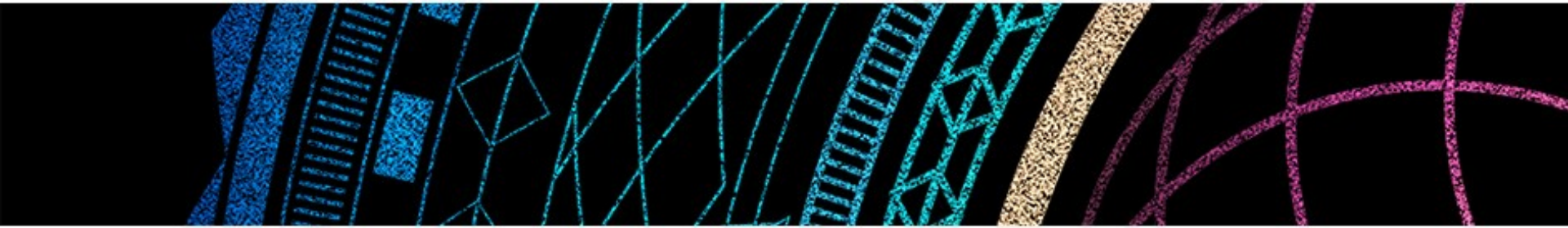
华为USG9580数据中心防火墙NSS测试

With Ixia PerfectStorm @NSS Lab



敏捷已来

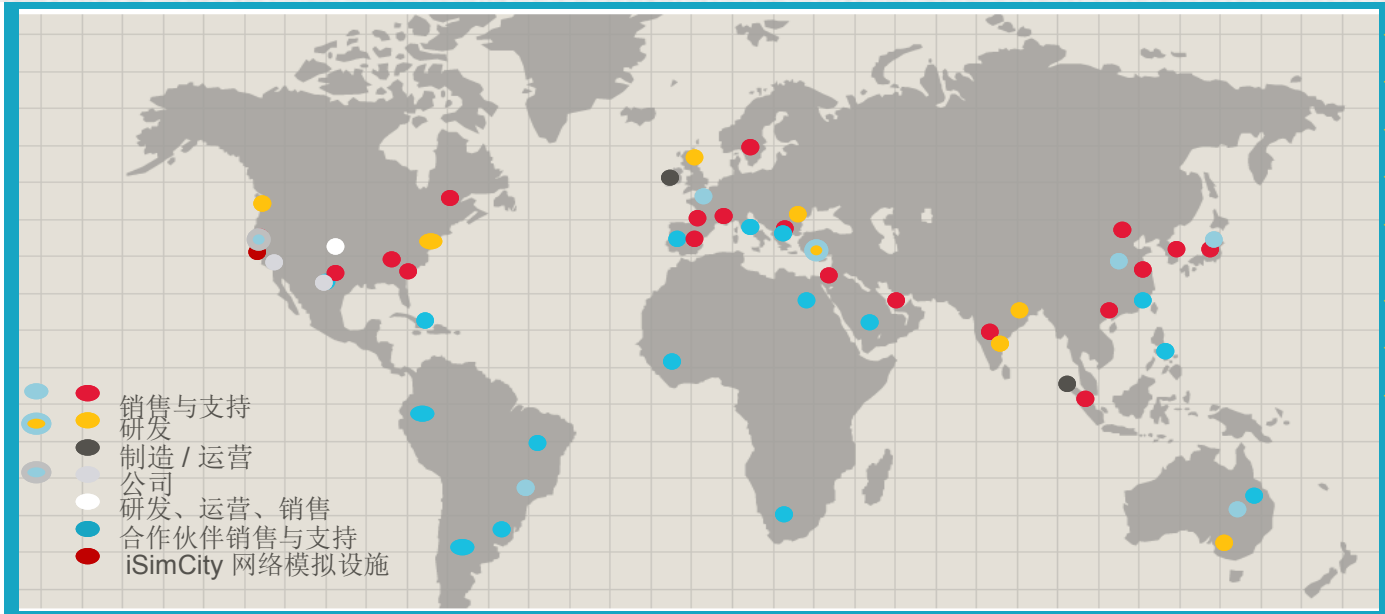
Weaving The Future

Envision A Better Connected World

ixia：一家全球性公司

解决方案和服务

- ✓ 设备、网络、应用和服务性能的端到端可视性
- ✓ 部署前和生产网络的安全



- ✓ 纳斯达克上市公司：XXIA
- ✓ 全球性公司
- ✓ **1,900 多名**员工
- ✓ **2,500 多个**忠诚的客户
- ✓ 2013 年《福布斯》“美国成长最快的高科技公司”年度排名位列14
- ✓ 2013 年 CRN 10 大最热门的技术公司
- ✓ 2013 年荣获网络创新奖
- ✓ 2013 年收购 Net Optics

ixia为网络、云、数据中心的运营和安全带来价值

HUAWEI


部署前


厂商选择


架构


部署


运营

测试与验证　　安全性与移动性评估　　网络可视性

我们帮助使其发挥作用

- 测试网络基础架构、性能和安全性
- 加速新服务和应用的推出
- 集成新设备

我们帮助打破它

- 评估网络处理业务和应用的能力
- 在不断变化的环境中验证安全性
- 验证**性能**边缘

我们帮助保持其运行

