

Traditional IT network security is based on the castle concept. In castle security, it is hard to obtain access from outside the network, but everyone inside the network is **trusted by default**.

Zero trust security is an IT security model that requires strict identity verification for every user and device trying to access resources on a network, regardless of whether they are sitting **within** or **outside** of the network **perimeter**.

Zero trust is a holistic approach to network security that incorporates several different principles and implementations. We will discuss the zero trust concept and how to implement it in your enterprise.

Zero Trusting Your Enterprise

A Technical Implementation Guide

By : Abdulrahman Al-Nimari, CISSP, CISM, CCISO, PMP, GCIH, GCIA, GREM, GCUX, GSEC
29, Aug., 2020

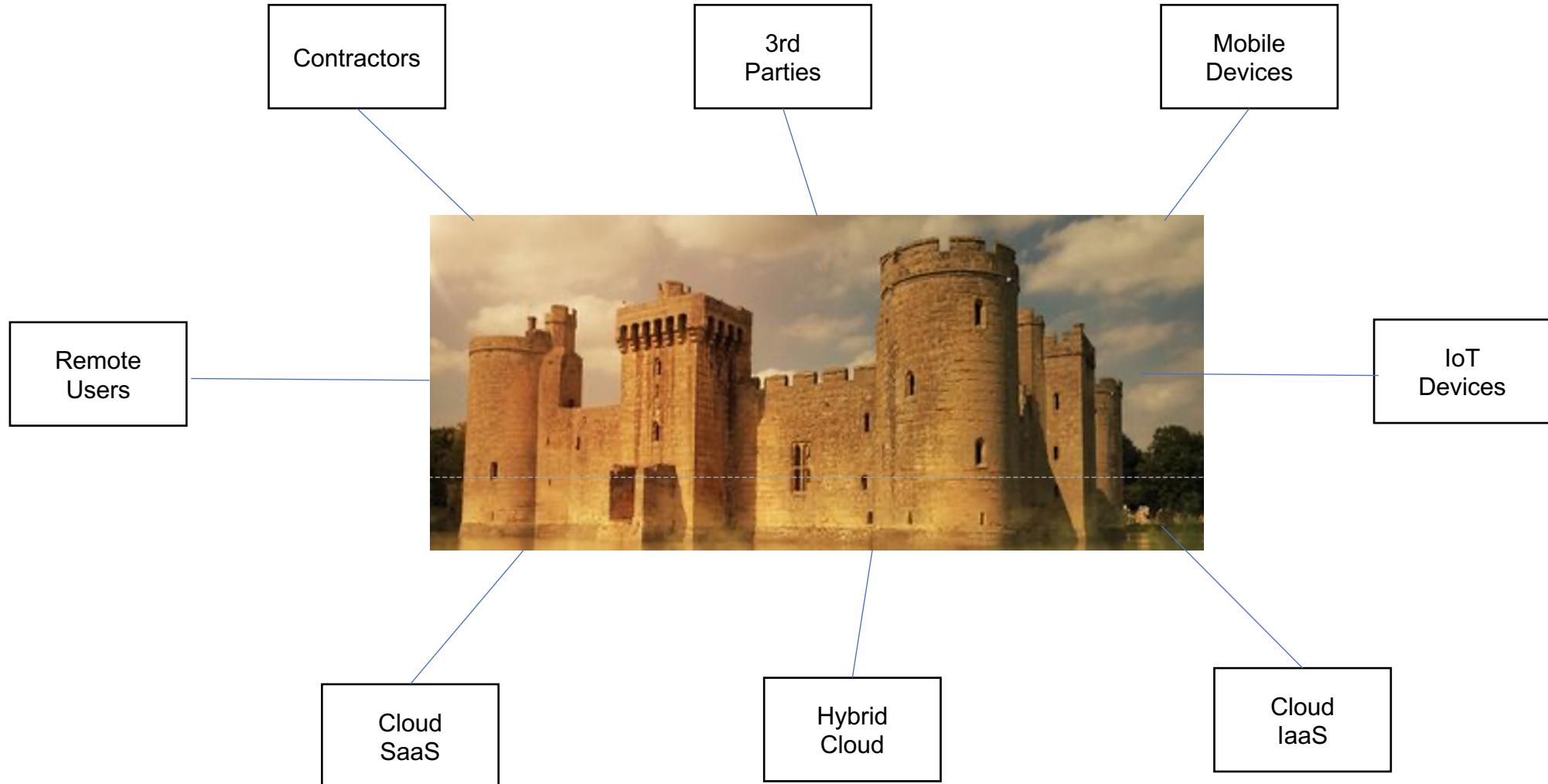
- ✓ Abdulrahman Al-Nimari
- ✓ Cyber Security Director, Architect, Consultant
- ✓ 25 Years IT & Cyber Security Experience
- ✓ Speaker : BSides, HITB, ICSC, AECT, ASC, MENAISC
- ✓ Awarded Arab Cybersecurity Social Network Influencer Prize 2019
- ✓ CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GREM, GSEC
- ✓  [@nimari](https://twitter.com/nimari)
- ✓  <https://www.linkedin.com/in/alnimari/>
- ✓  alnimari@gmail.com
- ✓  +966 (566) 465270

