End to End Protection
Implementing Best Practice Concepts

Sutjipto Budiman & Jeremy Andreas
27 April 2016
Hackers Lurked in Bangladesh Central Bank’s Servers for Weeks

Cybercriminals used malware, hacking tools and keylogger software to breach system, FireEye report says.
FireEye Company melakukan studi terhadap pertahanan cyber crime tertinggi pada enam bulan terakhir 2015 lalu.

Penelitian tersebut melibatkan mitra FireEye di dunia, termasuk Asia Tenggara dan Asia Pasifik. Hasil mengejutkan justru datang dari Indonesia.

Survei menunjukkan, 36 persen perusahaan di Indonesia menjadi target serangan kejahatan siber. Angka tersebut melebihi rata-rata global yang hanya 15 persen.

Dari data secara keseluruhan, perusahaan di Asia Pasifik mendapat serangan kejahatan siber sebanyak 27 persen, sementara Amerika Serikat 15 persen, dan Eropa 11 persen.

Kemudian berdasarkan hasil observasi FireEye, wilayah Asia Pasifik mendapat serangan terbanyak di sektor industri. Serangan advance persistent threat (APT) tersebut merupakan tindakan kejahatan tertinggi kelas dunia.

Dari hasil investigasi, pelaku penyerangan terbagi dalam empat kelompok. Tiga kelompok disinyalir berasal dari Cina, sementara satu kelompok dari Eropa.
The Attack Surface Has Increased Dramatically

Today’s Security is Borderless

- Network
- Applications
- Data
- People
Too Many **Security Vendors** Across the Enterprise

**Complexity is the Enemy of Security**
Too Many **Point Solutions**

### Networking
- Routing
- Switching
- Wi-Fi Controller

### Basic Security
- Firewall
- VPN

### Advanced Security
- IPS/ App Control
- Web Filtering
- Antivirus
- Advanced Threat Protection
- Cloud Application Control
End to End Segmentation Critical
Fortinet - Cooperative Security Fabric

Secures the Entire Attack Surface

- Client Security
- Secure Access
- Network Security
- Application Security
- Cloud Security

Eco System:
- Scalable
- Awareness
- Security

Actionable Threat Intelligence
Key Fabric Attributes

Eco Systems Alliance Partners

Scalability

Security

Awareness

Actionable
Scalable from IoT to Cloud

- Single Pane of Glass (Management)
- Single Source of Security Updates
- Single Network Operating System

<table>
<thead>
<tr>
<th>Device</th>
<th>Access</th>
<th>Network</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>WLAN</td>
<td>Enterprise Edge</td>
<td>Hybrid Cloud</td>
</tr>
<tr>
<td>BYOD</td>
<td>LAN</td>
<td>AppSec</td>
<td>Public Cloud</td>
</tr>
<tr>
<td>Endpoint</td>
<td></td>
<td>Segmentation</td>
<td></td>
</tr>
</tbody>
</table>

- WLAN
- LAN
- WAN
- Data Center & SDN
- ATP
- On Demand
- UTM
- NGFW
- ISFW
- FW
- DFW
- CDFW
- CFW
Security for the Cloud

**Virtualization**
Hypervisor Port

**Private Cloud**
SDN - Orchestration Integration

**Cloud**
On-Demand (Pay-as-you-Go)

- Connector
- API
- Flow

- Hypervisor
- East-West
- North-South

- Cloud Connector API
- East-West
- North-South

- NGFW
- WAF
- Management
- Reporting
- APT
Security for the Network

Slow is Broken

CPU Only

Parallel Path Processing (PPP)

- Policy Management
- Packet Processing
- Deep Inspection

- Packet Processing
- Policy Management
- Content Inspection

More Performance
Less Latency
Less Power
Less Space
Security for Access

WLAN

1. Infrastructure
   - On Premise Management

2. Integrated
   - On Premise Management

3. Cloud
   - Cloud Management

LAN

- Switch
- Network Security Platform
Key Fabric Attributes

Eco Systems Alliance Partners

Scalability  Security  Awareness  Actionable
Global and Local Security

Threat Intelligence Exchange
Threat Researchers

App Control
Antivirus
Anti-spam
Vulnerability Management
Web Filtering
Cloud Sandbox

IPS
Web App
Database
Botnet
Deep App Control
Mobile Security

Advanced Threat Protection

Endpoint Security
Network Security Platform
Email Security
Web & XML Application Firewall

Partner
## NSS Labs Certification

### NSS Labs Rating

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Center IPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGFW</td>
<td>Neutral</td>
<td>Recommended</td>
<td>Recommended</td>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>Recommended</td>
<td>Neutral</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGIPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Next Generation Firewall (NGFW) Security Value Map™

- **Products Tested:**
  - Juniper
  - Cisco ASA
  - Palo Alto Networks
  - Check Point
  - Forcepoint
  - Barracuda
  - Cisco FirePOWER
  - Dell SonicWALL
  - Huawei
  - Hillstone
  - Fortinet

- **Security Effectiveness:**
  - Average

- **TCO per Protected Mbps:**
  - Average

- **Product Categories:**
  - BREACH DETECTION
  - DATA CENTER IPS
  - FIREWALL
  - NGFW
  - IPS
  - WAF
  - NGIPS
  - ENDPOINT PROTECTION

- **Costs:**
  - $100
  - $80
  - $60
  - $40
  - $20
  - $0
Key Fabric Attributes