- 监测网络资源的使用情况、应用质量
- 了解流量性能和网络安全性

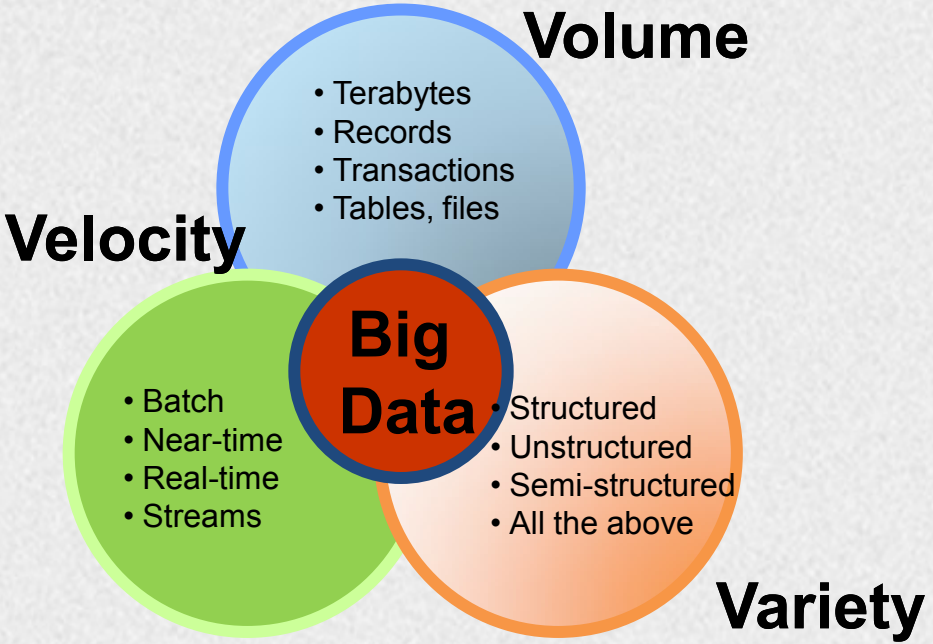
ixia

敏捷已来
Weaving The Future

USG9580测试情况介绍

敏捷已来
Weaving The Future

CATCH UP WITH BIG DATA ERA



USG9500 DC FW

- **Outstanding Performance**
- **All-in-one security (NAT, VPN, IPS , Virtualization, App QoS etc.)**
- **High Stability & Reliability**

HUAWEI DC FW CUSTOMER PROFILE

Cloud DC Supplier

Large Enterprise

ISP

MSSP

NSS Lab: Expert Testing & Certification

- Since 1991
- 全球最大的应用和安全第三方实验室，其测试结果和报告，广泛的被政府、银行、企业等机构采用
- 发布了FW，NGFW，IPS，IDS， UTM等系列设备的测试方法学
  https://www.nsslabs.com/
- NSS与BreakingPoint自2009年5月起，就建立了全面合作关系
- Offices in San Diego, CA & Austin, TX

