bittnet

cisco Gold Partner

Cisco Customer Satisfaction Excellence Gold Star Achivement

Fireproofing your network
Do your own security check !

Cisco Connect – 2016, October 19th

Cristian Ionescu, CTO, CCIE #20005

Cosmin Voicu, Senior Solution Engineer, CCIE #37076

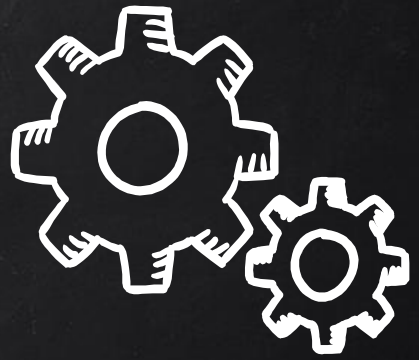
About us

bittnet

About us

IT Trainings

Market leader
Over 14.000 students taught



Top Integrator

Over 1000 IT Integration projects implemented in 9 years

Historical Highlights

bittnet

Deloitte. Technology Fast50 CE 2015 Rank 41

Ernst & Young Entrepreneur Of The Year®

2007 Best NetAcad EMEA

2007 BITTNET

2007 Cisco Premier

2011 LP of the Year

2014 Cisco Silver

2014 Decade of Training Excellence

2015 1st IT / BVB

2016 Cisco Gold

Future is Bright

Besides Cisco

www.bittnet.ro/certifications


bittnet

Range of services

bittnet

IT Training

- Cisco
- Microsoft
- AWS, ITIL
- Linux, Oracle, Citrix, IBM
- VMWare / 1500 other topics

IT Solutions

- Network Infrastructure & Security
- Servers, Datacenter & Virtualization
- Mobility & Unified Communications
- Hosted & Cloud Software

IT Services

- Consultancy & Design
- Implementation & Optimization
- Maintenance & Support
- Troubleshooting

Today’s story

bittnet

The Story for today

Is your network protected?

Is all your traffic legit?

Challenges comes from every direction

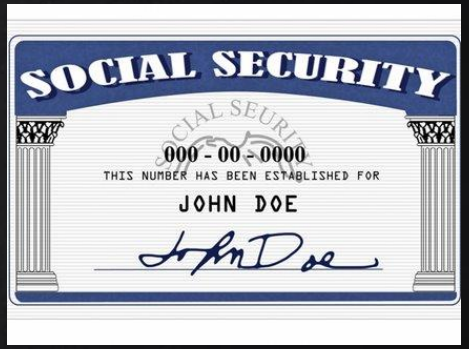
bittnet

Your Assets

$1 / acc
w 15 friends

$2500
development

aaS
$7/hour



$1 / SSN

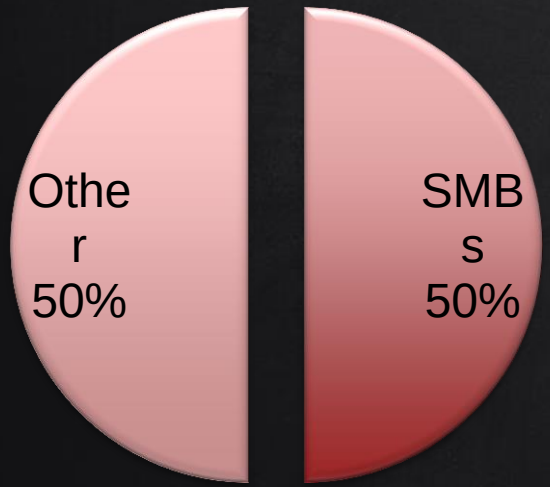
1,000,000,000,00 0

Market for cyber criminals

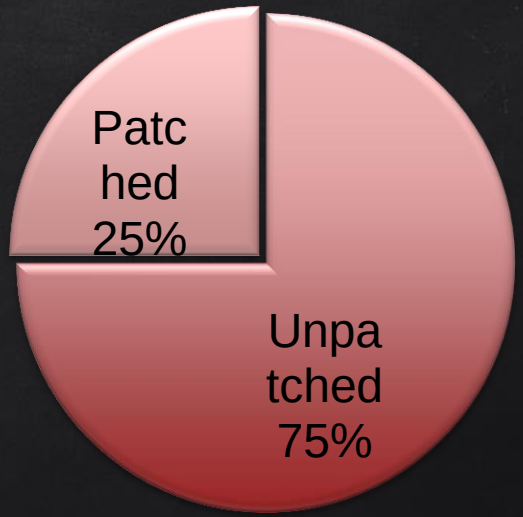
bittnet

The threat: record of mega breaches in 2015

Targeted Attacks



Website Vulerabilities



125% increase in attacks

bittnet

The threat: record of mega breaches in 2015

67% OF Victims were notified by an external entity

Source: M-Trends 2015

bittnet

So, how do organizations address this?

