2021-2022学年春季学期

网络空间安全态势感知

Cyber security situation awareness

授课团队：刘宝旭 卢志刚 刘玉岭

助　　教：李　宁

网络空间安全态势感知

Cyber security situation awareness

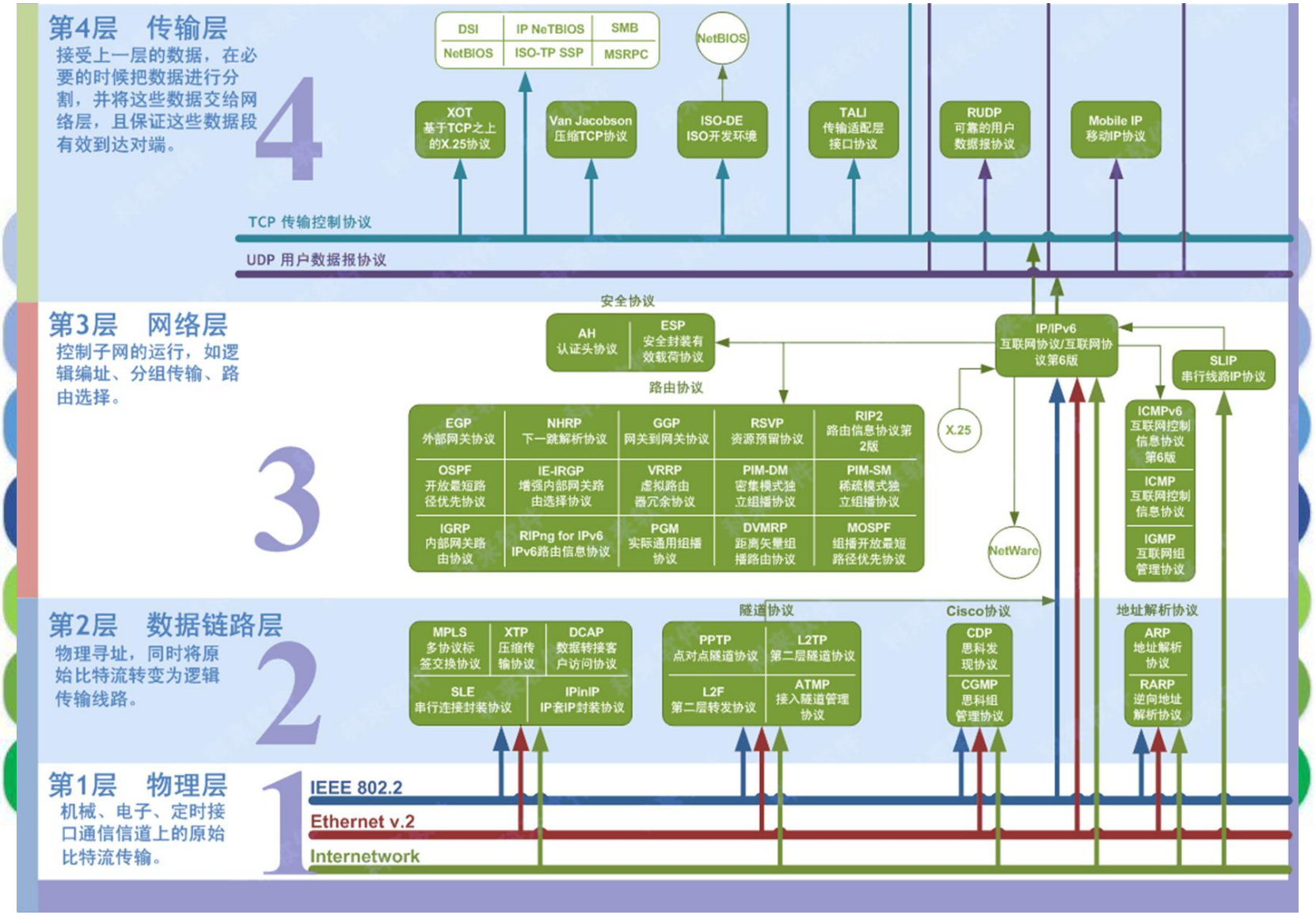
[第8次课] 深度包分析技术

授课教师：刘玉岭

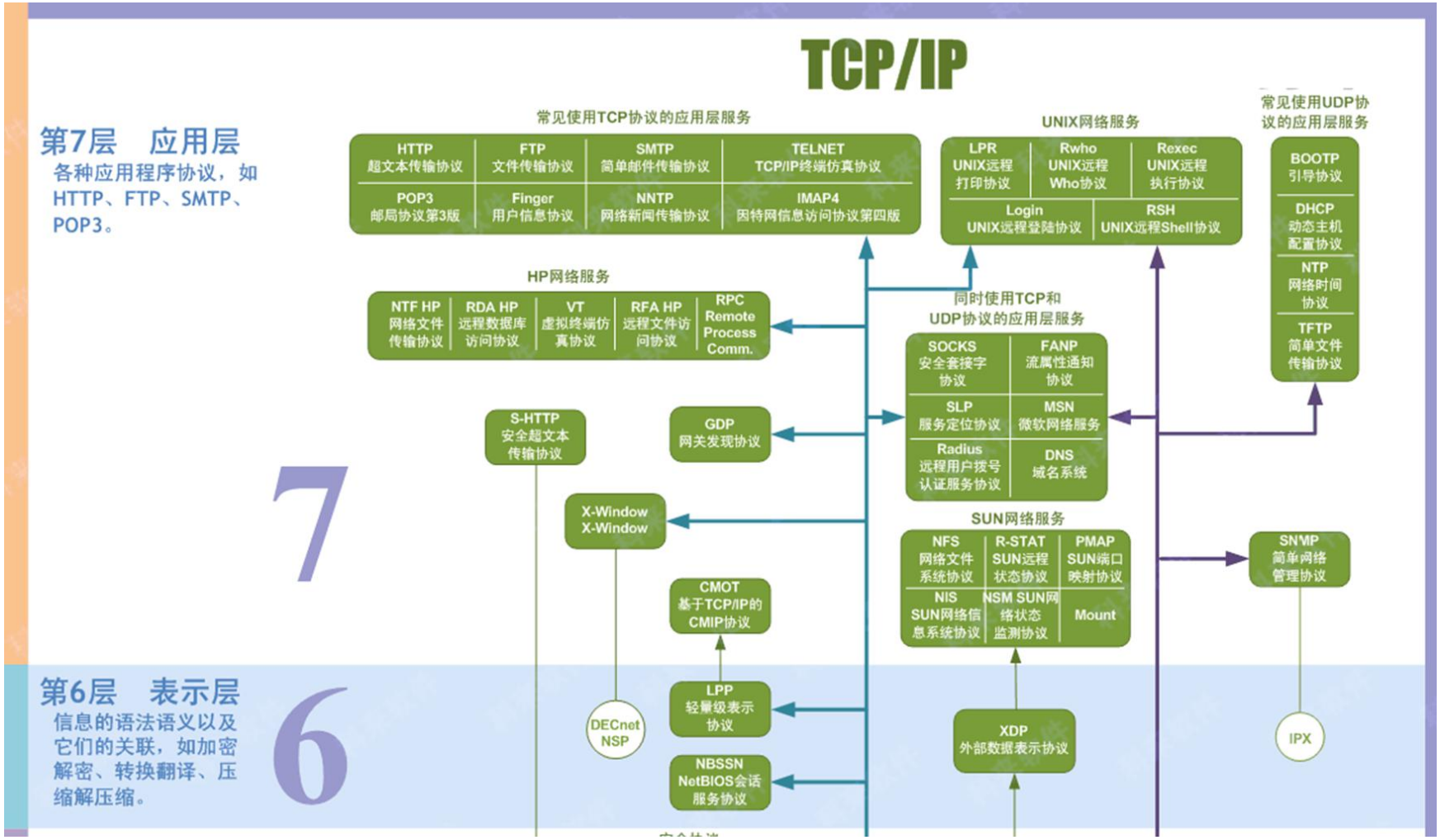
授课时间：2022.3.17

内容概要

概念与内涵（1）


第4层 传输层
接受上一层的数据，在必要的时候把数据进行分割，并将这些数据交给网络层，且保证这些数据段有效到达对端。
4
DSI
IP NeTBIOS
SMB
NetBIOS
ISO-TP SSP
MSRPC
NetBIOS
XOT
基于TCP之上的X.25协议
Van Jacobson
压缩TCP协议
ISO-DE
ISO开发环境
TALI
传输适配层接口协议
RUDP
可靠的用户数据报协议
Mobile IP
移动IP协议
TCP 传输控制协议
UDP 用户数据报协议
第3层 网络层
控制子网的运行，如逻辑编址、分组传输、路由选择。
3
安全协议
AH
认证头协议
ESP
安全封装有效载荷协议
路由协议
EGP
外部网关协议
NHRP
下一跳解析协议
GGP
网关到网关协议
RSVP
资源预留协议
RIP2
路由信息协议第2版
OSPF
开放最短路径优先协议
IE-IRGP
增强内部网关路由选择协议
VRRP
虚拟路由器冗余协议
PIM-DM
密集模式独立组播协议
PIM-SM
稀疏模式独立组播协议
IGRP
内部网关路由协议
RIPng for IPv6
IPv6路由信息协议
PGM
实际通用组播协议
DVMRP
距离矢量组播路由协议
MOSPF
组播开放最短路径优先协议
IP/IPv6
互联网协议/互联网协议第6版
SLIP
串行线路IP协议
X.25
NetWare
ICMPv6
互联网控制信息协议第6版
ICMP
互联网控制信息协议
IGMP
互联网组管理协议
第2层 数据链路层
物理寻址，同时将原始比特流转变为逻辑传输线路。
2
隧道协议
Cisco协议
地址解析协议
MPLS
多协议标签交换协议
XTP
压缩传输协议
DCAP
数据转接客户访问协议
SLE
串行连接封装协议
IPinIP
IP套IP封装协议
PPTP
点对点隧道协议
L2TP
第二层隧道协议
L2F
第二层转发协议
ATMP
接入隧道管理协议
CDP
思科发现协议
CGMP
思科组管理协议
ARP
地址解析协议
RARP
逆向地址解析协议
第1层 物理层
机械、电子、定时接口通信信道上的原始比特流传输。
1
IEEE 802.2
Ethernet v.2
Internetwork

概念与内涵（2）

