



物联网边界防护探讨

绿盟科技 创新中心 物联网安全实验室

张星

13426086697



CONTENTS



- 01 物联网边界威胁浅析
- 02 物联网安全网关进展介绍
- 03 软件定义边界在物联网安全中的应用
- 04 展望



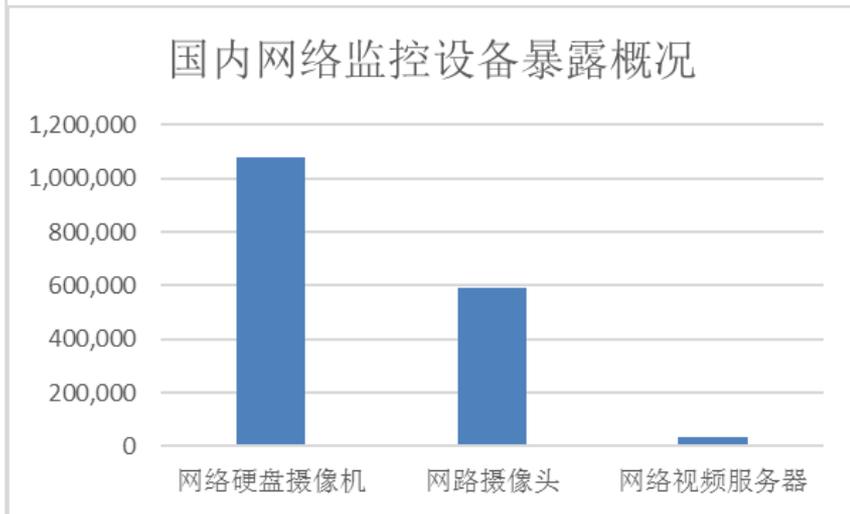
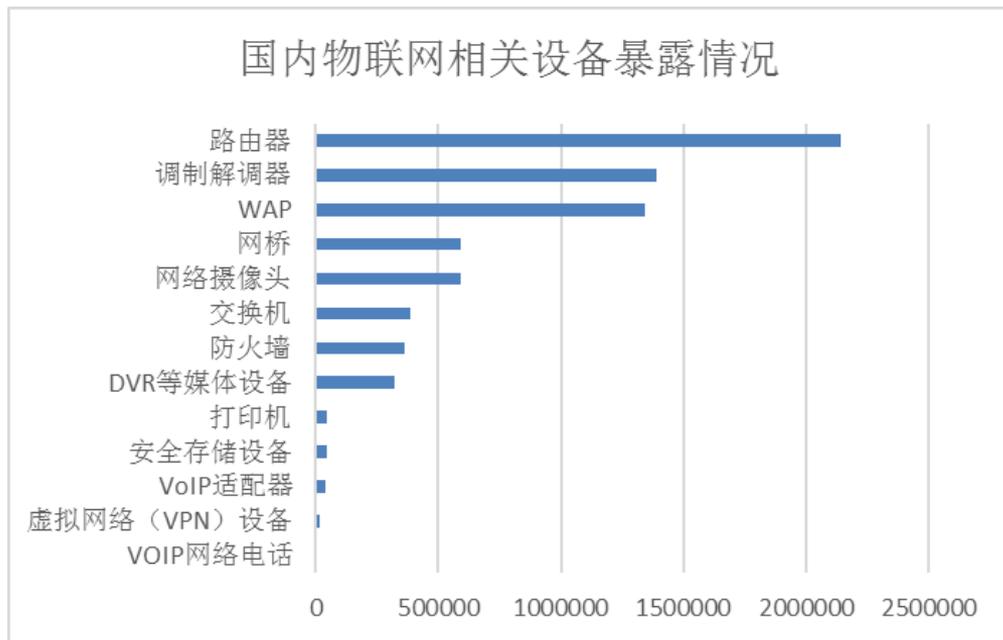
01

物联网边界威胁浅析

▶▶ 物联网安全事件层出不穷

- ❑ 2016年9月20日，著名的安全新闻工作者Brian Krebs的网站 KrebsOnSecurity.com受到大规模的DDoS攻击，其攻击峰值达到665Gbps，Brian Krebs推测此次攻击由Mirai僵尸发动。
- ❑ 2016年9月20日，Mirai针对法国网站主机OVH的攻击突破DDoS攻击记录，其攻击量达到1.1Tpbs，最大达到1.5Tpbs
- ❑ 2016年10月21日，美国域名服务商Dyn遭受大规模DDoS攻击，其中重要的攻击源确认来自于Mirai僵尸，美国东海岸地区遭受大面积网络瘫痪
- ❑ 2016年11月28日，德国电信遭遇断网时间，攻击源来自Mirai僵尸网络的新变种

物联网相关设备暴露情况严重



▶▶ 什么暴露在互联网上 (1)