We are all saying it will not happen to me, until **IT DOES**

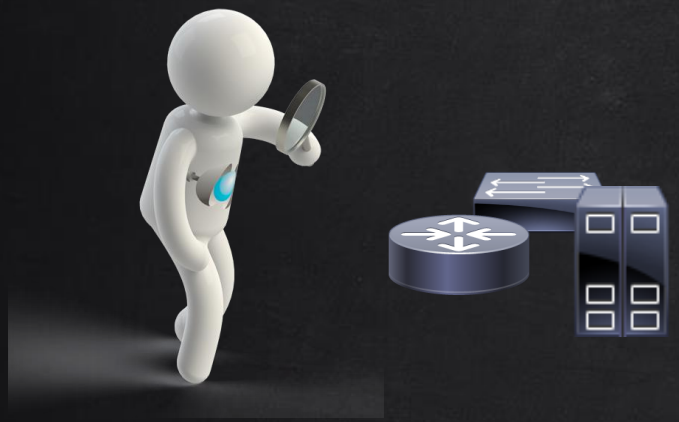
Case study

bittnet

Customer call

- ✓ Got oversize bill from voice provider
- ✓ Worried that somebody is stealing information

Bittnet Approach



- Assess the existing infrastructure
- Analyze the traffic flows

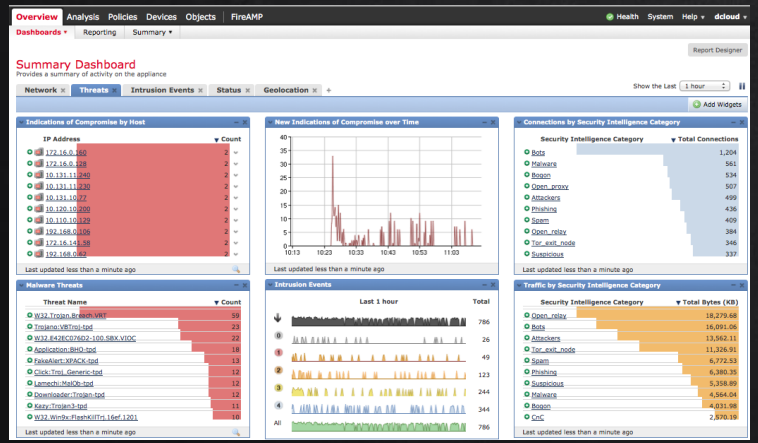
- Select the appropriate tool, best suited to customer’s network
- Prepare the network for the integration of FMC

bittnet

The Tools

Cisco ASA5512-X with FirePOWER

- ✓ SFR version 6.0.1
- ✓ Control, Protect, URL Filtering & AMP licenses



Firepower Management Center

- ✓ FMC version 6.0.1

Plugging In

- Non-invasive integration without any change to the logical or physical topology
- Mirror port carrying Internet traffic before NAT in both directions
- ASA must be in Transparent mode