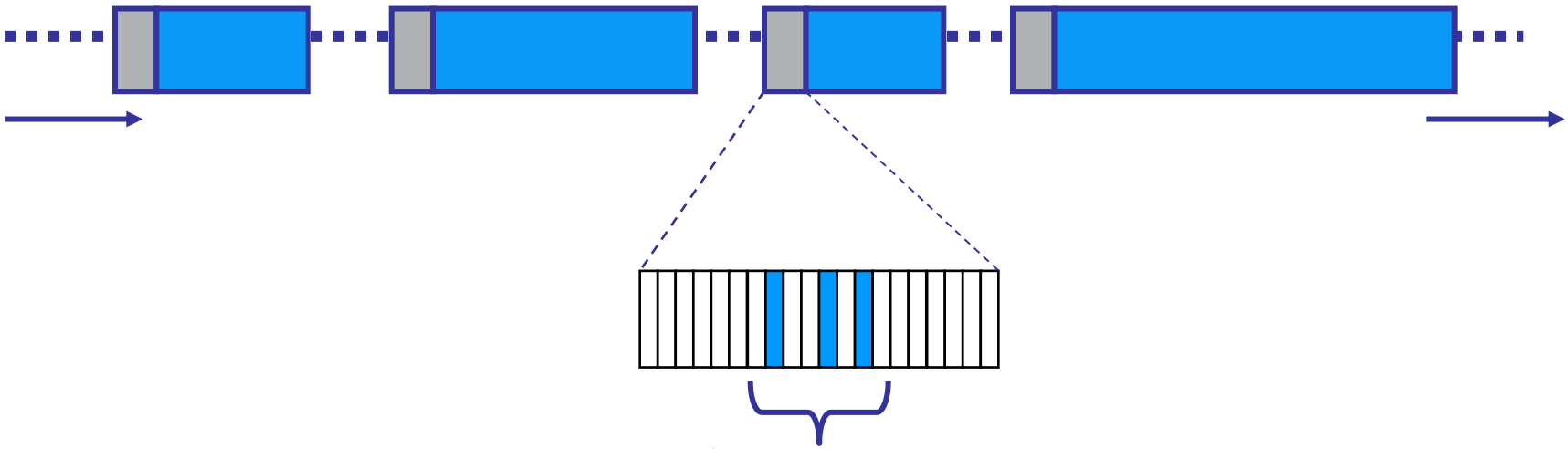

TCP/IP
第7层 应用层
各种应用程序协议，如HTTP、FTP、SMTP、POP3。
7
第6层 表示层
信息的语法语义以及它们的关联，如加密解密、转换翻译、压缩解压缩。
6
常见使用TCP协议的应用层服务
HTTP 超文本传输协议
FTP 文件传输协议
SMTP 简单邮件传输协议
TELNET TCP/IP终端仿真协议
POP3 邮局协议第3版
Finger 用户信息协议
NNTP 网络新闻传输协议
IMAP4 因特网信息访问协议第四版
UNIX网络服务
LPR UNIX远程打印协议
Rwho UNIX远程Who协议
Rexec UNIX远程执行协议
Login UNIX远程登陆协议
RSH UNIX远程Shell协议
常见使用UDP协议的应用层服务
BOOTP 引导协议
DHCP 动态主机配置协议
NTP 网络时间协议
TFTP 简单文件传输协议
HP网络服务
NTF HP 网络文件传输协议
RDA HP 远程数据库访问协议
VT 虚拟终端仿真协议
RFA HP 远程文件访问协议
RPC Remote Process Comm.
同时使用TCP和UDP协议的应用层服务
SOCKS 安全套接字协议
FANP 流属性通知协议
SLP 服务定位协议
MSN 微软网络服务
Radius 远程用户拨号认证服务协议
DNS 域名系统
S-HTTP 安全超文本传输协议
GDP 网关发现协议
X-Window X-Window
SUN网络服务
NFS 网络文件系统协议
R-STAT SUN远程状态协议
PMAP SUN端口映射协议
NIS SUN网络信息系统协议
NSM SUN网络状态监测协议
Mount
SNMP 简单网络管理协议
CMOT 基于TCP/IP的CMIP协议
LPP 轻量级表示协议
DECnet NSP
NBSSN NetBIOS会话服务协议
XDP 外部数据表示协议
IPX

概念与内涵（3）

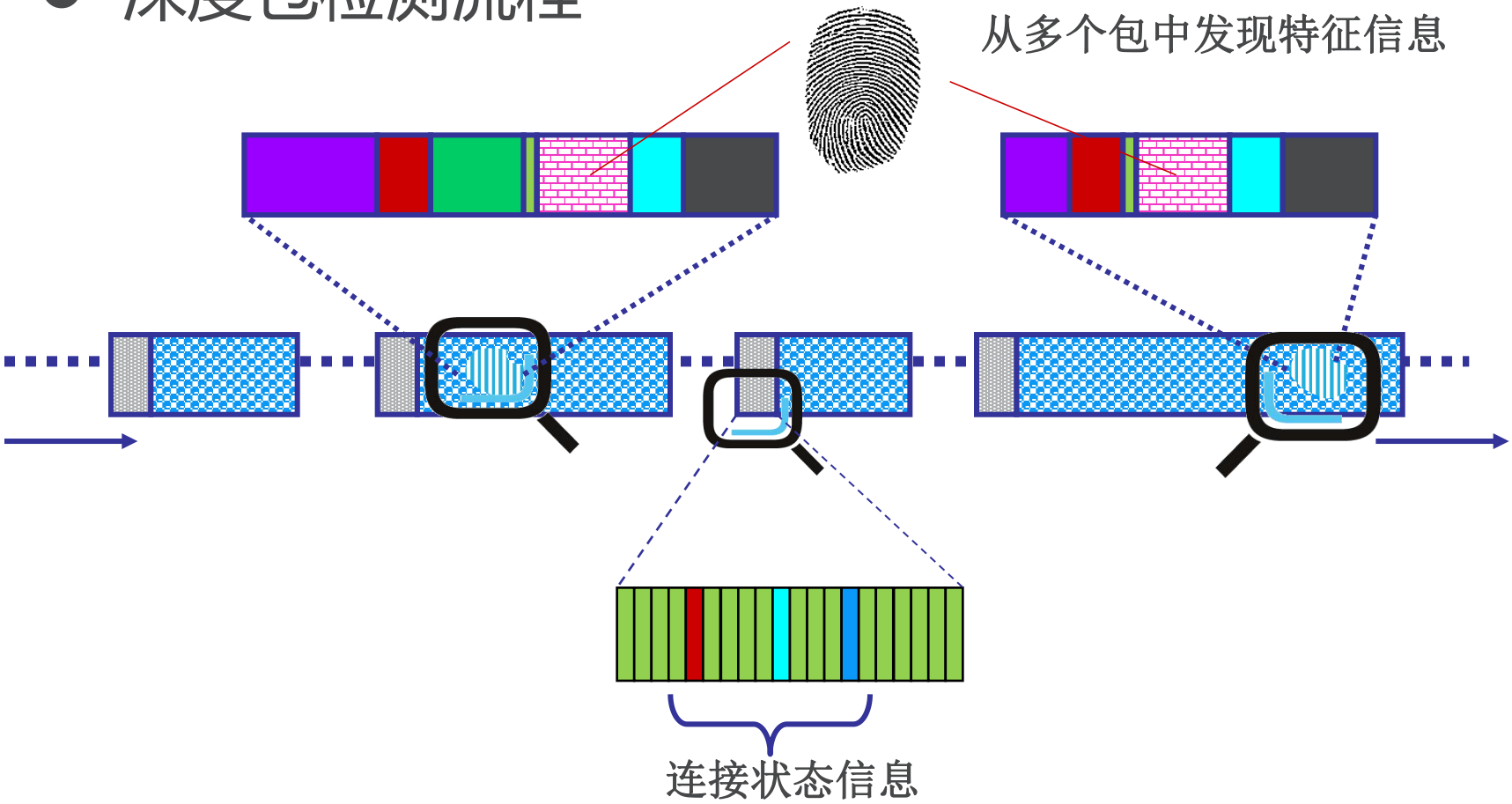
- 深度数据包检测（Deep packet inspection，DPI）
  - 完全数据包探测（complete packet inspection）或信息萃取（Information eXtraction，IX）
  - 技术原理：数据包过滤，即按照预定规则，对通过检测点的数据包的载荷部分（可能包括包头）进行检查
  - 目的：
    - 安全检测：查找不匹配预定定义规则的数据，可能是病毒、垃圾邮件、网络入侵等；
    - 路径判定：以预定之准则来决定数据包是否可通过或需被路由至其他不同目的地
    - 网络管理：收集统计数据
  - 检查方法：
    - 端口镜像（port mirroring，或 Span Port）
    - 分光器