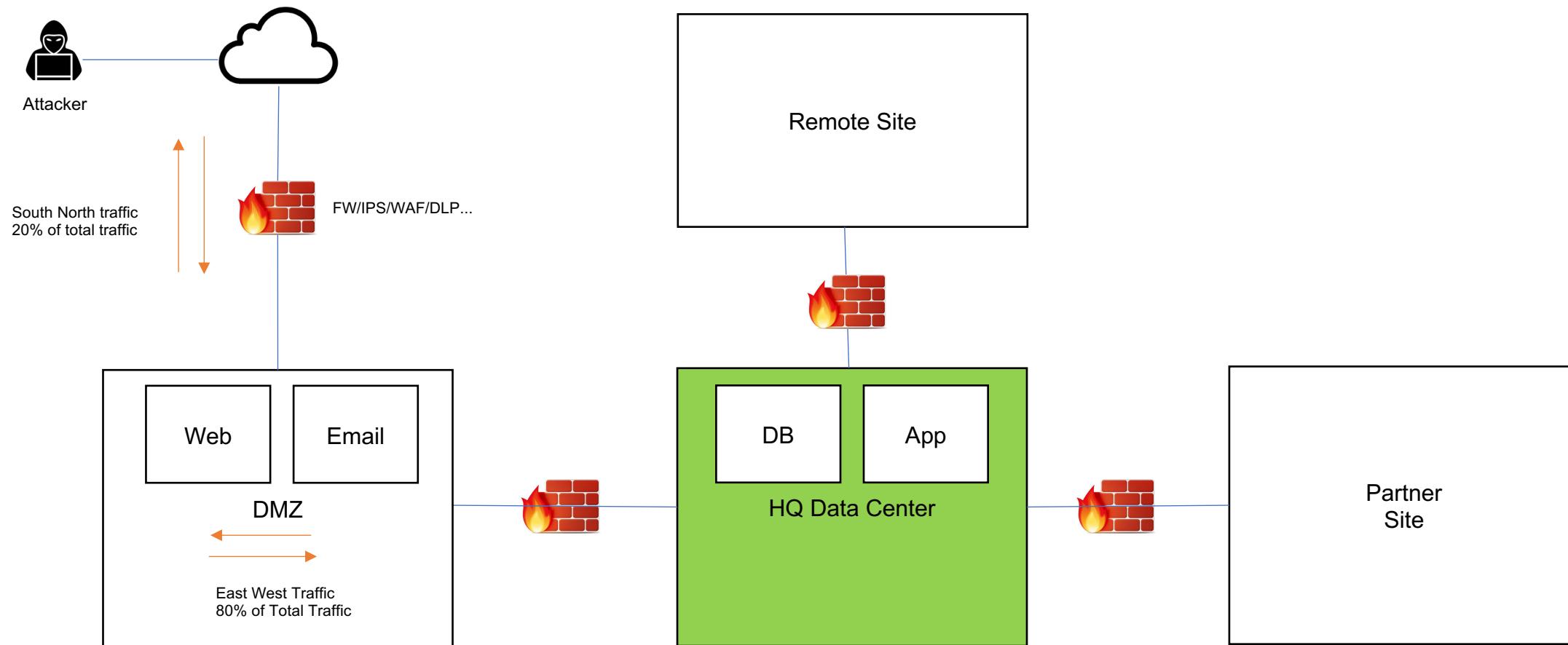


- ✓ Traditional Network Security
- ✓ What is bad about traditional approach?
- ✓ What is Zero Trust ?
- ✓ Zero Trust Building Blocks
- ✓ Steps To Zero Trust
- ✓ 'Plugging in' Zero Trust
- ✓ Resources

