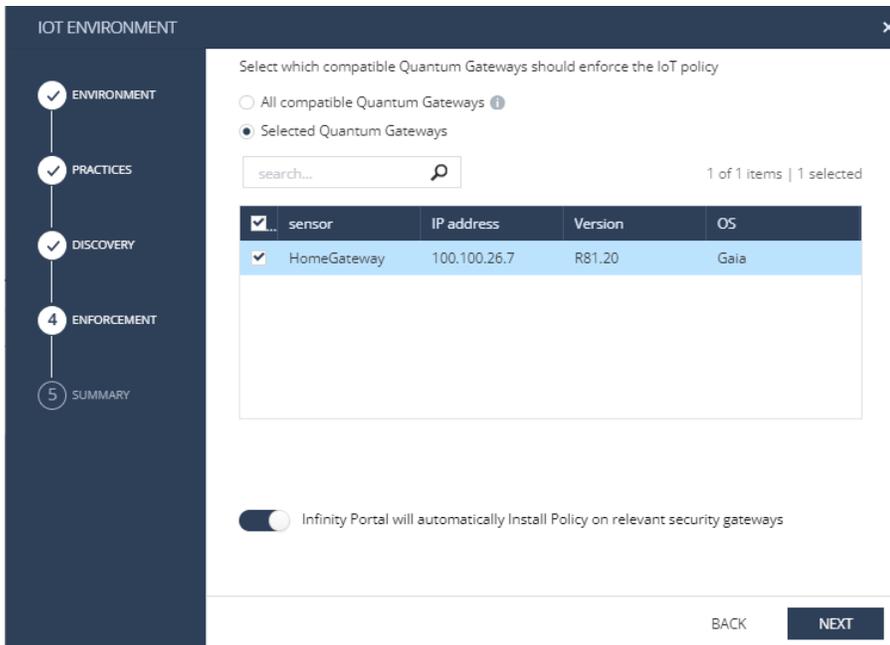


15- Na tela abaixo, Discovery, selecione apenas Quantum Gateway sensors, se ainda não estiver marcado. Note que outras fontes podem ser utilizadas para descoberta. Não trataremos destas outras fontes neste documento, nosso foco é ativar os serviços de descoberta e proteção nos Gateways de Segurança Check Point:

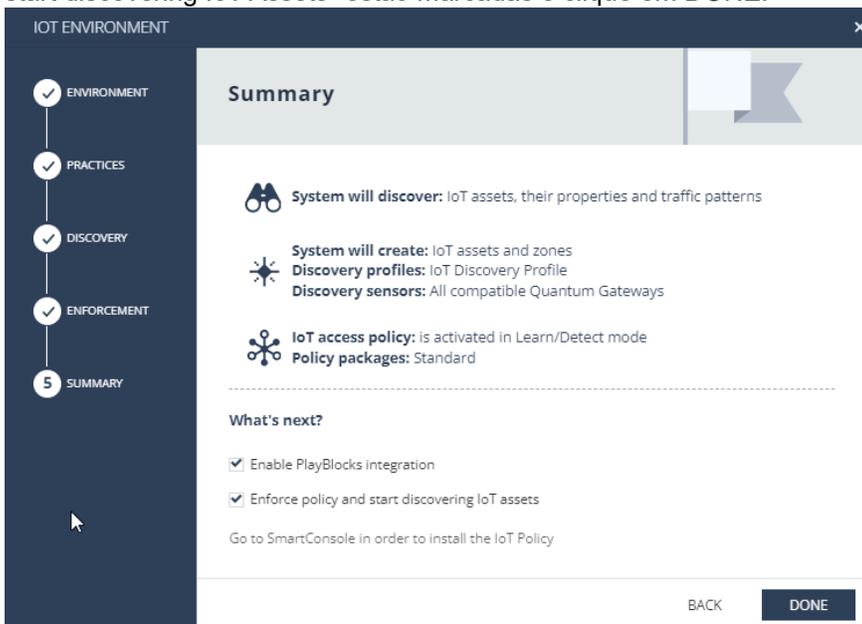


- 16- Selecione a política onde serão adicionadas as regras de acesso e proteção para IoT. Após selecionar a política, role a tela para baixo e escolha em quais Gateways você terá a layer de IoT e não esqueça de marcar a última opção, abaixo dos Gateways selecionados, onde diz "Infintiy Portal will automatically Install Policy on relevant security gateways". Clique em NEXT.