概念与内涵（4）

- 标准包检测流程
  - 仅检查包头，且一般是2和3两层



- 深度包检测流程



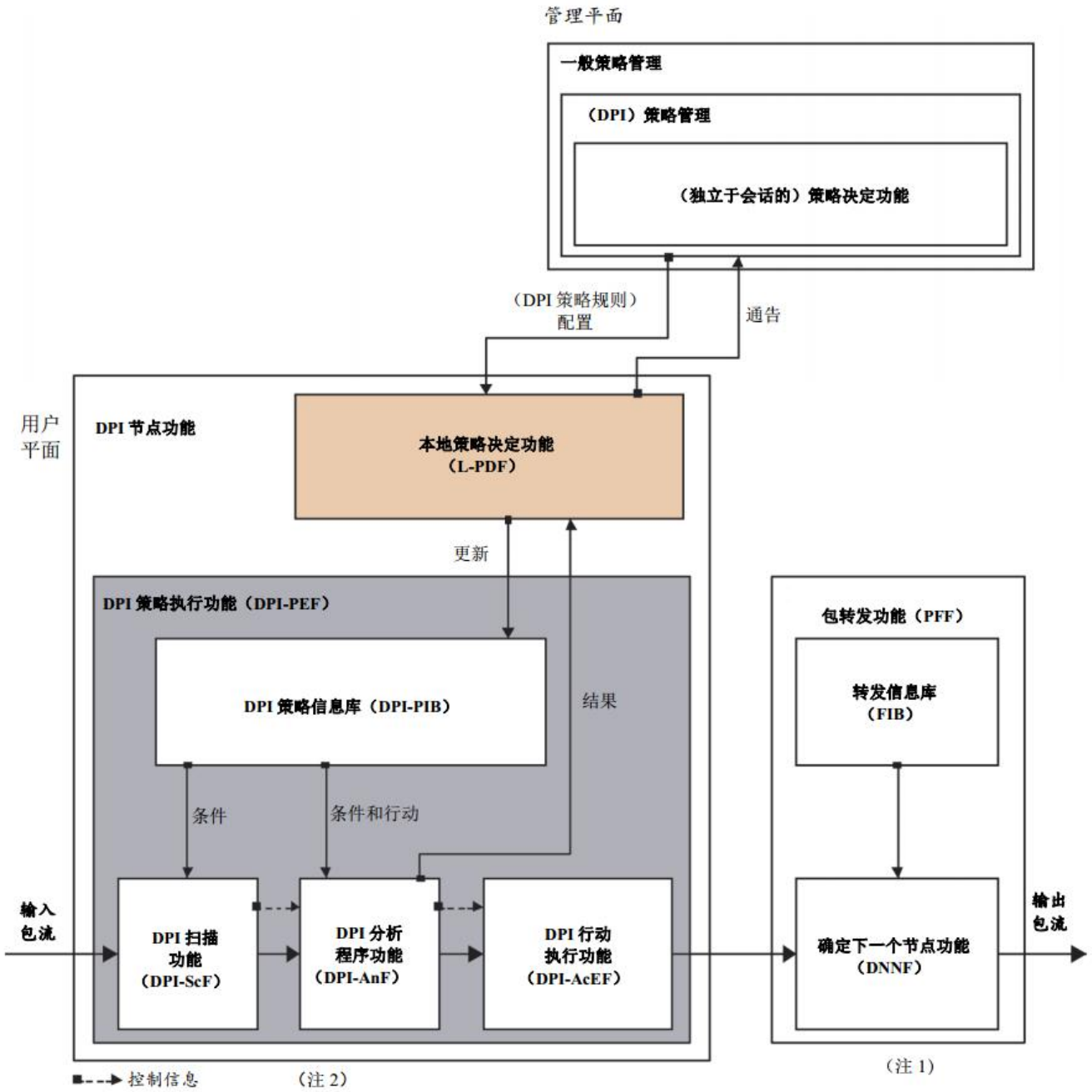
概念与内涵（6）

DPI策略条件必须包含应用级条件，并可包含其它选项，如状态条件与/或流级条件等：

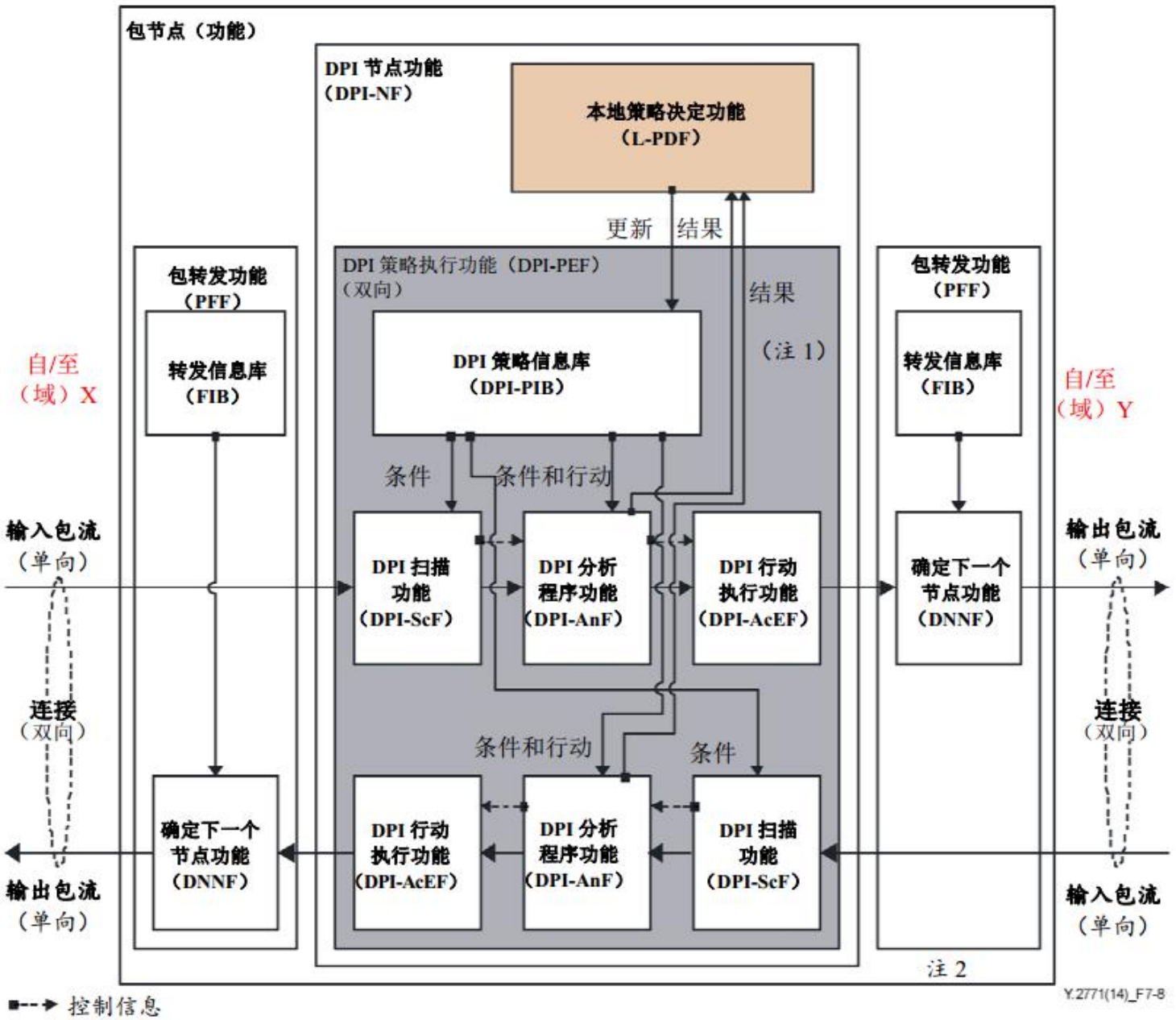
1) 状态条件（可选）：
   a) 网络业务等级条件（如包路径中遇到的拥塞）；或者
   b) 网络元素状态（如DPI-FE局部过载条件）。
2) 流描述符/流级条件（可选）：
   a) 包内容（包头字段）；
   b) 包特性（如MPLS标签的号码）；
   c) 包处理（如DPI-FE的输出接口）。
3) 应用描述符/应用级条件：
   a) 包内容（应用包头字段和应用负载）。

