



NETSCOUT 安全解决方案

全新的NETSCOUT 收购众多国际顶尖公司



服务保障领域的
市场领导者

- 业务性能保障
- 业务威胁防御



双市场携手并进

- 企业
- 运营商



成员公司历史总
和超过一百年
专注于全球最大的
IP和电信网络



国际覆盖
销售, 支持和服务
超过50个国家



上海中文技术支持中心

- 整合产品优势
- 基于数据流量分析
- 基于核心专利技术

NETSCOUT™



Sniffer母公司



1972年随尼克松
访华, 赠送中国

世界最大最早
DDOS公司



业界久负盛名的
福禄克



领先的NPB厂商

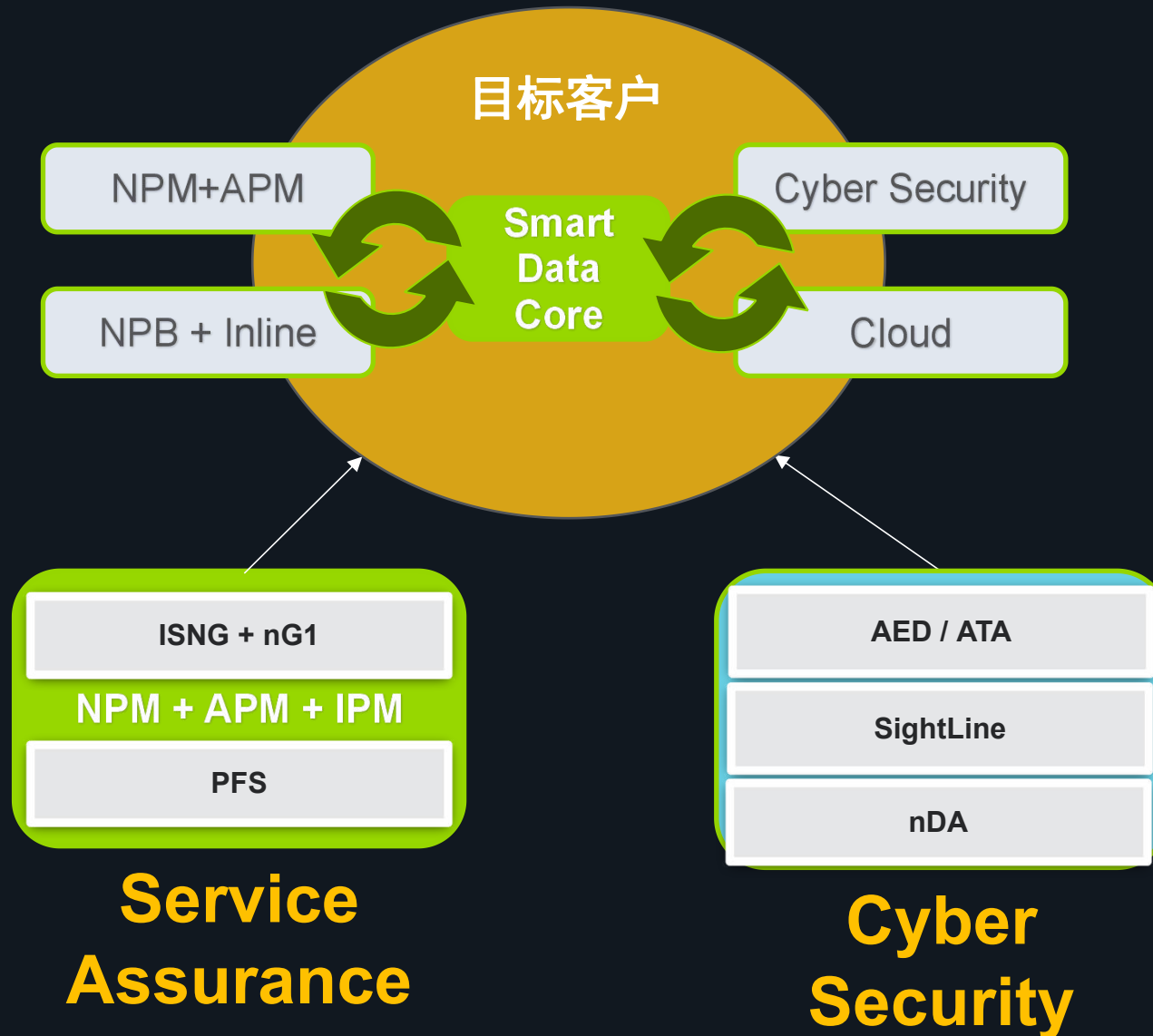


WiFi行业标准软件

业界称呼: 数据科学家公司



NETSCOUT整体解决方案



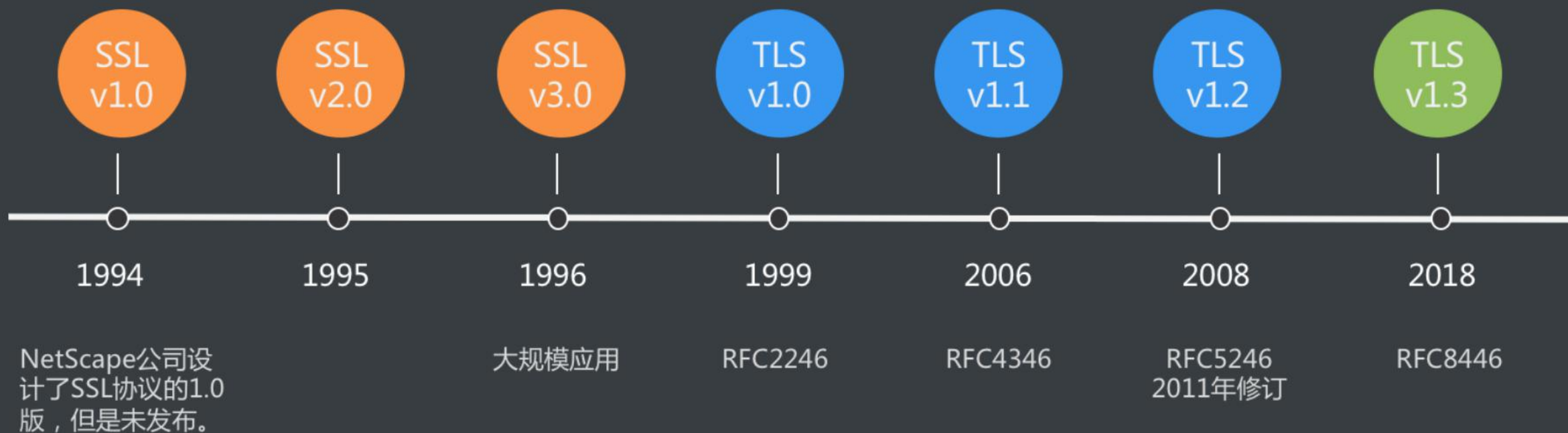
nDA



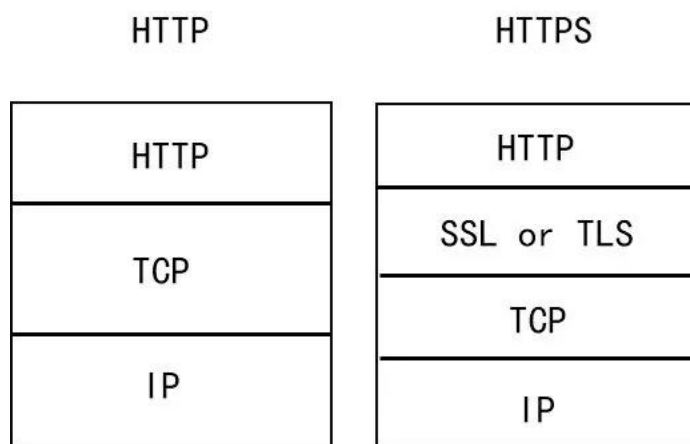
SSL加密发展历程

TLS 历史

- SSL (Secure Socket Layer 安全套接层) ，是Netscape (网景) 公司提出。
- TLS (Transport Layer Security Protocol) ：安全传输层协议。



简单介绍下TLS1.3协议及其版本变化

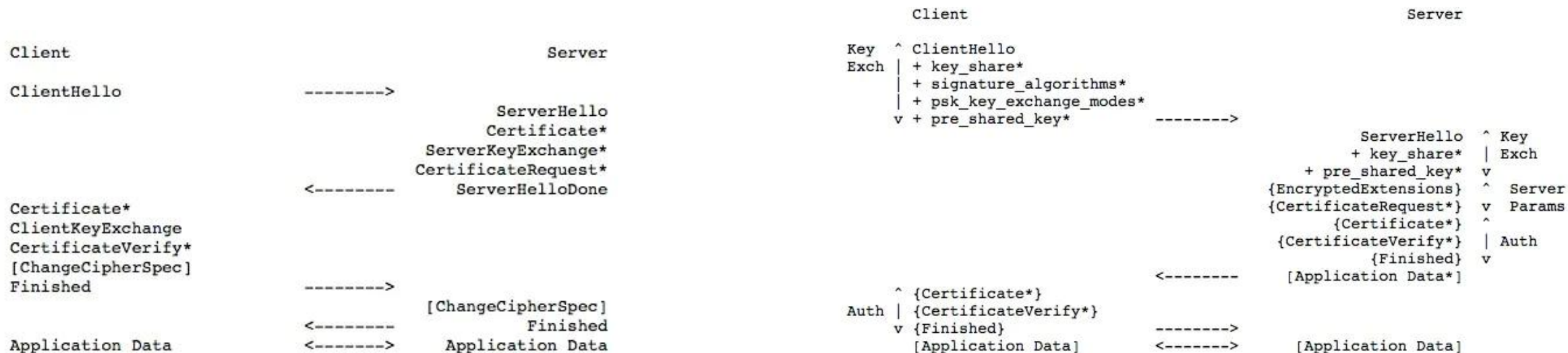


- ✓ 相比过去的版本，引入了新的密钥协商机制 — PSK 支持
- ✓ 0-RTT 数据传输，在建立连接时节省了往返时间
- ✓ 废弃了 3DES、RC4、AES-CBC 等加密组件，废弃了 SHA1、MD5 等哈希算法
- ✓ ServerHello 之后的所有握手消息采取了加密操作，可见明文大大减少
- ✓ 不再允许对加密报文进行压缩、不再允许双方发起重协商
- ✓ DSA 证书不再允许在 TLS 1.3 中使用



总结下TLS1.3的优势

更快的访问速度



△ TLS 1.2 完整握手框架 (来自 RFC 5246)

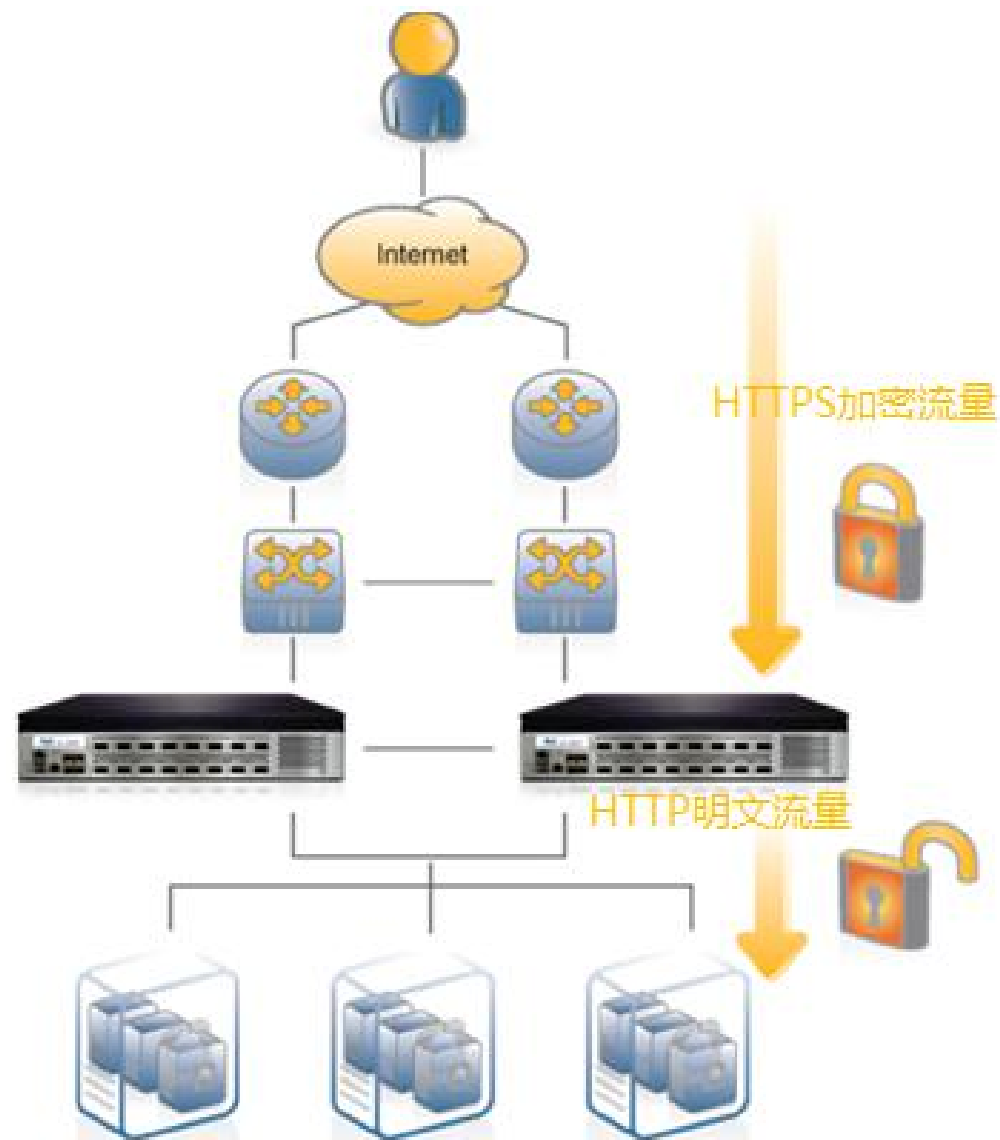
△ TLS 1.3 完整握手框架 (来自 TLS 1.3 最新草案)

使用 TLS 1.2 需要两次往返 (2-RTT) 才能完成握手, 然后才能发送请求。



客户如何实现SSL加密?

- 根据自身业务申请CA证书
- 搭建HTTPS业务服务器
(一般会在负载均衡或者nginx上实现)



为什么要nDA?

