

“And we are here as on a darkling  
Swept with confused alarms of str  
and flight,  
Where ignorant armies clash by n

-- Matthew Arnold, “Dover Beach”

# *As on a Darkling plain:* **Network Survival in an Age of Pervasive DDoS**

Steinthor Bjarnason - Arbor Networks

NANOG 71

October 3<sup>rd</sup> 2017

# Agenda

Thunderclouds appear on the horizon:

- The whole-sale weaponization of vulnerable IoT devices in 2016

The Necromancer:

- Transforming the innocent IoT population into zombies

Rallying the defenders:

- Implementing a multi-layered defense

# The Promises of IoT

## The Promise of IoT

- More personalized, automated services
- Better understanding of customer needs
- Optimized availability and use of resources

## Resulting in:

- Lower Costs
- Improved Health
- Service / efficiency gains
- Lower environmental impact



# The IoT Problem – Security

To fulfill these premises, IoT devices are usually:

- Easy to Deploy
- Easy to Use
- Require Minimal Configuration
- Low Cost

However...



**01/** Hard-coded usernames and passwords.



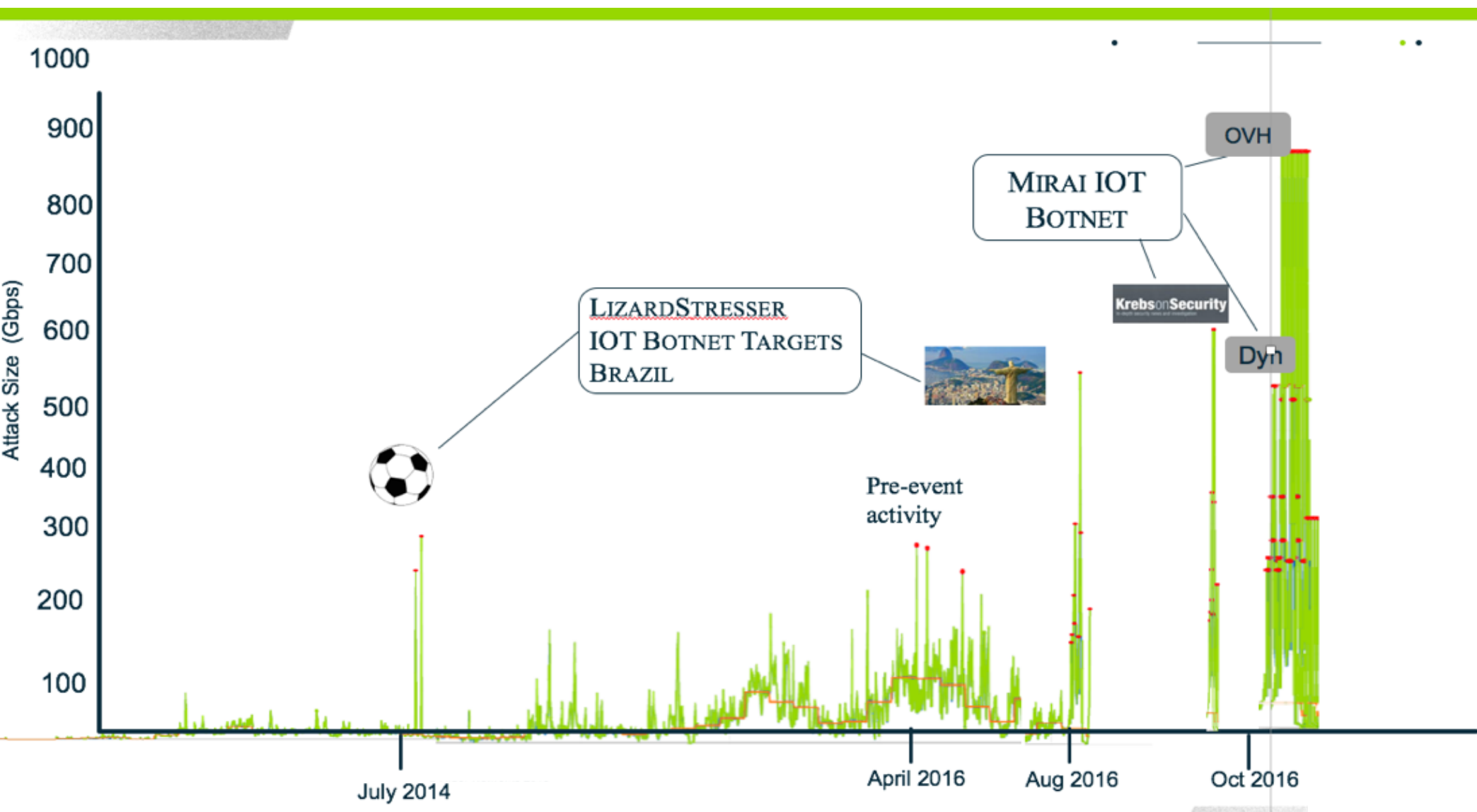
**02/** Unnecessary services enabled by default (Chargen, SSDP, DNS forwarder, et al).



**03/** Unprotected management services (Web, SNMP, TR-069, et al).



# The results: Unprecedented DDoS attack sizes



**with devastating Real-World consequences**



# The most popular IoT bot of 2016-17: The Mirai IoT bot

Created to take advantage of insecure IoT devices, source code released August 2016

1. Scans for devices on TCP ports 23,2323,23231,37777 and 7547 (+5555) (TR-069/TR-064 SOAP interface) using random IP's.
2. If a device responds, an attempt will be done to logon using a set of common username/password combinations
3. If successful, the IP address of the vulnerable device is sent to the C&C server
4. The C&C server will log onto the device, download the appropriate malware and compromise the device. The device will now start scanning, go to #1

Vulnerable devices come primarily from 3 manufactures in China, one of them released a patch in 2014 but only for the English version of their SW.

