Zero Trust Evolution

Randy Marchany

CISO, Virginia Tech

marchany@vt.edu

https://security.vt.edu

Twitter: @randymarchany

VIRGINIA TECH™

Most Common Security Mistakes Made by Individuals (2001)

- Poor password management
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- Not installing anti-virus software ✓
- Laptops on the loose
- Blabber mounts (file access open to the world)
- Plug and Play without protection
- Not reporting security violations
- Always behind the times (OS, application patches)
- Keeping an eye out inside the organization

*Zero Trust Networks(ZTN) Characteristics**

Network and user traffic patterns have changed dramatically in the past 20 years.

- Pillar 1: The network is always assumed to be **hostile**
- Pillar 2: Assume the hostiles are already **inside your network**
- Pillar 3: Network locality (segmentation) is **not sufficient** for deciding trust in a network
- Pillar 4: **Every** device, user and network flow is authenticated and authorized
- Pillar 5: **Policies** must be dynamic and calculated from as many sources of data as possible

** “Zero Trust Networks: Building Secure Systems in Untrusted Networks”, Evan Gilman, Doug Barth*

The Future: The Mobile Internet

Positioning IT for the future

- Pillar 6: The device is no longer the border. A **user's identity/Data pair is the new border.**
- Pillar 7: Containers, serverless and cloud computing are the new disruptors of traditional security architectures.
- Pillar 8: Mobile users, mobile apps, mobile storage

EDU (now) vs. Corporate Structure (future)

- **Administrative** – the process that runs the institution (**CORP**)
  - Payroll, HR, Purchasing, Facilities, Legal, etc.
  - **Security model closest to corporate model**
- **Academic/Instructional** – the process that supports teaching/learning (**ISP**)
  - Learning Mgt Systems such as CANVAS, Blackboard, Moodle
  - Course Delivery systems – Zoom, Webex, etc.
  - Heavily BYOD – all flavors, types
  - **Security model closest to an ISP**
- **Research** – **hybrid** of the previous 2
  - Intellectual Property protection, High risk, visibility
  - **Security model is a hybrid of corporate and ISP**

Hacker Attack Goals

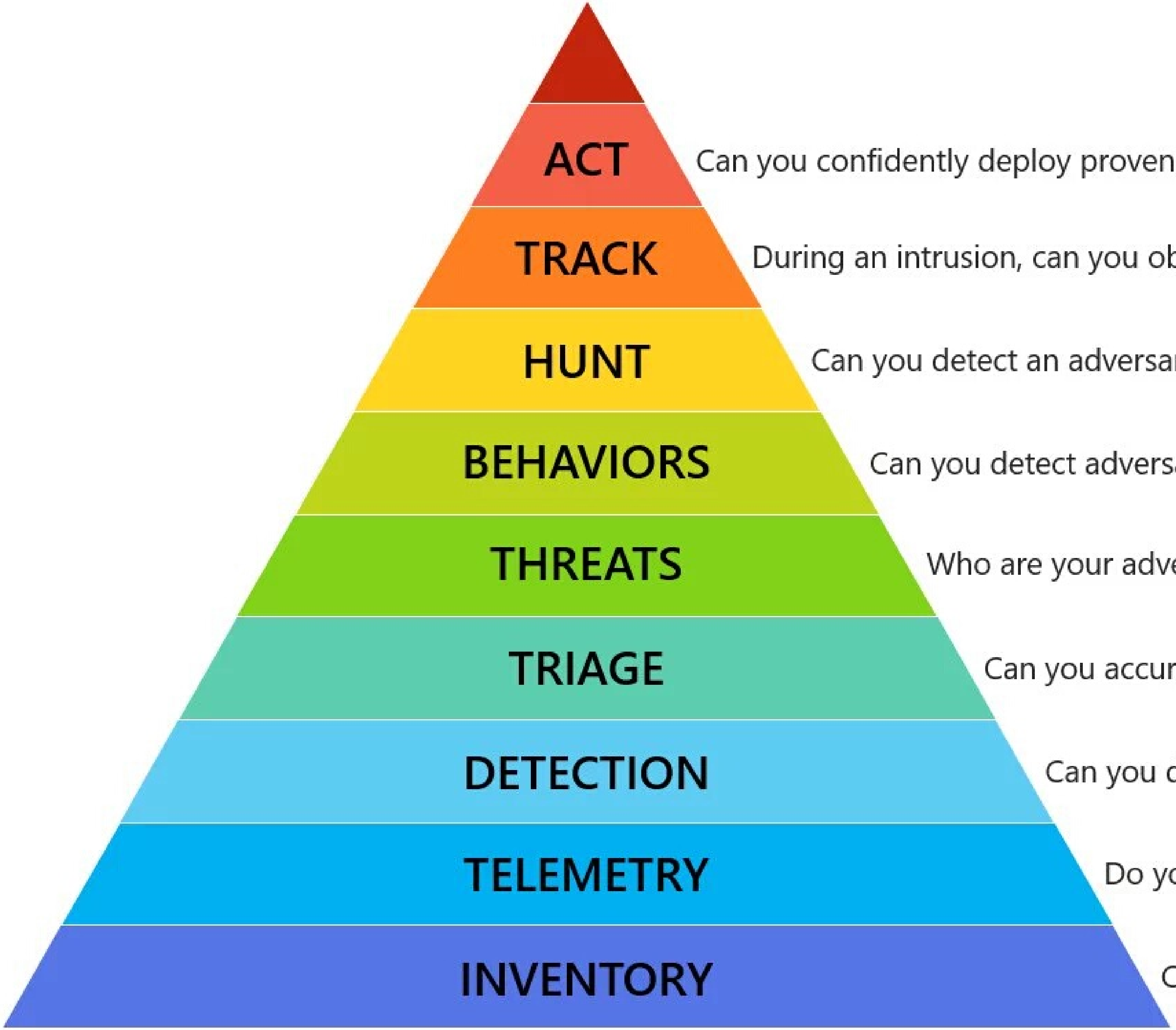
Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
- **ATTACK** other sites using hacked assets
- **DESTRUCTION** of company data (deletion or ransomware).