1. SSL卸载设备网络拓扑位置的局限性——一般都旁路在核心或者汇聚交换机上，导致之前网络设备的流量无法解密
2. SSL卸载设备只能处理入向流量的解密，出向流量不支持
3. SSL卸载设备无法做灵活的流量调度，配合第三方安全等其他设备稍显不足（同时只能做inline，不支持被动模式部署）

- 57%的受访者认为对SSL通信量的检查是必要的或非常重要的。
- 尽管SSL解密解决方案很重要，但61%的受访者表示，性能不足是实现此类解决方案的最大障碍。其他的障碍是没有合适的工具和缺乏内部专业知识。83%的受访者表示，在检查过程中解密SSL通信量会导致性能下降。

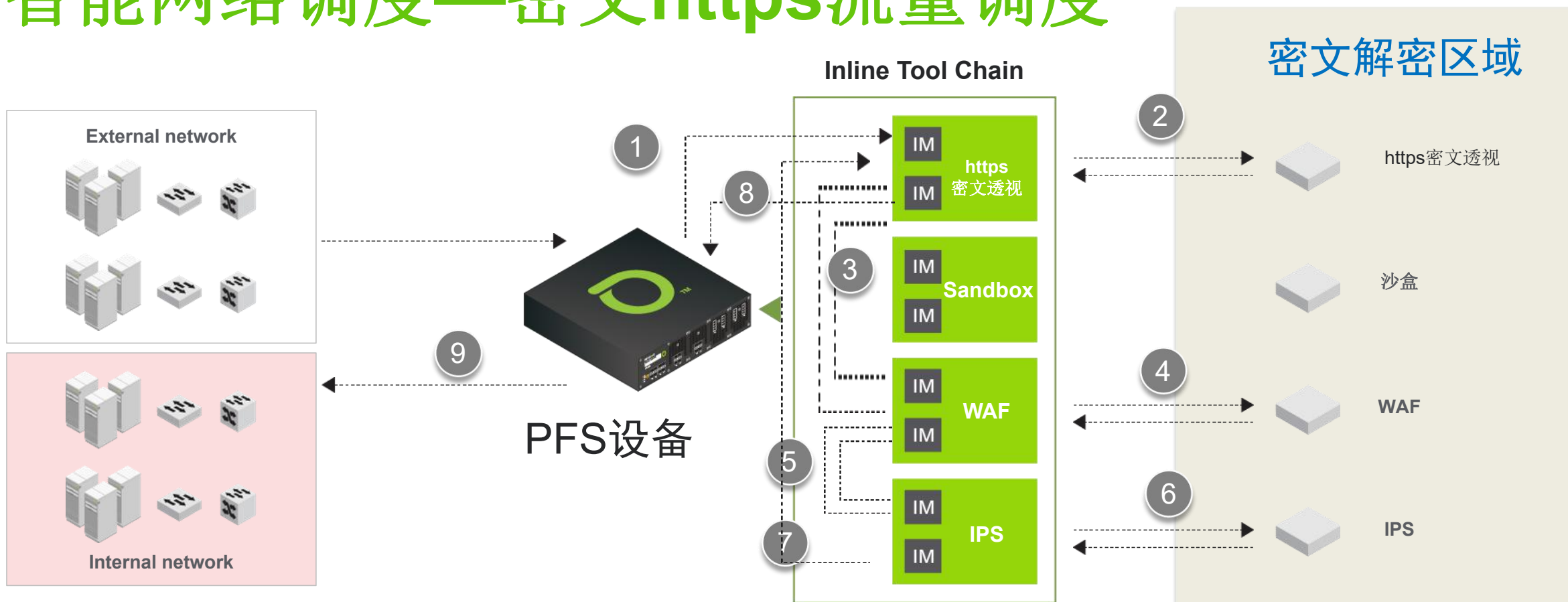
NETSCOUT™

Guardians of the Connected World

什么是nDA?



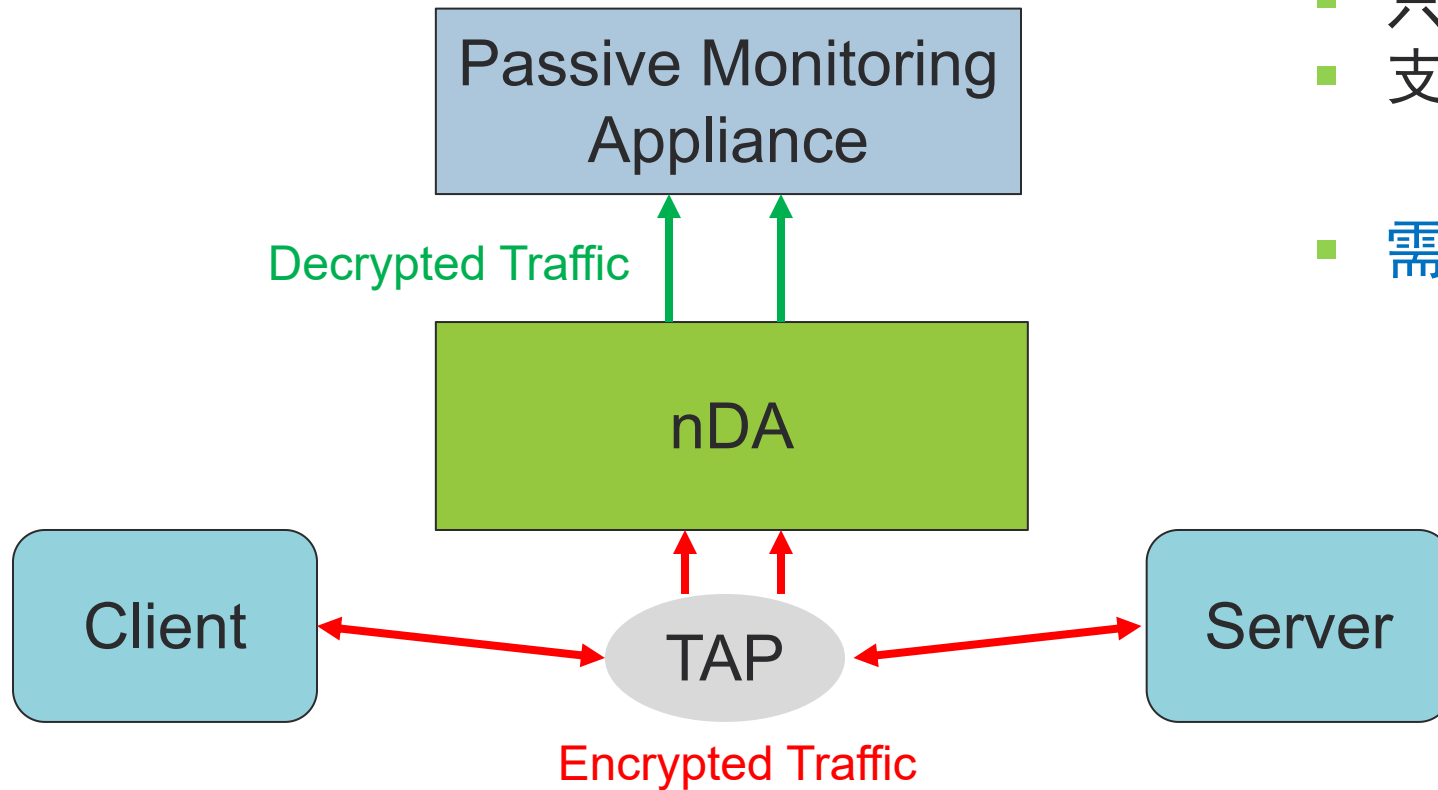
智能网络调度—密文https流量调度



实现SSL可视化编排

部署模式1-被动模式解密

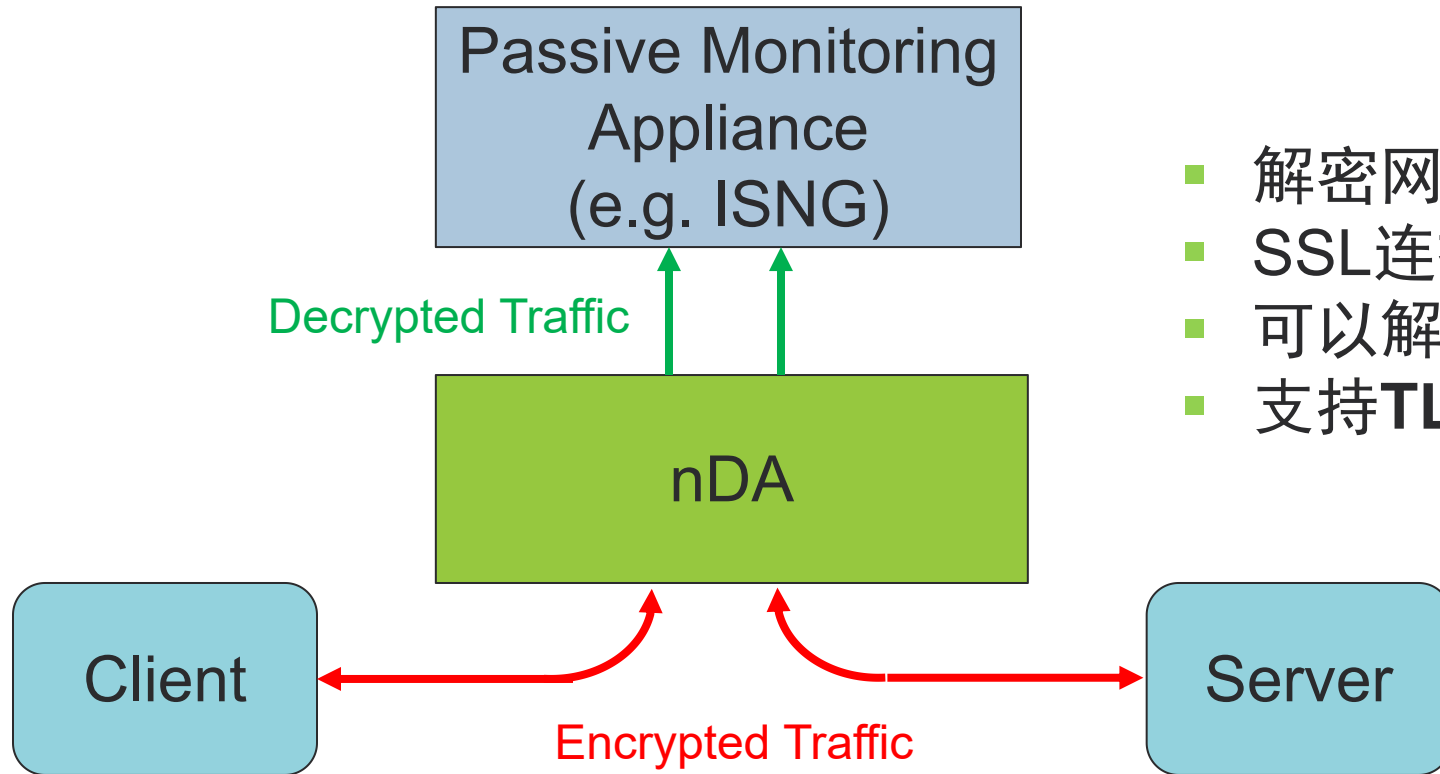
- 解密镜像流量
- 只能解密Static Keys
- 支持TLS 1.2和以前的
- 需要抓到完整的流量



Appliance receives copy of decrypted traffic



部署模式2-主动解密发送给被动监控工具



- 解密网络流量
- SSL连接中的参与者
- 可以解密 *Ephemeral* & Static Keys
- 支持 **TLS 1.3** 和更早的

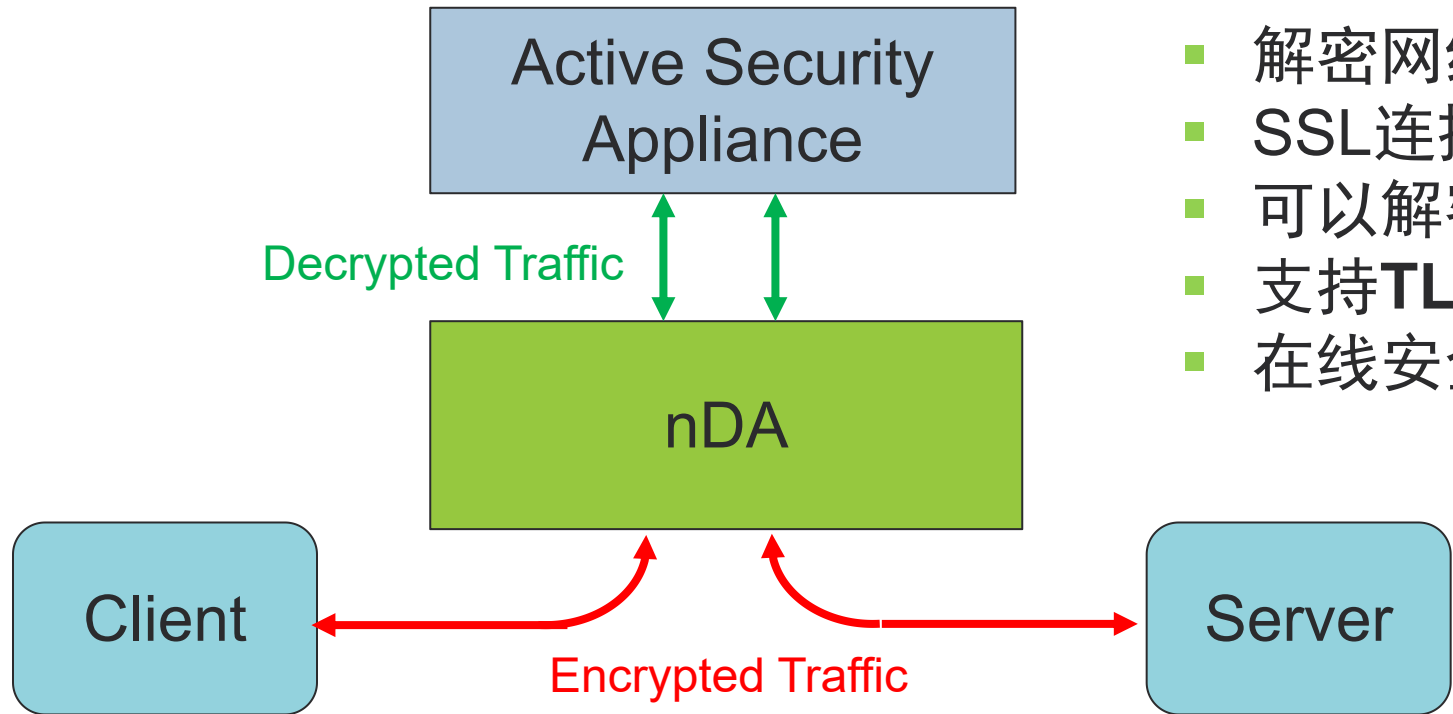
For all cases:
transparent device
(no L2 or L3 address)

not full / explicit proxy

Appliance receives copy of
decrypted traffic



部署模式3-主动解密发送给在线安全工具



- 解密网络流量
- SSL连接中的参与者
- 可以解密*Ephemeral* & Static Keys
- 支持**TLS 1.3** 和更早的
- 在线安全设备处理完后再次加密

- 设备接收解密流量
- 设备可以丢弃或者修改可以流量
 - 丢弃数据包的流将被终止
 - 不支持更改数据包数
 - 不支持增加或者删除数据
 - 修改数据包头, esp. 不支持IP地址
 - 不支持NAT
- 清理后的流量发送给 nDA