IP地址	国家	更新日期	标签	详情
46.173.162.185	 Ukraine, Berezhani	2017-08-24 22:00:00 GMT	SMB TCP HTTP +2 Port(s)	Native OS: Windows 10 Pro 14393 Native Lan Manager: Windows 10 Pro 6.3 Primary Domain: WORKGROUP
146.88.46.4	 Thailand, Bangkok	2017-08-24 22:00:00 GMT	Boa HTTPS SSL HTTP TCP +3 Port(s)	HTTP/1.0 302 Moved Temporarily Date: Sun, 20 Aug 2017 00:15:47 GMT Server: Boa/0.94.13
185.44.27.83	 Spain, Cartagena	2017-08-24 22:00:00 GMT	SSH SSH TCP HTTP +4 Port(s)	Version: 2.7 Sequence: 120 Flags: 102 Session ID: 1717336166
93.183.145.164	 Bulgaria, Khaskovo	2017-08-24 22:00:00 GMT	Dropbear dropbear SSH TCP HTTP +5 Port(s)	'HTTP/0.9 400 Bad Request\r\nConnection: Keep-Alive\r\nKeep-Alive: timeout=20\r\nContent-Type: text
131.108.118.16	 Brazil, Catalao	2017-08-24 22:00:00 GMT	Dropbear SSH TCP +2 Port(s)	HTTP/1.1 401 N/A Server: TP-LINK Router Connection: close WWW-Authenticate: Basic realm="TP-LINK"
170.0.168.68	-,-	2017-08-24 22:00:00 GMT	Dropbear SSH TCP HTTP +2 Port(s)	SSH-2.0-dropbear_2016.74 key type: \x07ssh-rsa key
177.52.87.225	 Brazil, Jardinopolis	2017-08-24 22:00:00 GMT	SSH TCP HTTP +5 Port(s)	HTTP/1.1 200 OK Server: Router Webserver Connection: close Content-Type: text/html
201.159.53.121	 Brazil, -	2017-08-24 22:00:00 GMT	Dropbear SSH TCP HTTP +3 Port(s)	HTTP/1.1 302 Found Set-Cookie: AIROS_DC9FDB786346=e2c7ef0e671c51bde090e9192af807e; Path=/; Version=1 Location: /cookiechecker?uri=/ Content-Length: 0 Date: Mon, 08 May 2017 17:48:01 GMT Server:
170.239.52.154	-,-	2017-08-24 22:00:00 GMT	Dropbear SSH TCP HTTP +2 Port(s)	HTTP/1.1 200 OK Server: Router Webserver Connection: close Content-Type: text/html

▶▶ 什么暴露在互联网上 (2)

- ❑ 远程通信统一网关，TGU，Telematics Gateway Unit
- ❑ 采用3G/4G/GPRS/LTE/EDGE/HSDPA等通信模式连接至互联网。很多TGU配置有互联网IP地址，并且有对应的Web管理面板或者Telnet管理接口。

C4 Max

The ultimate telematics gateway



- Wide array of interfaces to perform in complex projects
- Internal antennae for easy install
- Wireless connection to peripherals via Bluetooth
- Fully programmable with powerful SDK
- Full engine control module (ECM) capabilities
- Runs on morpheus3 OS

▶▶ 什么暴露在互联网上 (3)

```
Advanced[C4E]> help
Help :
cmd [option1]option2]{str

Builtins :
cversion          Conso
help              Displ
screen [(X)]      Chang
color [0|1]       Enabl
lang [(str)]      Set t
reboot [(waitTime)] Reboo
completion        Activ
exit              Quit

Advanced :
ip [(str)]        Displ
stats             Displ
llog [soft|gps|update|kst
stopsoft          Stop
usercpn [list|start|stop]
userapk [list|start|stop]
gprsupdate [start|stop] E
geomap [update|delete] Up
policies [update|delete]
update            Uploa
updateapk         Uploa
restore [all|write|pdm]db
restoreFull       Resto
sql [download|restore|upl
sqlimport [com.my.package
version           Displ
remote [(ip)]     Conso
cpu [(cpnName)]  Get C

Advanced[C4E]>
```

Shodan Developers Book View All...

SHODAN port:23 gps "on console" Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
739

TOP COUNTRIES



Spain	390
Morocco	14
United States	7
Germany	3
Chile	2

TOP ORGANIZATIONS

Vodafone Spain	29
Telefonica de Espana	9
AT&T Wireless	7
Meditel Mobile	6
Maroc Telecom	2

Shodan Developers Book View All...

SHODAN port:23 gps "on console" Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results