NSS DC FW TEST METHODOLOGY V1.0

Security Effectiveness

Performance

Stability & Reliability

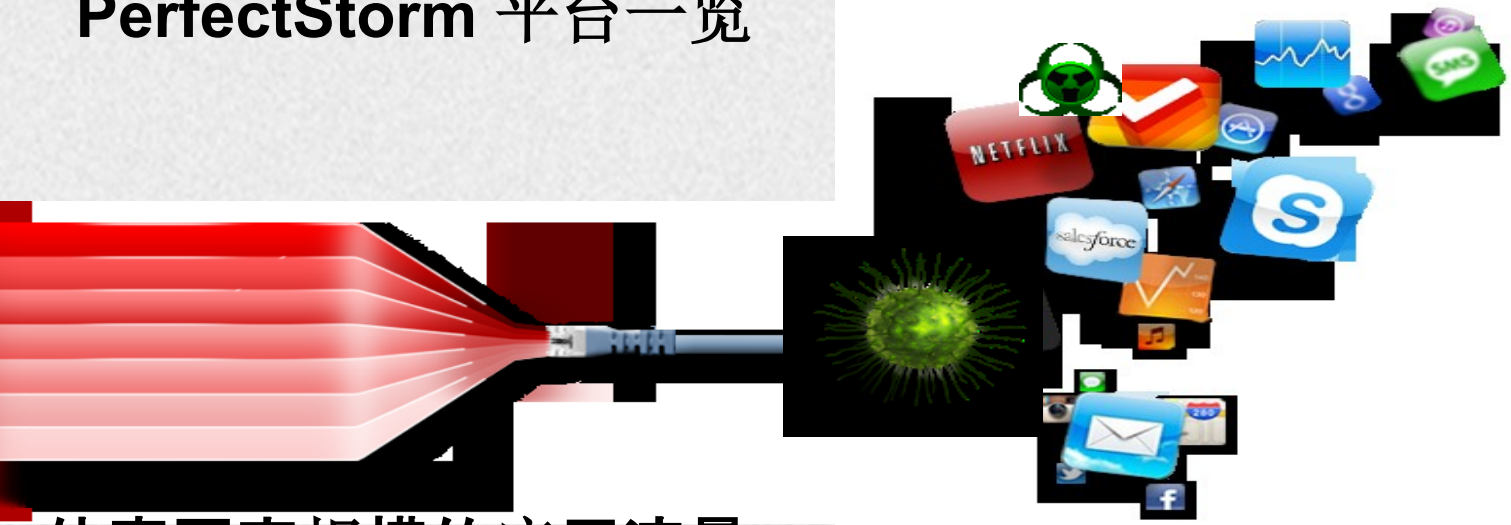
Management & Configuration

Total Cost of Ownership(TCO)

When considering firewalls for the data center rather than for the network perimeter, there are several key metrics. The main aspects evaluated are listed here but not all. A copy of the detailed test methodology is available on the NSS Labs website at www.nsslabs.com.

敏捷已来
Weaving The Future

PerfectStorm 平台一览



仿真国家规模的应用流量

- 960Gbps application throughput
- 720M concurrent HTTP sessions
- 24M new connections per second
- 1.1M concurrent SIP calls
- 480Gbps video throughput
- 12M concurrent SSL session
- 480Gbps IPsec throughput
- 480Gbps GTP throughput

- Highest density L4-7 testing solution – 11u @ nearly 1 Terabit
- Highest density L4-7 blade – 80Gbps
- 1st L4-7 testing solution with 40Gbps networking support
- 1st security testing solution with 40Gbps networking support
- 1st comprehensive data, voice, video, storage, mobile, and security testing solution