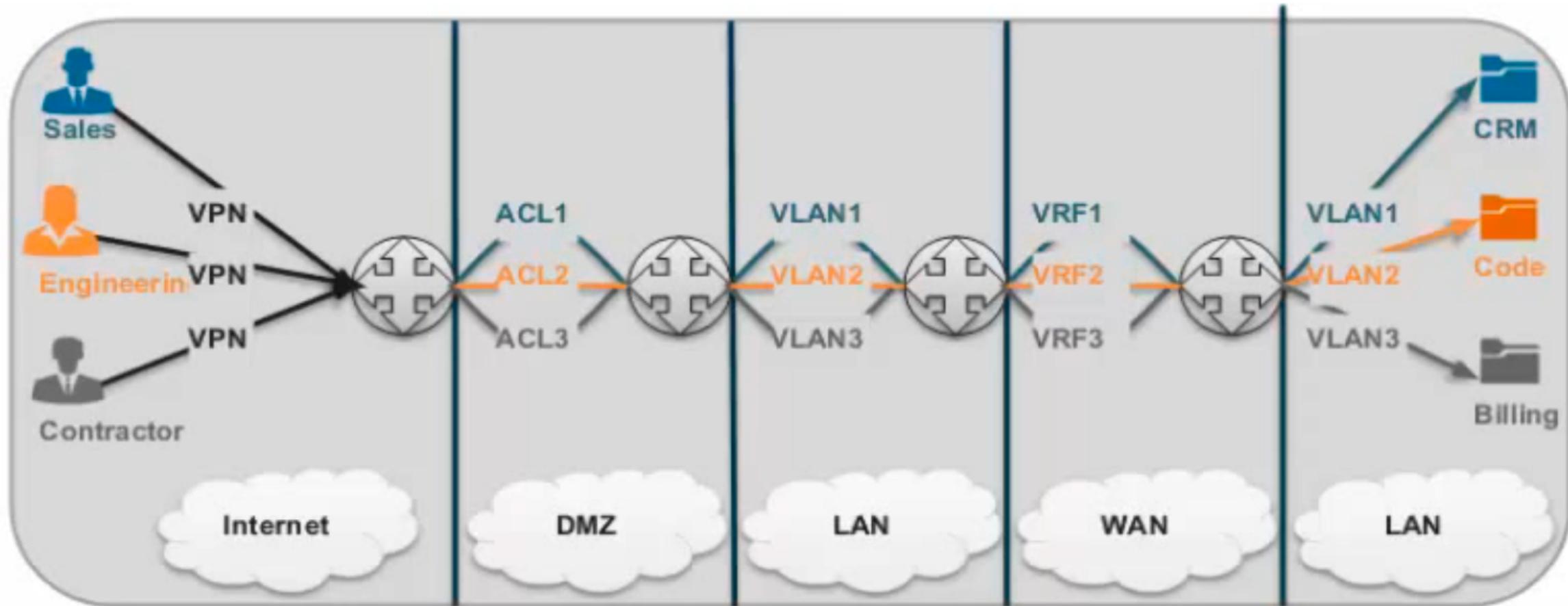








40 million credit card breached via HVAC system

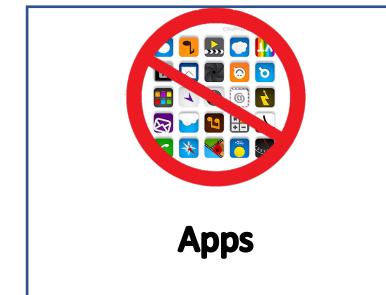
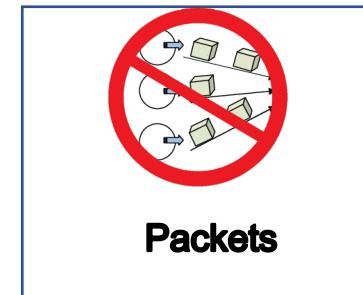