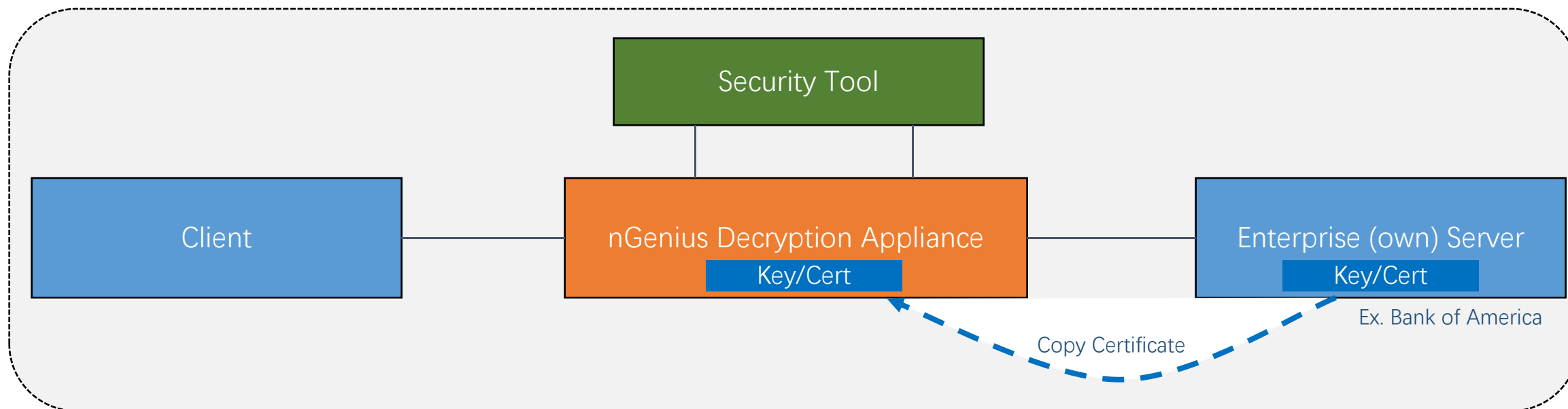
For all cases:
transparent device
(no L2 or L3 address)

not full / explicit proxy



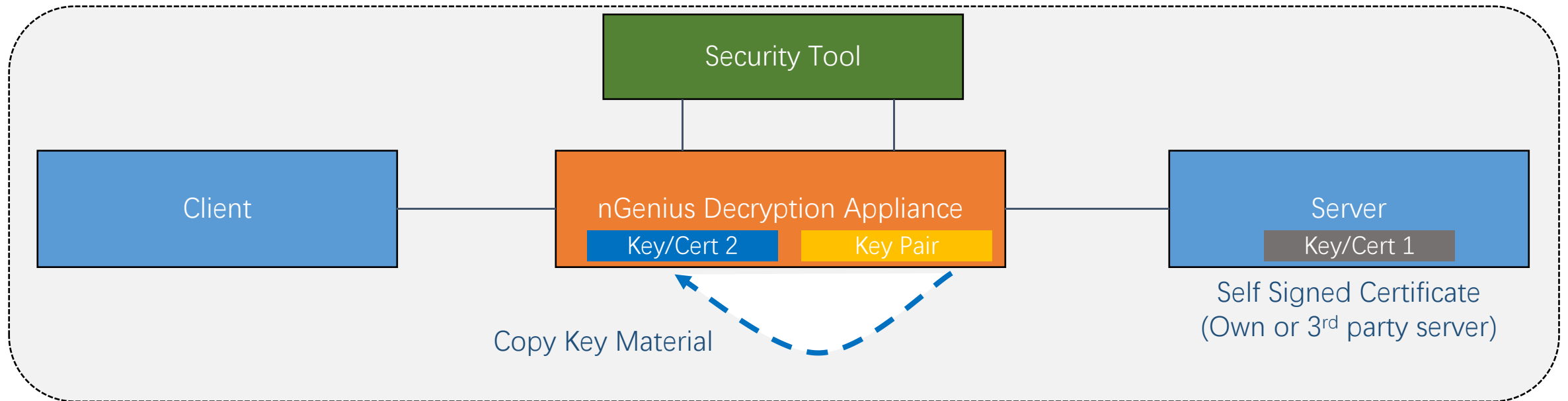
How nDA Works? 自有服务器情况

- 客户端需要信任nDA来解密
- 在自有服务器情况, 客户拥有服务器证书和key.
- 导入证书和key到nDA
- 客户和服务器的TLS握手使用Static Key
- nDA 知道对称密钥信息
- 策略行为–Use Known Key



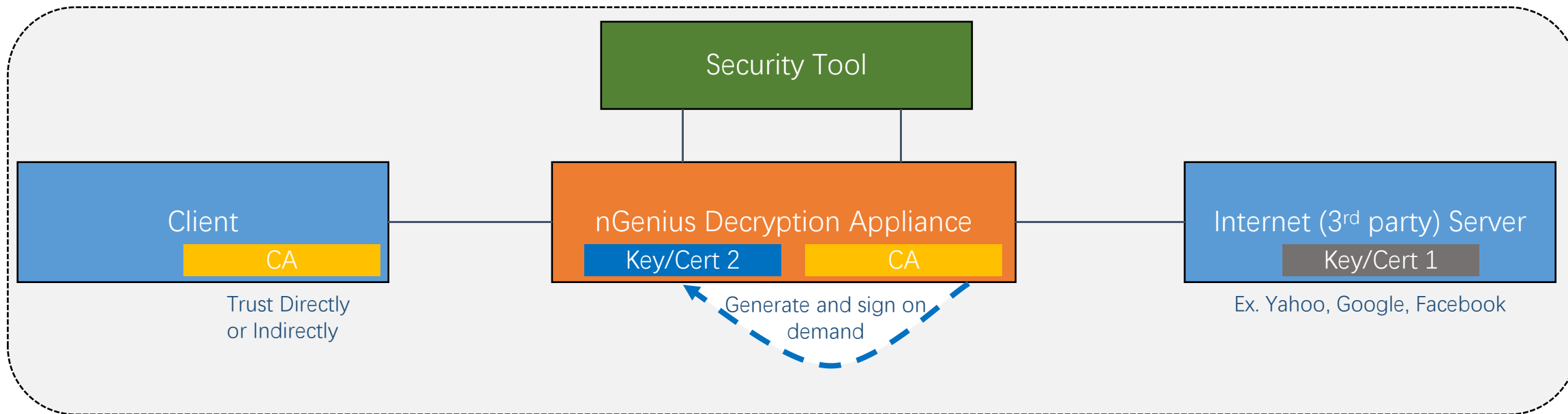
How nDA Works? 自签名证书case

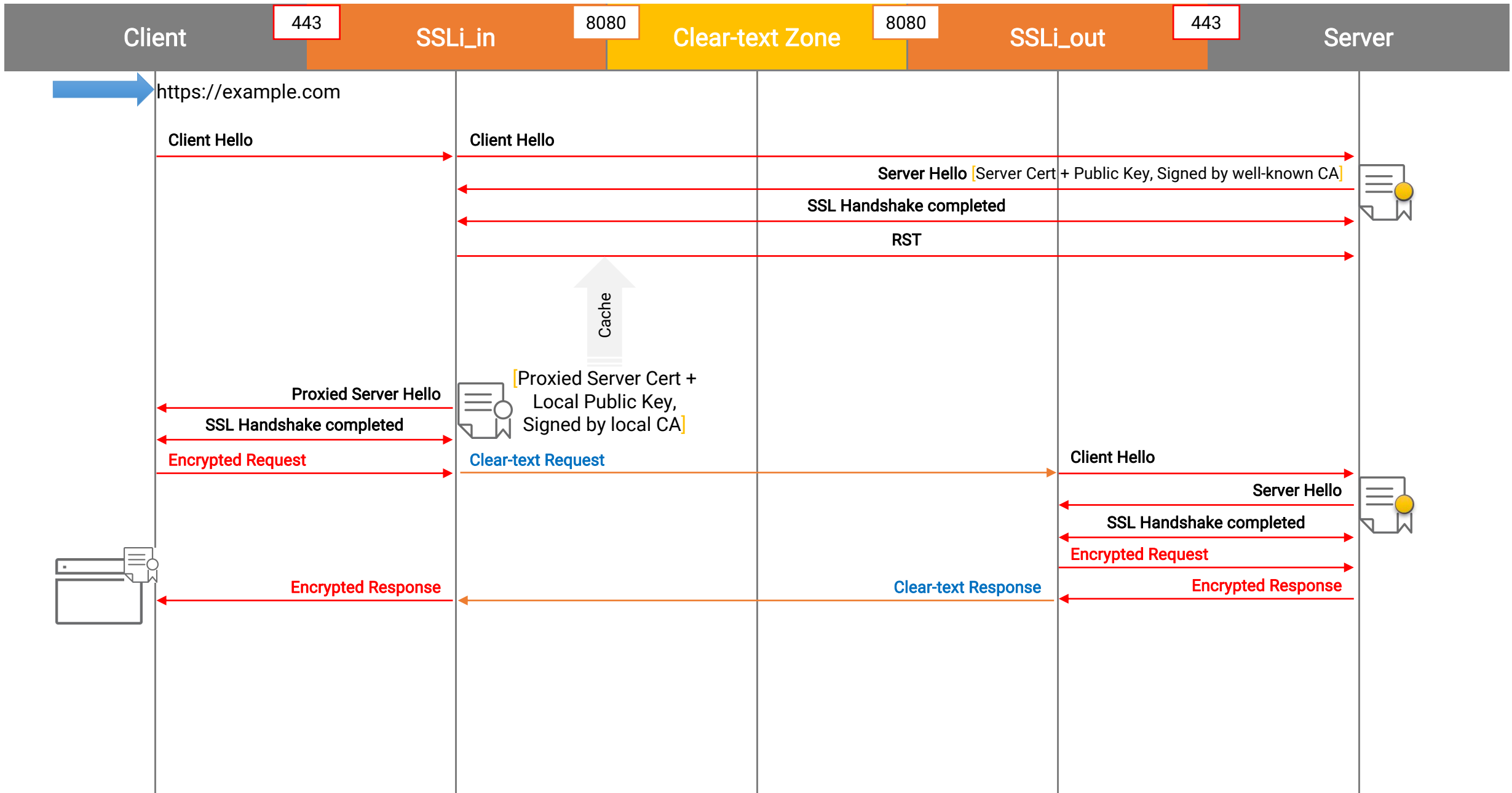
- 服务器上的自签名证书。
- 浏览器将发出安全警告
- 使用服务器证书，但使用nDA私钥对证书进行签名
- 客户与保密协议之间的TLS握手
- 保密协议和自有服务器之间的TLS握手
- 策略操作-替换密钥



How nDA Works? 第三方服务器case

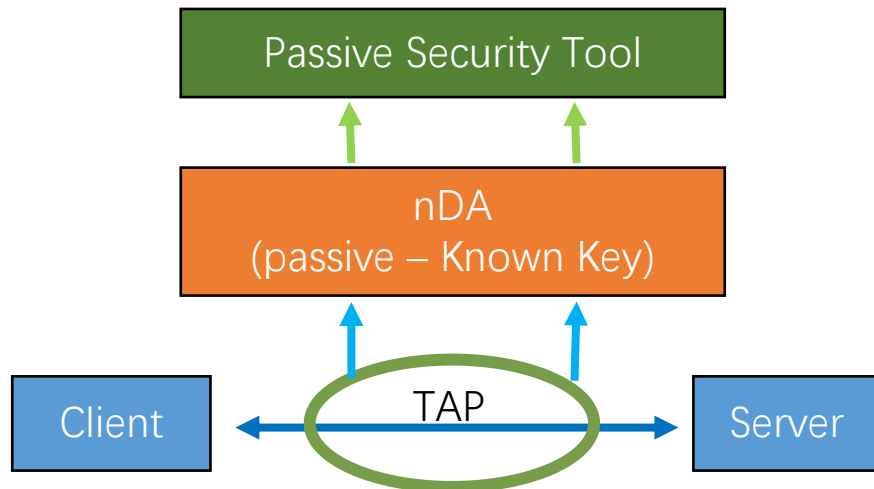
- 在第三方服务器case, 客户没有服务器的证书和key.
- 在nDA生产一张证书并让客户根CA签署证书
- 或者在nDA中生成自签名证书并将证书导入到所有客户端浏览器 (对于大型组织不实用)
- TLS 在客户端和nDA之间握手
- TLS 在nDA 服务器之间握手
- Policy Action – Resign



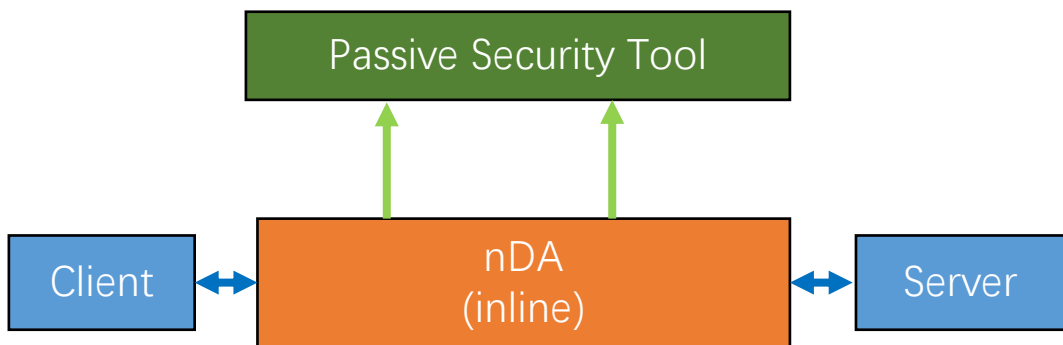


nDA Operation Modes

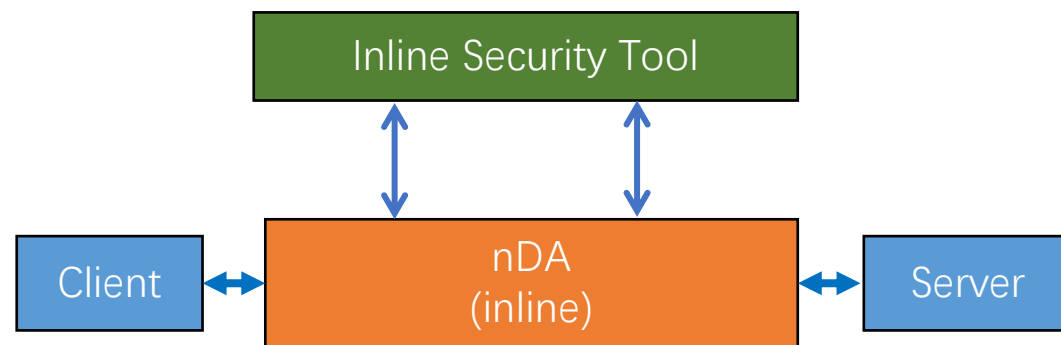
Passive - Passive



Inline - Passive



Inline - Inline



选型



nDA-2725 | 4端口1/10 GbE SFP28

nDA-4835 | 8端口1/10 GbE SFP28

SKU	描述
D-02725-XSJA1	nGenius Decryption设备, 4个1G/10G (SFP28)端口, 1U, 1颗Intel 6152 22-Core, 2.1GHz的CPU, 96GB内存, 32TB (4x 8TB)硬盘, AC 电源
D-04835-XSJA2	nGenius Decryption设备, 8个1G/10G (SFP28)端口, 1U, 2颗Intel 6152 22-Core, 2.1GHz的CPU, 192GB内存, 32TB (4x 8TB)硬盘, AC 电源
D-02725-XSJD1	nGenius Decryption设备, 8个1G/10G (SFP28)端口, 1U, 1颗Intel 6152 22-Core, 2.1GHz的CPU, 96GB内存, 32TB (4x 8TB)硬盘, DC 电源
D-04835-XSJD2	nGenius Decryption设备, 8个1G/10G (SFP28)端口, 1U, 2颗Intel 6152 22-Core, 2.1GHz的CPU, 192GB内存, 32TB (4x 8TB)硬盘, DC 电源
D-02725-00S-1	NETSCOUT认证的nGenius Decryption设备软件, 用于D-02725认证的设备硬件
D-04835-00S-1	NETSCOUT认证的nGenius Decryption设备软件, 用于D-04835认证的设备硬件