- **DEFEND** accordingly

What are You Defending? What Should You Defend?

- Systems? Not really but that’s what we thought should be defended.
- Networks? Safe answer.
- DATA – what we should be defending.



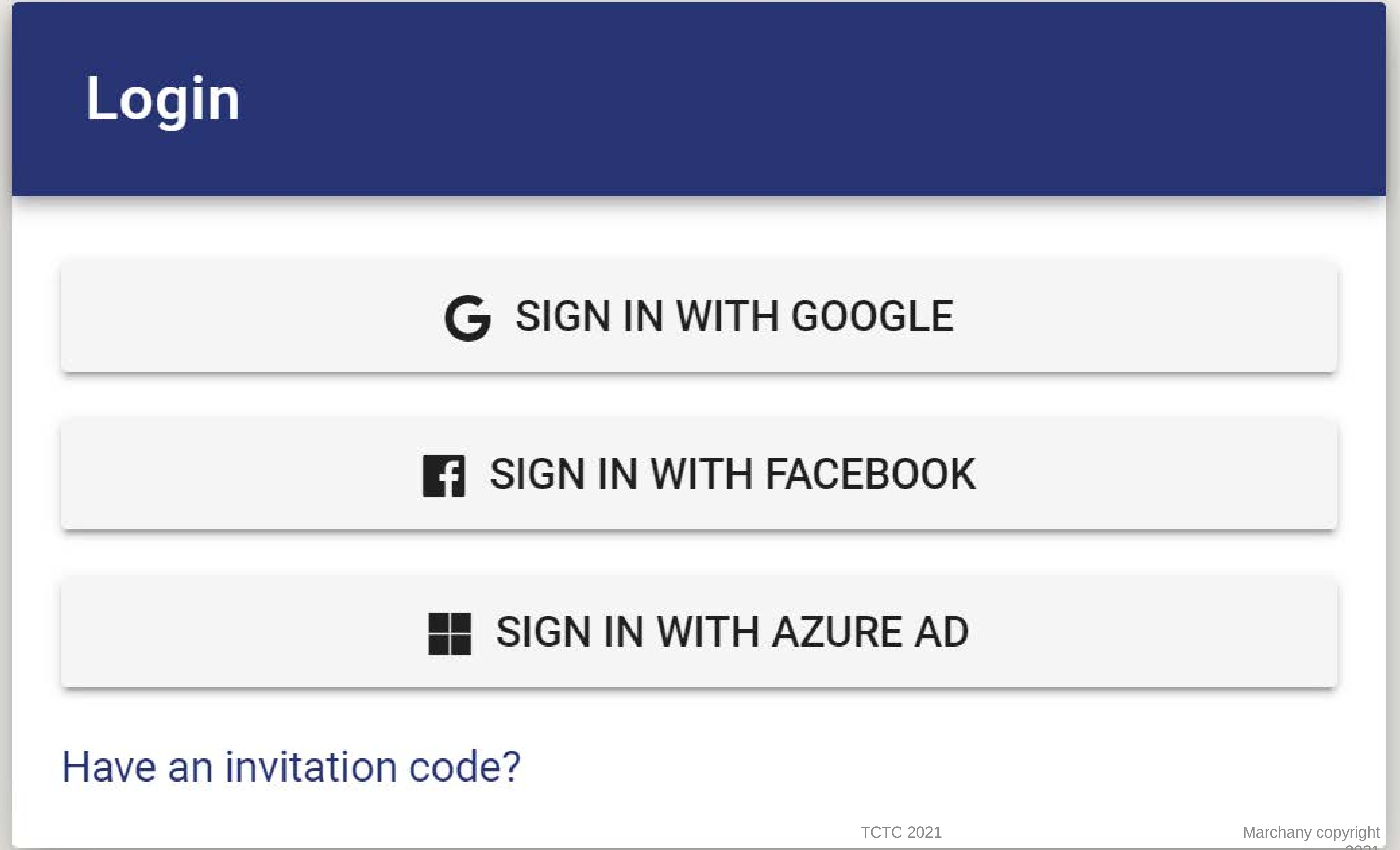
ACT	Can you confidently deploy proven countermeasures to evict and recover?
TRACK	During an intrusion, can you observe adversary activity in real-time?
HUNT	Can you detect an adversary that is already embedded?
BEHAVIORS	Can you detect adversary activity within your environment?
THREATS	Who are your adversaries? What are their capabilities?
TRIAGE	Can you accurately classify detection results?
DETECTION	Can you detect unauthorized activity?
TELEMETRY	Do you have visibility across your assets?
INVENTORY	Can you name the assets you are defending?