- ✓ **The Big Issue** : Internal Access is Trusted by Default
 - ✓ Laterla Movement is Possible
 - ✓ Pivoting is Possible
- ✓ Insider Threat not Considered

The Solution is to Implement Zero Trust

- ✓ It is a concept, NOT a technology or a device
- ✓ The concept : Do not trust anything, verify everything
- ✓ 'Zero Trust' term was coined by John Kindervag in 2010
- ✓ Buzzword nowadays, a game changer in Network Security
- ✓ Different Names : ZeroTrust, Perimeterless, BeyondCorp

In Zero Trust Model, **Data** becomes the New **Perimeter**



No Trust Assumed, Default **DENY ALL** Policy

What Do I Need To Zero Trust ?

- ✓ Identity Management
 - ✓ Users
 - ✓ Devices
- ✓ Network Segmentation. Segment as **granular** as needed
- ✓ Data Flow – Who is talking to Who ?

- ✓ Identify Zero Trust Scope (Could be implemented partially)
- ✓ Identify **Data Flows** (Who is talking to who ?)
- ✓ **Segment** Network as granular as needed
- ✓ Create **Access Control** Policy Based on Data Flows, User Roles
 - ✓ Need to Know
 - ✓ Least Privilege
- ✓ Architect Zero Trust Network
- ✓ Inspect, Log and Monitor Everything
- ✓ Automate and Orchestrate (Integrate tools to contain and mitigate)

- ✓ Flow Data Sources :
 - ✓ Log Files (Firewalls, Routers ..)
 - ✓ PCAP Data (packet header to reserve space)
 - ✓ NetFlow Data



```
rwfilter --type=all --pass=stdout --proto=0-255 --daddr=192.168.1.173 --packets=4 --ack-flag=1 | rwstats --count 20 --fields=sip,dip,sport,dport,proto
```

sIP	dIP	sPort	dPort	proto
52.109.88.76	192.168.1.173	443	64635	6
52.21.178.134	192.168.1.173	80	64476	6
52.21.178.134	192.168.1.173	80	64474	6
13.227.10.5	192.168.1.173	80	64481	6
172.217.19.10	192.168.1.173	443	64436	6
216.58.208.234	192.168.1.173	443	64412	6
149.154.164.250	192.168.1.173	80	64451	6
52.21.178.134	192.168.1.173	80	64475	6
3.235.72.247	192.168.1.173	443	64602	6
149.154.167.91	192.168.1.173	80	64591	6
89.44.169.132	192.168.1.173	80	64546	6

<https://tools.netsa.cert.org/silk/>



S	Segment	Subnet	Location
1	APP-1	192.168.1.0/24	Data Center
2	Email	192.168.2.0/24	
3	APP-2	192.168.3.10/32	
4	Finance	192.168.4.0/24	
5	HTTP	192.168.5.0/24	
6	ERP	192.168.6.0/24	
7	HR-1	10.0.0.0/24	HR Dept
8	HR-2	10.0.1.0/24	
9	Sales-1	10.0.10.0/24	Sales Dept
10	Sales-2	10.0.11.0/24	
11	R&D	10.0.20.0/24	R&D
..

Segment as **granular** as needed

	App1	Email	APP-2	Finance	HTTP	ERP	HR-1	HR-2	Sales-1	Sales-2	R&D
APP-1		25		22,443	80,443	675	22	3306	1433	21	
Email	25			25,22	80,443	1433	25	2525	2121	4434	
APP-2											443
Finance	80	25			80	443	80	8080	22	443	
HTTP	80	deny		25		432	22,25			1520	
ERP	443	deny		22	80		25	2525	1433	3500	
HR-1	443	25		21	443	2521		3006	5252	8082	
HR-2	443	21		3306	443	80	8081		141	25	
Sales-1	8080	25		8080	22	80	22	443		1433	
Sales-2	443	25		80	22				443		
R&D	2121	2525	443	1433							