AED

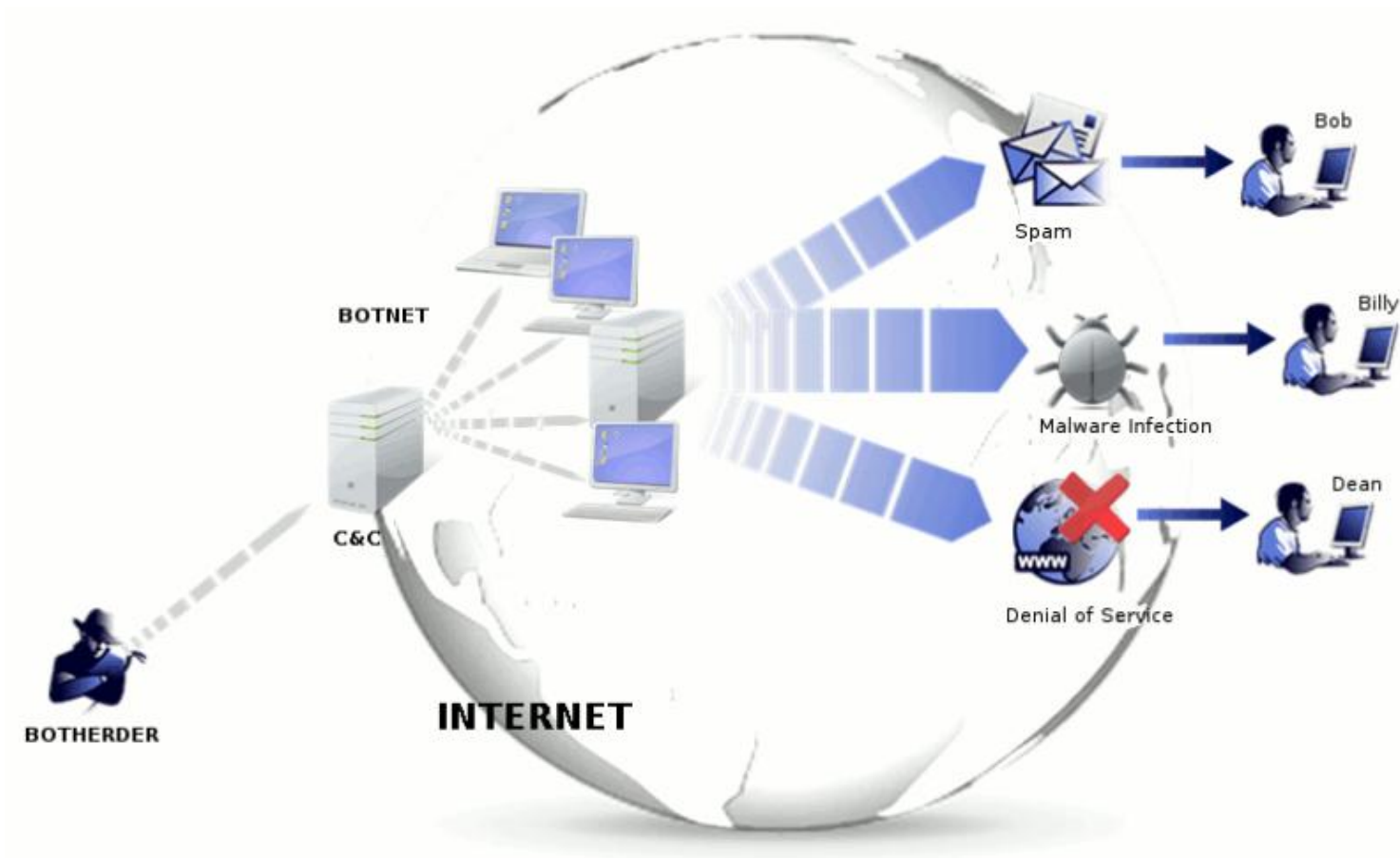


什么是僵尸网络（Botnet）？

僵尸程序（Bot）通常是指可以自动执行预定义指令或功能，可以被预定义指令控制的一种计算机程序。数量庞大的僵尸程序通过一定方式联合，就组成了僵尸网络。

僵尸网络的特点就是控制者和僵尸程序之间存在一对多的高度控制关系，控制指令下发后，僵尸程序往往会自行传播和执行，因此僵尸网络传播范围极广，其危害和防御难度更大。

DDoS攻击基本都是从僵尸网络发起攻击的。



什么是DDoS攻击？

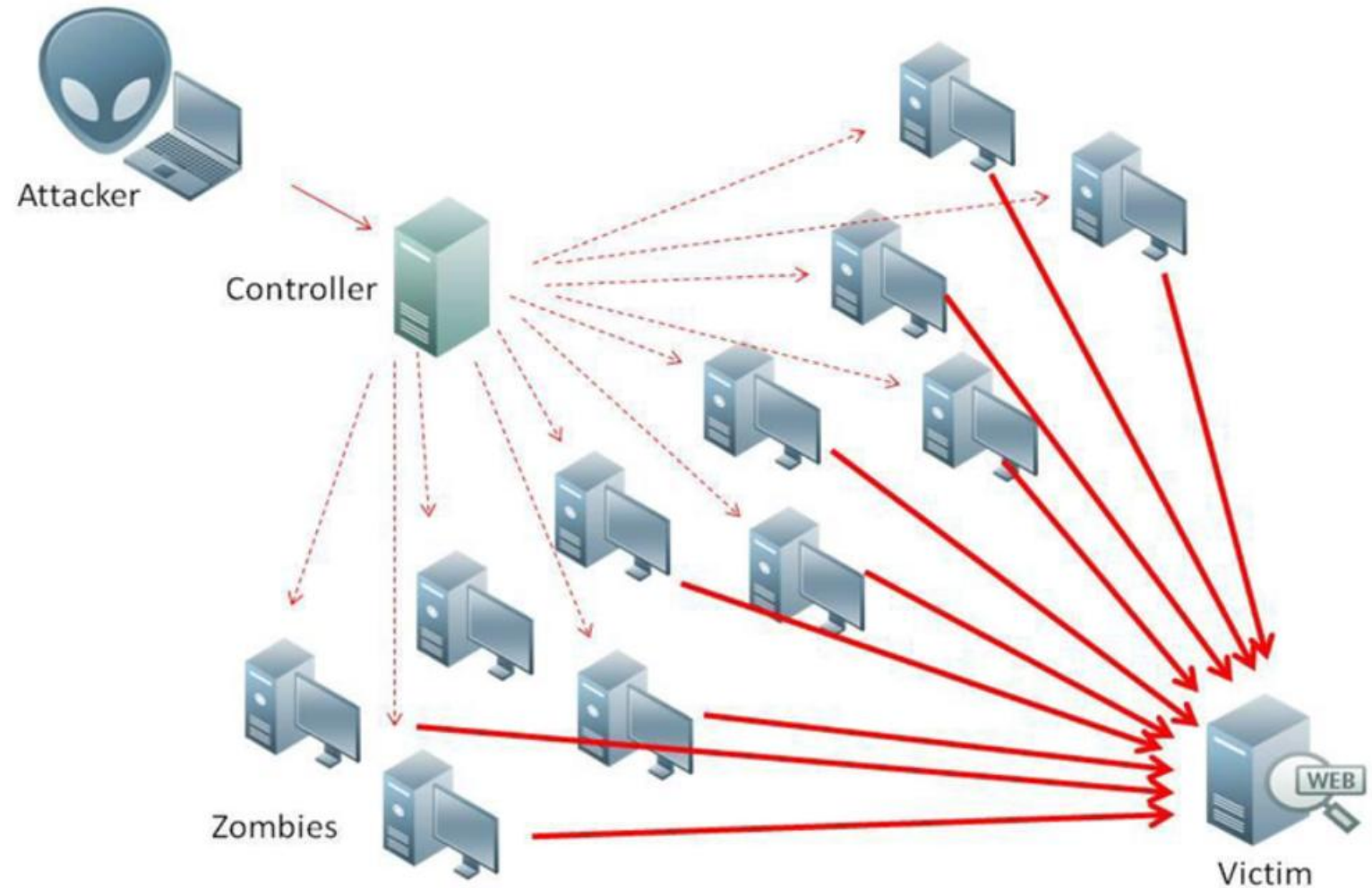
DDoS： 分布式拒绝服务

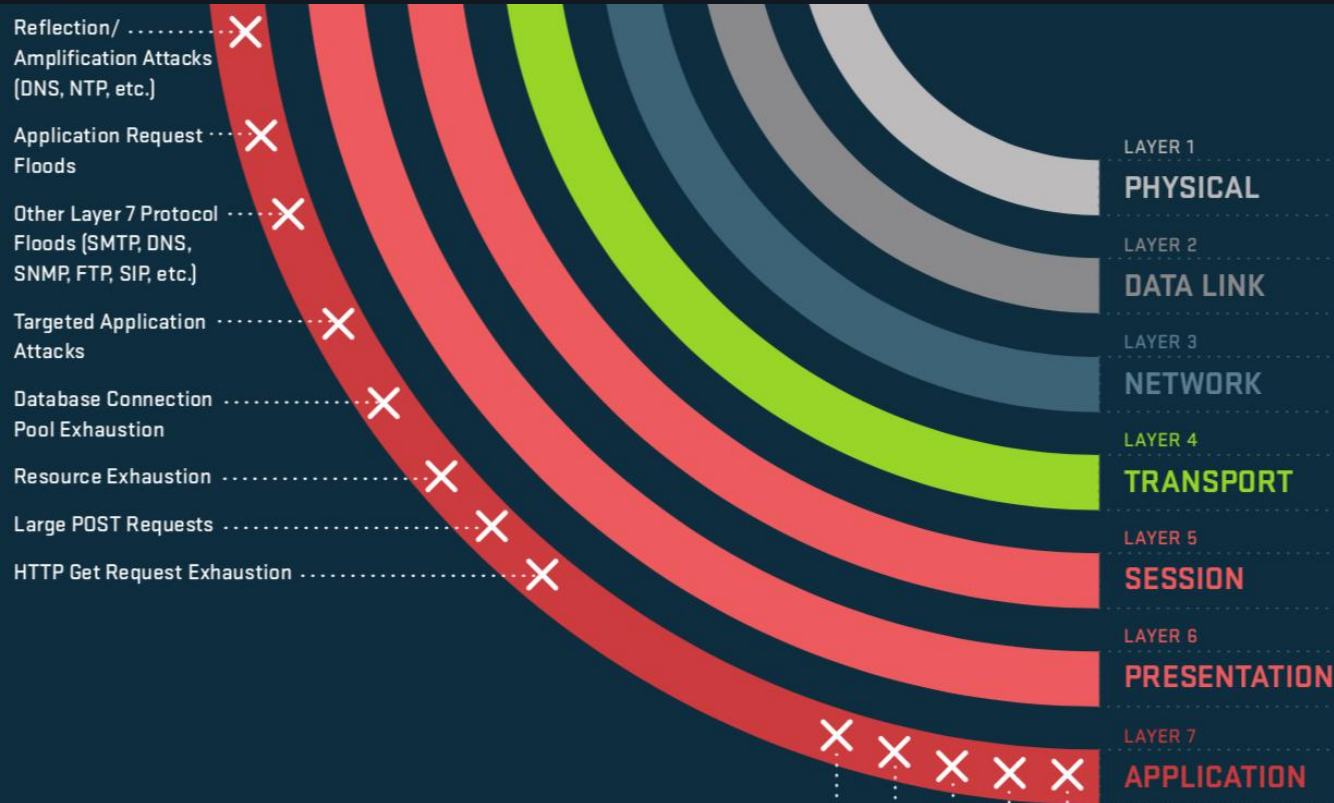
其主要方法是攻击者在Internet中控制大量的肉鸡一起向攻击目标发起攻击，通过大量泛洪攻击、资源耗尽攻击、协议漏洞攻击、应用层攻击等手段，使被攻击目标无法提供正常服务。

DDoS攻击这一名称包含了两个含义，其一是“拒绝服务”；其二是分布式，主要体现在攻击源往往非常离散，其中可能包含了大量伪装的虚假IP攻击源。

随着攻击的不断变化，目前一次DDoS攻击往往混杂着多种攻击手段，从不同层面、多个维度实施攻击。

英文缩写： Distributed Denial of Service





HTTPS Encrypted Attacks (any HTTP attack, Slow Loris, Slow POST, etc.)
 Mimicked User Browsing
 Slow Read
 Slow POST
 Slowloris



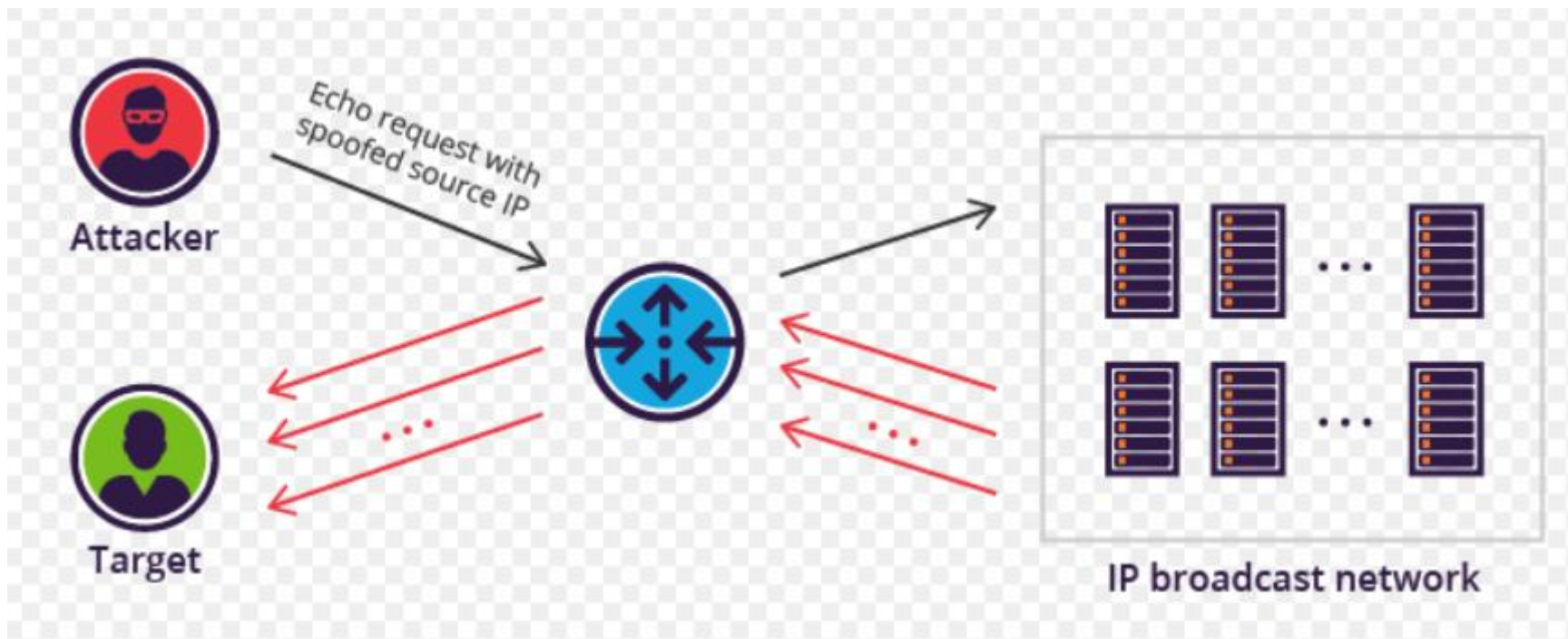
LEARN MORE ABOUT DDOS ATTACK PROTECTION




什么是带宽耗尽型攻击？

通俗来讲，带宽耗尽型攻击的主要手段就是通过泛洪或放大攻击“堵塞”被攻击目标所在网络的入口，例如“堵塞”被攻击目标所在数据中心的互联网入口链路，使得用户和应用服务器之间的通信链路出现拥塞，造成客户端访问进不来，服务应答出不去，使得服务无法提供。