TOTAL RESULTS
653

TOP COUNTRIES



Spain	370
Morocco	111
United States	75
Germany	39
Chile	27

```
Welcome on console

-[31mHelp :
cmd +[0m+[33m[option1]option2]{string}(number) +[0m

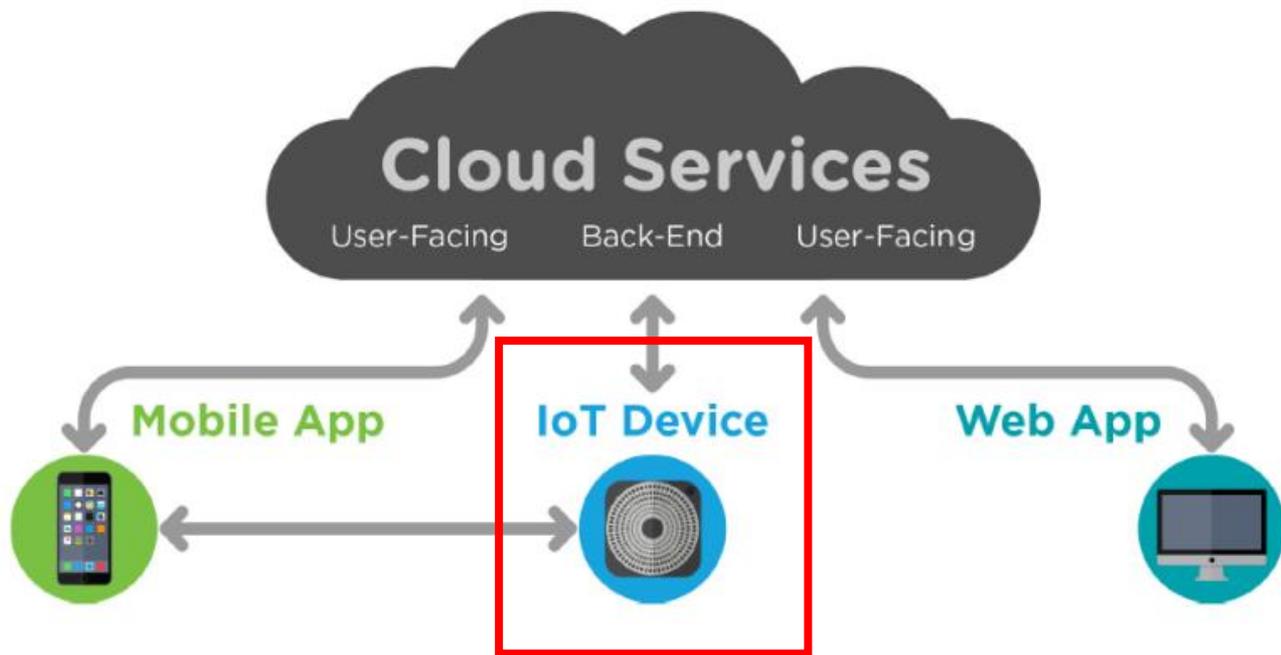
Builtins :
nversion +[0m+[33m +[0m          Console version
> +[0m+[33m +[0m          Display help
:en +[0m+[33m[(X)] +[0m          Change to s...

Welcome on console

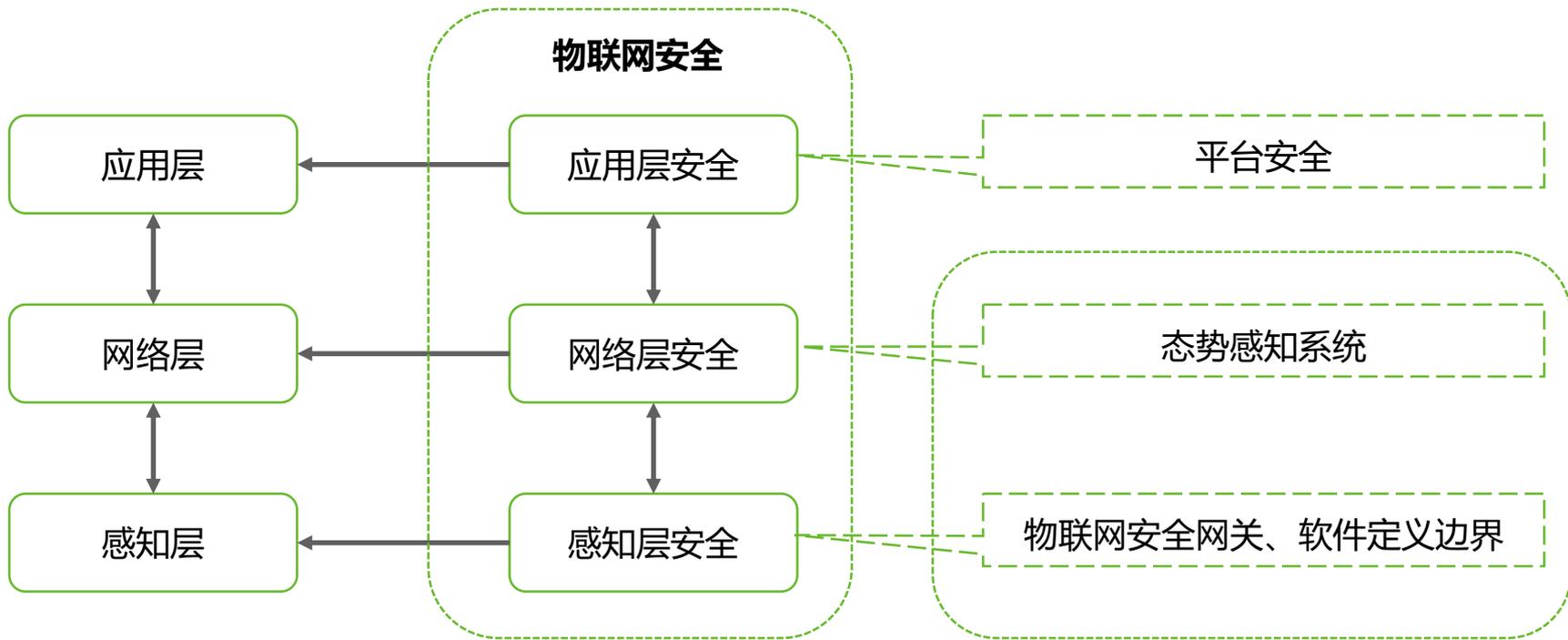
-[31mHelp :
ncmd +[0m+[33m[option1]option2]{string}(number) +[0m

Builtins :
ncversion +[0m+[33m +[0m          Console version
> +[0m+[33m +[0m          Display help
:en +[0m+[33m[(X)] +[0m          Change to s...
```