# Mirai IoT attack capabilities

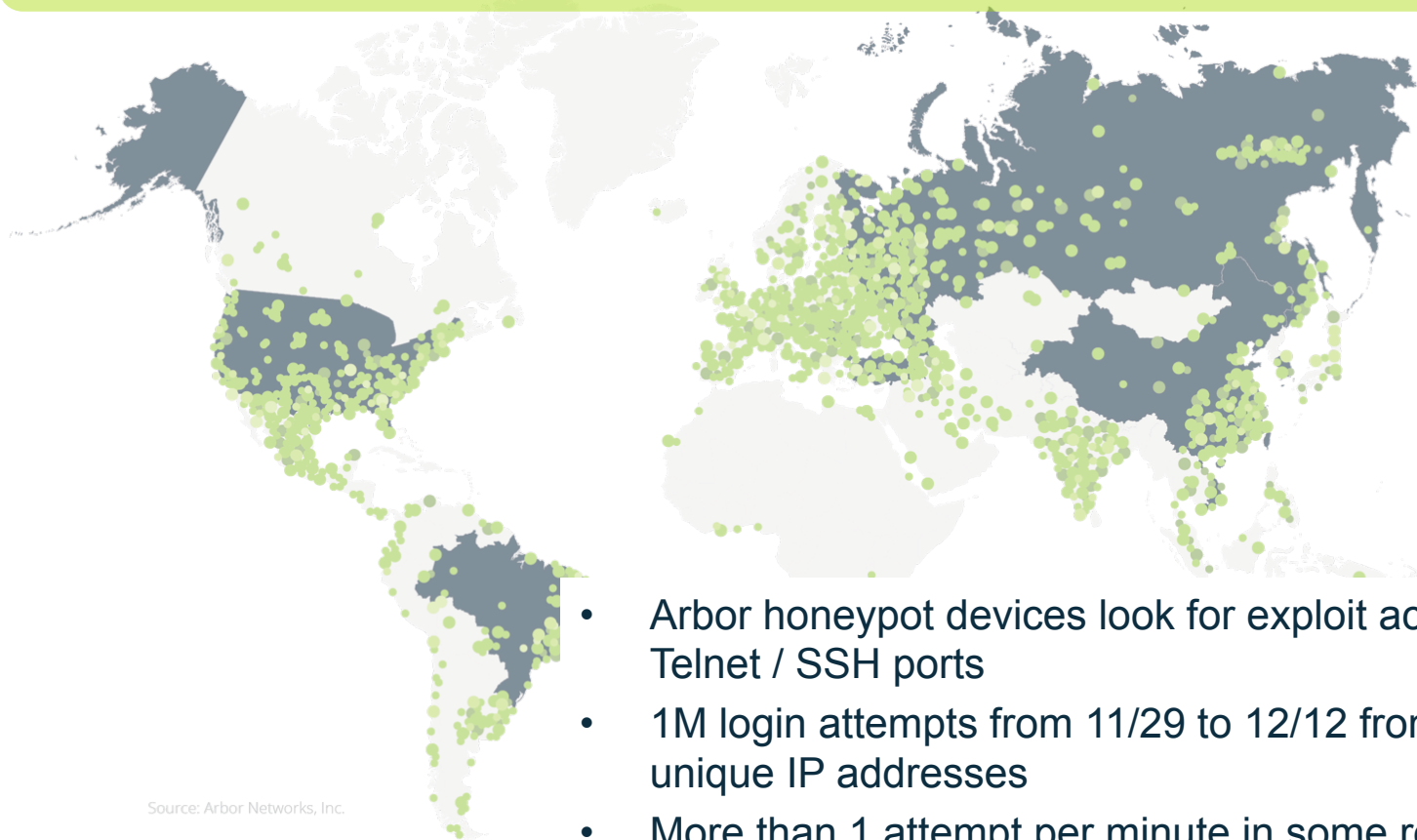
Attack types:

- UDP flooding
- Valve source engine flooding
- TCP ACK flooding
- TCP “Stomp” attack (ACK flooding on an established TCP connection, designed to bypass DDoS mitigation devices)
- TCP SYN flooding
- GRE Packet flooding
- HTTP request flooding (GET, POST, HEAD)
- DNS pseudo random label-prepend ( “DNS Water Torture” )

The initial version was unable to launch spoofed attacks, this changed in December 2016

# Worldwide Mirai infections in December 2016

Mirai is designed to infect and control IoT devices and contains the code necessary to manage and build large-scale botnets



Source: Arbor Networks, Inc.

- Arbor honeypot devices look for exploit activity on Telnet / SSH ports
- 1M login attempts from 11/29 to 12/12 from 92K unique IP addresses
- More than 1 attempt per minute in some regions

# The Situation Today...

Unprotected IoT devices on the Internet (est. 5%) will get infected within 1 minute.



IoT devices located behind NAT devices or Firewalls (est. 95%) are not accessible from the Internet and are therefore (mostly) secure.



But in January 2017, this all changed...



<http://marketingland.com/wp-content/ml-loads/2014/09/iceberg-ss-1920>



The background of the slide features a dark blue, textured globe. Overlaid on the globe is a complex, white, wireframe-like network of interconnected lines and nodes, resembling a digital or IoT network. The text is prominently displayed in the upper left quadrant of the image.

# **WINDOWS-BASED MIRAI IoT INFECTION: CROSSING THE MULTI-PLATFORM GAP**

# The Windows Mirai seeder: Crossing the gap from Windows to IoT

In February 2017 a new Windows seeder was detected in the wild which had the capability to infect IoT devices.

This is the **first** known multi-platform seeder to target IoT devices for infection.

Stuxnet was used to control directly connected devices, this seeder actually infects other devices.

Seems to be reusing trojan code which was discovered back in March 2016

Appears to be Chinese in origin, not nation-state related



Saalet Seed Master push seeder




# Subverting “innocent” IoT devices into zombies

After infecting Windows computers using remote brute-force attacks (MySQL, MSSQL, RDP, WMI), it proceeds to scan for and infect IoT devices with Mirai binaries using the Mirai scanning and spreading techniques earlier.

After infection, the IoT devices will connect back to the C&C server and will proceed to scan for and infect other IoT devices.

It is built in a modular fashion and has the capabilities to scan for, infect and control IoT devices of different architectures, all in a fully automated fashion.