UDP 泛洪和DNS放大攻击就属于此类型攻击，目前比较盛行。



什么是资源耗尽型攻击？

资源耗尽攻击主要采用大量请求消耗服务器系统资源，造成系统资源耗尽，无法及时有效的应答客户端请求。CC攻击（）是DDOS（分布式拒绝服务）的一种。

攻击方法：

攻击者通过代理服务器或者肉鸡向受害主机不停访问，造成服务器资源耗尽，一直到宕机崩溃。CC攻击利用代理服务器向网站发送大量需要较长计算时间的URL请求，如数据库查询等，导致服务器进行大量计算而很快达到自身的处理能力而形成DOS。而攻击者一旦发送请求给代理后就主动断开连接，因为代理并不因为客户端这边连接的断开就不去连接目标服务器，因此攻击机的资源消耗相对很小，而从目标服务器看来，来自代理的请求都是合法的。

CC攻击说明

我成功黑了一个访问量巨大的网站首页，在页面中添加了100个如下的代码：

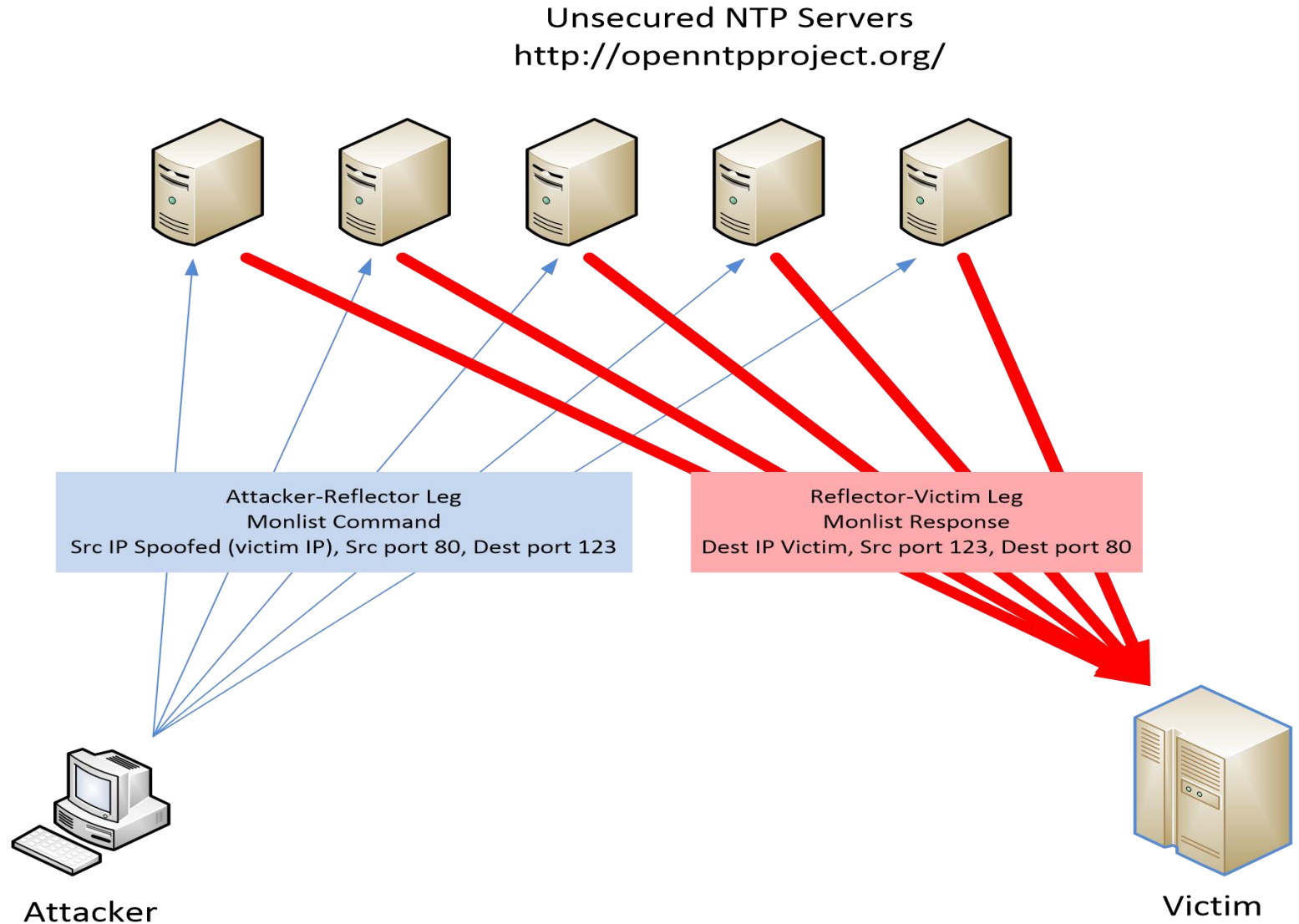
```
Ⓞ≡//Ⓞ∠(M)Ⓞ ⓄⓄⓄ∠=↗↗↗↗↗(P)://科来.∠□(M) ⊥□Ⓞ∠ⓄⓄ="0" √≡∠↗↗↗↗="0"  
↗Ⓞ≡↗↗↗↗="0" Ⓞ,Ⓞ/≡//Ⓞ∠(M)Ⓞ
```



什么是反射攻击？

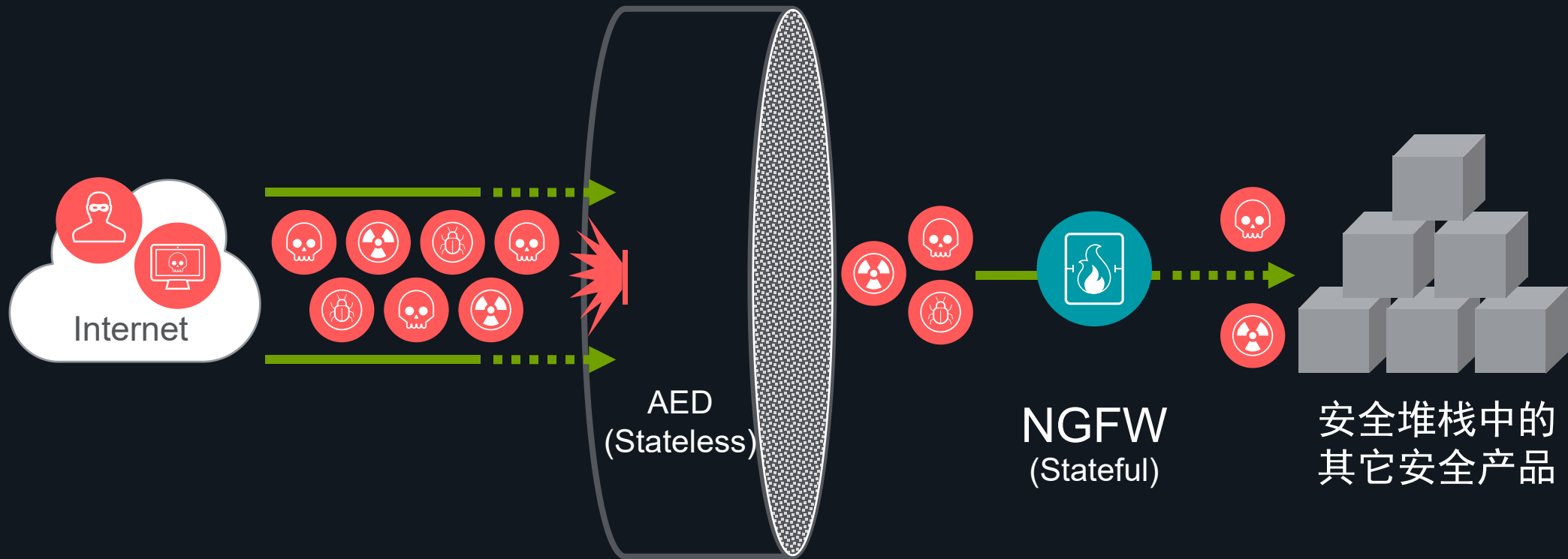
反射攻击往往会利用无需认证和握手的协议，因此绝大多数反射攻击采用UDP协议，其中以DNS反射放大攻击和NTP反射放大攻击最出名。

之所以出现“放大”这个效果，是因为攻击利用了请求和响应数据量不对称的情况，响应数据量比请求数据量越大，攻击效果越明显，例如通常DNS请求数据包大小是60个字节左右，而DNS响应数据包大小可以达到3000字节，甚至4000字节，相当于攻击流量被放大了50倍！而NTP反射放大攻击甚至会被放大几百倍。



无状态包处理以停止进站威胁

停止进站DDoS攻击和大量的商业威胁



- 拥有数百万基于声誉的IoC，无状态的边界防御就像一个“粗过滤器”，使有状态的防火墙更加高效

加载过多威胁防护功能，NGFW性能下降

厂商数据

Palo Alto

Performance	PA-7080 System	PA-7050 System
Firewall throughput (App-ID)	200Gbps	120Gbps
Threat Prevention throughput	100Gbps	60Gbps

- Throughput **degrades by 50%** with Threat Prevention
- Number of IOCs supported:
 - **Anti-virus signatures – 1 Million**
 - Wildfire signatures – 100K
 - DNS signatures – 100K

Fortinet

	FG-900D
Firewall Throughput (1518/512/64 byte UDP)	52 / 52 / 33 Gbps
Firewall Latency	3 μs
Concurrent Sessions	11 Million
New Sessions/Sec	280,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) ¹	25 Gbps
Max G/W to G/W IPSEC Tunnels	2,000
Max Client to G/W IPSEC Tunnels	50,000
SSL VPN Throughput	3.6 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10,000
IPS Throughput ¹ (HTTP / Enterprise Mix)	8 / 4.2 Gbps
SSL Inspection Throughput (IPS, HTTP) ³	4 Gbps
Application Control Throughput (HTTP 64K) ²	10 Gbps
NGFW Throughput (Enterprise Mix) ^{2,4}	4 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	3 Gbps
Max FortiAPs (Total, Tunnel)	1,024 / 512
Max FortiSwitches	64
Max FortiTokens	1,000
Max Registered Endpoints	2,000
Virtual Domains (Default/Max)	10 / 10

52Gbps



3Gbps



如何制造攻击?

TCP泛洪攻击: 常见的DDoS攻击方式

Attacker:

```
root@hunan-attacker:~# hping3 hunan-victim -p 80 -S -L 0 -c 10 --faster -q
HPING hunan-victim (eth0 192.168.1.8): S set, 40 headers + 0 data bytes

--- hunan-victim hping statistic ---
10 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@hunan-attacker:~#
```

Victim:

```
root@hunan-victim:~# tcpdump -i ens33 host hunan-attacker and dst port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
17:12:19.910526 IP hunan-attacker.sunclustermgr > hunan-victim.http: Flags [S], seq 1624593210, win 512, length 0
17:12:19.910724 IP hunan-attacker.rmiactivation > hunan-victim.http: Flags [S], seq 1454603507, win 512, length 0
17:12:19.910834 IP hunan-attacker.rmiregistry > hunan-victim.http: Flags [S], seq 1056552870, win 512, length 0
17:12:19.910929 IP hunan-attacker.mctp > hunan-victim.http: Flags [S], seq 1093113352, win 512, length 0
17:12:19.911002 IP hunan-attacker.pt2-discover > hunan-victim.http: Flags [S], seq 1219452628, win 512, length 0
17:12:19.911065 IP hunan-attacker.adobeserver-1 > hunan-victim.http: Flags [S], seq 1024248274, win 512, length 0
17:12:19.911128 IP hunan-attacker.adobeserver-2 > hunan-victim.http: Flags [S], seq 366219423, win 512, length 0
17:12:19.911153 IP hunan-attacker.xrl > hunan-victim.http: Flags [S], seq 1960717102, win 512, length 0
17:12:19.911164 IP hunan-attacker.ftranhc > hunan-victim.http: Flags [S], seq 459985935, win 512, length 0
17:12:19.911174 IP hunan-attacker.isoipsigport-1 > hunan-victim.http: Flags [S], seq 702332749, win 512, length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@hunan-victim:~#
```



如何制造攻击？

TCP空序列号：向服务器tcp 80端口使用空序列号进行TCP端口扫描

Attacker:

```
root@hunan-attacker:~# hping3 hunan-victim -p 80 -M 0 -c 10 --faster
HPING hunan-victim (eth0 192.168.1.8): NO FLAGS are set, 40 headers + 0 data bytes

--- hunan-victim hping statistic ---
10 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@hunan-attacker:~#
```

Victim:

```
[root@hunan-victim ~]# tcpdump -i ens33 host hunan-attacker and dst port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
17:16:52.967727 IP hunan-attacker.rmtserver > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.967845 IP hunan-attacker.composit-server > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.967869 IP hunan-attacker.cas > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.967873 IP hunan-attacker.attachmate-s2s > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.967876 IP hunan-attacker.dslremote-mgmt > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.967879 IP hunan-attacker.g-talk > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.968030 IP hunan-attacker.crmsbits > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.968151 IP hunan-attacker.rnrp > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.968164 IP hunan-attacker.kofax-svr > hunan-victim.http: Flags [none], win 512, length 0
17:16:52.968303 IP hunan-attacker.fjitsuappmgr > hunan-victim.http: Flags [none], win 512, length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
[root@hunan-victim ~]#
```



如何制造攻击？

ICMP泛洪攻击：常见的DDoS攻击方式

Attacker:

```
root@hunan-attacker:~# hping3 hunan-victim --icmp -c 10 --faster
HPING hunan-victim (eth0 192.168.1.8): icmp mode set, 28 headers + 0 data bytes

--- hunan-victim hping statistic ---
10 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@hunan-attacker:~#
```

Victim:

```
[root@hunan-victim ~]# tcpdump -i ens33 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
17:34:06.337673 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 0, length 8
17:34:06.337810 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 0, length 8
17:34:06.337949 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 256, length 8
17:34:06.337991 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 256, length 8
17:34:06.338070 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 512, length 8
17:34:06.338107 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 512, length 8
17:34:06.338177 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 768, length 8
17:34:06.338213 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 768, length 8
17:34:06.338394 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 1024, length 8
17:34:06.338435 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 1024, length 8
17:34:06.338793 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 1280, length 8
17:34:06.338837 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 1280, length 8
17:34:06.338960 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 1536, length 8
17:34:06.338998 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 1536, length 8
17:34:06.339088 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 1792, length 8
17:34:06.339124 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 1792, length 8
17:34:06.339488 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 2048, length 8
17:34:06.339532 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 2048, length 8
17:34:06.339611 IP hunan-attacker > hunan-victim: ICMP echo request, id 14344, seq 2304, length 8
17:34:06.339648 IP hunan-victim > hunan-attacker: ICMP echo reply, id 14344, seq 2304, length 8
^C
20 packets captured
20 packets received by filter
0 packets dropped by kernel
[root@hunan-victim ~]#
```



NETSCOUT 威胁情报团队

Arbor Security Engineering & Response Team (ASERT)



- 研究DDoS、僵尸网络和APT的安全专家
- 研究管道，逆向工程，蜜罐
- 为客户提供安全态势/战略情报
- 产生ATLAS Intelligence Feed (AIF)



ATLAS 情报

Arbor Edge Defense (AED) 的ATLAS情报更新



IP 地理定位



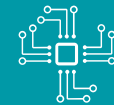
Crawler 爬虫



HTTP
Regex



IoCs
(3rd Party /
NETSCOUT)



Contextual
Intelligence
关联情报

One Threat Intelligence Feed. Multiple Components



AIF介绍

Reputation-Based Indicators of Compromise (IoCs) - Various types of threats that can be characterized by one or more communication endpoints including IP addresses, domains, and URLs. These types in this category include Adware, Backdoors, Banking, Credential Theft, Droppers, Exploit Kits, Fake AV, Point of Sale, Ransomware, Social, Spyware, Virtual Currencies, Webshells, worms, and others.