▶▶ 一个典型的物联网体系架构



物联网安全架构





02

物联网安全网关进展介绍

▶▶ 猜猜看？



▶▶ 物联网安全网关



Bitdefender Box



Home Network Security



Norton Core router



CUJO



Firewalla

物联网安全网关

□ 防火墙

- 威胁情报驱动：IP、URL信誉库
- 抵抗外部攻击

□ 异常检测

- 检测设备的异常行为，阻止异常设备的连接并预警

□ 内部资产管理和评估

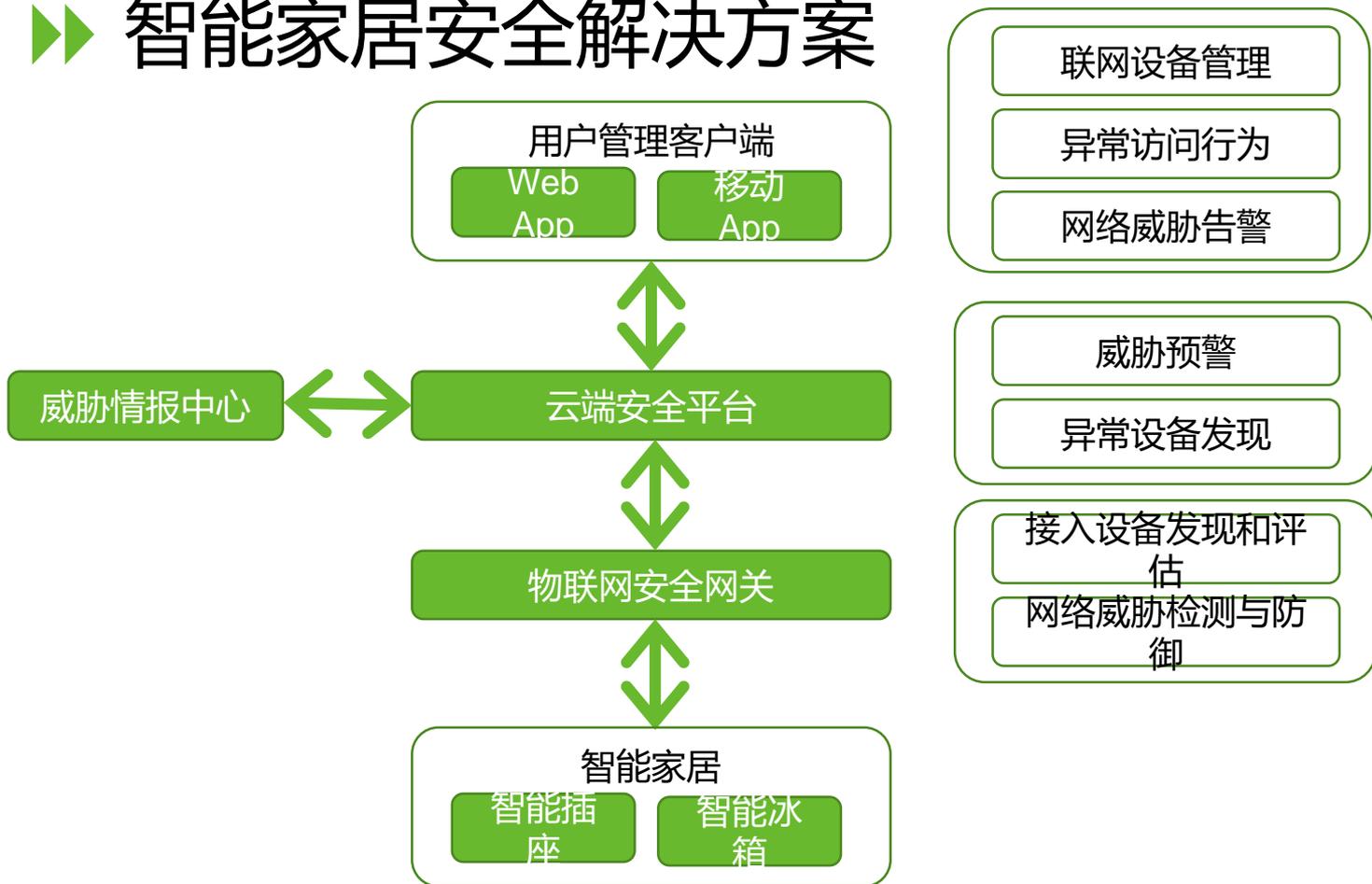
- 资产识别
- 漏洞扫描



□ 可采集的数据

- DNS信息
- NetFlow信息：源IP、源端口、目的IP、目的端口、包长度、时间戳等
- MAC地址

智能家居安全解决方案



绿盟科技物联网安全网关

绿盟物联网安全网关

Search...

帮助

资产

绿盟物联网安全网关

Search...

帮助

IDS告警

资产

绿盟物联网安全网关

Search...