国际电信联盟ITU-T Y.2771/2014:深度包检测框架

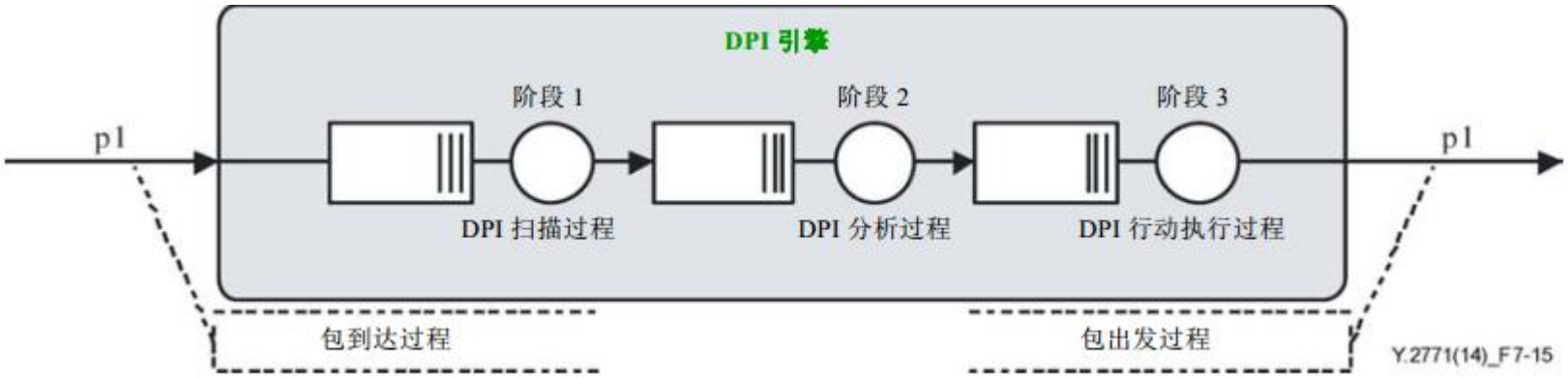
- 单


管理平面
一般策略管理
（DPI）策略管理
（独立于会话的）策略决定功能
（DPI 策略规则）
配置
通告
用户
平面
DPI 节点功能
本地策略决定功能
（L-PDF）
更新
DPI 策略执行功能（DPI-PEF）
DPI 策略信息库（DPI-PIB）
结果
条件
条件和行动
输入
包流
DPI 扫描
功能
（DPI-ScF）
DPI 分析
程序功能
（DPI-AnF）
DPI 行动
执行功能
（DPI-AcEF）
包转发功能（PFF）
转发信息库
（FIB）
确定下一个节点功能
（DNNF）
输出
包流
控制信息
（注 2）
（注 1）

- 双向[


包节点（功能）
DPI 节点功能
（DPI-NF）
本地策略决定功能
（L-PDF）
更新
结果
DPI 策略执行功能（DPI-PEF）
（双向）
结果
（注 1）
包转发功能
（PFF）
转发信息库
（FIB）
DPI 策略信息库
（DPI-PIB）
自/至
（域）X
自/至
（域）Y
条件
条件和行动
输入包流
（单向）
DPI 扫描
功能
（DPI-ScF）
DPI 分析
程序功能
（DPI-AnF）
DPI 行动
执行功能
（DPI-AcEF）
确定下一个
节点功能
（DNNF）
输出包流
（单向）
连接
（双向）
条件和行动
条件
确定下一个
节点功能
（DNNF）
DPI 行动
执行功能
（DPI-AcEF）
DPI 分析
程序功能
（DPI-AnF）
DPI 扫描
功能
（DPI-ScF）
输出包流
（单向）
连接
（双向）
输入包流
（单向）
注 2
控制信息
Y.2771(14)_F7-8

- 无状态DPI
  - 涉及到在每个包上单独执行的DPI策略规则，无关单向包流或双向包连接中的其它包
- 有状态DPI
  - 存在一种相关性，可通过一个（有限的）状态机来建模
    - 例如，一个带基于TCP的应用数据传输的IP应用。对TCP连接建立阶段，可能有专门的策略条件；对后续的通信阶段，可能有其它的策略条件



- DPI的主要性能评价指标
  - 节点内部传送延迟
  - 包处理速率
  - 错误率（误报率、漏报率）
  - 包成功识别率

测量名称：	N	节点内部传送延迟
符号：	I	τ_{TD}
测量描述：	N	通过一个DPI节点的包累积等待和服务时间。
度量或计算方法：	N	通过测量DPI节点功能物理或逻辑表示之包接 口处的单个包进和出时间（$T_{in,i}$和$T_{out,i}$），来计算该值。 前提条件：测量实体必须能够识别单个的包。 警告：该指标通常取决于负载，原因是，节点内部传送延迟由节点内部服务和等候时间构成。负载，或者更精确地为DPI提供的负载$A_{DPI\text{-}NF}$，由输入包速率$\phi_{P,In}$和每个包的平均服务时间$T_{H,Packet}$给出，根据以下公式： $A_{DPI-NF} = \phi_{P,In} \cdot T_{H,Packet}$ 主要负载依赖性（参见第8.3节）： $\tau_{TD} = f(A_{DPI\text{-}NF})$
度量单位：	N	ns
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	该度量可在很宽的时间间隔上使用。
实施：	I	–
验证：	I	–
使用和应用：	I	“实时DPI”
报告模型：	I	典型地，将作为性能管理的一部分。
类型“KPI”：是/否？	I	“KPI”
注 – N：规范性描述要素；I：说明性描述要素		

- 深度数据包检测：网络管理利器

企业级：提升网络安全	运营商：提高服务质量	国家级：保障国家安全
• 对抗蠕虫、间谍软件、病毒 • 缓冲器溢出攻击、DoS、复杂入侵 • 数据泄露等	• 合规性检查 • 定向广告 • 数据服务统计分析	• 网络监听 • 互联网审查

重定向、标记/标签、封锁、限速、上报

内容概要

深度包检测体现在三个方面：

协议深度：对被封装在标准应用协议中的私有协议检测和识别。

检测深度：为完成一次识别可能需要对多个IP数据包的检测。在网络数据包传输有序而不连续的环境下，并发会话的处理能力保证了包关联的完整性和一致性。

识别深度：协议的多种版本各有不同的指纹，多种版本可能同时存在（“迅雷”有至少十二种版本）。态势感知方法要求识别所有的版本。

- 端口检测
  - 很多应用和协议使用默认的端口
    - Email：进口110，使用SSL时是995，出口25
  - 方法简单有效，缺乏变化
- 字符串匹配
  - 很多应用程序标识符单一且纯文本
  - 易于查找，需要保证字符串的唯一性

Snort：微软XML核心服务跨站信息泄露：

```
<\x21DOCTYPE\s+[^>]*SYSTEM[^>]*>.*\x2EparseError
```

ClamAV ： Cabir.A computer worm signature

```
886f1f10123a00101904000e5f79547e6ad0100bd006f0064
00750063007400490044005400320020005200530033004
1005300789c
```

多特征组合使用：数据包大小、载荷长度、数据包中位置等

- 应用层网关识别技术
  - 应用场景：某些业务的控制流和业务流是分离的，业务流没有任何特征
  - 基本方法：应用层网关先识别出控制流，并根据控制流的协议通过特定的应用层网关对其进行解析，从协议内容中识别出相应的业务流
  - 对于每一个协议，需要有不同的应用层网关对其进行分析。

- 行为模式检测
  - 统计型：平均载荷大小在X和Y之间
  - 动作式：使用TCP连接登录后，紧跟着使用某端口的UDP连接
  - …
  - 方法复杂，但是适合对抗性分析，比如加密流量等