Campaigns and Targeted Attacks - This category includes various types of threats known to be associated with targeted attack activity. This category includes but not limited to elements such as Advanced Persistent Threats (e.g. APT DRPK, Operation Hangover, Fancy Bear), Hacktivism (e.g. Anonymous LOIC, JS-LOIC, SOIC tools), specific campaigns (e.g. Operation BlockBuster, Ghoul), RATs and Rootkits (e.g. Darkcomet, H-worm, njRAT, PPlugX, Betabot, Blackenergy, Spyeeye etc.)

Command & Control - Various types of cyber threats that generate outbound connectivity from internal compromised hosts to known Command and Control (C2) over HTTP (e.g. Emotet, LokiBot, Nymaim, TrickBot), IRC (e.g. DarkDOSer, pyLOIC), Peer-to-Peer (e.g. Hajime, Erzenel, Rex) and other protocols.

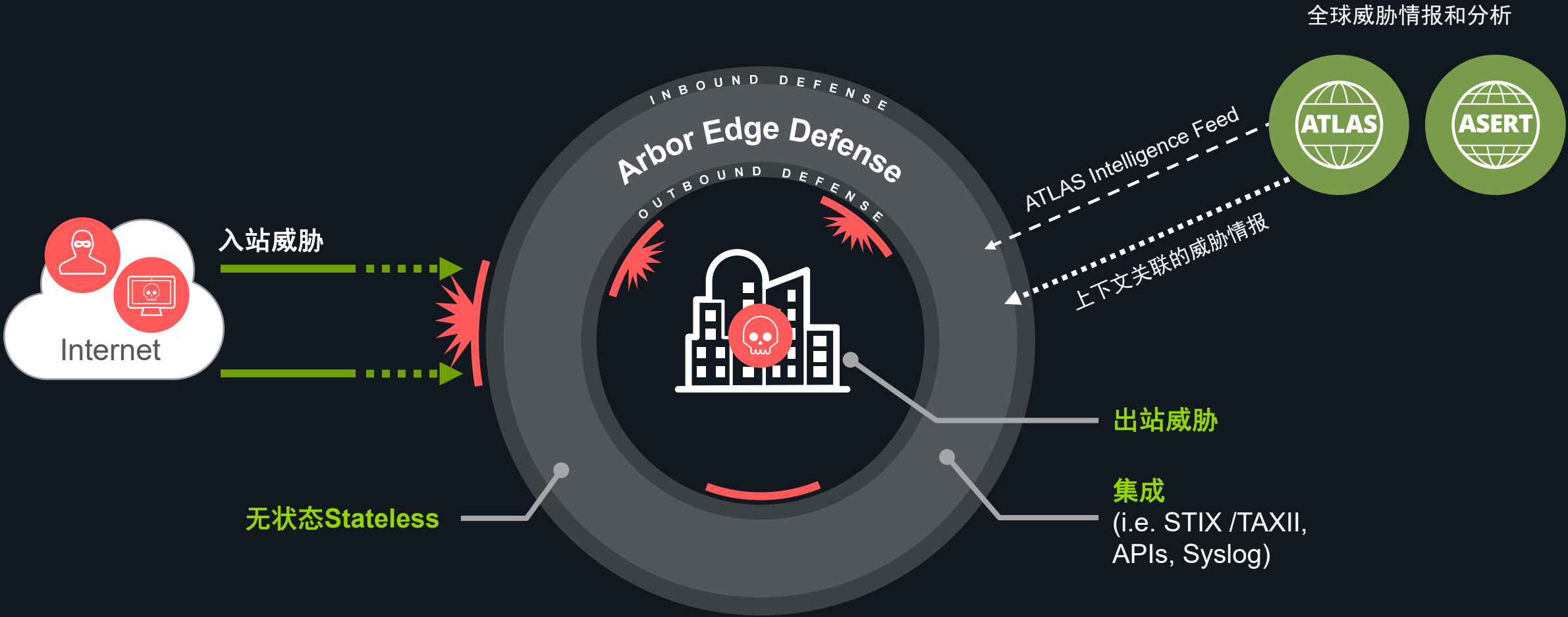
DDoS Attacks - Identify multiple types of DDoS attacks (i.e. Volumetric, TCP-state Exhaustion, Application-layer) that affect a variety of operating systems and infrastructure (e.g. Mirai, Emotet, Lizardstresser, XIR DOS, Armageddon, Athena, BroBot, DirtJumper, and many others)

Email and Mobile Malware - Various types of email threats (e.g. Phishing, SPAM) and mobile malware threats (e.g. malicious apps, spyware, CnC) that affect mobile devices such as Android and iPhone smartphones.



Arbor Edge Defense (AED)

智能、自动化的边界防御，第一道和最后一道安全防线



Arbor Edge Defense 使用场景

- 防御入站TCP状态耗尽DDoS攻击
 - 作为第一道安全防线
 - 保护状态型设备（如NGFW）
- 防御入站IoC
 - 作为第一道安全防线
 - 缓解状态型设备的负载（如NGFW）
- 阻止出站IoC
 - 作为最后一道安全防线
 - 阻止可能被安全堆栈错过的IoC，避免数据泄漏



选型

NETSCOUT AED Appliances

Features	2600	2800
Physical Dimensions	Chassis: 2U rack height; Height: 3.45 inches (8.67 cm); Width: 17.4 inches (43.53 cm); Depth: 20 inches (50.8 cm); Weight: 36.95 lbs. (17.76 kg)	
Power Options	DC: 2 x DC redundant, hot swap capable power supplies; DC Power Ratings: -40 to -72 Vdc, 28/14 A max (per DC input); AC: 2 x AC redundant, hot swap capable power supplies; AC Power Ratings: 100 to 240 VAC, 50 to 60 Hz, 12/6 A max; Watts: 315 typical, 375 max	
Hard Drives	2 x 240 GB SSD in RAID 1 Configuration	2 x 240 GB SSD in RAID 1 Configuration
Environmental	Operating: Temperature : 41°F to 104°F (5° to 40°C) Humidity: 5–85%; Non-Operating: Temperature -40° to 158°F (-40° to 70°C); Humidity 95%	
Memory	32 GB	64 GB
Processor	2 x Intel Xeon E5-2608L v3 (6 cores) 2 GHz; Watts: 315 typical, 375 max	Dual Intel Xeon (12-core) E5-2648L v3 -1.80GHz
Operating System	Our proprietary ArbOS® operating system	
Management Interfaces	2 x 10/100/1000 BaseT Copper; RJ-45 serial console port	2 x 10/100/1000 BaseT Copper; RJ-45 serial console port
Protection Interface	<ul style="list-style-type: none"> • 4, 8 or 12 1G bypass ports (copper, sx fiber, lx fiber) • 4 x 10 G bypass ports plus 0, 4 or 8, 1 G bypass ports 	<ul style="list-style-type: none"> • 4x10 GigE bypass ports (SR or LR mixed fiber) • 8x10 GigE bypass ports (SR or LR mixed fiber) • 8x10 GigE bypass ports (SR or LR mixed fiber) plus 4x1 GigE bypass ports (SR or LR fiber or copper)
Traffic Bypass Options	Integrated hardware bypass; Internal “software” bypass to pass traffic without inspection	
Latency	Less than 80 microseconds	
Availability	Inline bypass, dual power supplies, solid-state hard drive RAID cluster	
MTBF	44,000 hours	
Regulatory Compliance	FIPS 140-2 Level 1 UL60950-1/CSA 60950-1 (USA/Canada); EN60950-1 (Europe); IEC60950-1 (International), CB Certificate & Report including all international deviations; GS Certificate (Germany); EAC-R Approval (Russia); CE—Low Voltage Directive 73/23/EEE (Europe); BSMI CNS 13436 (Taiwan); KCC (South Korea); RoHS Directive 2002/95/EC (Europe)	

选型

DDoS & Advanced Cyber Threat Protection

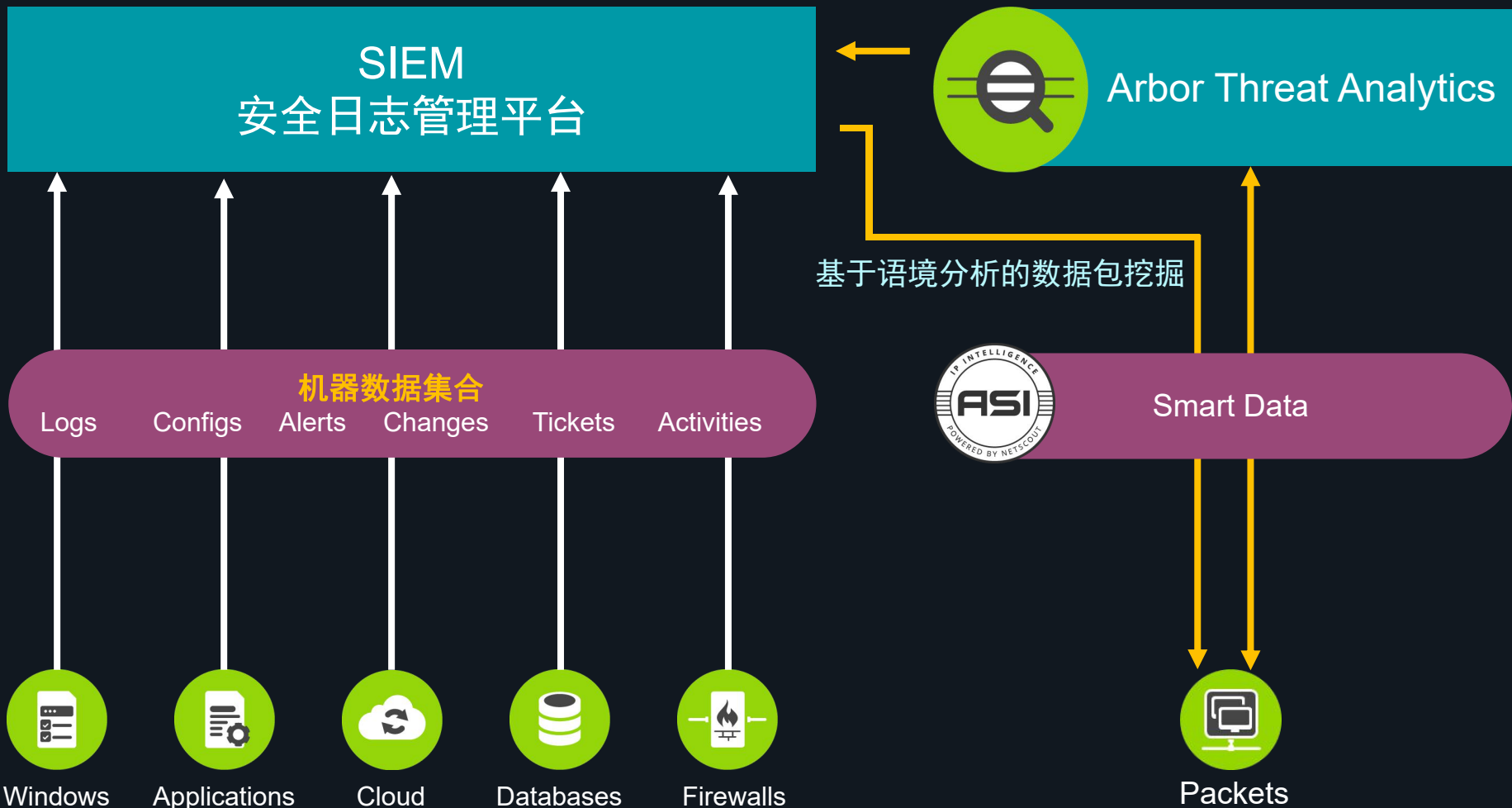
Features	2600	2800
Inspected Throughput	Licenses for 100 Mbps, 250 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps	Licenses for 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps; software upgradeable
Maximum DDoS Flood Prevention Rate	Up to 15 Mpps	Up to 28.80 Mpps
HTTP(s) Connections/SEC	368K at recommended protection level; 613K filter list only protection	1,351K at recommended protection level; 1,497K filter list only protection
Protected Endpoints	Unlimited	
Authentication	On device, RADIUS; TACACS	
Management	SNMP gets v1, v2c; SNMP traps v1, v2c, v3; CLI; Web UI; HTTPS; SSH customizable, role-based management; Up to 50 AED (appliances and/or virtual AED running KVM hypervisor) can be managed by the AED Console; managed AED must at least be running v5.11; vAED Console can run on VM hypervisor.	
Protection Groups	100	
Reporting and Forensics	Real-time and historical IPV4 and IPV6 traffic reporting, extensive drill-down by protection group and blocked host including total traffic, passed/blocked,top destination URLs/services/domains, attack types, blocked sources, top sources by IP location. Packet visibility in real-time.	

ATA



Arbor Threat Analytics(ATA)安全分析与追溯平台

基于NETSCOUT专利技术的全新安全分析与威胁追溯平台



01

检测



- 攻击识别
- 流量异常
- 应用风险

02

分析



- 安全分诊
- 安全溯源

03

回溯&调查



- 真实数据验证
- 审计与合规验证



ATA的典型功能

预警、事件调查、原始数据以及第三方集成

发现与预警

- 基于安全风险与威胁指标的攻击检测
- 签名与指标匹配
- ATLAS Intelligent Feed (AIF) 威胁情报库

语境调查

- 基于主机IP与时间语境的主机调查
- 基于服务器、应用、会话逐步深入的网络调查
- 原始数据包的回溯与审计
- 电子取证与证据保存

第三方安全平台集成

- SOC 集成
与第三方安全平台集成，实现安全告警与语境分析调查
- 集成ARIN，确定安全威胁的来源位置与机构



语境分析的事件调查

风险可视化 > 主机调查 > 会话分析 > 证据追溯

The screenshot displays the Arbor Threat Analytics interface, which is divided into several overlapping windows and panels. At the top, the 'Enterprise' view shows 'Security Risks' with 7373 risks, 'External DNS Servers' at 62.15%, 'Threat Indicators', 'Violations' at 3918, and 'mDNS' at 18.22%. Below this, the 'Host Investigation' window shows an aggregated view for IP 192.168.152.100. The 'Matrix View' window displays a 'Session Overview' table with columns for ME Name, App, and other session details. The 'Session Trace' window shows a detailed view of a packet, including its absolute time, delta time, length, source, and destination. The 'Session Summary' window provides a high-level overview of the session, including query type, class, name, and resolved IP. The 'Session Information' window shows a list of session details. The 'Risk Visualization' window shows a table of packets with columns for Packet, Absolute Time, Delta Time, Length, Source, Destination, Interpretation, and Status. The 'Self-Signer' window shows a graph of activity over time. The 'Evidence' window shows a detailed view of a packet, including its structure and raw data. The 'Evidence' window also shows a hex dump of the packet data.