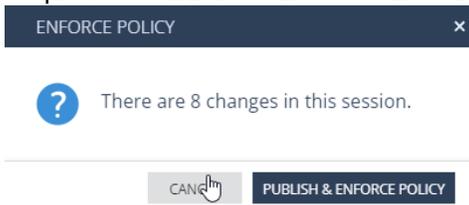




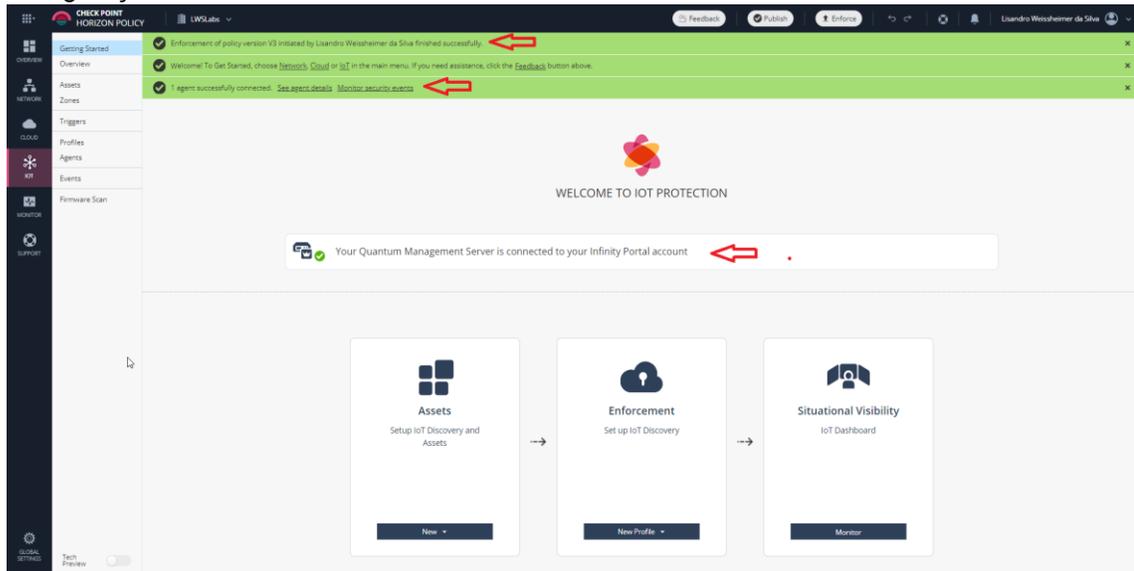
17- Na tela final, certifique-se que as opções “Enable [PlayBlocks](#) Integration” e “Enforce policy and start discovering IoT Assets” estão marcadas e clique em DONE:



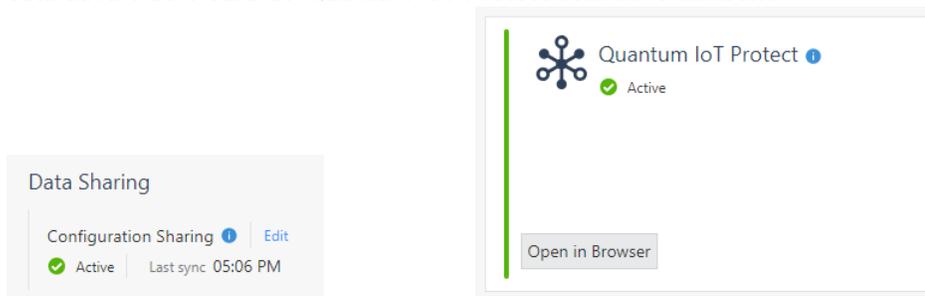
18- Será exibida a mensagem abaixo, indicando quantas alterações foram feitas nesta sessão. Clique em PUBLISH & ENFORCE POLICY:



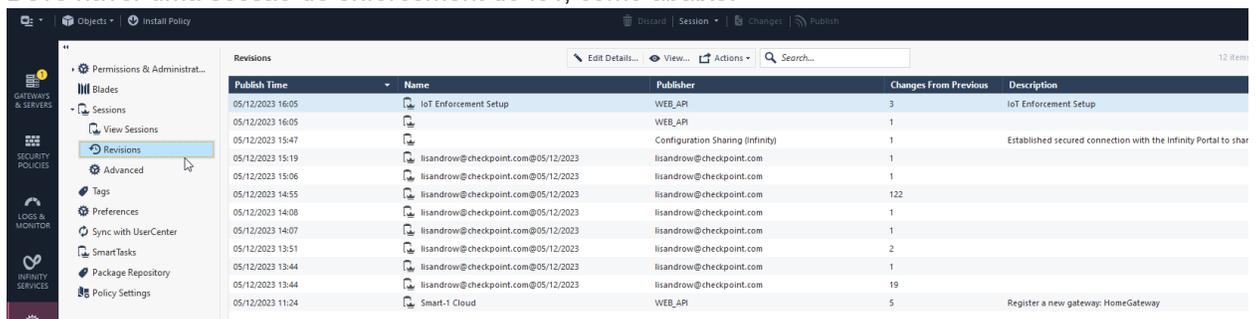
19- Ao término do enforce, você será direcionado para esta tela, indicando que houve sucesso na configuração:



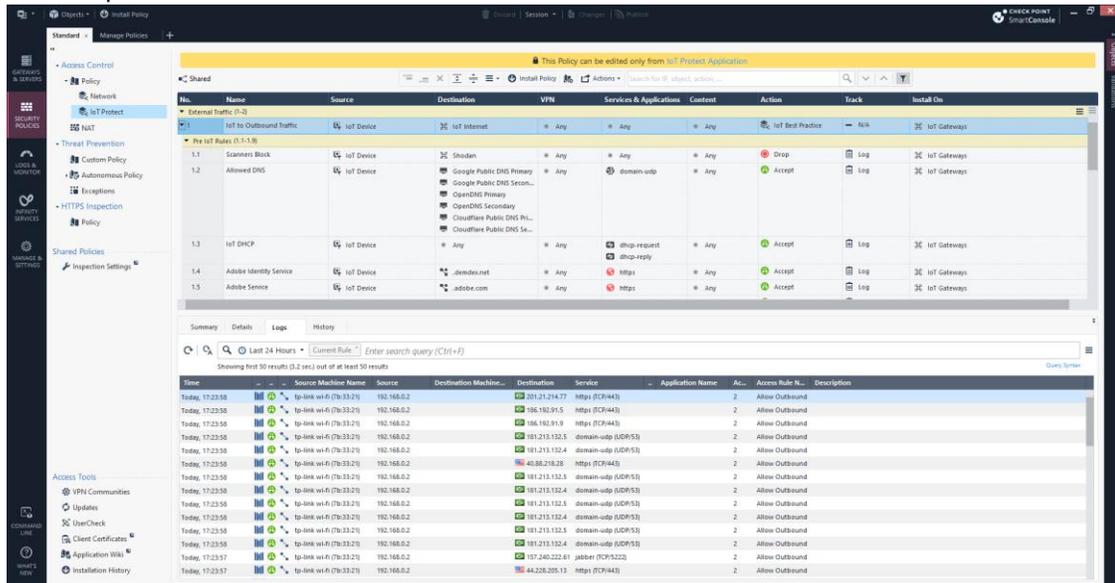
20- Retorne a SmartConsole no item Infinity Services e verifique se a opção Configuration Sharing está ativa e se o card do Quantum IoT Protect está ativo também:



21- Na SmartConsole, vá em MANAGE & SETTINGS e selecione Sessions e depois Revisions. Deve haver uma sessão de enforcement do IoT, como abaixo:



22- Na aba SECURITY POLICIES da SmartConsole você deve encontrar agora a layer IoT Protect e as suas políticas de acesso associadas:



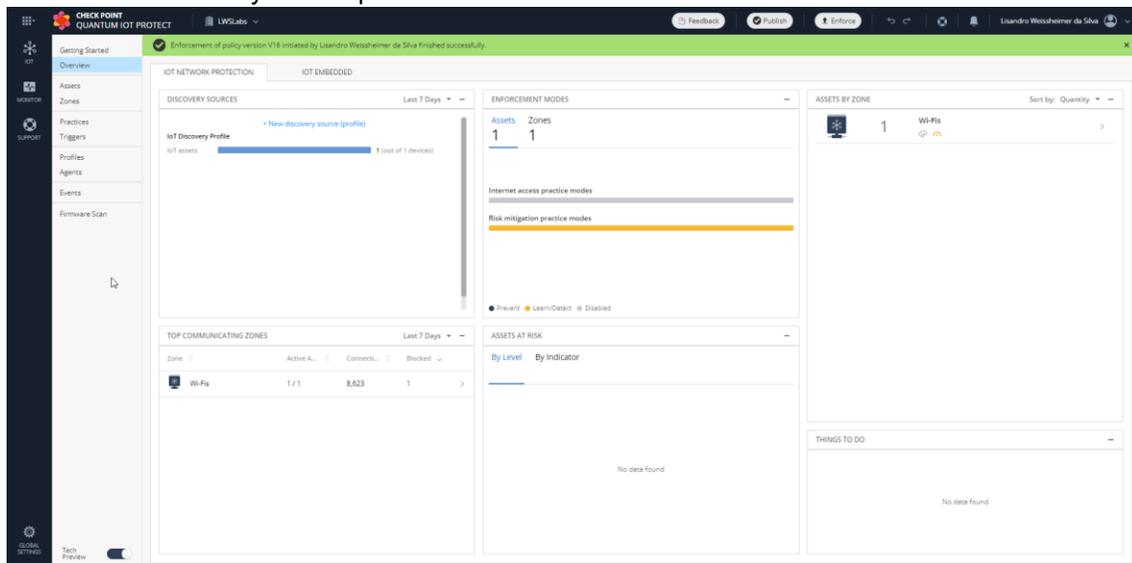
The screenshot shows the 'Security Policies' configuration page in SmartConsole. The left sidebar is set to 'Security Policies' and 'IoT Protect' is selected. The main area displays a table of rules for 'External Traffic (In)'.

Id	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track	Install On
1	IoT to Outbound Traffic	IoT Device	IoT Internet	Any	Any	Any	IoT Best Practice	N/A	IoT Gateways
* Pre IoT Rules (1.1-1.6)									
1.1	Scanners Block	IoT Device	Shodan	Any	Any	Any	Drop	Log	IoT Gateways
1.2	Allowed DNS	IoT Device	Google Public DNS Primary, OpenDNS Primary, OpenDNS Secondary, Cloudflare Public DNS Pri...	Any	domain-udp	Any	Accept	Log	IoT Gateways
1.3	IoT DHCP	IoT Device	Any	Any	dhcp-request, dhcp-reply	Any	Accept	Log	IoT Gateways
1.4	Adobe Identity Service	IoT Device	adobe.net	Any	https	Any	Accept	Log	IoT Gateways
1.5	Adobe Service	IoT Device	adobe.com	Any	https	Any	Accept	Log	IoT Gateways

Below the rules table, there is a log view showing traffic details for the selected rule.