实现DPI的两种技术类型：

软件型：以服务器（或x86结构的工控机）为平台。

硬件型：以可编程集成电路构建的可扩展系统为平台。

为了在骨干网和大规模网上运行又不成为瓶颈，DPI必须采用综合高速集成电路、高速多核处理器、高速总线等技术的硬件产品。

“网络态势感知”的另一个关键是“指纹/特征库” 。由于“指纹/特征”是在实际应用环境中不断积累的，所以需要即时更新 。

对网络态势的实时感知和“指纹/特征库”的更新升级能力是网络安全防御的基本保证，这 也是产品研发企业的发展方向和运营模式。

深度包检测关键技术

互联网上存在大量的未被识别的私有协议。对私有协议进行逆向解析，获得协议规范，是态势感知中一项重要的基础研究工作。

协议逆向解析方法的要点：

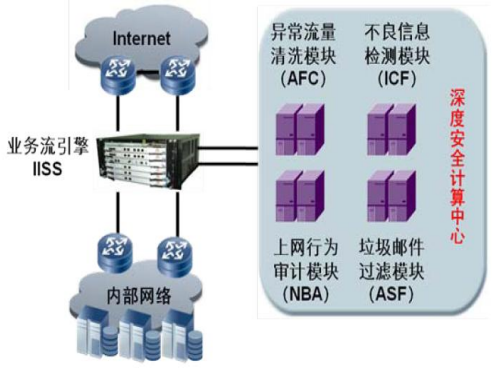
- 内外结合（网络协议会话分析×协议处理程序分析）
- 动静结合（程序静态分析＋程序动态执行）
- 黑白结合（优先分析灰色的协议）
- 快慢结合（超阈值的会话、精细分析，即时感知与实时处置）
- 疏堵结合（精细管理，保证关键业务的生存性）

深度包检测关键技术

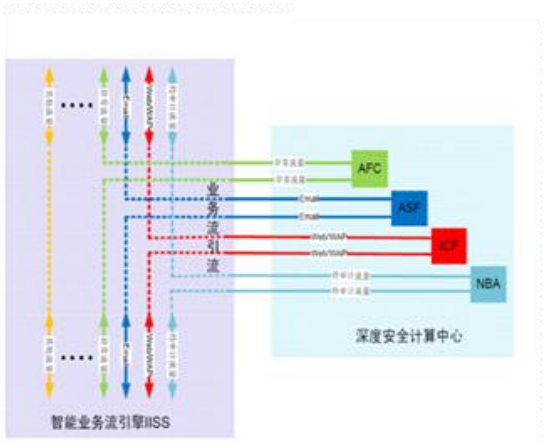
基于逆向感知原理兼有流量管控和安全态势分析两种功能。当用作态势分析时，设备在网络中有两种部署方式：

透明串连模式：直接嵌入网络，不改变网络的拓扑，不需要配置IP地址。数据流直接转发或按按策略重定向，是隐形的或透明的接入方式。

旁路并联模式：除将数据流通过网络分光或镜像外，其余与透明串连模式的性能一致。



透明串连模式

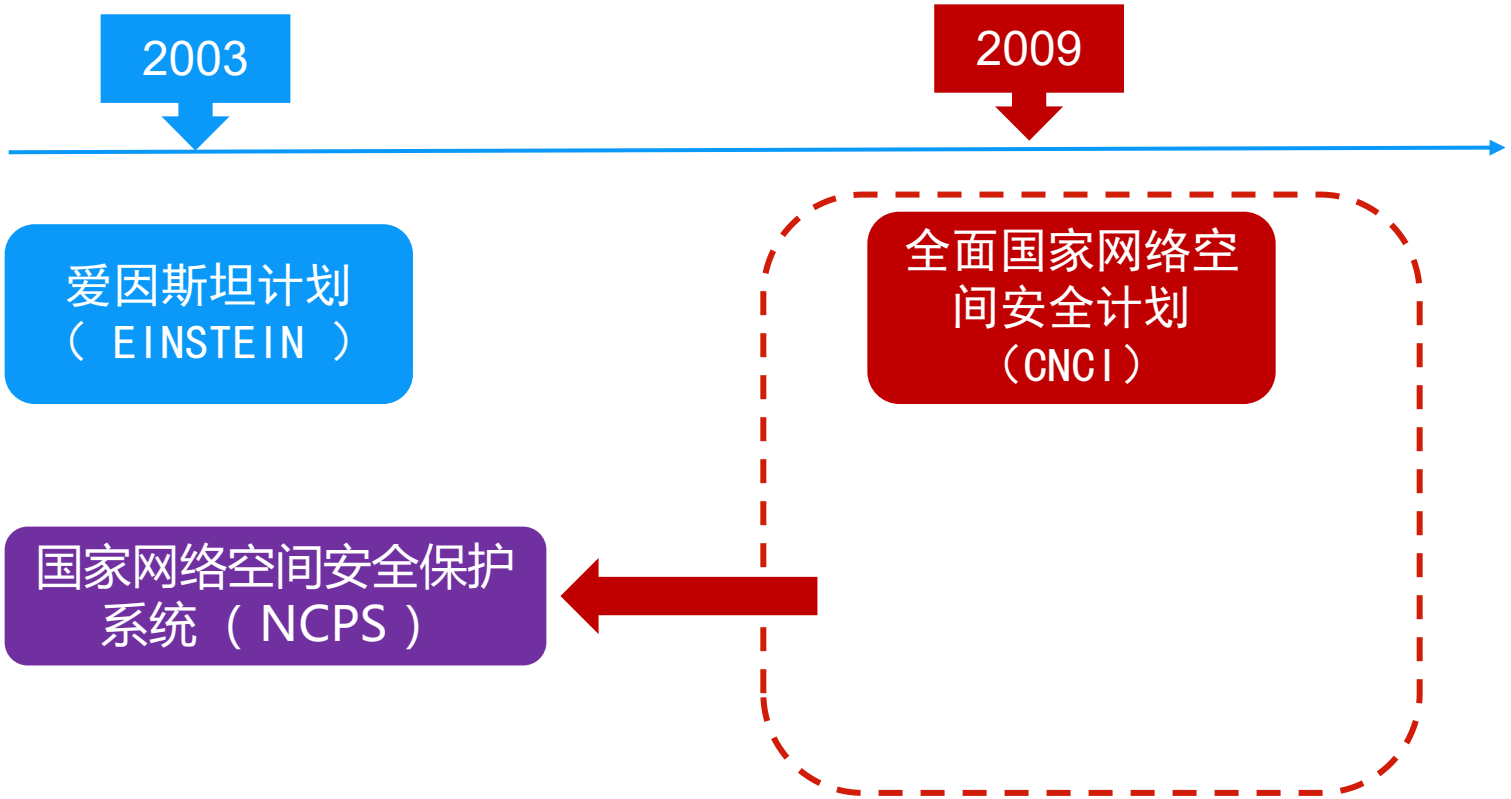


旁路并联模式

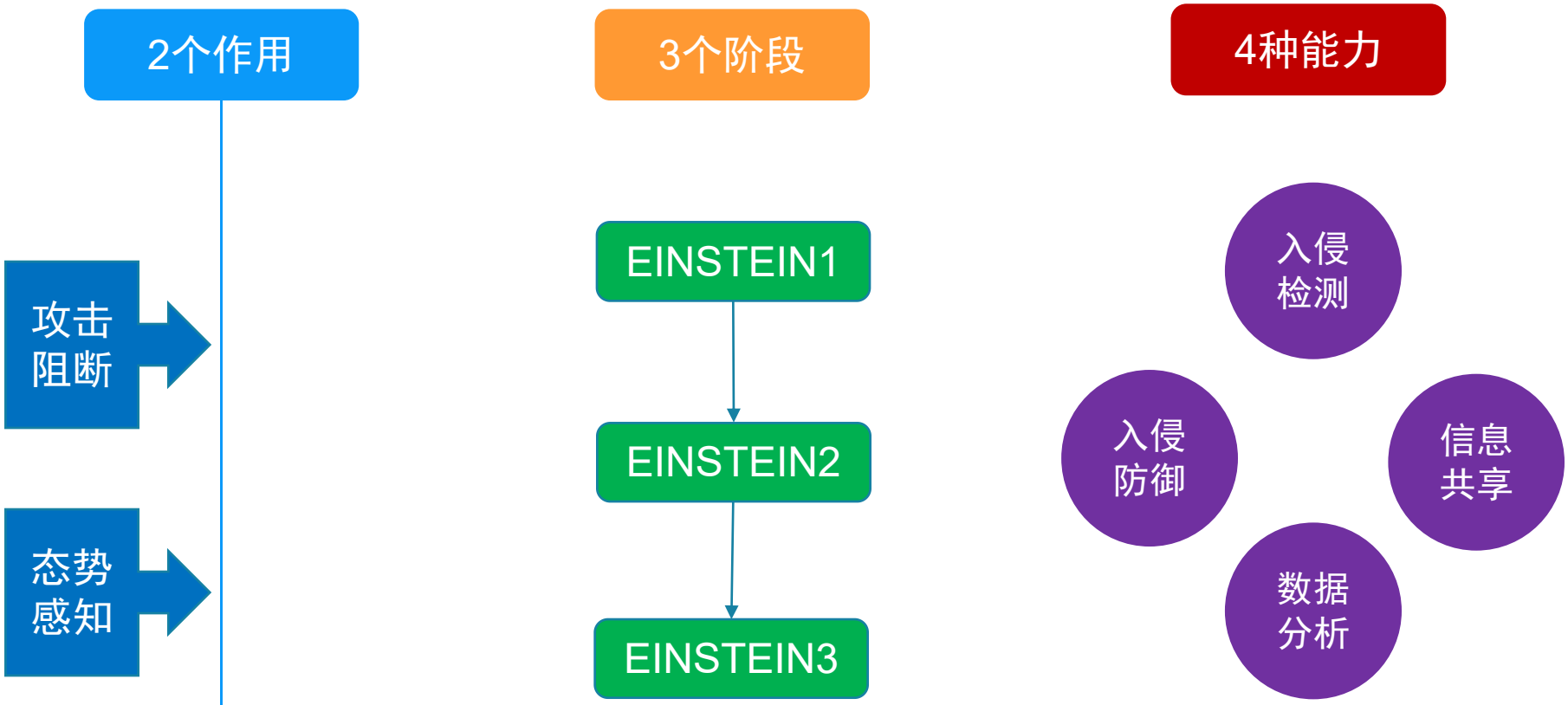
内容概要

爱因斯坦计划

- 爱因斯坦计划（EINSTEIN）于2003年启动，
- 在2009年美国政府启动了CNCI（全面国家网络空间安全计划）
- 爱因斯坦计划并入CNCI，并改名为NCPS（国家网络空间安全保护系统），但依然称为爱因斯坦计划