Packet	Absolute Time	Delta Time	Length	Source	Destination	Interpretation	Status
3	4:10:25.938.023.480 PM PDT	0.000.065.980	74	sjcopendns1.netscout.com	resolver4.opendns.com	TCP: S=20445 D=53(DNS) LEN=0 SEQ=2677089890 ACK=2676359	
4	4:10:26.670.110.720 PM PDT	0.732.087.240	106	sjcopendns1.netscout.com	resolver4.opendns.com	DNS: C ID=11831 OP=QUERY PTR NAME=222.220.67.208 in-addr	
5	4:10:26.672.039.700 PM PDT	0.001.928.980	141	resolver4.opendns.com	sjcopendns1.netscout.com	DNS: R ID=11831 OP=QUERY Response PTR STAT=No Error NAME	
6	4:10:26.914.973.080 PM PDT	0.242.933.380	74	sjcopendns1.netscout.com	resolver4.opendns.com	TCP: S=20445 D=53(DNS) LEN=0 FIN SEQ=2677089890 ACK=2676	

```
PACKET: #3 2019/03/28 23:10:25.938.023.480(UTC); Length=74 bytes; Captured=74 bytes
ETHERNET: S=[00-08-E3-FF-FD-94], D=[18-E7-28-2E-4F-2F], EtherType=0x8100
802.1q: VLAN ID=111
IP: S=[10.1.6.11] D=[208.67.220.222] LEN=32, ID=46774, Offset=0, Proto=TCP;
TCP: S=20445 D=53(DNS) LEN=0 SEQ=2677089890 ACK=2676359277 WIN<<=29312
  Source port      = 20445
  Destination port = 53 (DNS)
  Sequence number  = 2677089890
  Next expected Seq number = 2677089890
  Acknowledgment number = 2676359277
  Data offset      = 32 bytes (4 bits)
  Reserved Bits:  = Reserved for Future Use (3 bits)
  ECN Nonce-Sum:  = 0 (1 bit)
  Flags            = 0x10
    0... .. = (Congestion Window Reduced (CWR) NOT set)
    0... .. = (ECN Echo NOT Set)
    0... .. = (No urgent pointer)
    0... .. = (No push)
    0... .. = (No reset)
    0... .. = (No SYN)
```



Arbor Threat Analytics

可检测的内部攻击种类

VOLUMETRIC流量攻击

- Total Traffic
- Chargen Amplification
- DNS Amplification
- ICMP
- IP Fragment
- IPv4 Protocol 0
- L2TP
- mDNS
- DNS
- MS SQL RS Amplification
- NetBIOS
- NTP Amplification
- RIPv1
- Rpcbind
- SNMP Amplification
- SSDP Amplification
- TCP ACK
- TCP RST
- TCP SYN / ACK Amplification
- UDP
- TCP



检测内部DDoS

STATE EXHAUSTION 状态耗尽攻击

- TCP SYN
- New Sessions
- Connect Time
- Total Active Sessions

APP LAYER 应用层攻击

- HTTP Flood
- DNS Flood



Arbor Threat Analytics

应用协议风险检测

证书Certificates

- 自签名, 不可信
- 超期证书

SSL / TLS

- 过时的版本
- 弱密文

DNS 安全

- 反向查寻
- 非企业DNS服务器



不安全的应用

- SMB v1
- Telnet / RDP
- SNMP v1 / v2

扫描事件

- 网络扫描(ARP / ICMP)
- 端口扫描

NTP

- 非企业的NTP服务器

不安全的文件传输协议

- CIFS / FTP



案例1 – 内部DNS Amplification

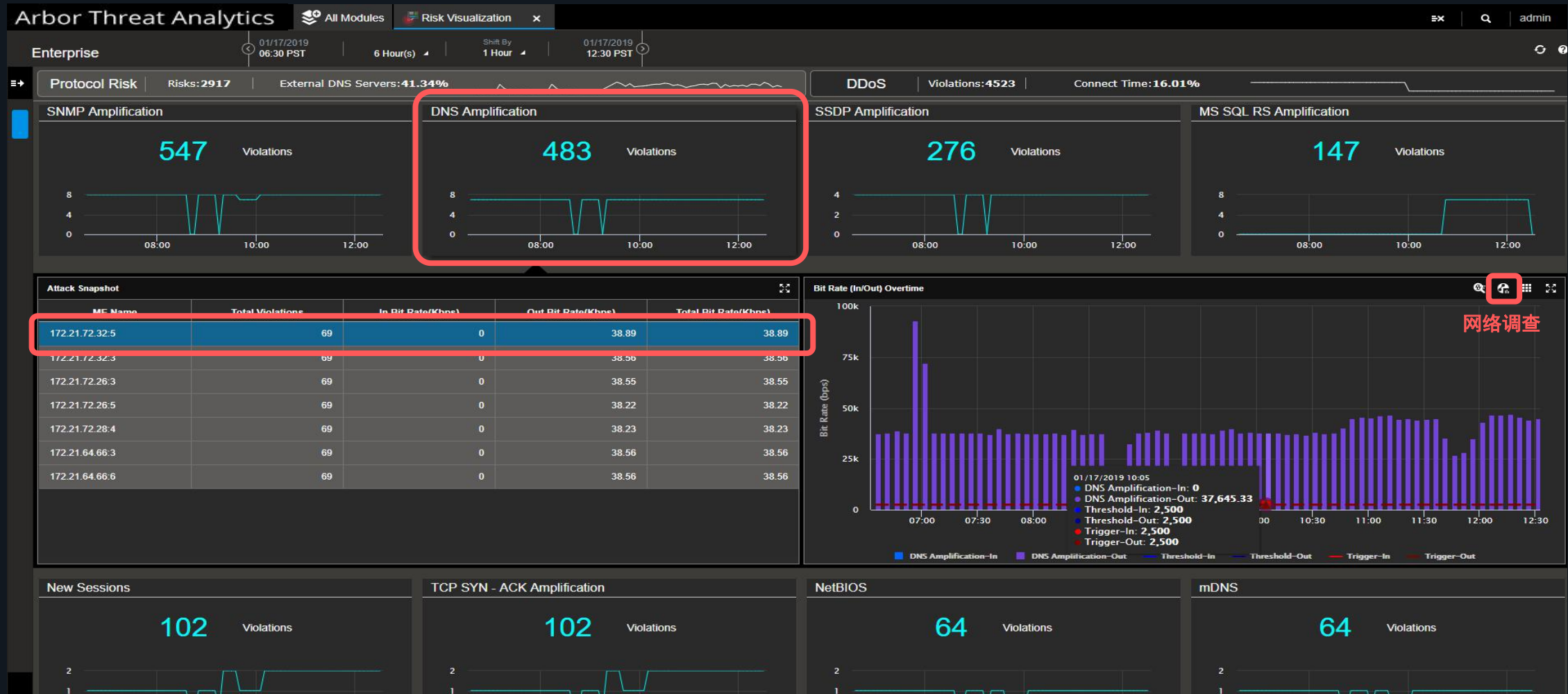
使用实例

- 问题：
 - 攻击者欺骗受害者的IP地址，发送大量DNS请求（例如:Type =任何已知区域的请求）到DNS解析器，这些解析器响应受害者计算机，在单个包中向受害者计算机发送大量DNS响应
- ATA应对：
 - ATA可以主动检测DNS放大攻击，并提供跟踪调查和攻击证据以确定攻击
 - 识别伪冒的客户端和源
 - 收集会话和包级别的证据，以了解攻击所使用的方法



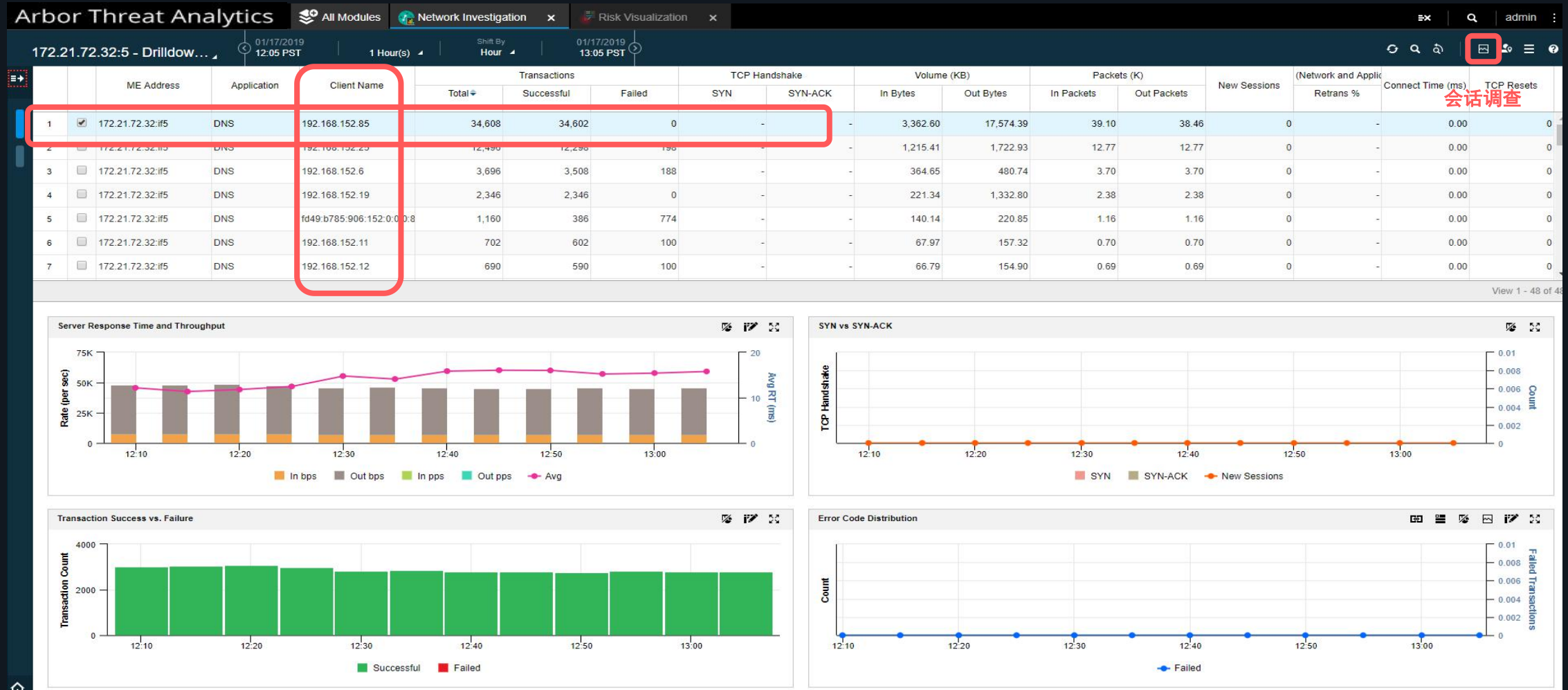
案例1 – 内部DNS Amplification

风险可视化



案例1 – 内部DNS Amplification

风险可视化 > 网络调查



案例1 – 内部DNS Amplification

风险可视化 > 网络调查 > 会话调查

Arbor Threat Analytics

172.21.72.32:5 - Drilldown... 01/18/2019 10:00 PST 01/18/2019 11:00 PST

Session Overview

	ME Address	Application	Server Name	Client Name	Identity	Avg RT (ms)	App Errors	Retries	Timeouts	Ageouts	Start time	Duration	Status
1	172.21.72.32:if5	DNS	192.168.152.100	192.168.152.85	NETTSCOUTT.COM	0.21	0	3	0	0	01/18/2019 10:00:00	00:00:00.000	✓
2	172.21.72.32:if5	DNS	192.168.152.100	192.168.152.85	NETTSCOUTT.COM	0.05	0	1	0	0	01/18/2019 10:00:00	00:00:00.000	✓
3	172.21.72.32:if5	DNS	192.168.152.100	192.168.152.85	NETTSCOUTT.COM	0.07	0	0	0	0	01/18/2019 10:00:00	00:00:00.000	✓
4	172.21.72.32:if5	DNS	192.168.152.100	192.168.152.85	NETTSCOUTT.COM	0.08	0	1	0	0	01/18/2019 10:00:00	00:00:00.000	✓
5	172.21.72.32:if5	DNS	192.168.152.100	192.168.152.85	NETTSCOUTT.COM	0.04	0	0	0	0	01/18/2019 10:00:00	00:00:00.000	✓
6	172.21.72.32:if5	DNS	192.168.152.100	192.168.152.85	NETTSCOUTT.COM	0.10	0	0	0	0	01/18/2019 10:00:00	00:00:00.000	✓

Session Trace

Description	Relative Time	192.168.152.85 Client 172.21.72.32:if5	192.168.152.100 Server 172.21.72.32:if5
DNS Query	00:00:00.000.000		
DNS Response	00:00:00.000.212		00:00:00.000.212

数据包证据

Session Summary

Session Information			Flow Information		
	Entity	Value		Interface	172.21.72.32:if5*
1	Query Type	*: A request for all records	1	TCP Flags	Not Available
2	Query Class	IN: Internet	2	Server to Client Bytes	457
3	Query Name	NETTSCOUTT.COM	3	Client to Server Packets	4
4	Resolved IP	0.0.0.0	4	Client to Server Bytes	344
5	Resolved Name		5	Retries	3
6	Entity		6	Client IP - Port	192.168.152.85:53



案例1 – 内部DNS Amplification

风险可视化 > 网络调查 > 会话调查 > 数据包证据

The screenshot shows the Arbor Threat Analytics interface with two windows open. The top window displays a list of packets for the IP 172.21.72.32:5. The bottom window shows a detailed view of a packet, highlighting the DNS query and response details.

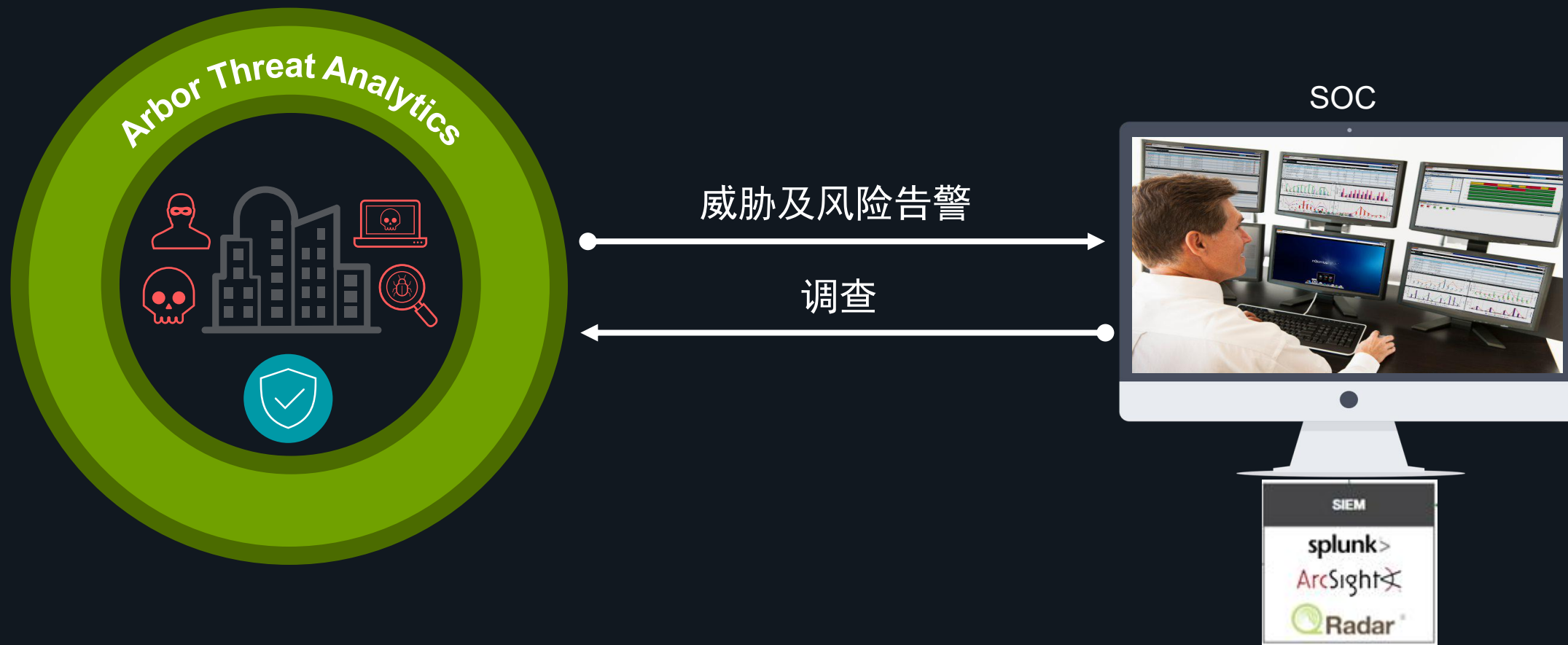
Packet	Absolute Time	Delta Time	Length	Source	Destination	Interpretation	Status
1	10:00:00.000.024.730 PST	0.000.000.000	86	192.168.152.85	nettscout.com	DNS: C ID=0 OP=QUERY ? NAME=nettscout.com	-
2	10:00:00.000.025.690 PST	0.000.000.960	86	192.168.152.85	nettscout.com	DNS: C ID=0 OP=QUERY ? NAME=nettscout.com	-
3	10:00:00.000.192.530 PST	0.000.166.840	86	192.168.152.85	nettscout.com	DNS: C ID=0 OP=QUERY ? NAME=nettscout.com	-
4	10:00:00.000.200.580 PST	0.000.008.050	86	192.168.152.85	nettscout.com	DNS: C ID=0 OP=QUERY ? NAME=nettscout.com	-
5	10:00:00.000.237.720 PST	0.000.037.140	457	nettscout.com	192.168.152.85	DNS: R ID=0 OP=QUERY Response ? STAT=No Error NAME=nettscout.com	-