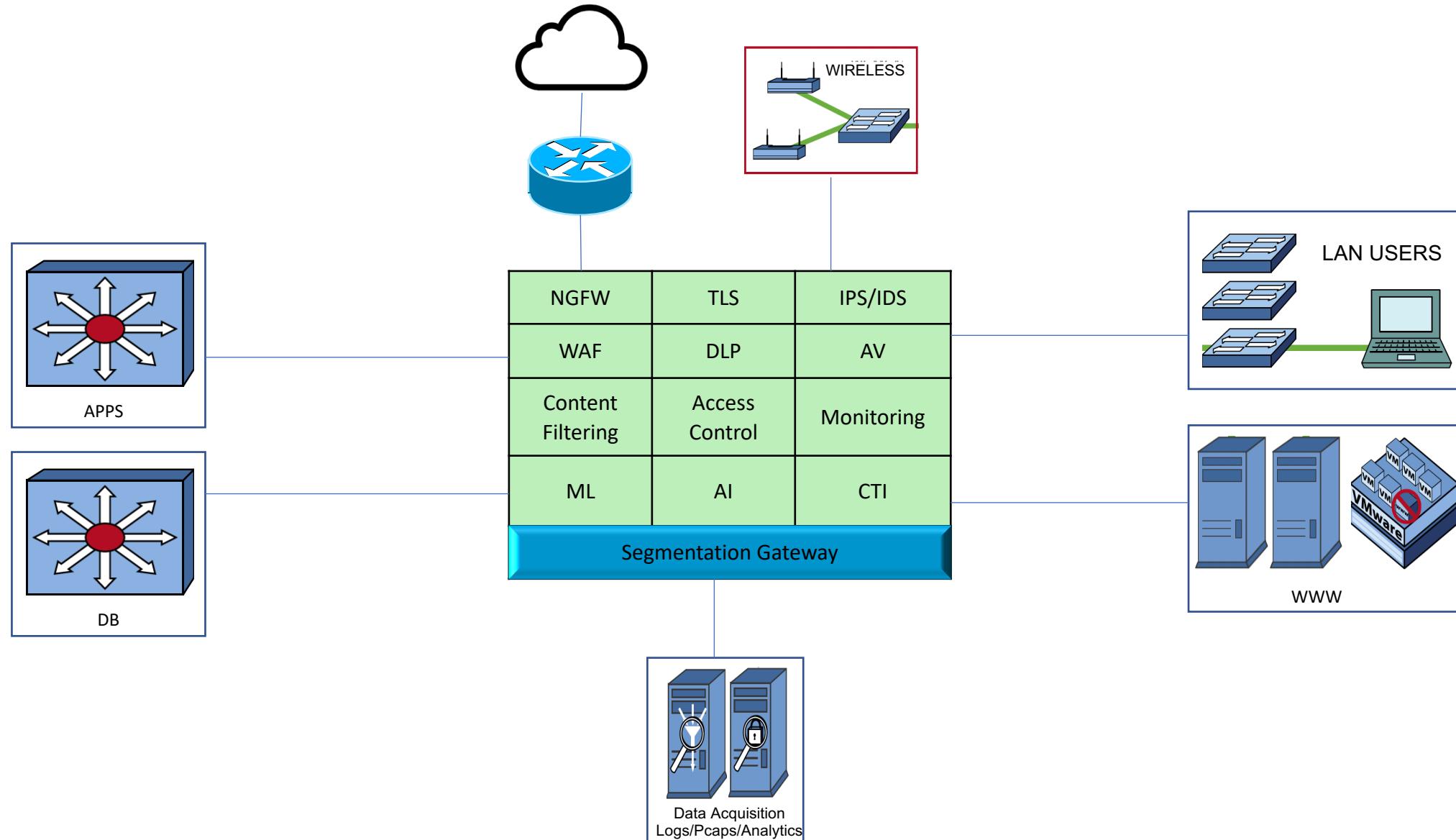
No Access

Firewall Rules

Src	Dst	Service/Port	Policy	Notes
192.168.1.0/24	192.168.2.0/24	25	Allow	
192.168.3.10	10.0.20.0/24	443	Allow	
192.168.4.0/24	192.168.1.0/24	80	Allow	
...	
Any	Any	Any	Log	