The background of the slide features a dark blue, textured globe. Overlaid on the globe is a complex, white, wireframe-like network of interconnected lines and nodes, resembling a digital or cybernetic structure. The text is prominently displayed in the center-left of the image.

# **RANSOMWARE + DDOS:**

## **BLURRING THE LINES BETWEEN DIFFERENT SEGMENTS OF ATTACKERS**

# Ransomware + DDoS!

In mid-2016, a variant of Cerber ransomware was discovered which had vestigial DDoS capabilities added by the malware author – could only DDoS the local network segment.


Historically, attackers focused on ransomware and other malware variants haven't really focused on DDoS.

Historically, attackers focused on DDoS haven't focused on ransomware and other forms of malware.

The fact that DDoS capabilities were added to a ransomware variant indicates that attackers targeting hosts within enterprise networks are now interested in launching DDoS attacks *from within* those enterprise networks – at targets *on the same networks*!







# **IMPLICATIONS & CONSEQUENCES: INFECTING THE REMAINING 95% OF THE IOT POPULATION**

# mplications & Potential Consequences

## The Zombie horde

A single infected Windows computer has now the capability to infect and subvert the “innocent” IoT population behind Enterprise firewalls into zombies.

## The attackers weapon arsenal

The attacker can then use the zombies to:

1. Infect other IoT devices.
2. Launch outbound attacks against external targets.
3. Perform reconnaissance on internal networks, followed by targeted attacks against internal targets.



Game of Thrones 2011



# Example of how to isolate IoT devices – my home network! 😊

In 2011, I connected 3 IP Web Cams to my home network. These devices communicate with a Synology NAS which provides video portal and stores all video recordings.



The network is segmented into 2 areas:

- User VLAN
- Video subnet where an (old) Cisco ASA 5505 controls all communication between the Webcams and the the NAS.

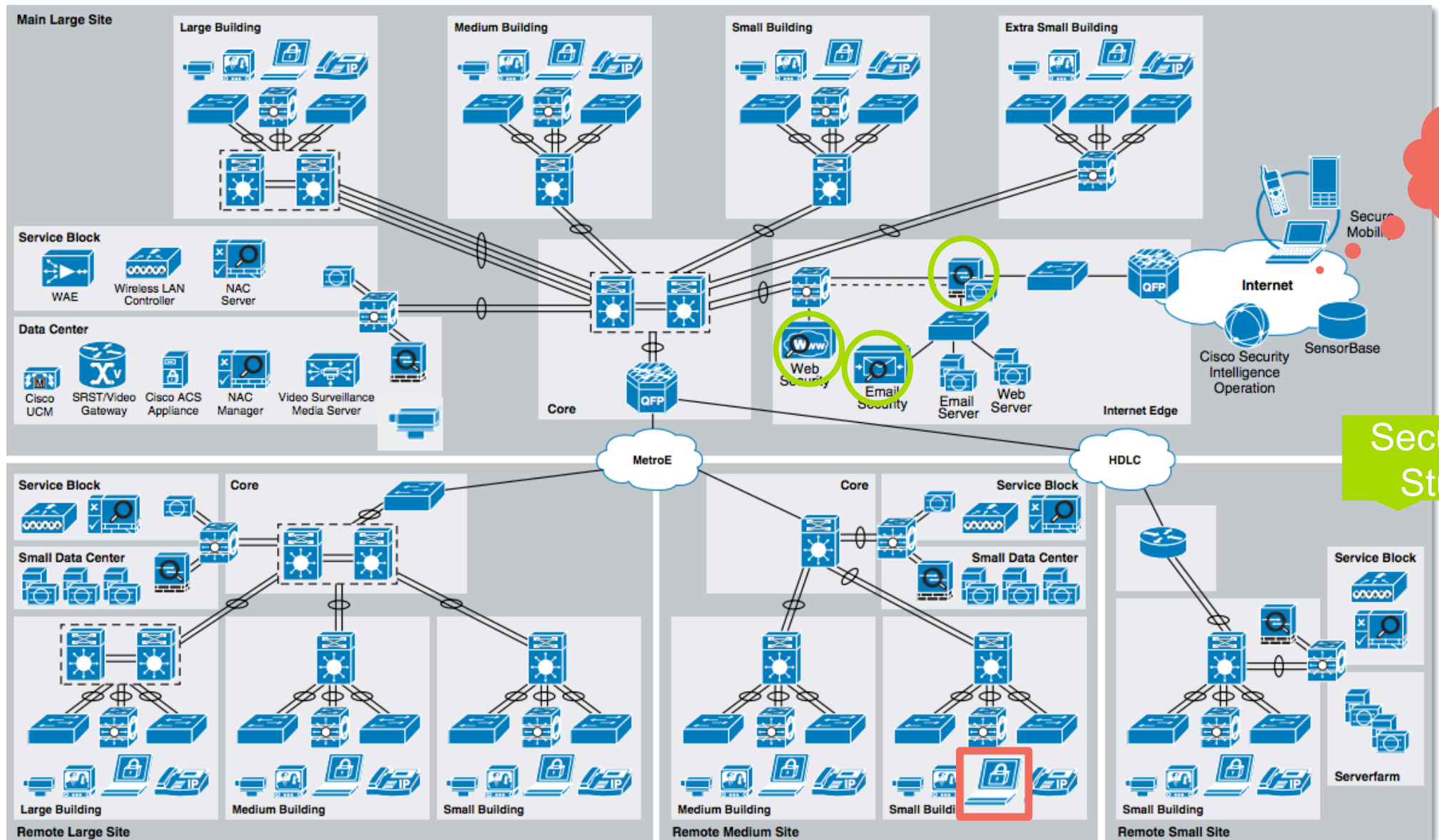


VideoCameras (5 incoming rules)									
1	<input checked="" type="checkbox"/>	any	SynologyNAS	IP> ip	✓ Permit	TOP 10 3975813			
2	<input checked="" type="checkbox"/>	any	any	ICMP echo-reply	✓ Permit	0			
3	<input checked="" type="checkbox"/>	any	any	UDP domain	✓ Permit	0			
4	<input checked="" type="checkbox"/>	any	any	UDP ntp	✓ Permit	160			
5		any	any	IP> ip	✗ Deny				Implicit rule