爱因斯坦计划


2个作用
攻击阻断
态势感知
3个阶段
EINSTEIN1
EINSTEIN2
EINSTEIN3
4种能力
入侵检测
入侵防御
信息共享
数据分析

爱因斯坦计划——2个作用

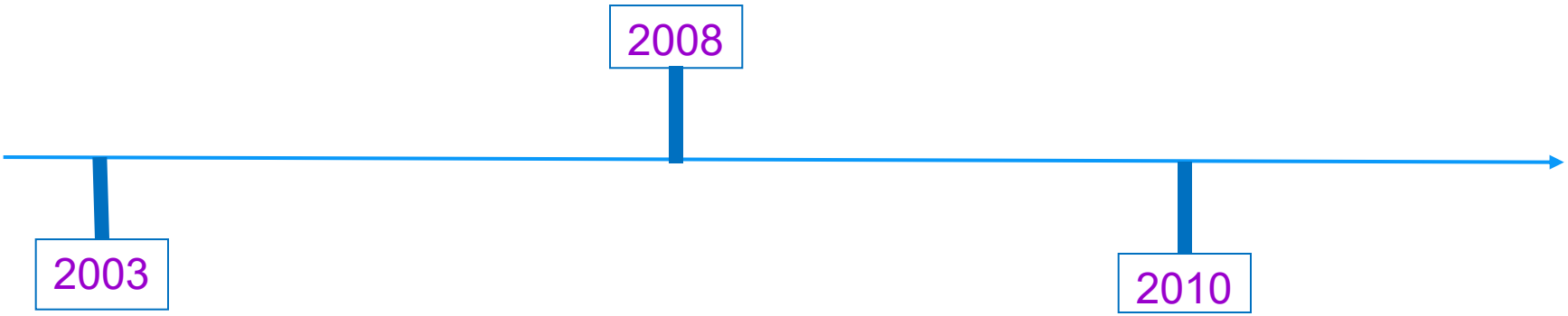
攻击阻断

- 爱因斯坦计划**基于入侵检测和入侵防御机制**来检测并阻断针对联邦机构的攻击

态势感知

- 提供给DHS(国土安全部)态势感知能力，可以**使用在一个机构中检测到的威胁信息保护政府的其他部门以及帮助私营企业保护自身安全**

爱因斯坦计划——3个阶段



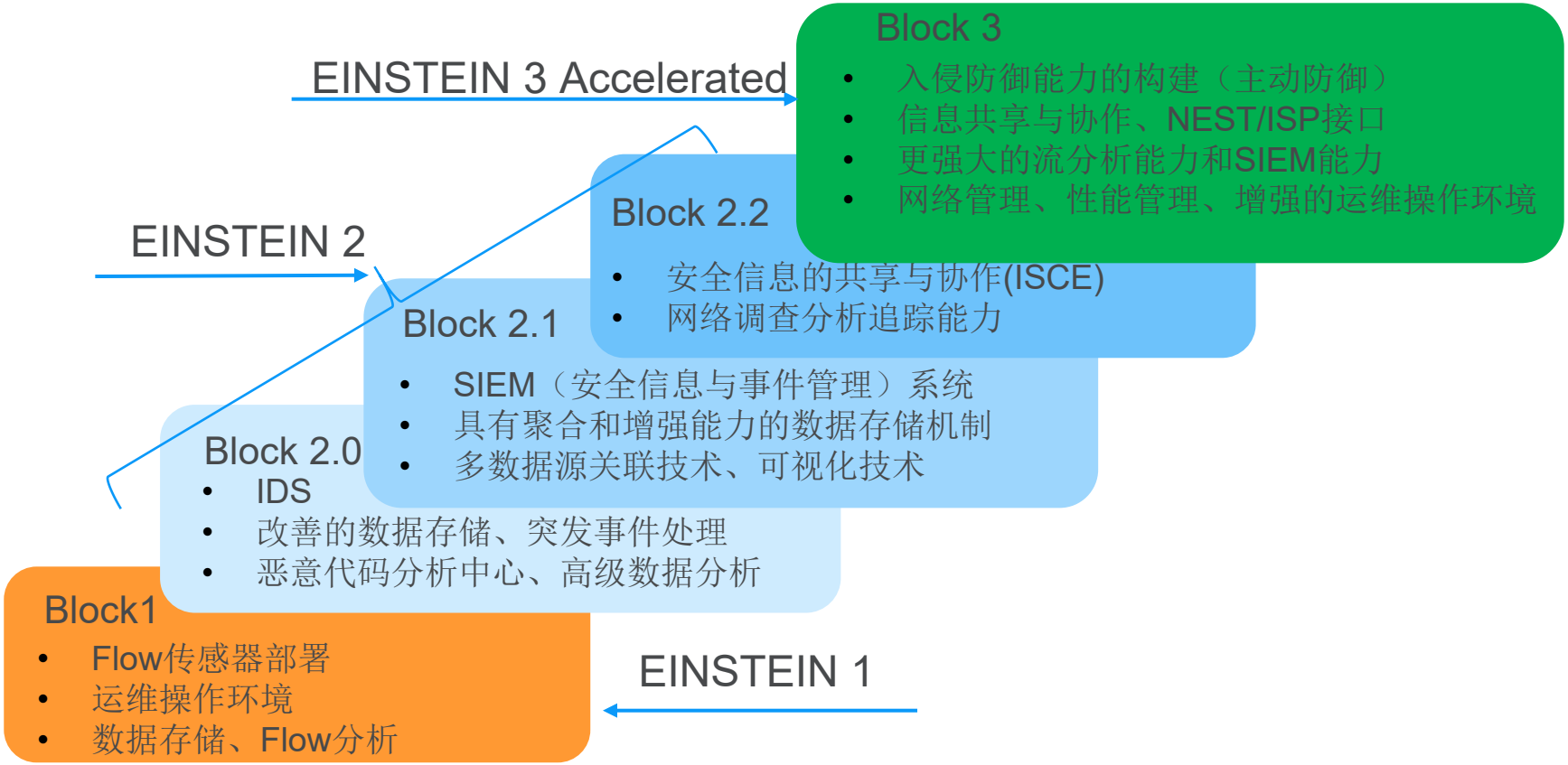
- 2008年起实施**EINSTEIN2**，2009年部署，该系统在原来对异常行为分析的基础上，增加了对恶意行为的分析能力，本质上依然是入侵检测系统，特点是被动响应