Border? What Border?

- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- Internet 3.0 – mobile servers (containers, serverless), mobile endpoints (laptops, phones, tablets, IoT, ICS)
- Current security architectures are somewhere between Internet 1.0 and Internet 2.0.
- We need to adapt to Internet 3.0 now.

Another View of ZTN

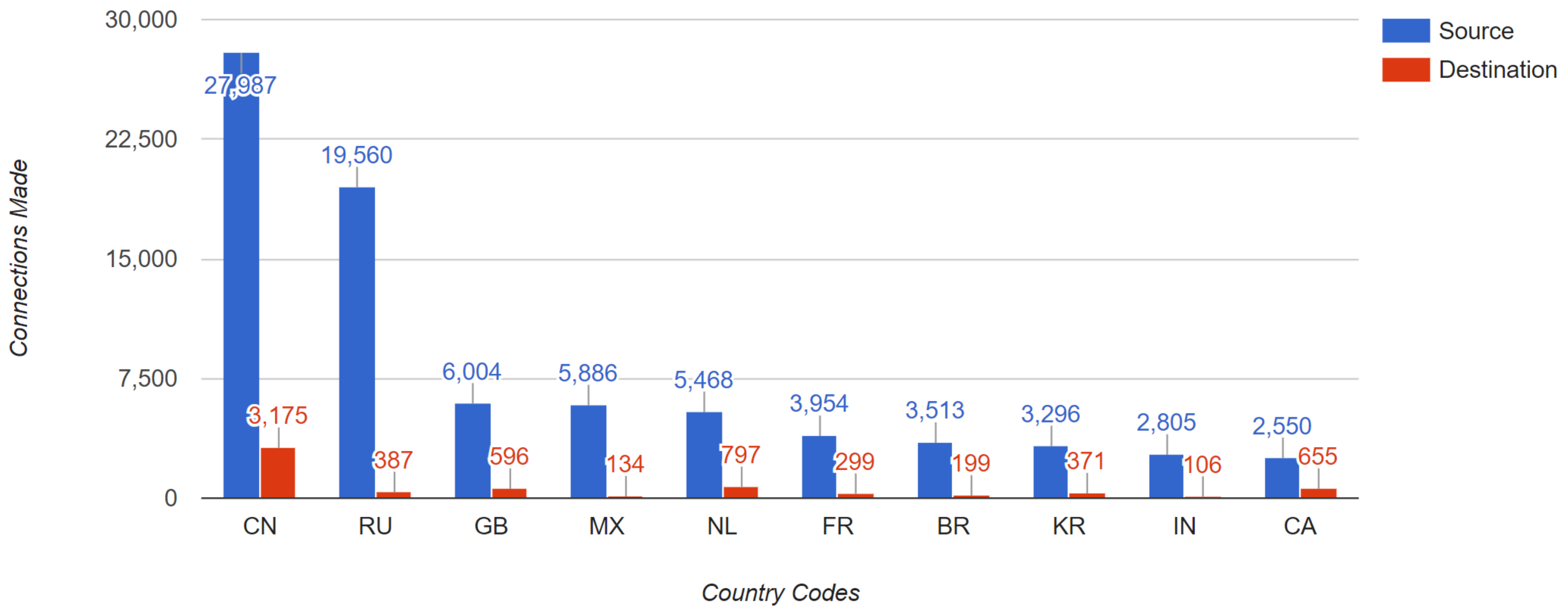
- "As we move our data outside of the firewall, we have to adopt a zero-trust type model, " [Chris] Townshend said. "We are shifting our security enforcement out to the data itself, and **you have to have a security policy that follows that user no matter where that user is or what device they are using to access the data"**
  - "The new cyber landscape", Patrick Marshall, GCN Magazine, vol 37, #1
- In other words, data becomes the border.