Time	Source Machine Name	Source	Destination Machine...	Destination	Service	Application Name	Ac...	Access Rule No.	Description
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	201.21.214.77	https (TCP/443)	https (TCP/443)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	196.192.91.5	https (TCP/443)	https (TCP/443)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	186.192.91.9	https (TCP/443)	https (TCP/443)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	181.211.132.5	domain-udp (UDP/53)	domain-udp (UDP/53)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	181.211.132.4	domain-udp (UDP/53)	domain-udp (UDP/53)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	181.211.132.5	domain-udp (UDP/53)	domain-udp (UDP/53)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	181.211.132.4	domain-udp (UDP/53)	domain-udp (UDP/53)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	181.211.132.5	domain-udp (UDP/53)	domain-udp (UDP/53)	2	2	Allow Outbound
Today, 17:23:58	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	181.211.132.4	domain-udp (UDP/53)	domain-udp (UDP/53)	2	2	Allow Outbound
Today, 17:23:57	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	187.240.222.61	jabber (TCP/5222)	jabber (TCP/5222)	2	2	Allow Outbound
Today, 17:23:57	tp-link-wifi (79:33:21)	192.168.0.2	192.168.0.2	44.208.205.13	https (TCP/443)	https (TCP/443)	2	2	Allow Outbound

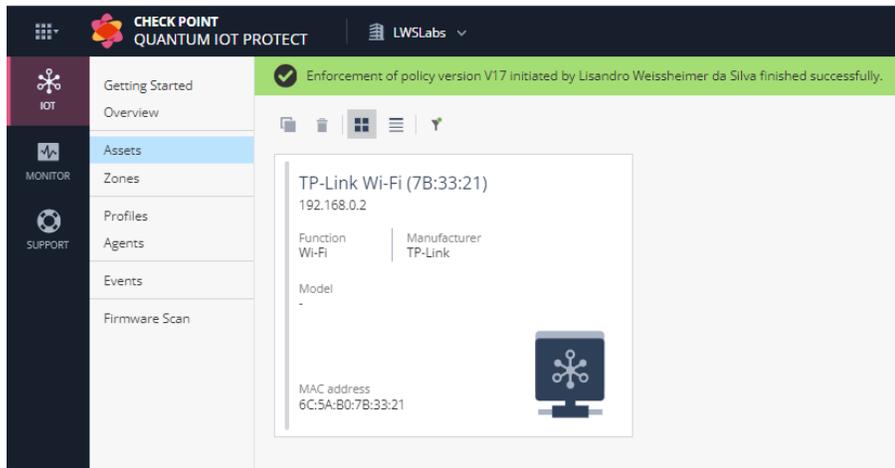
23- Volte ao Portal Infinity e verifique se existem dados na aba Overview:



The screenshot shows the 'Overview' page of the Check Point Quantum IoT Protect portal. The page displays various metrics and charts related to IoT network protection.

- DISCOVERY SOURCES:** Shows 1 IoT Discovery Profile and 1 IoT asset (1 out of 1 devices).
- ENFORCEMENT MODES:** Shows 1 Assets and 1 Zones. Includes sections for Internet access practice modes and Risk mitigation practice modes.
- TOP COMMUNICATING ZONES:** Shows 1 zone (Wi-Fi) with 1/1 Active Assets, 8,623 Connects, and 1 Blocked.
- ASSETS BY ZONE:** Shows 1 Assets in the Wi-Fi zone.
- ASSETS AT RISK:** Shows no data found.
- THINGS TO DO:** Shows no data found.

24- Na aba Assets você terá a lista dos ativos descobertos até o momento:



Deste ponto em frente, novos ativos serão descobertos e adicionados ao Quantum IoT Protect.

Para saber mais sobre Quantum IoT Protect, [clique aqui](#).

Para saber mais sobre Smart-1 Cloud, [clique aqui](#).