NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

Zero Trust Networking:
A Cynic's Guide To the Evolution of Trust on the Network

Sam Grosby

Stardate: 2019

- A Zero Trust Architecture (ZTA) strategy is one where there is **no implicit trust granted to systems based on their physical or network location** (i.e., local area networks vs. the Internet). Access to data resources is granted **when** the resource is required, and authentication (both user and device) is performed **before the connection is established**.

Elements of Zero Trust

- Know what's on your network: Discover data, assets, services, and applications by sensitivity or criticality across locations.
- Have technologies that enable isolation and segmentation of critical network.
- Authenticate devices and users to corporate networks and apps/systems.

Elements of Zero Trust

- Know what's on your network: Discover data, assets, services, and applications by **sensitivity or criticality across locations**
- Have (*pervasive, generally available*) technologies that enable isolation and segmentation of critical network.
- Authenticate devices and users to corporate networks and apps/systems.

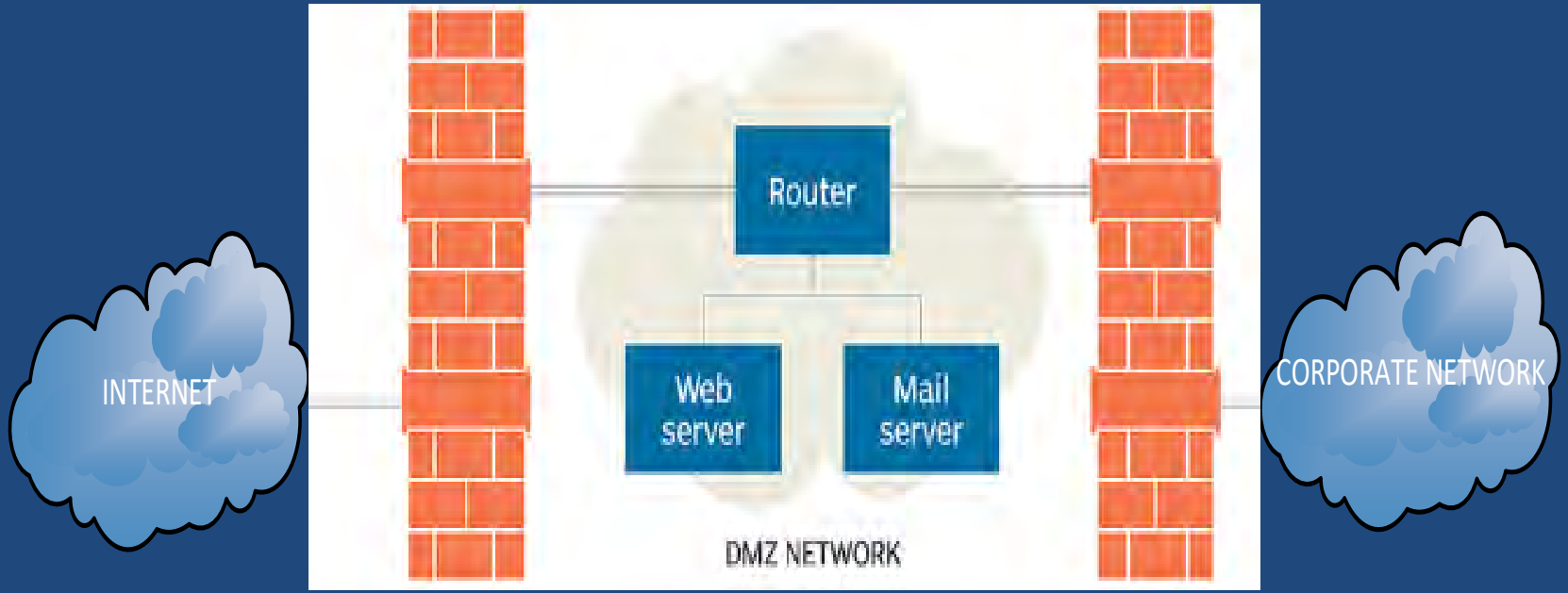
There's No Such Thing As A Zero Trust Network

- Well, maybe at Google.
- We've been trying to reduce trustedness of the internal network for 25 years.
- Zero Trust is possible for individual application or small collection of applications.
- Inflection points where you can drive a big reduction in trust: data tagging, cloud apps, automation, and application modernization.