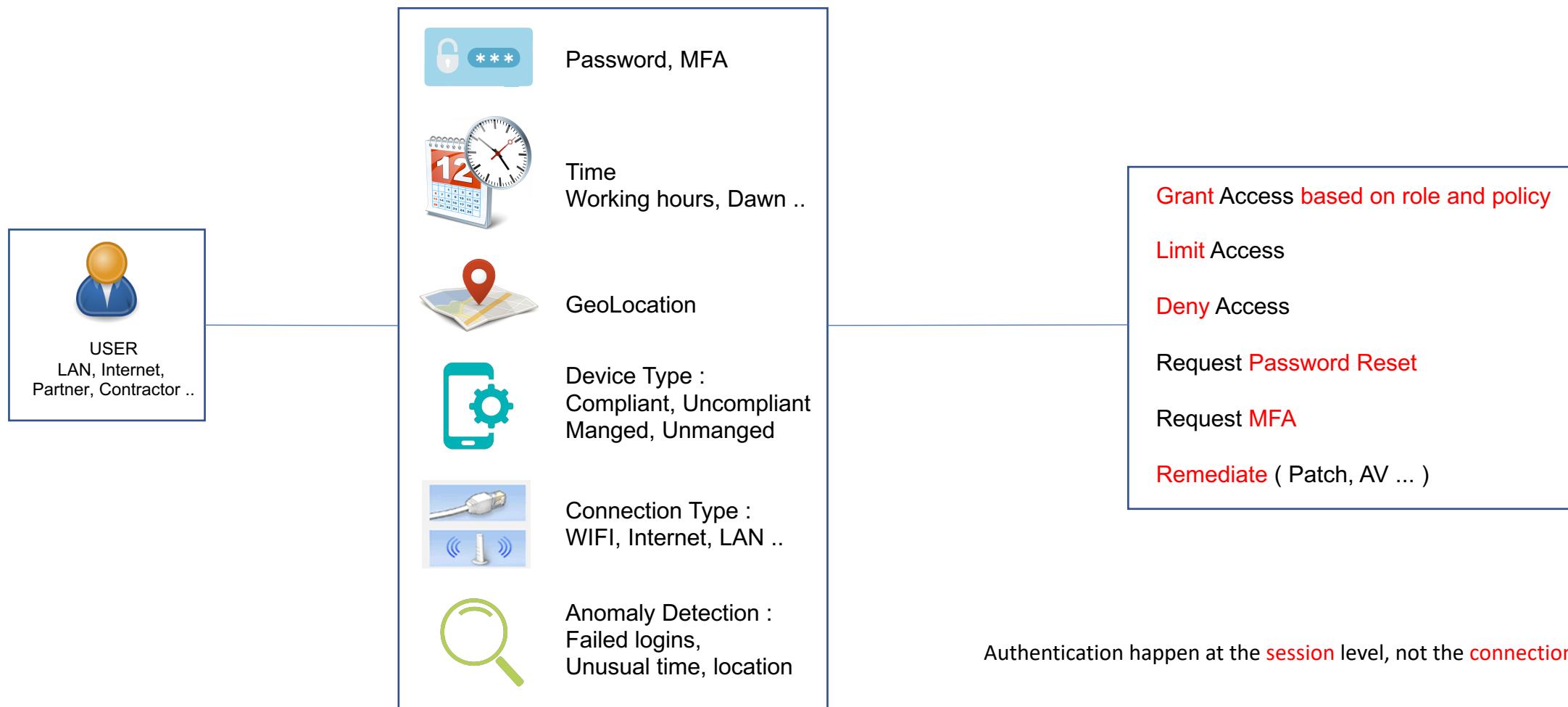
Allow Business Traffic -> LOG Other Traffic -> Revise Logs -> Update Rules