Eco Systems Alliance Partners

Scalability | Security | Awareness | Actionable

CPU | Shield | OS | Diagrams
A Learning Mode

Complexity is the Enemy

**User Identification**
Who is connected?

**Device Identification**
What devices do we have?

**Physical Topology**
How are they connected?

**Network & Application Topology**
What Policies do we need?

MONITOR AND LEARN
Fabric Awareness Critical

Topography and Data Flow

- IoT
- Access Point
- Seg FW (FGT 100D)
- Seg FW (FGT 100D)
- Seg FW (FGT 100D)
- Seg FW (FGT 1500D)
- Edge Firewall
- FGT 3700D
- IaaS Firewall
- FGT VM
- FGT API
- 192.1.2.08
- Port 442
- Cloud App 1
- Domain

Cooperative Security Fabric

- Network Security
- Client Security
- Secure Access
- Application Security
- Cloud Security
Key Fabric Attributes

Eco Systems Alliance Partners

- Scalability
- Security
- Awareness
- Actionable
## Actionable Threat Intelligence

<table>
<thead>
<tr>
<th>Incident Response Services</th>
<th>Single Pane of Glass</th>
<th>Migration to Cloud Based Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Technical Support" /></td>
<td><img src="image" alt="Centralized Device Management" /></td>
<td><img src="image" alt="Cloud-based Wireless and Security Management" /></td>
</tr>
<tr>
<td>Cloud Based Management of NGFW + Access Point</td>
<td>Cloud Based Management of NGFW + Access Point</td>
<td>Cloud Based Management of NGFW + Access Point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Threat Protection</td>
</tr>
</tbody>
</table>

### Diagram

- **IoT**
- **Mobile**
- **Access**
- **WAN**
- **Data Center**

- **PoS**
- **Windows**
Multiple Levels of Fabric API’s for Partner Integration

Eco System Alliance Partners

Cooperative Security Fabric
## Eco System Integration Points

<table>
<thead>
<tr>
<th>Cloud</th>
<th>SDN</th>
<th>Sandbox</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Cloud</td>
<td>VMware NSX</td>
<td>openstack</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>big switch networks</td>
<td>Bit9+ CARBON BLACK</td>
</tr>
<tr>
<td>amazon web services</td>
<td>Microsoft Hyper-V</td>
<td>Huawei acquaintedness</td>
</tr>
<tr>
<td>HP Cloud Services</td>
<td>PLUMgrid</td>
<td>Citrix</td>
</tr>
<tr>
<td>NTT</td>
<td>PLURIBUS NETWORKS</td>
<td>nuagenetworks</td>
</tr>
<tr>
<td>KVM</td>
<td>Citrix</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test/SSO</th>
<th>System Integrator</th>
<th>SIEM</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>ixia</td>
<td>Hewlett Pack Enterprise</td>
<td>splunk</td>
<td>REDSEAL</td>
</tr>
<tr>
<td>Centrify</td>
<td>IBM</td>
<td>ArcSight</td>
<td>RedSeal</td>
</tr>
<tr>
<td>Capgemini</td>
<td></td>
<td>LogRhythm</td>
<td>Tufin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Practical Solutions That Solve Customer Problems

<table>
<thead>
<tr>
<th></th>
<th>Enterprise Firewall</th>
<th>ATP Framework</th>
<th>Data Center Security</th>
<th>Cloud Security</th>
<th>Secure Access Architecture</th>
<th>Connected UTM (SMB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Extensive Range of NetSec Hardware, Virtual and Cloud options</td>
<td>Advanced Threat Protection – Sandbox</td>
<td>North - South (High Speed Appliance) + East West (Virtual &amp; SDN)</td>
<td>Public Cloud Security (AWS, Azure ...)</td>
<td>WLAN Access</td>
<td>All In One Security</td>
</tr>
<tr>
<td></td>
<td>Different personalities for each Deployment mode</td>
<td>Network+Email+Web +Client Security</td>
<td>Application Security</td>
<td>Hybrid Cloud</td>
<td>LAN Access</td>
<td>Cloud Management</td>
</tr>
</tbody>
</table>

Management, Analytics & APIs (Appliance, Virtual machine & Cloud)
ENTERPRISE FIREWALL

- ASIC
- Real time Security Services
- Centralized Device Management
- Identity Based Access Solution
- Centralized Logging and Reporting
- Network Security Platform

SDN

Identity Based Access Solution

Centralized Device Management

Network Security Platform

5.4

Specialize Network CPU

Real time Security Services

Single Network Operating System

Single Network Security OS

Cloud

CFW

Single Policy

Network Security Platform

Rugged

Virtual

Cloud

5.4

Real time Security Services

Single Network Operating System

Centralized Device Management

Identity Based Access Solution

Network Security Platform

Single Network Security OS

Cloud

CFW

Single Policy
DATA CENTER SECURITY

Processor Security
Real time Security Services
Single Network Operating System

Physical
Virtual

Centralized Logging and Reporting
Centralized Device Management

Dynamic Software-Defined Networking
Network Security Platform (VMX)

Physical
Virtual

Network Security Platform

SDX
Physical/Virtual/SDN

North
East
West
South

Splunk

VMware
Citrix
KVM
FortiAnalyzer
FortiManager
FortiSandbox
FortiGate
VMX

FortiGate
Virtual Cloud
Virtual Cloud

CLOUD SECURITY
Real Time Security Services
Software Security

Centralized Logging and Reporting
Cloud Virtual
Centralized Device Management

Advances Threat Protection
Network Security Platform (VMX)

Microsoft Azure
HP Cloud Services

IBM Cloud
Amazon Web Services
OpenStack

On Demand Security