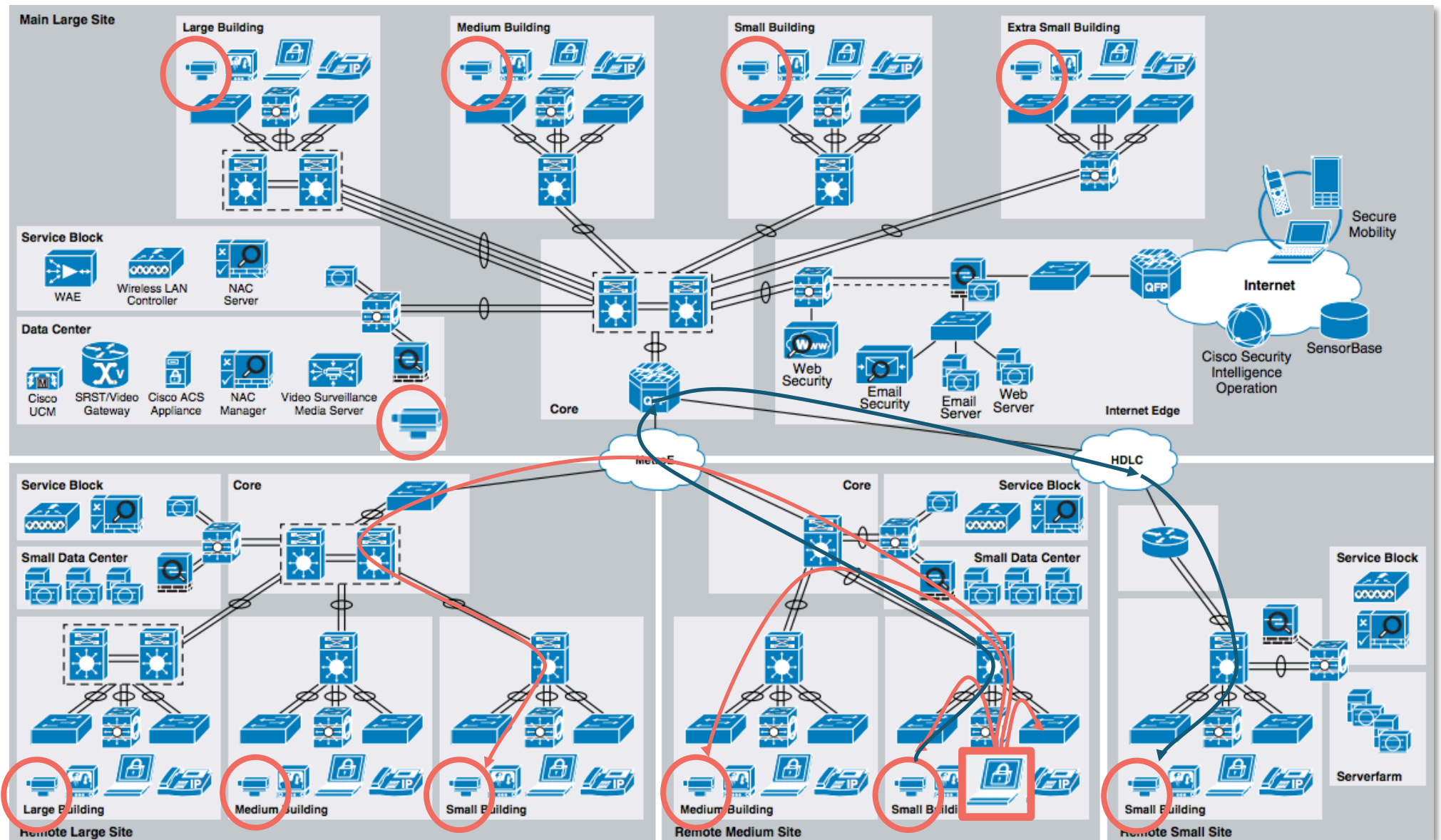
L3 VPN is used to allow remote access to the webcam portal running on the Synology.



# A Typical Enterprise Network



# I. Scanning for Devices to Infect





# I. Scanning for Devices to Infect

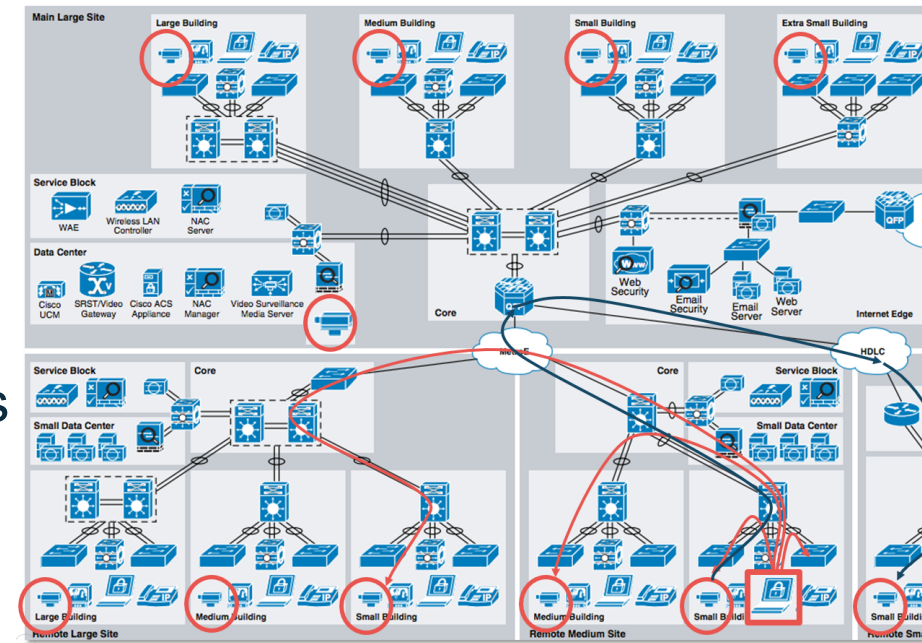
The Scanning activity generates:

- Flood of ARP requests

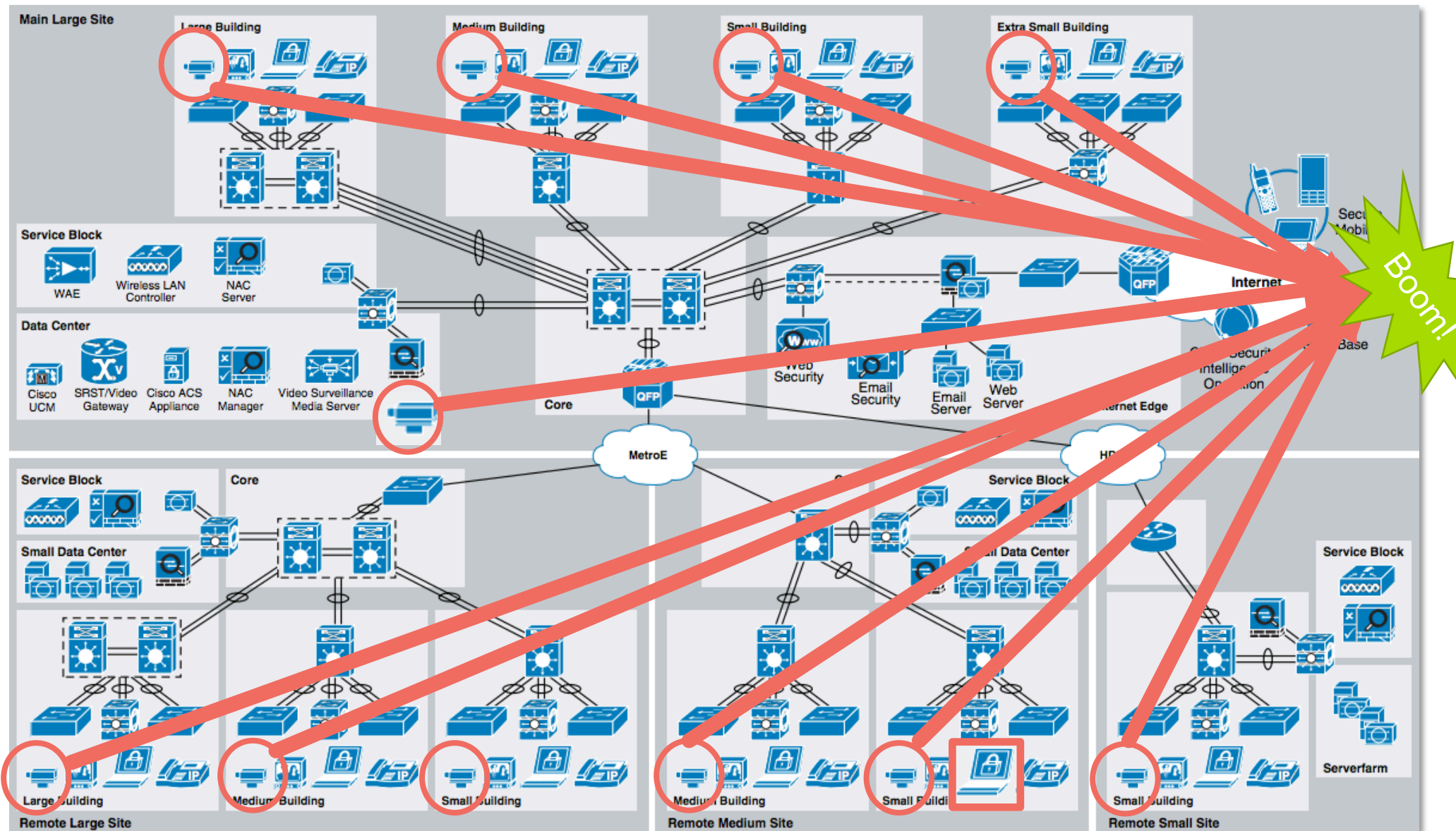
- Lots of small packets, including TCP SYN's

As more devices get infected, the scanning activity will increase, potentially causing serious issues and outages with network devices like firewalls, switches and other stateful devices.

These kinds of outages have repeatedly happened in the wild, both during the NIMDA, Code Red and Slammer outbreaks in 2001 and also recently during large scale Mirai infections at large European Internet Service Providers