Login
SIGN IN WITH GOOGLE
SIGN IN WITH FACEBOOK
SIGN IN WITH AZURE AD
Have an invitation code?

Sample In/Out Traffic Profile

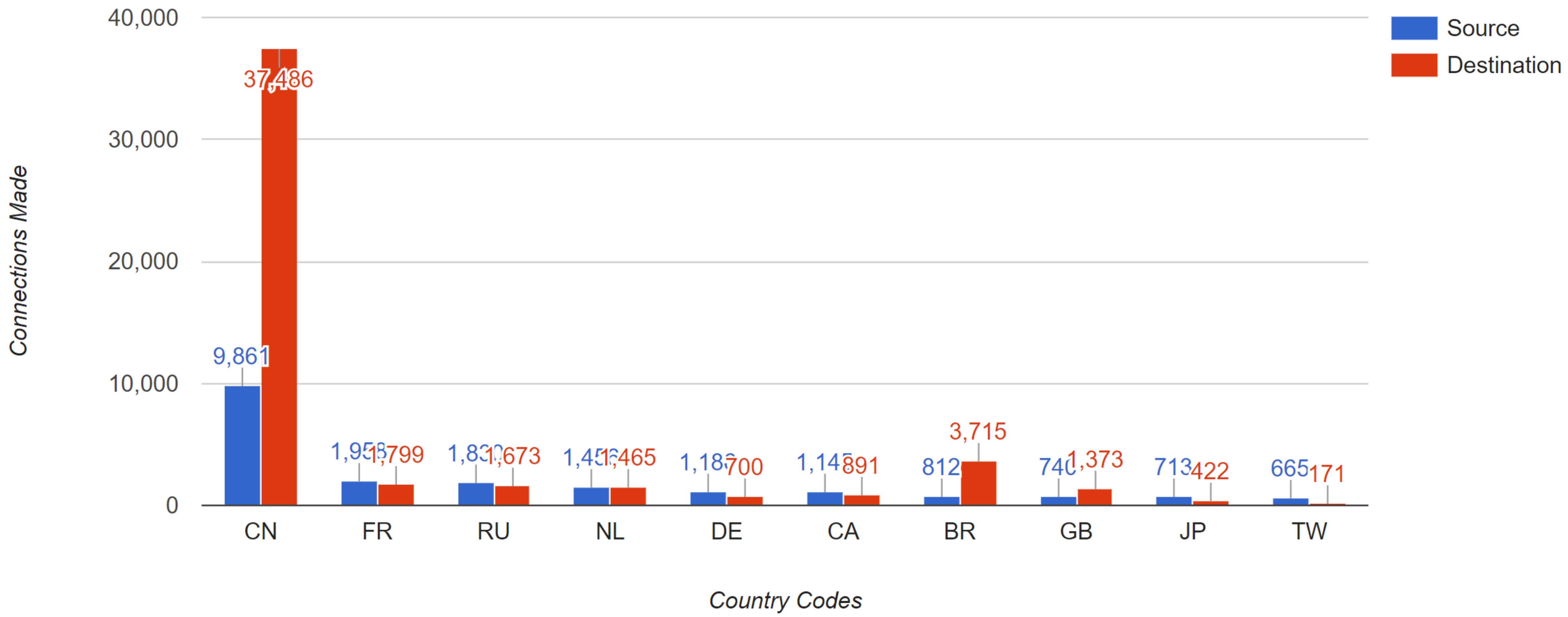
Top Source & Destination Countries - By Connection