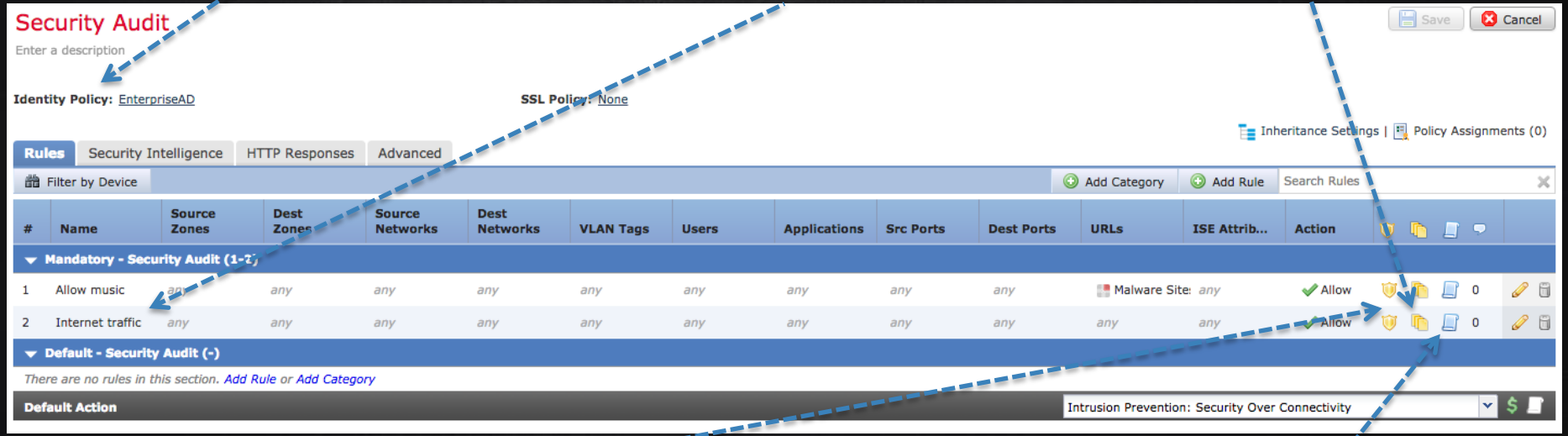
```
interface GigabitEthernet0/0
  description *** To Switch SPAN Port ***
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

Configuring the FMC

Identify users with AD integration and user agent

Rule referring URL category/reputation in order to get URL statistics

File policy to scan for malware



Intrusion policy to inspect traffic. Security over Connectivity to get more events

Log at the end of connection for complete session data

bittnet

First findings

- Four hosts are infected with malware and connected to Command & Control Centers (marked with IoC)

- Two of them have soft phones installed

- Correlate with Call Manager logs

- Identified host making rogue calls

Remediation

- ✘ Configure the customer's network to use OpenDNS
- ✘ Configure access code for international calls
- ✘ Implement time-based policy for international calls
- ✘ Clean infected hosts with AMP for Endpoints

OpenDNS

Other key points

- ✘ YouTube and Torrents taking up a large portion of bandwidth
- ✘ Hosts visiting malicious URLs

- Some employees are using anonymizing services (e.g. Hola, Squid), possibly to evade IT policies
- DoS attacks on Internet exposed web servers

Recommendations

✘ A redesign to better segment the network and protect the valuable resources

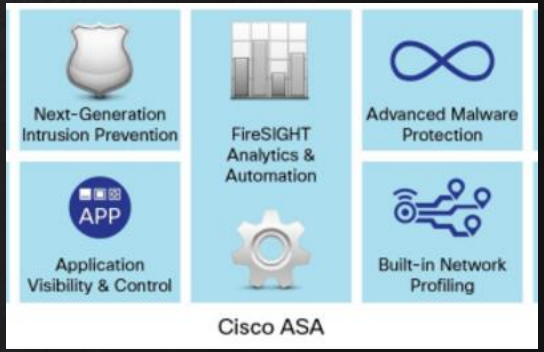
- ✘ Migrate to Cisco ASA with FirePOWER services for the following benefits:
- ✘ SSL remote access VPN with AnyConnect
- ✘ Migrate to AMP for Endpoints, a more efficient tool than the traditional

{

- Real-time protection against ever evolving malware
- Highly effective threat prevention with industry leading IPS
- Take control over the network with unprecedented visibility into applications, hosts and users provided by Firepower Management Center

Run your own check-up

- ASA with FirePOWER and TAMC license bundle (demo licenses available)
- Firepower Management Center VM or appliance



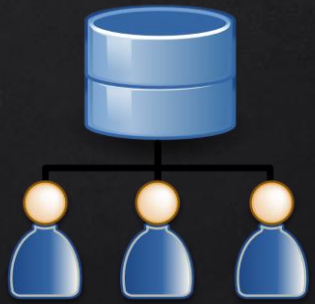
- Go to Reporting tab in FMC
  - Choose an existing template
  - Customize your own template
  - Generate the report

bittnet

Drawbacks

Proxy servers

No AD, no ID



SSL Encryption

Getting attacked

~~**If**~~

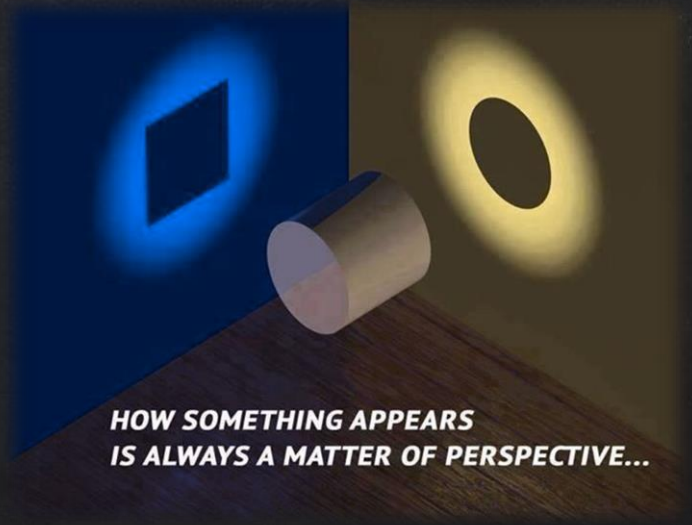
When

Are you ready to make a stand?

Check your network with

bittnet

bittnet



Bittnet Systems SA
Bucharest, Romania | 7-11 Iuliu Maniu , 6th District
Cluj-Napoca, Romania | Impact Hub, Building A, 21 Garii Str.,
E-mail: askformore@bittnet.ro | Web: www.bittnet.ro