仿真国家规模的应用流量

HUAWEI

PerfectStorm

42u Rack

960Gbps application throughput

42u Rack

720M concurrent application sessions

42u Rack

Pop: 733M

24M new sessions per second

42u Rack

Pop: 23M

150, CA, US

ixia

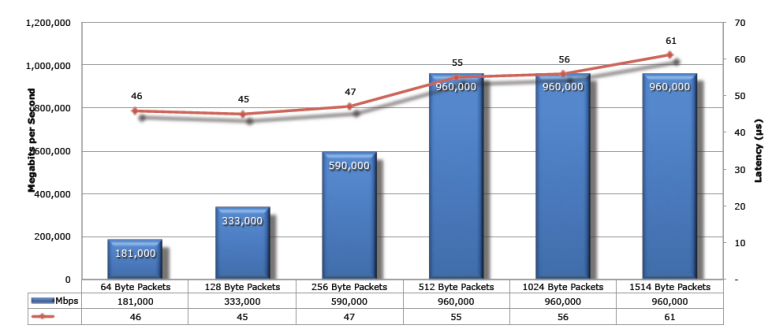
敏捷已来

Weaving The Future

PerfectStorm –单一的集成方案应对数据中心测试的挑战

PERFORMANCE TEST RESULT

MAX. UDP THROUGHPUT[1]



MAX. CONCURRENT CONNECTIONS

USG9580 730 M[2]

[1] *Huawei USG9580 demonstrates line rate throughput with 96 10GE ports during UDP testing at packet size 512, 1024 and 1514 bytes.*

[2] *The limit of 730 million is the limit of the test gear,*

REAL-WORLD TRAFFIC MIXES

USG9580 About 390 Gbps[3]

[3] Different protocol mixes were utilized based on the intended location to reflect the real use cases. The real world traffic that was used targeted Financial, Virtualized infrastructure, Mobile Applications, Web Apps and ISP.
Due to specifications of the NSS methodology, TCP tests are run in only a single direction, which will limit the throughput of the device to 10Gbps per port pair. As part of this testing, the Huawei USG9500 was configured with 48 port pairs, limiting the maximum potential throughput to 480Gbps.

敏捷已来
Weaving The Future

NSS 定义的真实世界流量场景

HUAWEI

4.7 "Real-World" Traffic

Where previous tests provide a pure HTTP environment with varying connection rates and average packet sizes, the goal of this test is to simulate a "real-world" environment by introducing additional protocols and real content while still maintaining a precisely repeatable and consistent background traffic load.

The result is a background traffic load that is closer to what may be found on a heavily-utilized "normal" production network.

4.7.1 "Real-World" Protocol Mix (Enterprise Perimeter)

Traffic is generated across the DUT comprising a protocol mix typically seen in an enterprise perimeter.

4.7.2 "Real-World" Protocol Mix (Financial)

Traffic is generated across the DUT comprising a protocol mix typical of that seen in a large financial institution.

4.7.3 "Real-World" Protocol Mix (Education)

Traffic is generated across the DUT comprising a protocol mix typical of that seen in a large educational environment.

4.7.4 "Real-World" Protocol Mix (Datacenter)

Traffic is generated across the DUT comprising a protocol mix typical of that seen in a large datacenter.

4.7.5 "Real-World" Protocol Mix (US Mobile Carrier)

Traffic is generated across the DUT comprising a protocol mix typical of that seen in a large US mobile carrier.

4.7.6 "Real-World" Protocol Mix (European Mobile Carrier)

Traffic is generated across the DUT comprising a protocol mix typical of that seen in a European mobile carrier.

如何仿真真实世界流量？

HUAWEI

仿真和测试平台

ATI智能库

每2周一次的应用和安全库更新

Real Attacks

- 6,000+ live security attacks
- 35,000+ pieces of live malware
- 180+ evasions
- DDoS and botnet simulation
- Custom attacks
- Research and frequent updates

Real-World Applications

- 250+ application protocols
- Social, peer-to-peer, voice, video
- Web, enterprise applications, gaming
- Mobile
- Storage workloads
- Custom applications
- Frequent updates