Aug 01, 2017 to Aug 31, 2017 - ITSO Argus Data

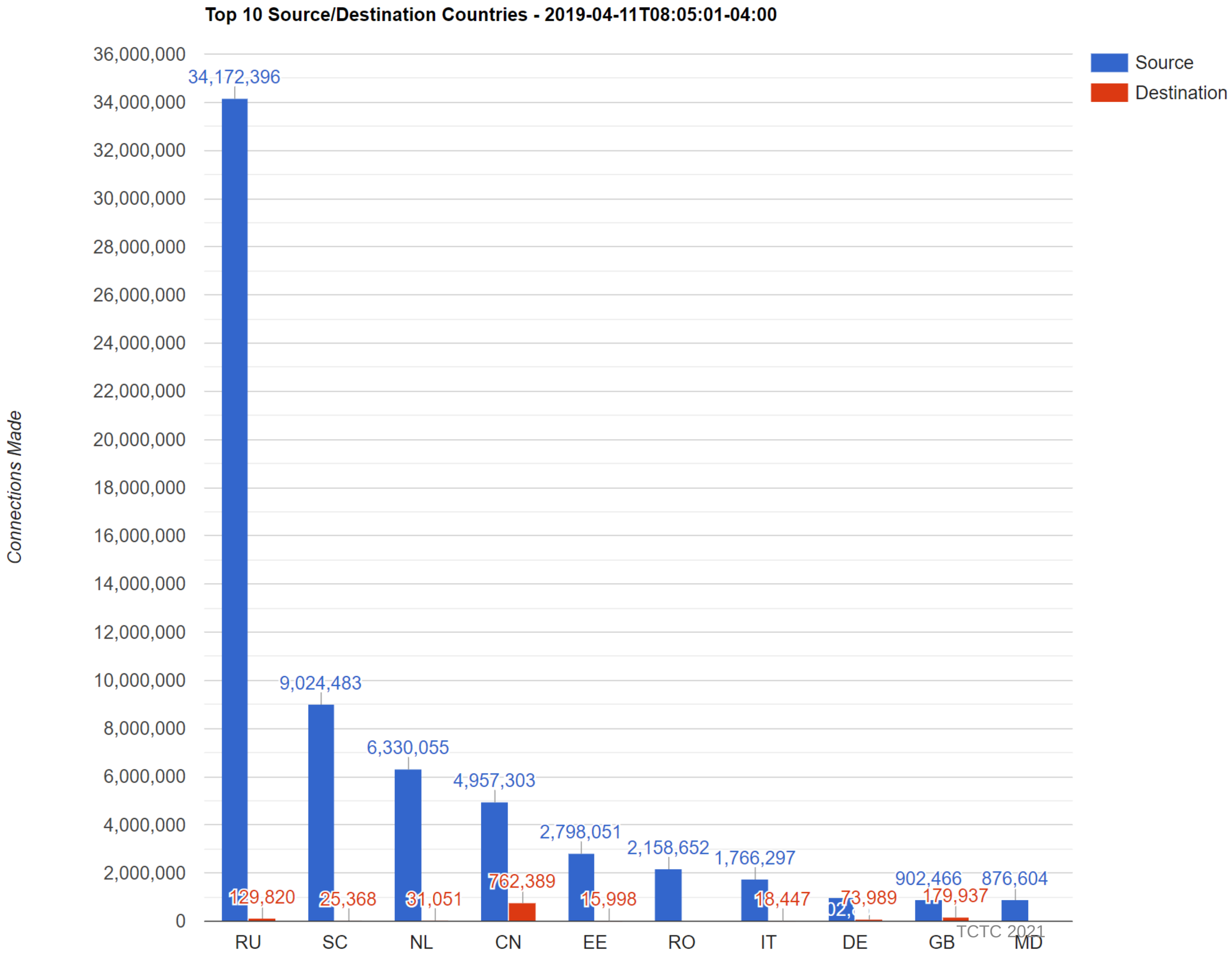


Country Code	Country Name	Source Count	Destination Count
US	United States	91396	206186

Nov 01, 2014 to Dec 01, 2014 - ITSO Argus Data



Country Code	Country Name	Source Count	Destination Count
US	United States	136701	104575