帮助

无线网络分

IDS告警

资产

智能QOS

无线网络分析

IDS告警

VPN

智能QOS

无线网络分析

黑白名单

VPN

智能QOS

MAC绑定

黑白名单

VPN

MAC绑定

黑白名单

MAC绑定

signal



HaiDilaoDianCai
channel : 6
ap_signal : -89
mac : ec:8c:a2:8d:08:68

10.24.35.201/c

10.24.35.201/docs



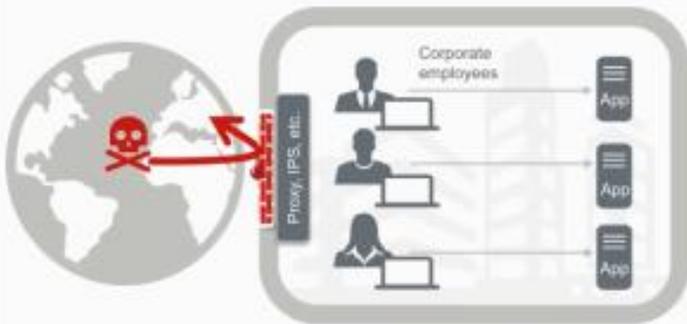
03

软件定义边界在物联网安全中的应用

▶▶ 传统的固定边界模型正在变得过时

Enterprise Perimeter: Then & Now

THEN:
Fixed Perimeter blocked attackers



Fixed perimeter protected traditional enterprise and kept the attackers out

NOW:
Attackers are Inside the Perimeter



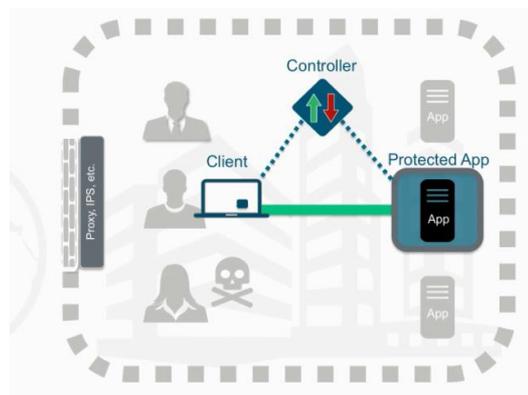
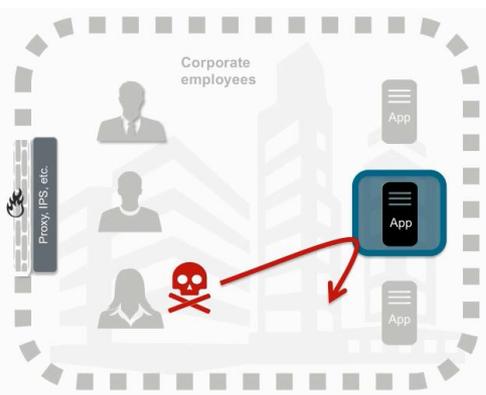
Sophisticated attacks, like phishing, bring the attackers inside the fixed perimeter

Lesson learned:
Perimeters can isolate critical infrastructure

软件定义边界

Software Defined Perimeter, SDP

- 由云安全联盟（CSA）于2013年提出
- 用应用所有者可控的逻辑组件取代了物理设备
- 只有在设备认证和身份认证之后，SDP才提供对于应用基础设施的访问
- SDP 使得应用所有者部署的边界可以保持传统模型中对于外部用户的不可见性和不可访问性
 - 该边界可以部署在任意的位置，如网络上、云中、托管中心中、私有企业网络上



▶▶ New technology trends in 2k17

Group	2016	2017	
Threat-Facing	Adaptive Security Architecture	Cloud Workload Protection Platforms	
	EDR	EDR	
	Nonsignature Approaches for Endpoint Prevention	Managed Detection and Response (MDR)	
	Remote Browser	Remote Browser	
	Microsegmentation and Flow Visibility		Microsegmentation
			Network Traffic Analysis
Deception	Deception		
Enablement- and Access-Facing	CASB	CASB	
	UEBA	SDP	
	Pervasive Trust Services		
Secure Development	DevSecOps	DevSecOps	
		Container Security	
iSOC	iSOC Orchestration Solutions		

▶▶ 在SDP中，控制平面和数据平面分离

- SDP包含两部分：SDP主机和SDP控制器
- SDP主机可以创建连接（IH）或者接受连接（AH）
- SDP控制器主要进行主机认证和策略下发
 - SDP主机和SDP控制器之间通过一个安全的控制信道进行交互

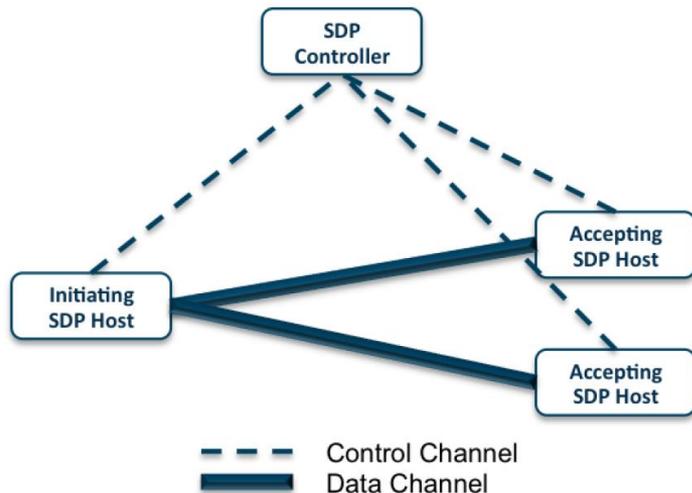


Figure 1: The architecture of the Software Defined Perimeter consists of two components: SDP Hosts and SDP Controllers

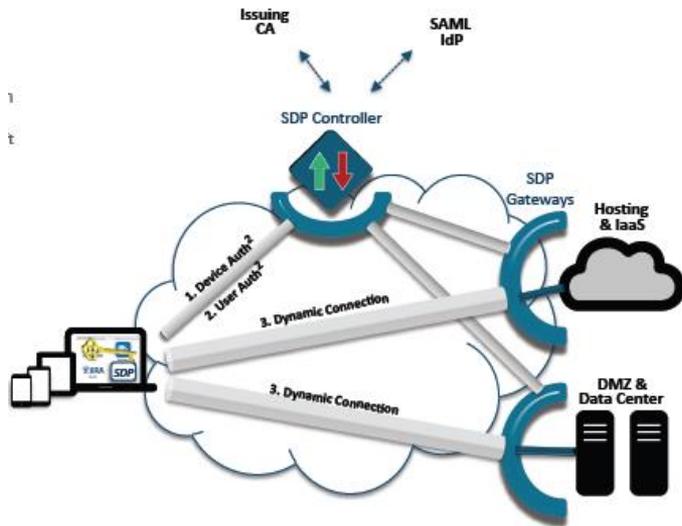
SDP提供了安全防护的新思路

□ 改变了客户端与服务端建立连接的方式

- 传统
 - Connect
 - 服务端暴露在公网中, 若服务端有漏洞, 则有可能被利用
 - Log in
 - 有可能使得用户名和密码被窃取
 - MFA
 - 可以抵抗用户名和密码的丢失, 但是多因素认证对于用户而言不是很友好
- SDP
 - MFA (用户无感知) -> Log in-> Connect