1990: Packet Filters Roamed the Earth

- DEC develops the first packet filtering firewall; it becomes commercially available as DEC SEAL in 1990. Cheswick and Bellovin publish “Firewalls and Internet Security” (First edition).
- Bill Cheswick describes perimeter firewalls as “a sort of crunchy shell around a soft, chewy center”. Things stayed that way for a long time.

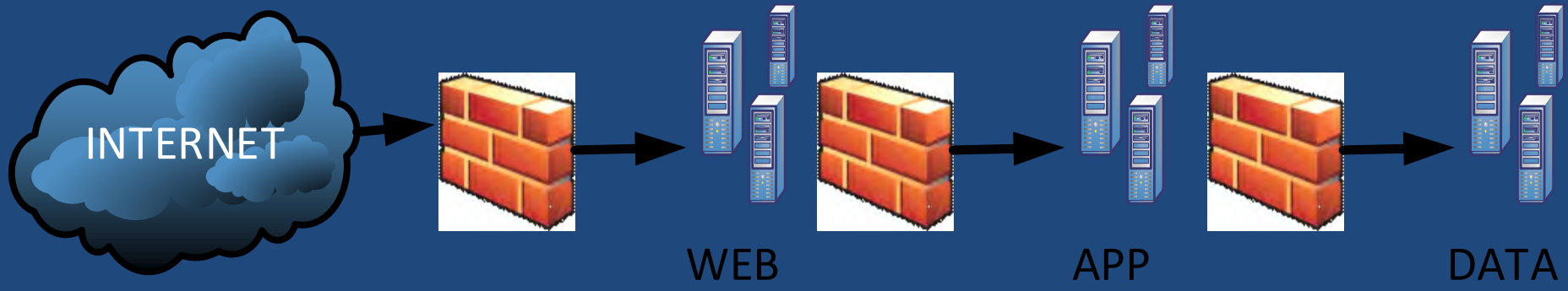
1995: Dual Firewall DMZ Architecture, aka the Firewall Sandwich



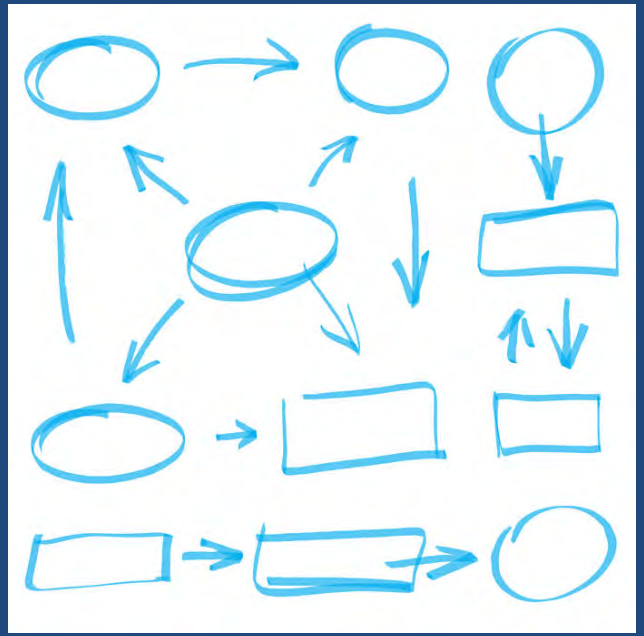
2000: Network Access Control

- Allows you to know, via a service account, not just who is on your network but what machines are on your network. But only if they're all Windows machines.
- Allows us to replace 'physical location' with a different trust factor.