Top 10 Source/Destination Countries - 2019-04-11T08:05:01-04:00

TCTC 2021

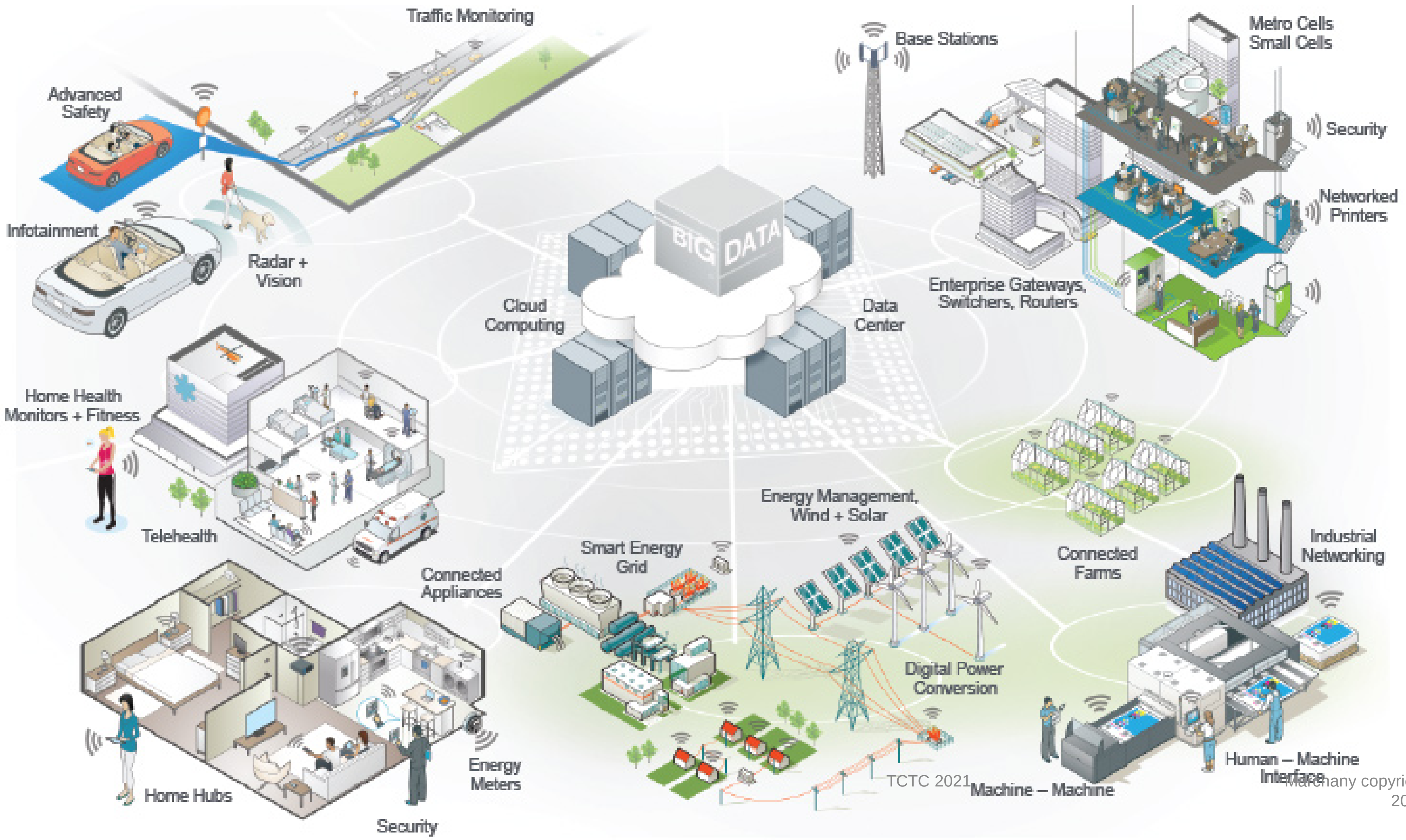
Museum Defense in Depth

©2018 FireEye | Private & Confidential

- Control access points
  - Limited but **free flowing** access points
  - Additional barriers around high risk assets
- Pervasive Monitoring tools
  - Cameras, motion sensors, etc.
- Active Response
  - Guards, on-demand barriers, fire suppression
- Recovery Measures
  - Insurance
  - Tracking devices
- Assume hostiles are inside.

Used with permission of Christian Schreiber

ENABLING SMART CONNECTED SOLUTIONS FROM THE END NODE TO THE CLOUD



ZTN - Theory

- Easier said than done. Not all of the technology and components available today….not yet.
- **All data must be secured regardless of location.** Encryption at rest or in transit. Have to find it first!
- **User identities must be confirmed.** Access to data strictly enforced. Default of minimum privileges
- **All network traffic should be logged and analyzed**.
  - “trust but verify” -> “Verify and never trust”
- Eliminates distinction between trusted-inside-perimeter and untrusted activity that crossed the perimeter