□ 通过三种方式对抗基于网络的攻击

- 透明MFA可以抵抗用户凭据丢失
- 服务器隔离可以抵抗服务器利用
- TLS双向认证可以抵抗连接劫持



▶▶ SDP的优势

- 以用户为中心的、灵活的访问控制
 - 可依据用户访问时的位置、时间、认证情况等上下文信息，做出更加灵活的访问控制决策
- 用户的访问行为具有可见性和可控性
 - 所有的访问流量都需要经过SDP的AH组件
- 能够实现服务的隔离和隐藏
 - 能够防止服务端漏洞被利用
 - 减轻拒绝服务攻击

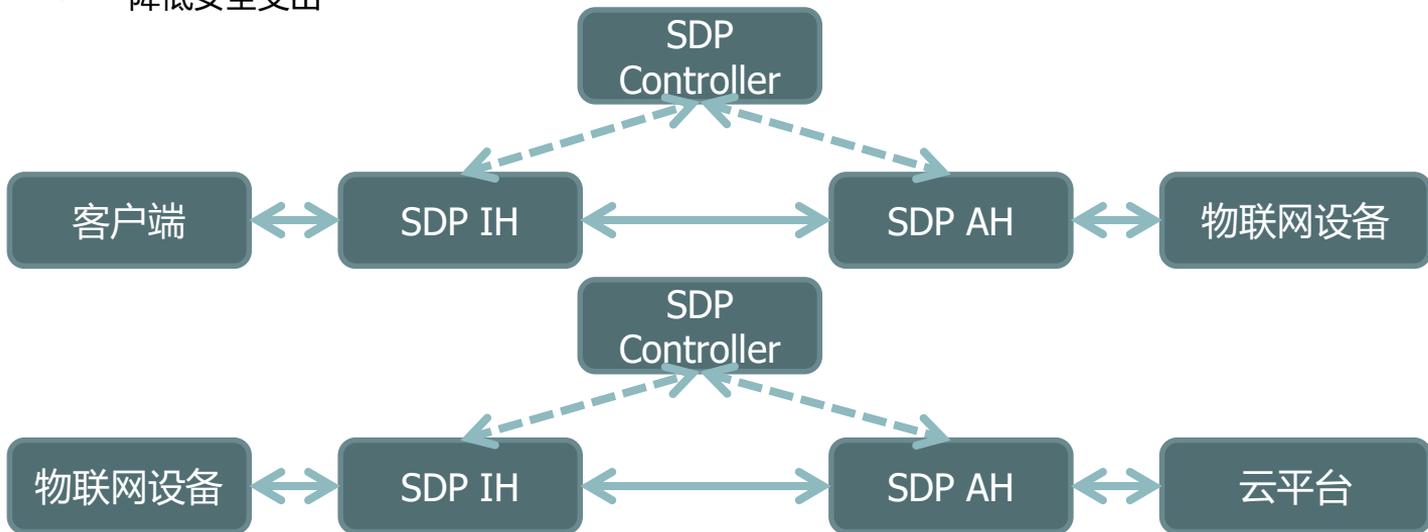
▶▶ 应用场景广泛

- 企业应用隔离
 - 邮箱、FTP、代码服务器等
- IaaS
 - CSA SDP for IaaS 2017年2月13日正式发布
- IoT
 - 视频监控设备、车联网、智能家居等
- SaaS、PaaS、Cloud-Based VDI、私有云和混合云



软件定义边界与物联网

- 对于部署在公网的设备，若是存在漏洞，有可能会被利用
 - Mirai，弱密码·更多漏洞
- SDP
 - 既提供服务，同时又对未授权用户不可见
 - 降低安全支出