- **EINSTEIN1**始于2003年，本质上是入侵监测系统，主要任务是监听、分析、共享安全信息，特点是信息采集。

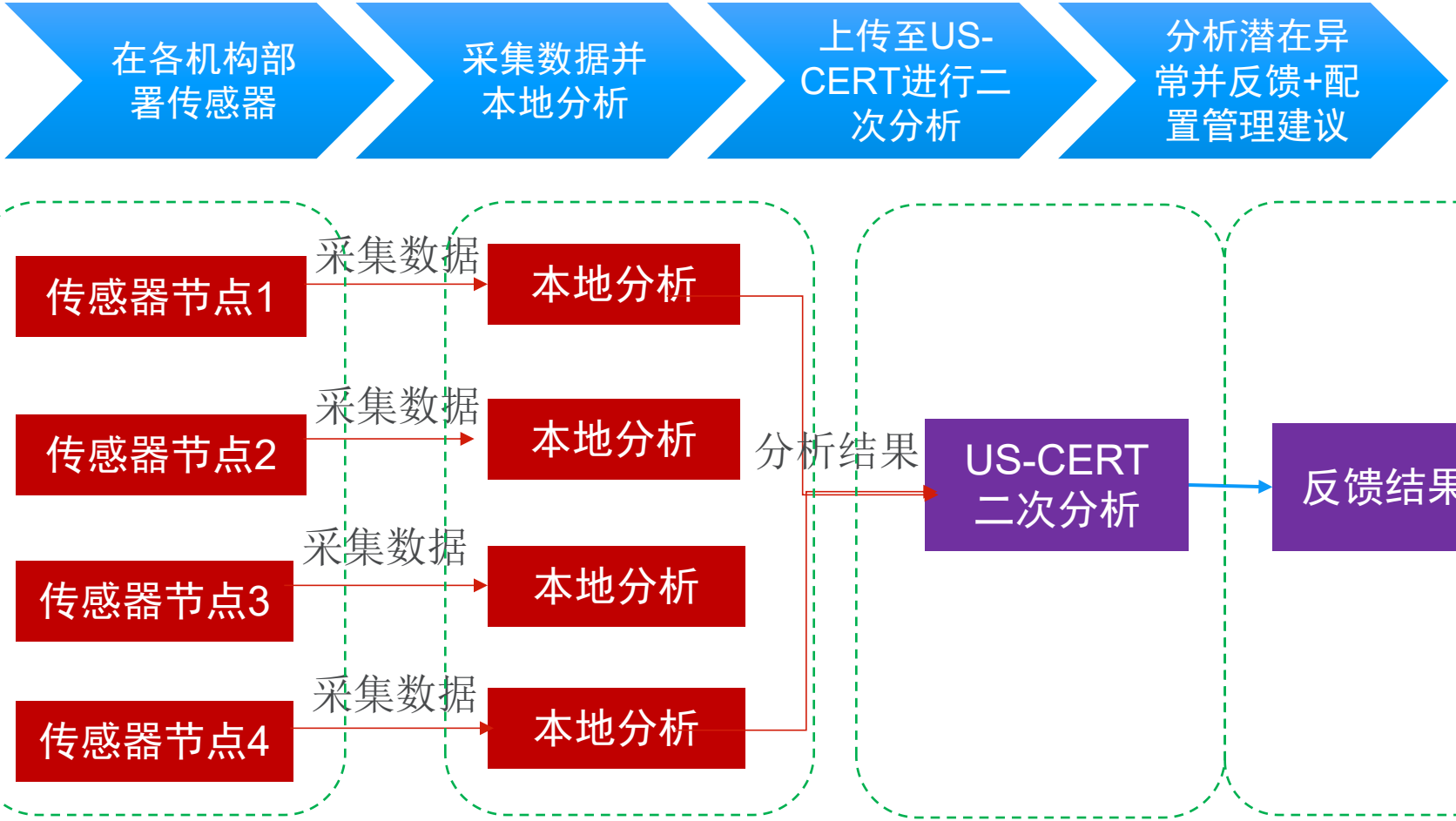
- 2010年，DHS（国土安全部）开始计划设计与部署入侵防御系统（即EINSTEIN3）来识别和阻止网络攻击。
- 在2012年DHS转变为使用一种新的方法，在这种方法中互联网服务提供商（ISPs）使用商业技术为联邦政府机构提供入侵防御安全服务，被称为**EINSTEIN 3 Accelerated** (E^3A)，
- 作为EINSTEIN3的第一阶段计划，E^3A是一种入侵防御系统

爱因斯坦计划路线图

- **该计划采用了渐进式迭代开发的方法论，并将整个任务分解为不同的子系统（Blocks）。每个子系统都有自己的迭代周期。而三个子系统之间是逐步增强、同时也不是完全取代的关系。**

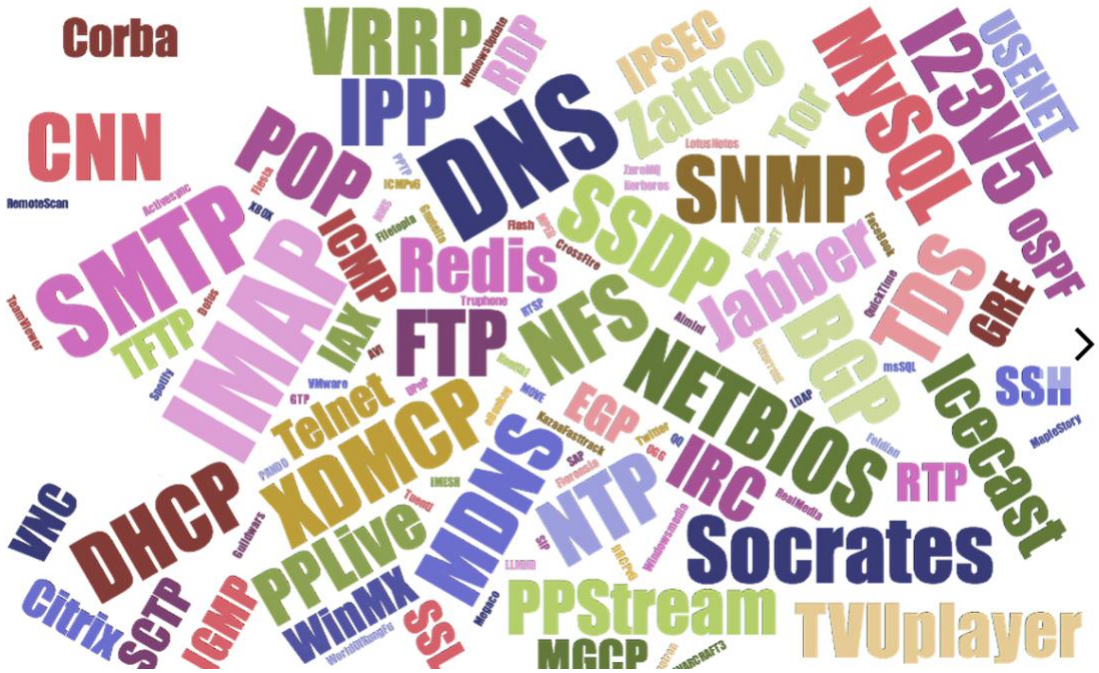


系统工作流程


在各机构部署传感器
采集数据并本地分析
上传至US-CERT进行二次分析
分析潜在异常并反馈+配置管理建议
传感器节点1
传感器节点2
传感器节点3
传感器节点4
采集数据
采集数据
采集数据
采集数据
本地分析
本地分析
本地分析
本地分析
分析结果
US-CERT二次分析
反馈结果

- OpenDPI和nDPI
  - 开源项目OpenDPI已不再维护，更新为nDPI，由ntop.org负责维护
  - 支持跨平台：Linux、Windows、Mac

- 可识别用随机端口的应用的流量或在常用端口上的非常规协议的流量
- 可扩展性好：协议解析器通过插件进行实现
- 目前支持185种协议解析



https://www.ntop.org/products/deep-packet-inspection/ndpi/

- L7-Filter
  - 开源工具，linux Netfilter的应用层数据包分类器
  - 技术原理：使用正则表达式来匹配应用层的数据，基于数据流工作，只分析关键数据包的载荷或连接信息
  - 可分类Kazza、HTTP、Jabber、Citrix、BitTorrent、FTP、Gnucleus、eDonkey2000与其他软件
  - 可分类流、电子邮件、P2P、网络电话、协议及游戏等应用

- Libprotoident
  - 新西兰怀卡托大学网络研究组（WAND）开发的DPI库
  - 引入轻度数据包检测（LPI），只检查每个方向载荷的头4个字节，组合使用载荷模式匹配、载荷大小、端口号与IP匹配等方法
  - 支持200多协议

- Software
  - AMP
  - Bearwall
  - BSOD
  - Configuration System
  - Darpwatch
  - DCCP
  - dhcparpd
  - globaliser
  - Libconfig
  - Libflowmanager
  - Libprotoident
  - Libtcpcsm
  - Libtrace
  - Libwandevent
  - Libwandio
  - maji
  - nettest
  - Network Simulation Cradle
  - Scamper
  - SRG
  - WDCap