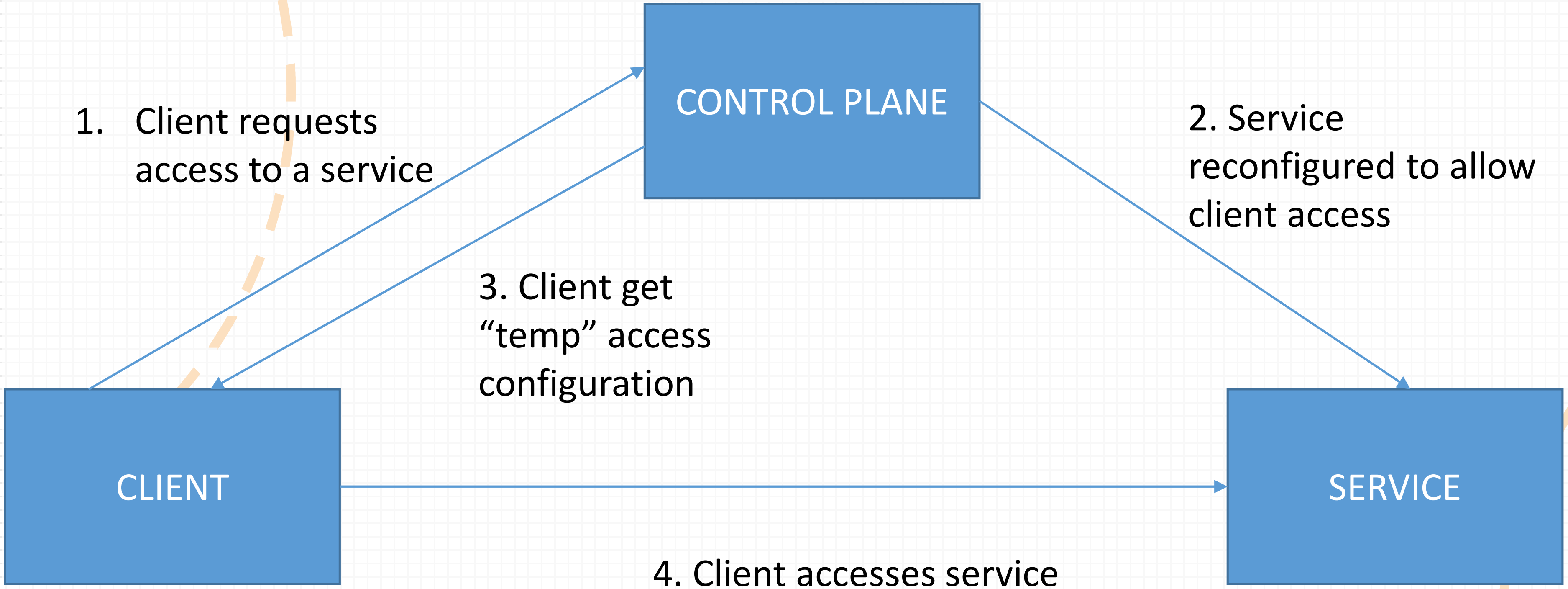
ZTN Characteristics

- Treat all hosts as internet-facing (take that, .com, .gov, .mil ….)
- Use existing tech in novel ways
- Perfect fit for cloud

ZTN Components (Theory)

- Control Plane
  - Processes requests from data plane devices that want to access or grant access (to) network resources
  - User, device authentication & authorization done here
  - Stronger authentication to higher risk resources done here
- Data Plane
  - Components include applications, firewalls, proxies, routers that process network traffic
  - Handles high traffic rates

ZTN Client-Control Plane Interaction (Theory)