软件定义边界与物联网

- CSA SDP - Automotive Secure Communications

- Objective: Utilize SDP for secure vehicle to cloud communications

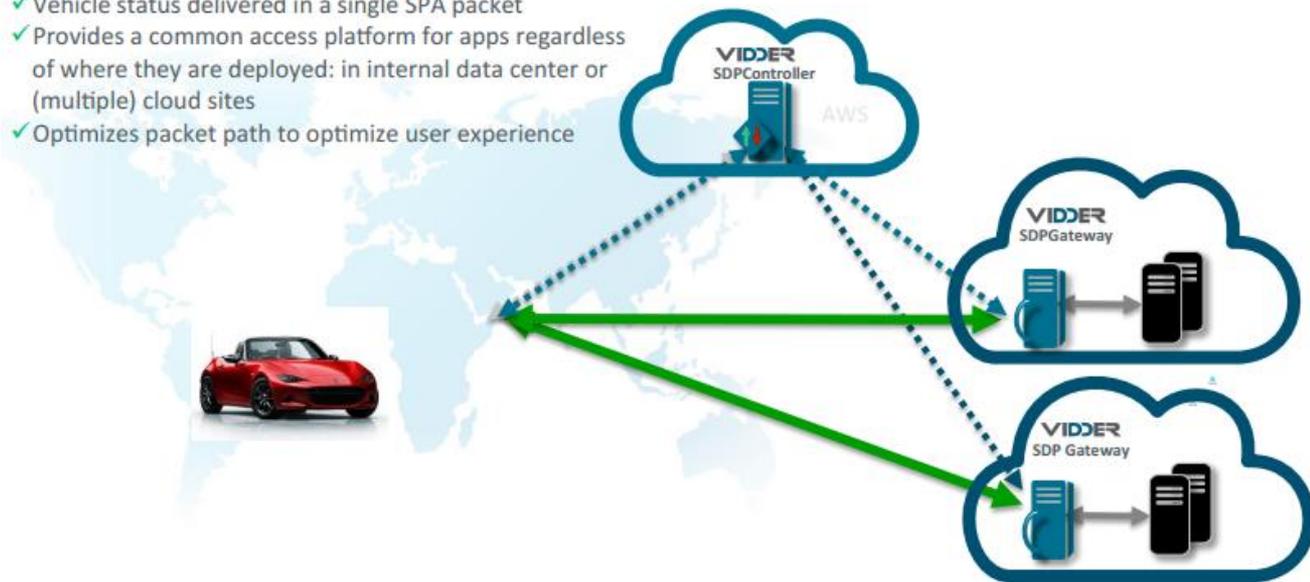
- Application: Secure telematics data transfer, OTA IVI software update

Global Automotive Company

Business Objective: Enable in field vehicle upgrades to retain customers and "sell" new features

Vidder SDP Solution:

- ✓ Vehicle status delivered in a single SPA packet
- ✓ Provides a common access platform for apps regardless of where they are deployed: in internal data center or (multiple) cloud sites
- ✓ Optimizes packet path to optimize user experience



▶▶ SDP Company

□ Vidder

- 产品名称：PrecisionAccess
- 基于 SDP 的第一个商业解决方案
- 保护企业关键服务、IaaS、SaaS 的安全
- 已有客户：Nokia

□ Cryptzone

- 产品名称：AppGate、AppGate for AWS
- 场景：工控、零售、教育、金融服务等
- 通过访问控制，保证系统、数据的安全

□ Verizon

- a scalable Software-as-a-Service (SaaS) solution, provides pre-authenticated, context-aware, secure access to enterprise applications

▶▶ SDP Company-Cryptzone

Cryptzone Solutions for ICS/SCADA

Cryptzone's AppGate, a network access security solution offers ICS/SCADA an approach to network security that includes the ability to:

- Tightly restrict who can access the information stored on your ICS/SCADA systems, making non-authorized resources invisible and inaccessible to any users that do not have access rights.
- Take both identity and context into consideration when granting access and can force authentication if contextual parameters change during the course of a session.
- Provide a [secure gateway between ICS and business networks](#).
- Provide only the degree of connectivity required by your personnel, by dynamically creating a *segment of one* between the user and the network resource they are entitled too.
- Monitor and enforce compliance with NERC CIP and ISA/IEC standards.
- Reduce operational complexity, eliminating the need for both 'truck rolls' (putting data diodes on all endpoints) and 'VPN management isolation' (vendor specific Firewall / VPN device for each site management interface).

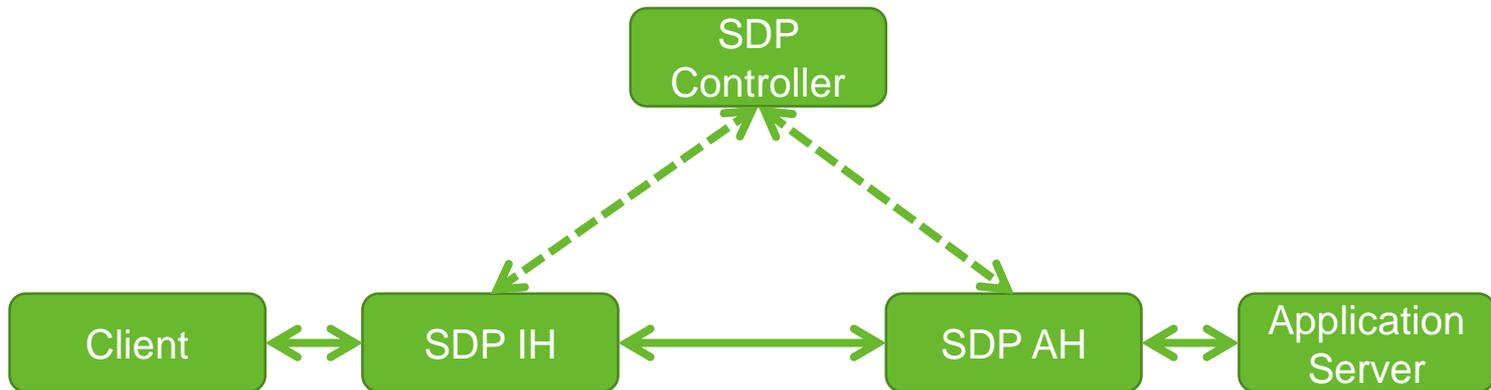
PSE S.A

Electricity company uses AppGate® to secure their SAP/ERP environment and other critical systems

FOCUS

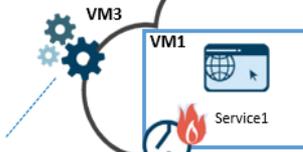
▶▶ 我们是怎么做的（1）

- 面向企业关键服务的软件定义边界防护
- 面向 IaaS 的软件定义边界防护
- 面向物联网环境的软件定义边界防护
 - 对于部署在公网的设备，若是存在漏洞，有可能会被利用。可以使用SDP，只有认证的用户才能访问到该设备
 - 如果认证通过不了，实际上是看不到这个设备的，也就没法去利用了