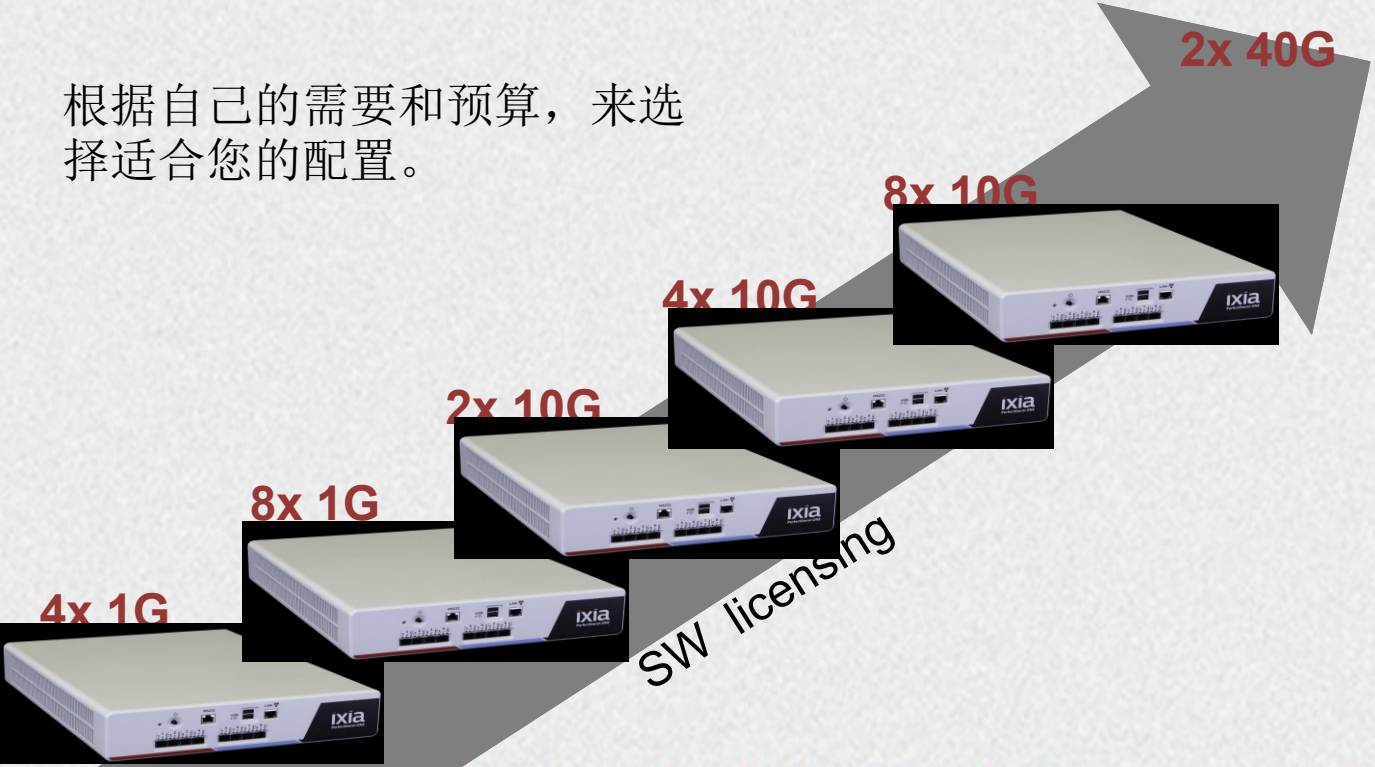
Unprecedented Performance

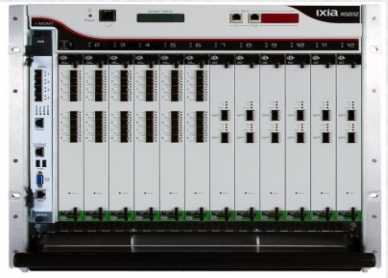
- 960 Gbps blended application traffic
- 720M concurrent HTTP sessions
- 24M HTTP sessions/second
- 12M CC SSL sessions/second

可扩展的真实世界流量仿真测试

HUAWEI

根据自己的需要和预算，来选择适合您的配置。





PerfectStorm
960 Gbps

2-ports of 40GE

8-ports of 10GE

ixia

敏捷已来
Weaving The Future

OTHER TEST RESULTS

Security Effectiveness **100% PASS**

- *Baseline Policies* ✔
- *Baseline Policies* ✔
- *Complex Policies* ✔
- *Static NAT* ✔
- *Dynamic/Hide NAT* ✔
- *SYN Flood Protection* ✔
- *Address Spoofing Protection* ✔