Application	Classifier	% cor.	% wr.	% unc.
4Shared	PACE	27.08	0.00	72.92
	OpenDPI	27.08	0.00	72.92
	L7-filter-all	0.00	1.39	98.61
	L7-filter-com	0.00	0.00	100.00
	nDPI	0.00	0.00	100.00
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	0.00	100.00
America's Army	PACE	0.00	0.00	100.00
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	97.71	2.29
	L7-filter-com	0.00	97.43	2.57
	nDPI	4.00	0.00	96.00
	Libprotoident	0.00	89.14	10.86
	NBAR	0.00	72.00	28.00
BitTorrent clients (encrypted)	PACE	78.68	0.05	21.27
	OpenDPI	0.27	0.00	99.73
	L7-filter-all	40.54	10.17	49.29
	L7-filter-com	40.62	7.30	52.08
	nDPI	54.41	0.18	45.41
	Libprotoident	60.31	0.02	39.67
	NBAR	1.29	0.63	98.08
BitTorrent clients (non-encrypted)	PACE	99.87	0.00	0.13
	OpenDPI	80.61	0.00	19.39
	L7-filter-all	94.56	0.49	4.95
	L7-filter-com	94.60	0.42	4.98
	nDPI	99.41	0.02	0.57
	Libprotoident	99.30	0.00	0.70
	NBAR	77.84	0.36	21.80
Dropbox	PACE	94.62	0.00	5.38
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	0.00	100.00
	L7-filter-com	0.00	0.00	100.00
	nDPI	98.92	0.00	1.08
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	0.00	100.00
eDonkey clients (obfuscated)	PACE	36.06	7.26	56.68
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	11.64	16.59	71.77
	L7-filter-com	11.64	11.09	77.27
	nDPI	11.04	2.67	86.29
	Libprotoident	11.47	0.00	88.53
	NBAR	0.00	15.93	84.07
eDonkey clients (non-obfuscated)	PACE	16.50	3.74	79.76
	OpenDPI	3.98	0.30	95.72
	L7-filter-all	17.97	16.32	65.71
	L7-filter-com	17.99	10.79	71.22
	nDPI	15.57	2.28	82.23
	Libprotoident	17.86	0.31	81.83
	NBAR	2.05	11.19	86.76
Freenet	PACE	79.26	0.00	20.74
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	20.00	80.00
	L7-filter-com	0.00	14.07	85.93
	nDPI	0.00	3.70	96.30
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	15.56	84.44
FTP clients (active)	PACE	5.56	0.00	94.44
	OpenDPI	97.62	0.00	2.38
	L7-filter-all	5.56	92.06	2.38
	L7-filter-com	5.56	90.47	3.97
	nDPI	98.41	0.00	1.59
	Libprotoident	100.00	0.00	0.00
	NBAR	50.79	0.00	49.21
FTP clients (passive)	PACE	4.92	0.00	95.08
	OpenDPI	67.21	0.00	32.79
	L7-filter-all	4.92	76.23	23.77
	L7-filter-com	4.92	73.77	26.23
	nDPI	72.95	0.00	27.05
	Libprotoident	73.77	22.95	32.80
	NBAR	50.00	0.00	50.00
iTunes	PACE	77.45	0.00	22.55
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	63.83	6.81	29.36
	L7-filter-com	63.83	0.00	36.17
	nDPI	13.19	0.00	86.81
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	0.00	100.00
League of Legends	PACE	0.00	13.04	86.96
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	69.57	30.43
	L7-filter-com	0.00	4.35	95.65
	nDPI	0.00	13.04	86.96
	Libprotoident	0.00	4.35	95.65
	NBAR	0.00	0.00	100.00
Pando Media Booster	PACE	99.45	0.39	0.16
	OpenDPI	99.23	0.54	0.23
	L7-filter-all	0.00	0.74	99.26
	L7-filter-com	0.00	0.55	99.45
	nDPI	99.26	0.63	0.11
	Libprotoident	99.26	0.41	0.33
	NBAR	0.00	0.36	99.64
PPLive	PACE	88.21	0.00	11.79
	OpenDPI	0.07	0.13	99.80
	L7-filter-all	0.00	56.03	43.97
	L7-filter-com	0.00	17.15	82.85
	nDPI	43.91	1.05	55.04
	Libprotoident	43.91	1.05	55.04
	NBAR	0.00	0.40	99.60
PPStream	PACE	79.32	0.00	20.68
	OpenDPI	0.79	0.00	99.21
	L7-filter-all	0.00	38.39	61.61
	L7-filter-com	0.00	15.07	84.93
	nDPI	0.53	0.26	99.21
	Libprotoident	0.96	0.00	99.04
	NBAR	0.00	5.26	94.74
RDP clients	PACE	99.69	0.00	0.31
	OpenDPI	99.70	0.00	0.30
	L7-filter-all	0.00	92.25	7.75
	L7-filter-com	0.00	92.25	7.75
	nDPI	99.69	0.02	0.29
	Libprotoident	99.66	0.01	0.33
	NBAR	0.00	0.67	99.33
Skype (all)	PACE	83.51	5.05	11.44
	OpenDPI	38.49	0.32	61.19
	L7-filter-all	59.21	31.70	9.09
	L7-filter-com	62.52	24.67	12.81
	nDPI	99.82	0.00	0.18
	Libprotoident	88.75	0.00	11.25
	NBAR	70.37	3.40	26.23
Skype (audio)	PACE	100.00	0.00	0.00
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	85.71	14.29	0.00
	L7-filter-com	100.00	0.00	0.00
	nDPI	0.00	0.00	100.00
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	0.00	100.00
Skype (file transfer)	PACE	0.00	100.00	0.00
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	100.00	0.00
	L7-filter-com	0.00	100.00	0.00
	nDPI	0.00	0.00	100.00
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	0.00	100.00
Skype (video)	PACE	0.00	100.00	0.00
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	100.00	0.00
	L7-filter-com	0.00	100.00	0.00
	nDPI	0.00	0.00	100.00
	Libprotoident	0.00	0.00	100.00
	NBAR	0.00	0.00	100.00
Sopcast	PACE	66.27	3.07	30.66
	OpenDPI	66.27	2.59	31.14
	L7-filter-all	0.00	99.06	0.94
	L7-filter-com	0.00	74.76	25.24
	nDPI	63.68	1.18	35.14
	Libprotoident	46.70	0.24	53.06
	NBAR	0.00	0.00	100.00
Spotify	PACE	37.64	2.25	60.11
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	43.26	56.74
	L7-filter-com	0.00	10.11	89.89
	nDPI	0.56	3.93	95.51
	Libprotoident	0.56	0.00	99.44
	NBAR	0.00	0.56	99.44
Steam	PACE	55.19	0.75	44.06
	OpenDPI	0.33	0.00	99.67
	L7-filter-all	0.00	65.89	34.11
	L7-filter-com	0.00	4.73	95.27
	nDPI	76.02	0.42	23.56
	Libprotoident	75.85	0.00	24.15
	NBAR	0.00	0.58	99.42
TOR	PACE	85.95	0.00	14.05
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	0.00	100.00
	L7-filter-com	0.00	0.00	100.00
	nDPI	33.51	0.00	66.49
	Libprotoident	33.51	0.00	66.49
	NBAR	0.00	2.16	97.84
World of Warcraft	PACE	27.27	0.00	72.73
	OpenDPI	0.00	0.00	100.00
	L7-filter-all	0.00	86.36	13.64
	L7-filter-com	0.00	22.73	77.27
	nDPI	13.64	13.64	72.72
	Libprotoident	13.64	0.00	86.36
	NBAR	0.00	0.00	100.00

Protocol
DNS
HTTP
ICMP
IMAP STARTTL
IMAP TLS
NETBIOS Name Service

内容概要

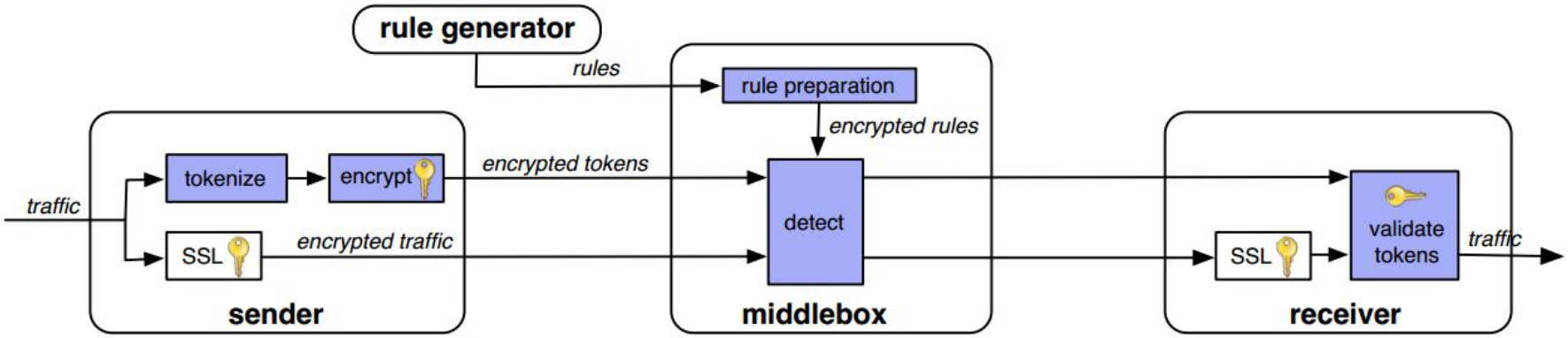
- 安全对抗技术

加密代理法
- **TOR**
- **ssh -D**
- gappproxy
- Psiphon
- 无界
- 自由门
- ……

变更协议
- UDP
- IPv6
- SDPY(不成熟)

VPN法
- PPTP
- L2TP
- **OpenVPN**

- 安全对抗技术
  - 数据加密与包检测
    - UC Berkeley提出的BlindBox，同时实现数据加密以增强隐私性，和数据包检测以增强安全性
    - DPIEnc and BlindBox Detect： 可搜索加密方案



BlindBox: Deep Packet Inspection over Encrypted Traffic

深度包检测面临挑战

- 下一代互联网技术
  - IPv6协议的普及
  - 物联网协议的检测
  - 工控协议的检测
- 数据包的分拆与合并
  - 多个数据包组成一个

深度包检测技术