2005: How to segment an N-Tiered Architecture

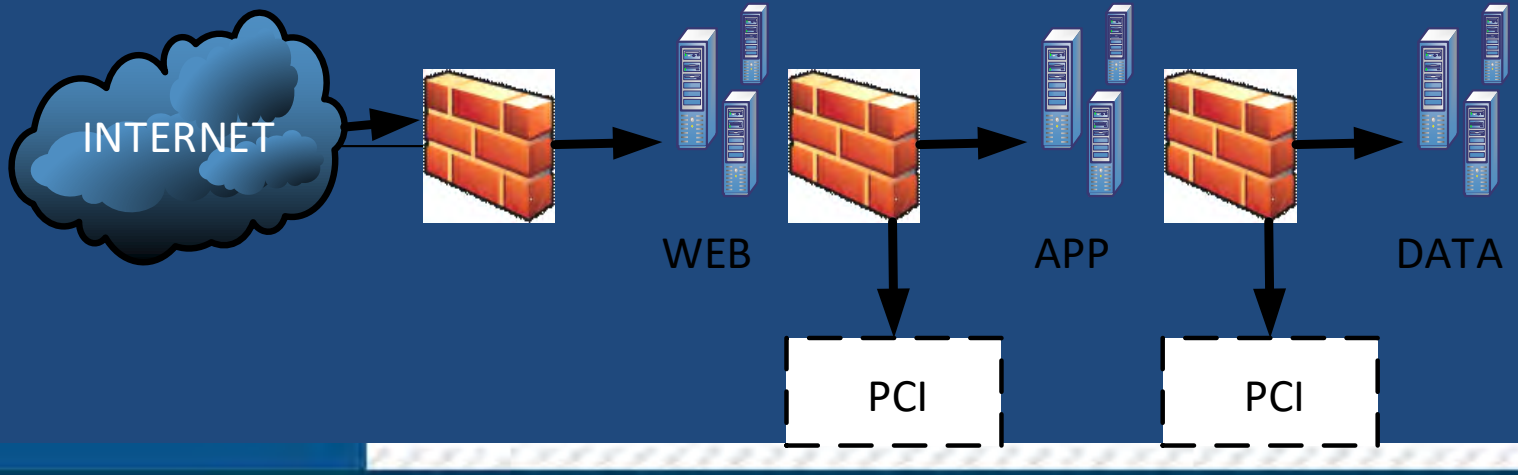


Application Conceptual and As-Built



2005: Contractual reasons to Segment

- PCI DSS 1.0 compliance requires a Cardholder Data Environment (segment) with authenticated flows for network control.



Other Roads We Go Down: Endpoint IPSEC Mesh/Host Based Controls

- Where ‘n’ is the number of nodes, n x (n-1)/2= number of tunnels in a full mesh. For every 100 machines, 4,950 tunnels to troubleshoot, and no centralized controller. Also, Linux RPM doesn’t natively come with IPSEC.
- IPTables and other host based controls are appealing as virtualization takes off but have similar scale issues without a centralized controller.

2009: Forrester publishes Zero Trust Networking

- And quickly becomes an industry buzzword meaning: multifactor authentication, least privilege, white list instead of black list, per-application segmentation, and de-perimeterization.
- Microsegmentation gets all the play.
- Start by classifying and identifying *all* your data. This is great advice. If it were easy, it'd be done already.

2014: Session Defined Perimeter

- Assets are ‘hidden’ on the network prior to authentication by the requesting resources
- Original spec written by Cloud Security Alliance
- Software based on-demand IPSEC/mTLS based on traditional L3 5 tuple plus identity – not application aware.
- Uses MFA with the device certificate as a factor.

2015: Automation

- We continue to abstract compute, and move toward containers and on-demand workloads, and integrate more context into our rules wherever the tools allow it.
- IoT is getting big and device discovery is getting harder because of it.
- Hypervisor based firewalls are easier to manage than endpoint firewalls and are locally context aware.

2016: BeyondCorp

- Google BeyondCorp: BeyondCorp began as an internal Google initiative to enable every employee to work from untrusted networks without the use of a VPN. BeyondCorp is used by most Googlers every day, to provide user- and device-based authentication and authorization for Google's core infrastructure.

2017: 12 Factor Application Modernization

- **Dependencies, Processes, and Port Binding**
- **Apps must know what they talk to! Manifests instead of writing rules to monitored traffic flows.**

2018: Cloud Workloads

No, it's not going to crush your town. But maybe your data center.

Today

- Traditional perimeters are moving. We'll always have an internet-facing firewall, but what was formerly COTS on prem is probably SaaS hosted today.
- Look for opportunities to reduce blast radius even as your machines become less homogenous.