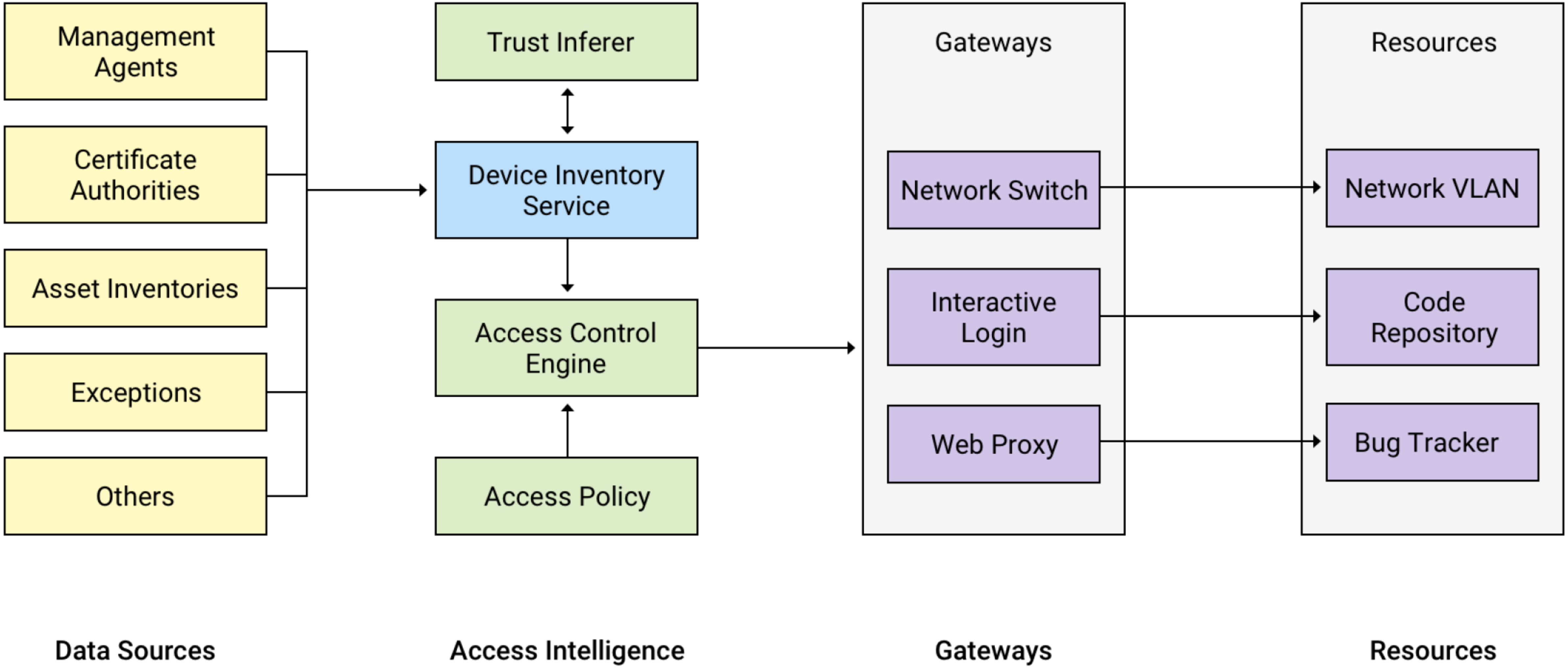
1. Client requests access to a service

2. Service reconfigured to allow client access

3. Client get “temp” access configuration

4. Client accesses service using access configuration info

Zero Trust Networks, Fig. 2-5



BeyondCorp Infrastructure Components

ZTN Authorization Architecture

- Enforcement
  - Critical to place these as close to endpts as possible
  - Reference a policy, decide and enforce application of this
- Policy Engine
  - Has power to make decision to grant/reject resource requests
  - Best defined in logical network terms

ZTN: Trusting Devices

- Device Certificates
  - Used to create, validate Device Inventory DB
  - HSM, TPM , X.509 certs
  - Used in all communications to enterprise services
- Define in SW
  - Clean images (CIS Benchmark scored)
  - SSO to validate users wanting access to enterprise stuff
- Use/create device certificates

ZTN Authorization Components

- Trust Engine
  - Google BeyondCorp a pioneer in this area
  - New concept – calculates a trust score of components based on historical behavior
- Data Stores
  - 2 types: Inventory, Historical
  - Ex: User inventory stores relevant user info (AD, LDAP)
  - Ex: Device inventory has info on every device connected to the network (CSC #1)

ZTN Trust: Users

- Informal identity
  - Standard use – pseudonymous accounts
- Authoritative identity
  - MFA
- Trust scores determine if additional authentication is required
- Single Sign-on

ZTN Trust: Network Traffic

- Traditional net filtering, monitoring - significant factor in ZTN.
- Its application is non-traditional
- Net flow authentication/authorization a key component
- How to trust net traffic – Single Packet Authorization(SPA)
  - How do you allow a trusted connection but dropping others?
  - Preauthentication, SPA
  - Fwknop - http://www.cipherdyne.org/blog/2012/09/single-packet-authorization-the-fwknop-approach.html

ZTN Trust: Network Traffic

- Where to apply ZTN controls in the network stack
  - TLS – used mostly application layer protocols
  - IPsec – used mostly to secure traffic (VPN). Well positioned to provide secure comms for all traffic
- Filtering
  - Host – filter traffic at the host. Handles inbound traffic
  - Bookend – apply policy in both directions. Egress filtering
  - Intermediary – “traditional” FW placement

ZTN: Requirements

- All network flows must be authenticated before processing
- All network flows should be encrypted before xmission
- Authentication, encryption (A&E) must be done at the endpoints
- All net flows must be enumerated so access can be enforced

ZTN: Requirements

- The strongest A&E suites should be used
- Authentication should not rely on public PKI providers. Private PKI systems should be used
- Devices should be scanned, patched and rotated regularly

Some Suggestions

- Start small – ZTN a lab or smaller departmental net
- Build a system diagram of your network traffic patterns
- Profile your traffic
  - Do you know where your inbound traffic originated?
  - Where does your outbound traffic go?
- Do you trust your network?

ZTN and Today’s Network

- Assume net is hostile & hackers already inside
  - Monitor outbound traffic with threat intel data
  - Configure host based FW/IDS
  - Profile your net traffic
    - Direct lateral movement between hosts is rare? y/n
- Log, Log, Log

ZTN and the 20 Critical Security Controls

- HW Inventory
- SW Inventory
- Continuous Vuln Mgmt
- Controlled use of Admin Priv
- Secure config for devices
- Log Analysis, maintenance

- Email, Browser Security
- Malware Defenses
- Limit Ports, Protocols, Services
- Data Recovery
- Secure config for net device
- Boundary Defense

ZTN and the 20 Critical Security Controls

- Data Protection
- Need to Know
- Wireless Access Control
- Acct Monitoring, Control
- Security Training
- Application Software Security
- Incident Response & Mgmt
- Penetration Testing and Red Team Exercises

Summary

- Need an architecture that can handle:
  - Data mobility, protection
  - Cloud, containers, serverless apps
- What will the tech environment be in 5 yrs? 10yrs?
- We’ve been doing pieces of ZTN for years.

References

- “Zero Trust Networks”, Gilman, Barth, http://shop.oreilly.com/product/0636920052265.do
- “Building Security into Your Network’s DNA: The Zero Trust Approach”, John Kindervag, 2010
- “Single Packet Authorization: A Comprehensive Guide to Strong Service Concealment using fwknop”, Michael Rash, http://www.cipherdyne.org/fwknop/docs/fwknop-tutorial.html#design