## 2. Launching Outbound DDoS Attacks

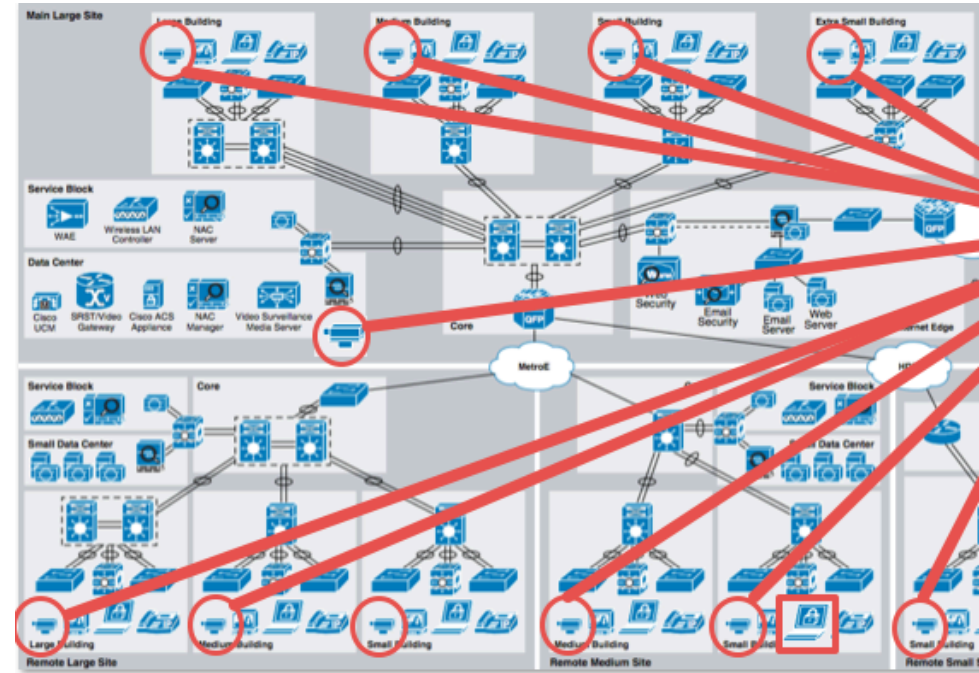


## 2. Launching Outbound DDoS Attacks

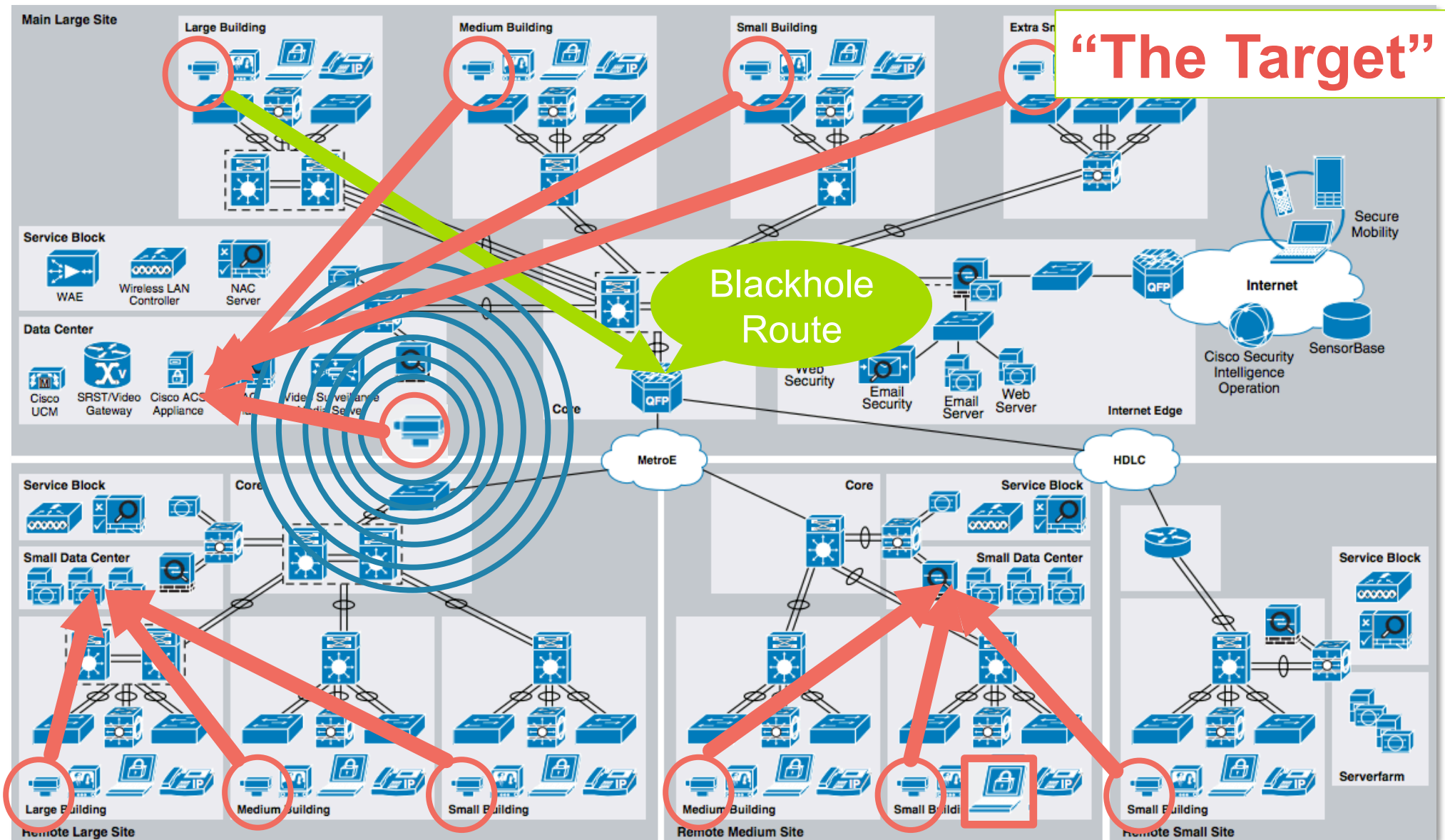
Attack activity generates a lot of traffic. Mirai can for example launch:

- UDP/ICMP/TCP/GRE/RST/SYN-ACK packet flooding
- Reflection attacks using UDP packets with spoofed source IP addresses
- Application level attacks (HTTP/SIP attacks).
- Pseudo random DNS label prefix attacks against DNS servers.

This attack traffic will quickly fill up any internal WAN links and will also will cause havoc with any stateful device on the path, including NGFWs.



# 3. Reconnaissance & Internally Facing Attacks





# 3. Reconnaissance & Internally Facing Attacks

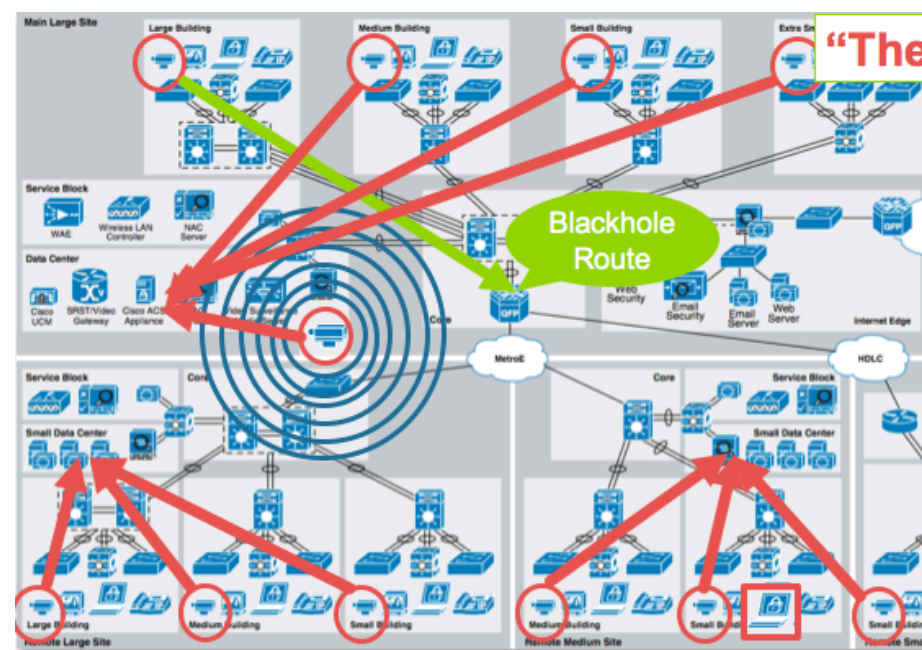
A clever attacker would scan the internal network to identify vulnerable services and network layout.