Packet 1 Details:

- ETHERNET: S=[00-50-56-81-04-F2], D=[00-50-56-BF-78-32], EtherType=0x8100
- IP: S=[192.168.152.85] D=[192.168.152.100] LEN=40, ID=1, Offset=0, Proto=UDP;
- UDP: S=53(DNS) D=53(DNS) LEN=40
- DNS: C ID=0 OP=QUERY ? NAME=nettscout.com
 - ID = 0
 - Msg Type = 0(Query)
 - Flags = 0x0100
 - 0... = Query
 - 0.000 0... = Opcode: Query (0)
 - ...0... = Not truncated
 - ...1... = Recursion desired
 - ...0... = Z: Reserved
 - ...0... = Checking Enabled(Unicast packet)
 - Opcode = 0(Query)
 - Question count = 1
 - Answer count = 0
 - Authority count = 0
 - Additional record count = 0
 - Question Section:
 - Name = nettscout.com
 - Type : All records (*,255)



案例2 – 与SIEM集成



案例2 – 与SIEM集成

从SIEM中的事件启动 – 例如: Splunk

The screenshot shows the Splunk interface for a search. The search query is: `host="172.21.63.111" NetScoutServerIP="172.21.74.63" "cat=ssl/tls"`. The search results show 61 events. A red box highlights a specific event with a context menu open. The event details are:

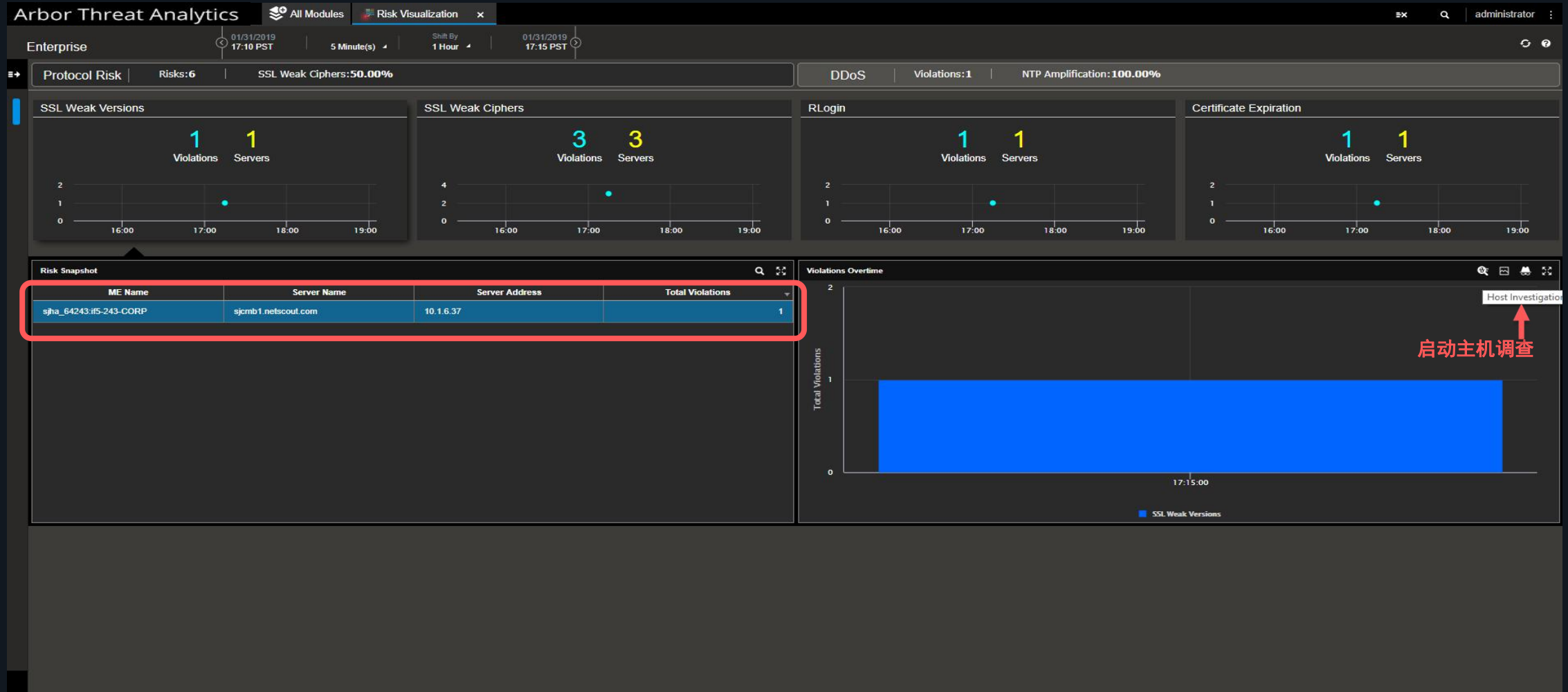
Time	Event
1/31/19 5:15:07.000 PM	Jan 31 17:15:07 172.21.74.63 CEF: 0 NetScout Systems NETSCOUT Cyber Investigator 6.1.1 CIPHERQUALITY Servers running weak ciphers 1 type=0 cat=SSL/TLS Security cnt=1 NetscoutNsaDeviceType=InfiniStream NetscoutNsaDeviceName=sjha_64243 NetscoutNsaDeviceIP=172.21.64.243 NetscoutNsaInterfaceNumber=5 dvchost=10.1.6.37 NetscoutNsaHostType=Server app=SSL start=1548983400000 end=1548983700000 NetscoutNsaUrl=https://172.21.74.63:8443/console/?modID=idRiskIdentification&modMsg=params&type=0&cat=CIPHERQUALITY&name=SSLVERSION&dvchost=10.1.6.37&NetScoutNsaDeviceIP=172.21.64.243&Ifn=5&app=SSL&start=1548983400000&end=1548983700000

The context menu options are: Copy (Ctrl+C), Go to <https://172.21.74.63:8443/console/?modID=...>, and Inspect (Ctrl+Shift+I). A red arrow points from the text "从Syslog事件中启动ATA" to the "Go to" option.



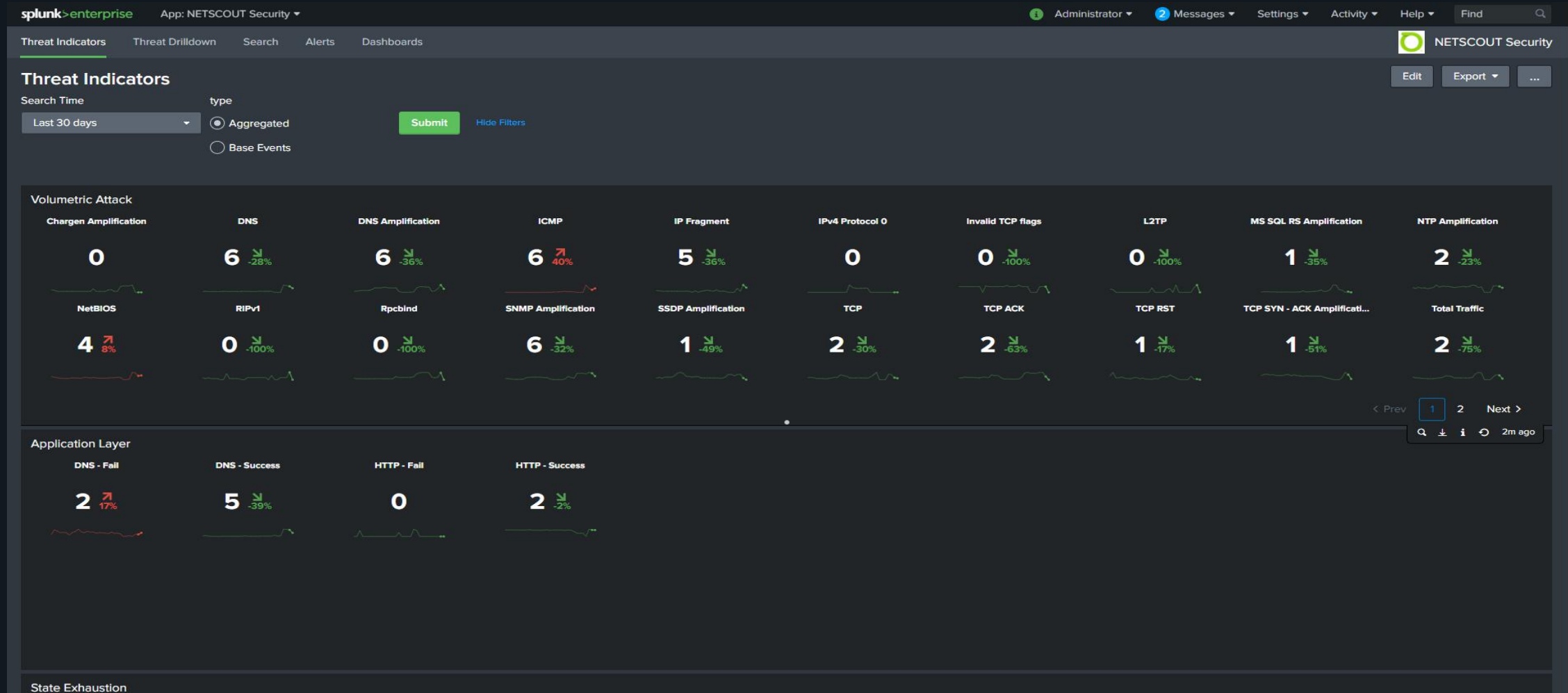
案例2 – 与SIEM集成

直接导航到ATA中语境相关的事件



案例2 – 与SIEM集成

NETSCOUT 安全威胁仪表盘



案例2 – 与SIEM集成

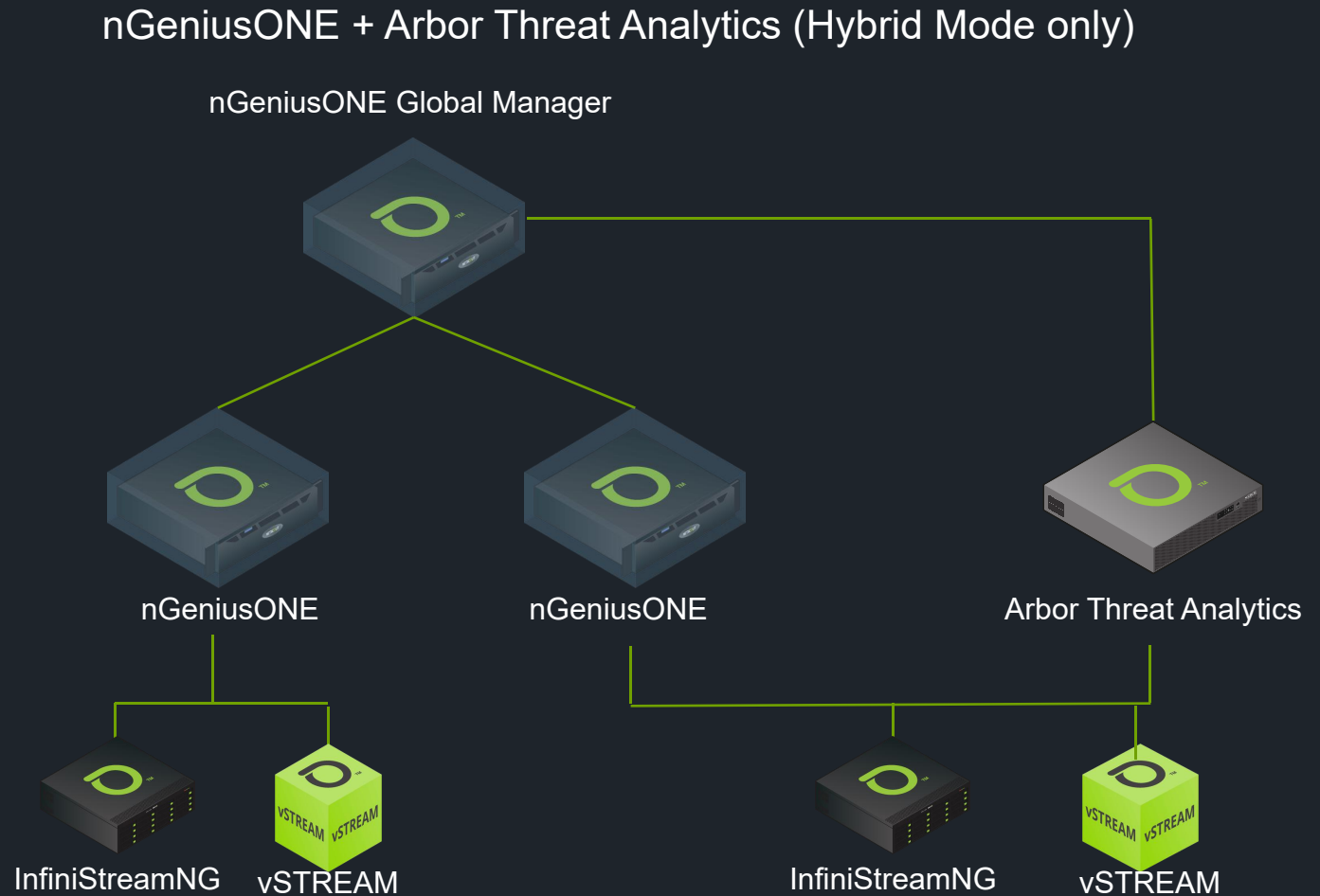
可视化ATA检测到的安全事件



ATA部署架构

混合模式：与nG1并存

- 单一平台实现服务保障和安全威胁分析
 - ✓ ATA软件和nG1软件分别部署在不同的服务器上
- 共用数据源
 - ✓ InfiniStreamNG/vSTREAM为ATA和nG1同时提供分析数据
- 集中管理
 - ✓ 通过nG1 Global Manager可以同时管理ATA和nG1



**THANK
YOU**