▶▶ 我们是怎么做的 (2)

NSDP_Controller:
192.168.19.243



NSDP_AH_1:
192.168.19.226



Coffee Shop
IH: 10.63.10.128

```
Xshell 5 (Build 0964)
Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[c:\>]ls

Looking up proxy server '127.0.0.1'...
Host '127.0.0.1' resolved to 127.0.0.1.
Connecting to 127.0.0.1:8088...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-68-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Fri May 19 06:24:40 UTC 2017

System load:  0.0          Processes:      80
Usage of /:   4.7% of 39.34GB    Users logged in:  0
Memory usage: 9%          IP address for eth0: 30.0.0.13
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

176 packages can be updated.
0 updates are security updates.
```

```
Last login: Wed May 3 08:20:48 2017 from 30.0.0.13
ubuntu@star-ah:~$
```

TestSSH1属性

类别(C):

- 连接
 - 用户身份验证
 - 登录提示符
 - 登录脚本
 - SSH
 - 安全性
 - 隧道
 - SFTP
 - TELNET
 - RLOGIN
 - SERIAL
 - 代理
 - 保持活动状态
 - 终端
 - 键盘
 - VT 模式
 - 高级
 - 外观
 - 边距
 - 高级
 - 跟踪
 - 日志记录
 - 文件传输
 - X/YMODEM
 - ZMODEM

连接

常规

名称(N): TestSSH1

协议(P): SSH

主机(H): ssh1.sdp.com

端口号(O): 22

说明(D):

重新连接

连接异常关闭时自动重新连接(A)

间隔(I): 0 秒 限制(L): 0 分钟

TCP选项

使用Nagle算法(N)

确定 取消

192.168.19.226:8080

192.168.19.226:8088

192.168.19.236:8099

Apache Tomcat Service 1.

Apache Tomcat Service 2.

Apache Tomcat Service 3.

Apache Tomcat Service 4.

you've successfully installed Tomcat. Co

installed Tomcat. Co

访问场景	服务	A	T	S
公司内部访问		√		√
员工家中访问		√		√
咖啡店中访问		√		√



Recommended Reading:
[Security Considerations HOW-TO](#)
[Manager Application HOW-TO](#)
[Clustering/Session Replication HOW-TO](#)



04

展望

▶▶ 展望 (1)

- 随着边缘计算的兴起，物联网安全网关将变得越来越重要
- 应用场景
 - 智能家居
 - 工业物联网
 - ...

▶▶ 展望 (2)

- Gartner预测，到2017年底，至少10%的企业组织（目前低于1%，2016年）将利用SDP技术来隔离敏感的环境。
- 到2021年，60%的企业将逐步淘汰VPN，改而采用SDP。

- SDP + 异常行为分析提供了轻量级普适性防护
 - SDP + SDS

- 越来越多的SDP应用将出现
 - 企业环境
 - IaaS
 - IoT
 - SaaS
 - PasS
 - Cloud-Based VDI
 - 私有云和混合云

▶▶ 期待



2017年RSA大会主题--机会的力量

□ 工控安全-NexDefense

- 建于2012年，致力于实时保护关键基础设施中的系统的完整性，打击复杂的安全威胁。
- Sophia是一个工业网络异常检测系统，由美国能源部、Battelle Energy Alliance和Idaho National Laboratory (INL) 的网络安全专家协作完成



谢谢！

▶▶ vs. VPN

- VPN适用于传统的企业固定边界环境，用户和服务器资源是固定的
- VPN的不足
 - 仅提供对于特定网络的粗粒度、all-or-nothing的访问
 - VPN只是做到了对于远程用户接入的控制，但是对于接入用户的安全防护还需要部署相应的安全设备
- Gartner
 - DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses.

▶▶ vs. Firewall

- 防火墙是一种基于预定的安全规则来监视和控制进入和输出网络流量的网络安全系统。防火墙可以将外部网络与内部可信区域隔离开来，对网络边界进行有效保护，防火墙是**抵抗外部黑客入侵**的重要手段。但是防火墙也存在着一定的缺陷：
 - (1) 为它所保护的所有的服务提供**粗粒度**的访问控制
 - (2) **IP地址和用户没有任何关联**，攻击者可以伪造IP，进行攻击
 - (3) 规则无法根据用户位置和权限的变化做出及时修改
 - (4) 对**规则的管理非常复杂**

▶▶ vs. CASB

CASB (Cloud Access Security Broker) 介绍

CASB (Cloud Access Security Broker) 概念在2012年由 Gartner 提出，定义了在新的云计算时代，企业或用户掌控云上数据安全的解决方案模型。Gartner 预测从2012年不到1%的企业使用CASB，到2020年会有85%的大型企业会使用 CASB。

CASB 模型已成为第三方安全服务商的指导标准，其主要从四个方向进行了产品定义：



可视化

提供针对企业内部使用的云服务、影子服务的自动发现支持，以及集中化的视图展示，包括用户行为、客户端设备的统计支持；对异常行为进行检测、阻断和记录。



合规性

帮助企业 IT 系统往云上迁移后，仍能满足合规性要求，并对云服务商进行信任评级、提供内容监控、审计日志功能。



数据安全

结合人员、设备、内容和应用等多个维度，提供 DLP、Encryption、Tokenization 等数据安全保护，防止云端数据泄露。



威胁防护

监控云端数据、用户资源使用状态，及时发现威胁并且做出防御。