Stability & Reliability **100% PASS**

- *Blocking Under Extended Attack* ✔
- *Passing Legitimate Traffic Under Extended Attack* ✔
- *Protocol Fuzzing & Mutation* ✔
- *Power Fail* ✔
- *Redundancy* ✔
- *Persistence of Data* ✔

Management & Configuration

PASS

Total Cost of Ownership

3 years TCO $ 688,208

TCO per protected Mbps $1.74

测试为企业网络提升价值

敏捷已来
Weaving The Future

网络投入和风险

我们面临网络攻击的风险？ 等等，我们早知道这个了。
然而下面这些需要我们关注：

网络安全使得投入了大量资于：

- 性能
- 规模扩展
- 安全防范能力
- 弹性

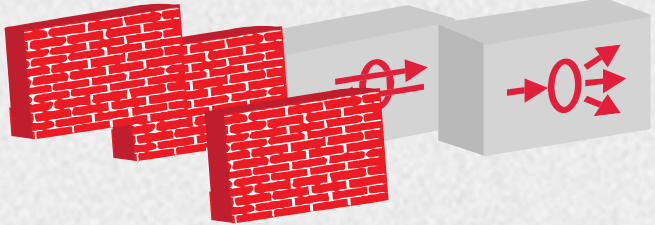
然而我们的信心度仍然不够

- 盲目的相信
- 基于假设/最佳估计
- 未经探索验证
- 对于网络的知识有限
- 其它潜在问题

网络安全投入的
被动反应或冲动决策

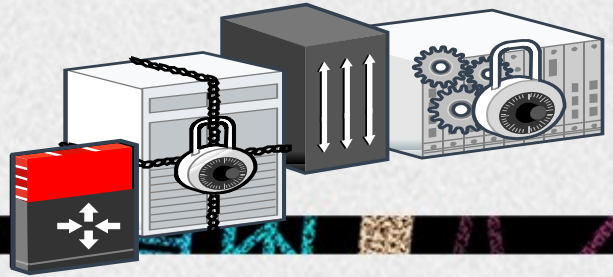
盲目投资?

组织-B



组织-A

未经完善的供应商产品评估
对于安全状态没有办法知晓
没有对于网络的可视性
随性的变化管理
缺乏网络安全的最佳实践



组织-C

网络基础架构安全性的评估，审计和验证

通过对于真实环境中的应用和攻击行为进行模拟和仿真，来建立恰当的网络基础架构安全性评估体系

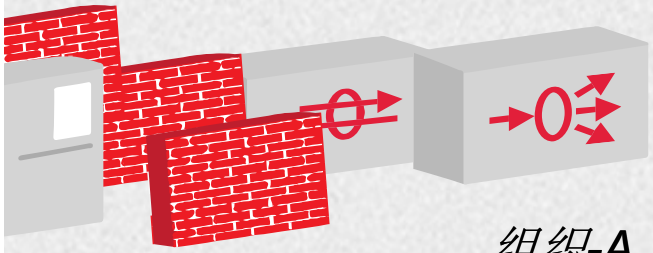
网络的安全性评价指标值，是网络的一系列基于最佳实践的测试方法论基础上的评估值进行风险加权后的函数结果。