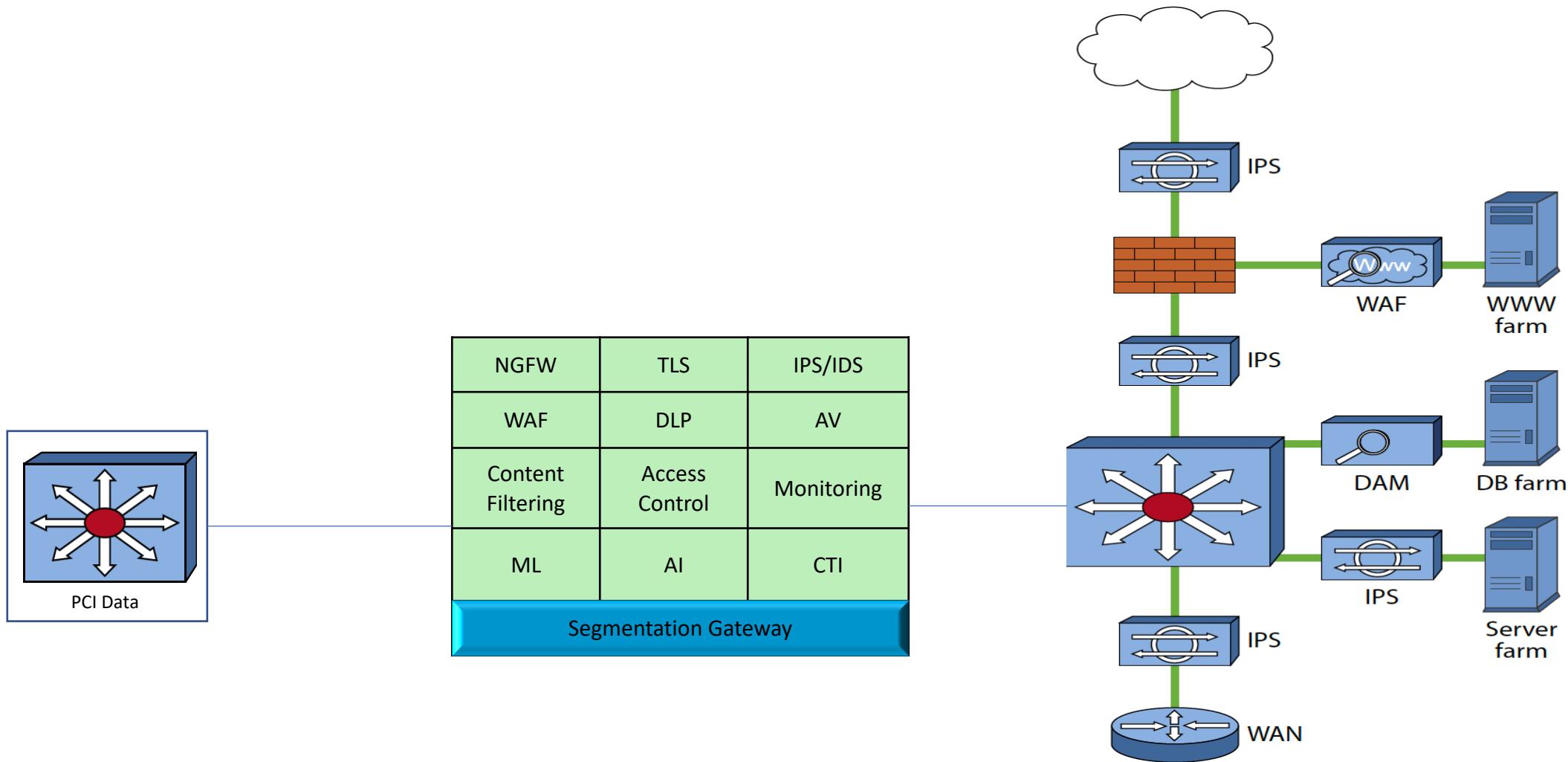
Keep on **LOGGING** and **REVISING** logged traffic until you are ready to **DENY**



Graphics Portions By Forrester Research, Inc.

Dynamic, Variable, Adaptive Trust





NIST SP 800-207, August 2020

<https://csrc.nist.gov/publications/detail/sp/800-207/final>

Useful Zero Trust resources on github

<https://github.com/pomerium/awesome-zero-trust>

Pritunl Zero, Free Open Source SSH and Web ZT

<https://zero.pritunl.com/>

Infection Monkey – Zero Trust Assessment

<https://www.guardicore.com/infectionmonkey/zero-trust.html>

سُبْحَانَكَ اللَّهُمَّ وَ بِحَمْدِكَ
أَشْهُدُ أَنْ لَا إِلَهَ إِلَّا أَنْتَ
أَسْتَغْفِرُكَ وَ أَتُوْبُ إِلَيْكَ