He would then launch attacks against unprotected IGP to disable DDoS mitigation services and/or shut out the NOC/SOC

He would then either launch DDoS attacks against internal services or against the now unprotected outside facing services.

An internal facing attack would be devastating as if there are no internal barriers in place, the network would simply collapse.

Remember that ALL networks have IoT devices these days, can be used against After a while, the clever attacker would then stop the attack and send a ransom email asking for his BTCs...



# Are IoT Devices Capable of Causing So Much Harm?

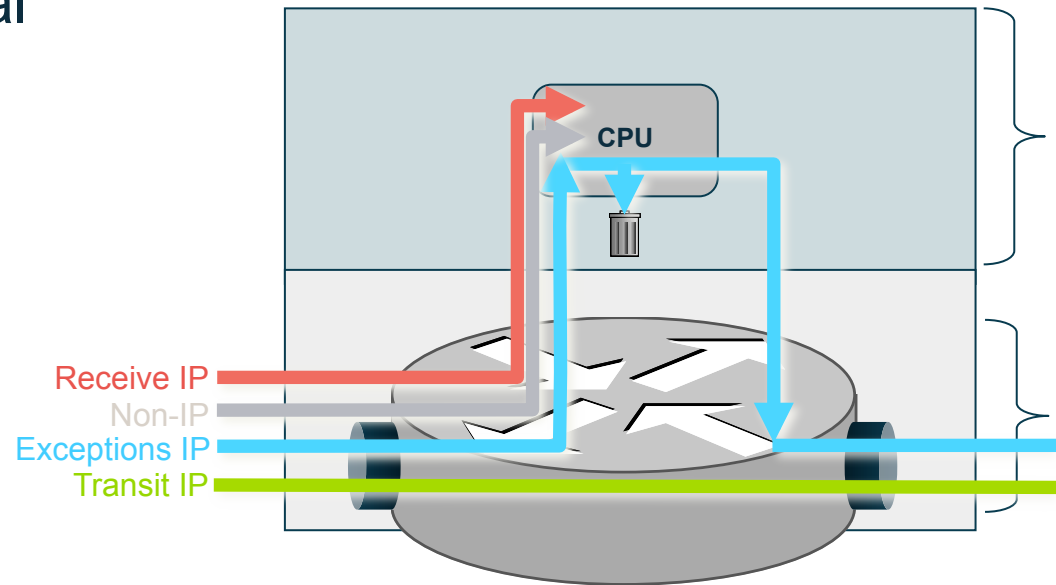
First, let's look at the anatomy of a typical network device. It has a:

- Fast path
- Slow path

And there are 4 main groups of packets to be handled:

- Transit packets
- Received packets (for the device)
- Exception packets
- Non-IP packets

If an attacker can force the device to spend cycles on processing packets, it won't have cycles to send or process critical packets!



A carefully crafted 300pps flood against typical (unsecured) high-end routers / switches will cause those to lose their routing adjacencies...

The background of the image is a dark blue globe. Overlaid on the globe is a complex network of white lines and dots, resembling a global communication or data network. The lines connect various points across the globe, creating a web-like structure. The globe itself shows some landmasses in a lighter blue tone.

# **RALLYING THE DEFENSE**



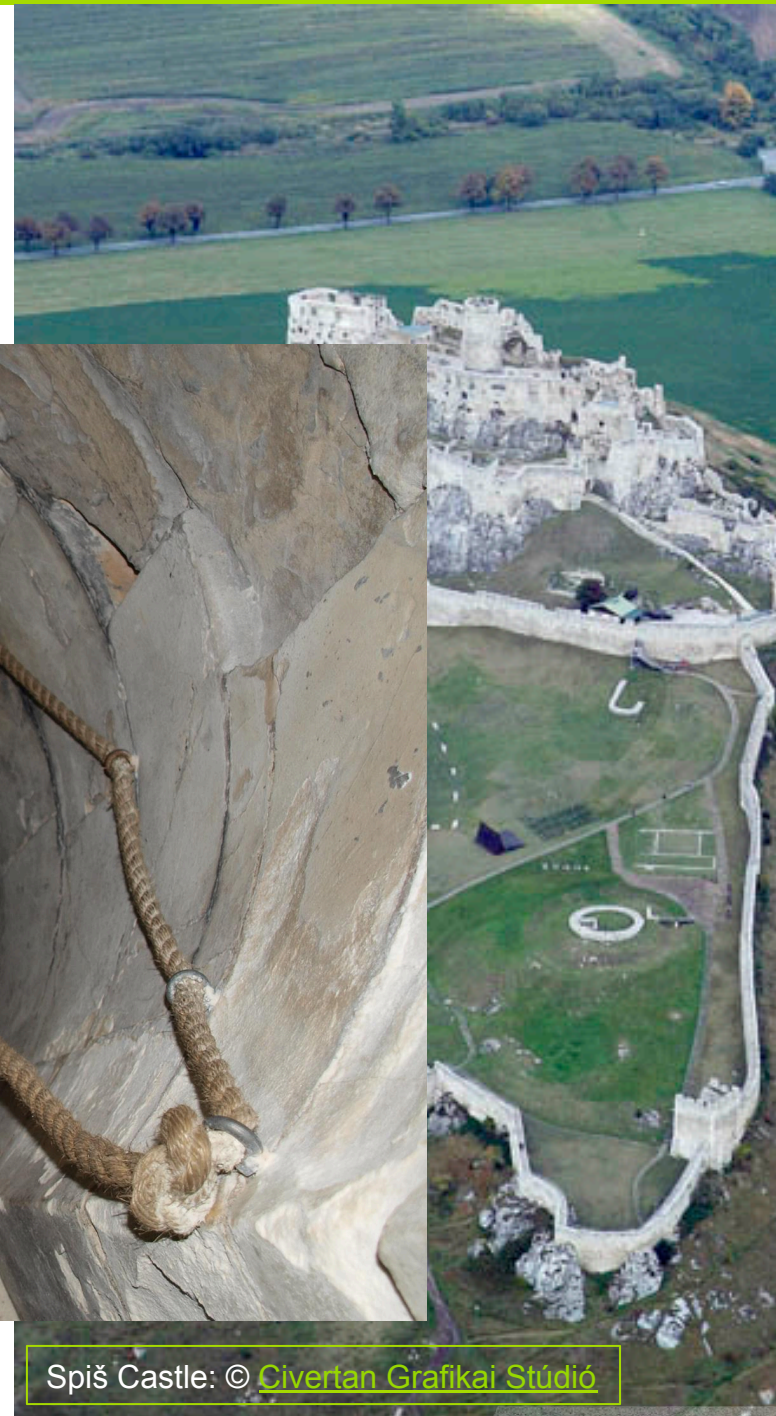
# Learning from History: Implementing a Layered Defense