$$\acute{R} = \sum(f\{\text{Assessment Score} * \text{Risk weight}\})$$

网络安全评价指标

4.0

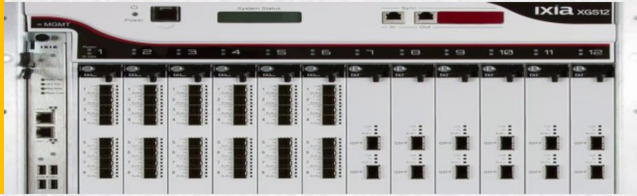
网络安全的弱点取决于全部环节中最弱的一环



组织-A

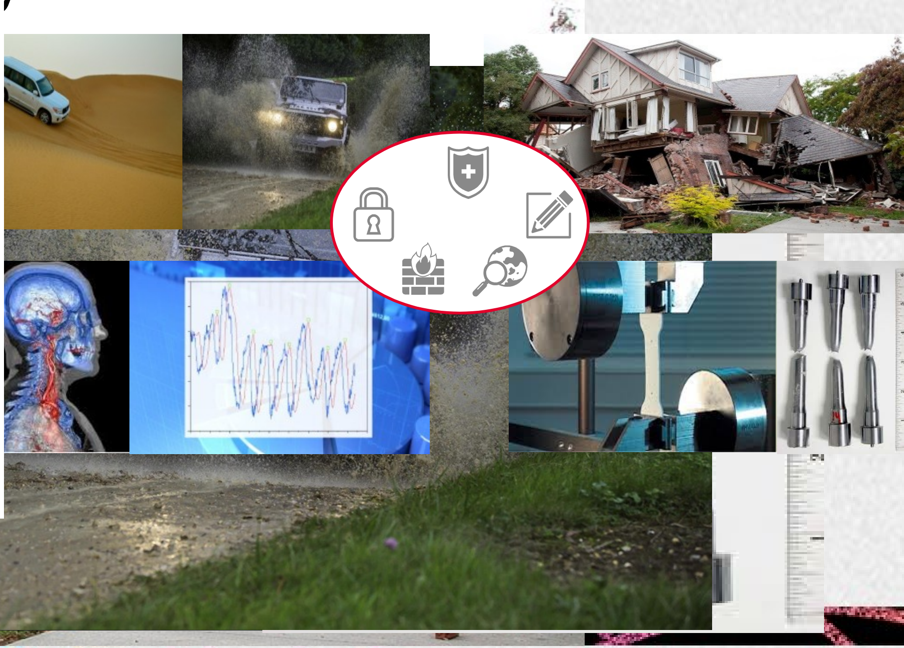
评估领域	分值	风险加权系数
防火墙功能	9	10
应用及网络功能	7	4
事件反应能力	4	8
DDOS防范能力	8	9

Ixia公司是做什么的？



我们希望房产商有办法对所建房屋模拟测试其面对自然灾害的极

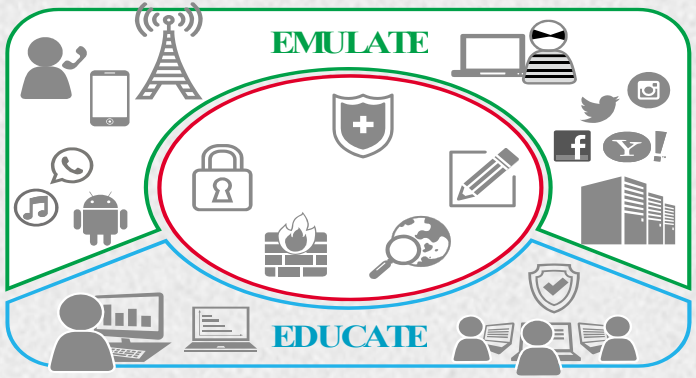
- ✓ Ixia提供工具和服务，来帮助实施上述所有的测试...对你的网络
  - *通过把你的网络放入模拟真实的应用和真实的攻击流量，来“试驾”网络*
  - *通过仿真网络可能出现的灾难性大型安全攻击来帮助了解你的网络的安全性*
  - *评估和诊断当前网络存在的问题，从而帮助决定如何对于网络进行调较。*
  - *找出您的网络可以“拉伸”的程度以及“断点”极限*



网络评估怎么可能提升网络安全？

医生诊断能治愈疾病吗?

- ✓ 网络评估是最佳实践的一部分
  - *真实的* 安全态势
  - *实际的* 性能
- 恰当的 *供应商* 筛选
- *可量化的* 网络安全指标
- 您的决策能够 *有据可依*
- *人员* 培训



HUAWEI

谢谢！

www.ixiacom.com

ixia

敏捷已来

Weaving The Future