© Pierre Bona / Wikimedia  
[CC-BY-SA-3.0](#) / [GFDL](#)



[Friends of York walls](#)



Spiš Castle: © [Civertan Grafikai Stúdió](#)



# Defending against attacks from the inside

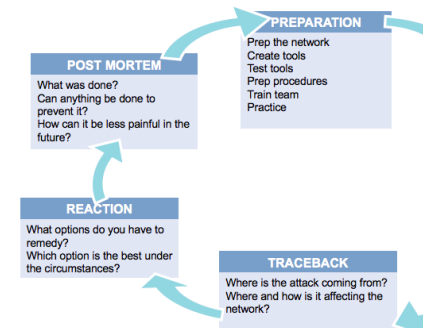
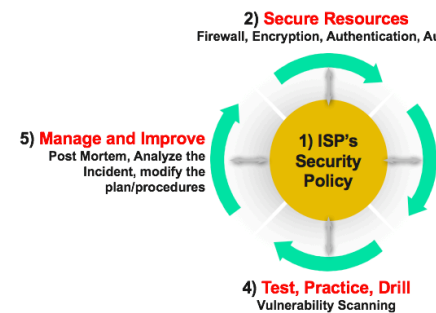
- Enterprises are NOT prepared to deal with these kind of scenarios and drastic steps will have to be taken to survive in this new environment,
- SPs have more than 20 years experience in Infrastructure security, this could be an opportunity to help your customers to secure their networks by implementing Security Best Current Practices (BCP's).
- An Enterprise which is compromised using these new attack vectors, will start launching large-scale outbound attacks, potentially leading to collateral damage.



<https://hdwallstbox.com/army-undead-fantasy-art-armor-skeletons-artwork-w>

# Defending against attacks from the inside

- SPs should therefore start educating their customers on this new threat and help them to implement the 6 phase methodology:
  - Preparation:** Prepare and harden the network against attack.
  - Detection and Identification:** Identify that an attack is taking place.
  - Classification:** Classify the attack.
  - Traceback:** Where is the attack coming from.
  - Reaction:** Use the best tool based on the information gathered from the Identification, Classification and Traceback phases to mitigate the attack.
  - Post-mortem:** Learn from what happened, improve defenses against future attacks.



# Defending against attacks from the inside

- Example of Enterprise Security Best Practices:
  - Implementing full Network segmentation and harden (or isolate) vulnerable network devices and services using iACL, LPTS and CoPP.
  - Harden routing protocols, use passive IGP on access and internal facing networks.
  - Developing a DDoS Attack mitigation process.
  - Utilizing flow telemetry to analyze external and internal traffic. This is necessary for attack **detection**, **classification** and **traceback**.
  - Deploying a multi-layered DDoS protection.
  - Scanning for misconfigured and abusable services, this includes NTP, DNS and SSDP service which can be used for amplification attacks.
  - Implementing Anti Spoofing mechanisms such as Unicast Reverse-Path Forwarding, ACLs, DHCP Snooping & IP Source Guard on all edge devices.



# Can SPs Defend Enterprise Customers Being Attacked from Within?

- Service Providers have great success in offering Clean Pipes-type solutions to Enterprises.
- An internal facing attack against an Enterprise customer will NOT be visible by the SP and traditional DDoS mitigation service will not help!
- The customer under attack will request assistance from Service Providers to deal with these kind of attacks as well – even though the SP can't see the DDoS attack and can't mitigate it!
- This is therefore a new opportunity to extend Clean Pipes mitigation type services within the Enterprise perimeter.
- Other services like network hardening Best Practices and internal network monitoring can apply as well.



Clean P



Anti-DD



Secur  
Monito

# Summary

## The attackers are now inside the castle!

The Windows spreader has opened up the possibility to infect internal IoT devices and use them to launch outbound attacks and/or internally facing attacks from your customers.

## Internal network defenses and security architectures need to be adapted to meet this new threat.

Stateful devices will collapse both due to persistent scanning active and also when DDoS attacks are launched.

## Implementing Security BCPs will help

SP customers will be needing help to mitigate these threats, this might be good opportunity to both locking down the hatches and offer managed security services.



The Walking Dead, Season 6



Zombie Horde by Joakim Olofsson

# Q&A / THANK YOU

## *Contact Information:*

Steinthor Bjarnason  
[sbjarnason@arbor.net](mailto:sbjarnason@arbor.net)