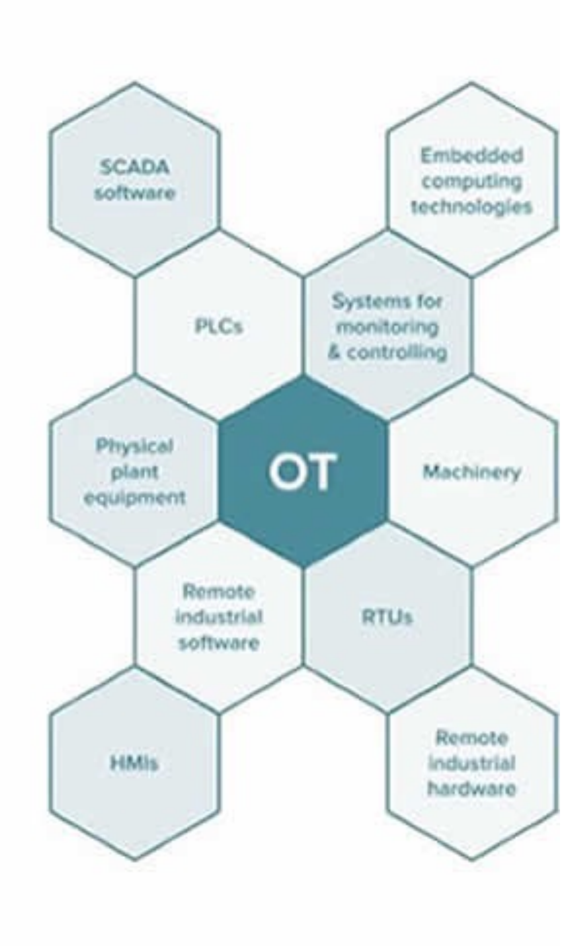
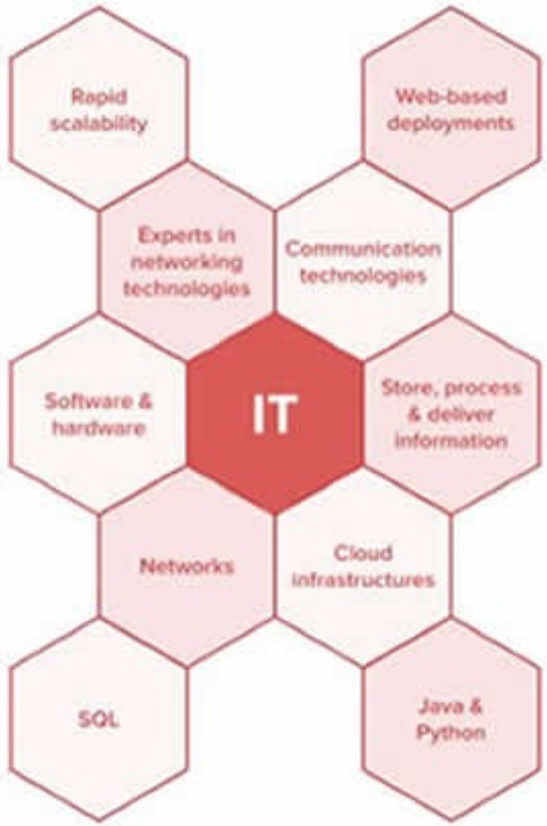
DEFENDING OPERATIONAL TECHNOLOGY (OT) NETWORKS WITH SECURE SD-WAN

JORDAN & YUAN

INTRODUCTION

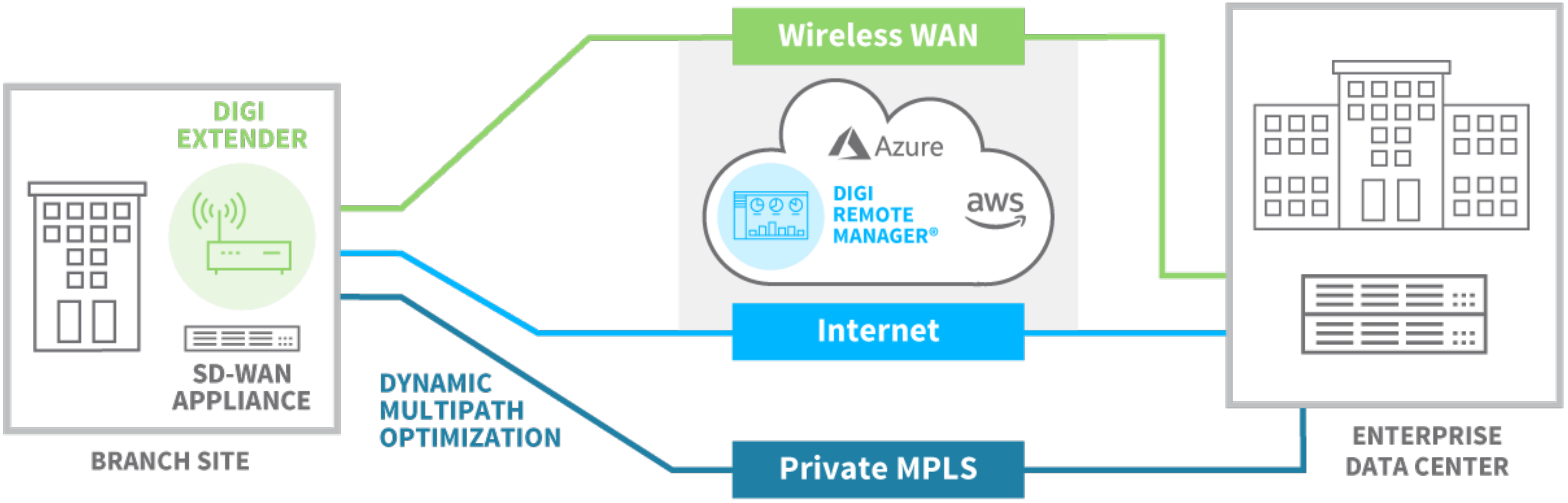

SCADA software
Embedded computing technologies
PLCs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
HMIs
Remote industrial hardware

- Attacks against critical infrastructure and operational technology (OT) systems is constantly increasing
- Multifactorial causes, but can be largely attributed to the natural evolution of business processes
- The result is formerly isolated OT being susceptible to cyber attacks that currently plague IT networks
- Critical OT Technologies:
  - Nuclear Power Plants
  - Oil and Gas Pipelines
  - Fire Control Systems
  - Hydroelectric Dams



SD-WAN

- Software-defined wide area networking system that is a software-defined approach to managing the wide-area network (WAN)
- Allows secure, private connectivity to applications
- Leverages any combination of transport services including LTE, MPLS, and 5G
- Accelerates traffic flow and improves communication

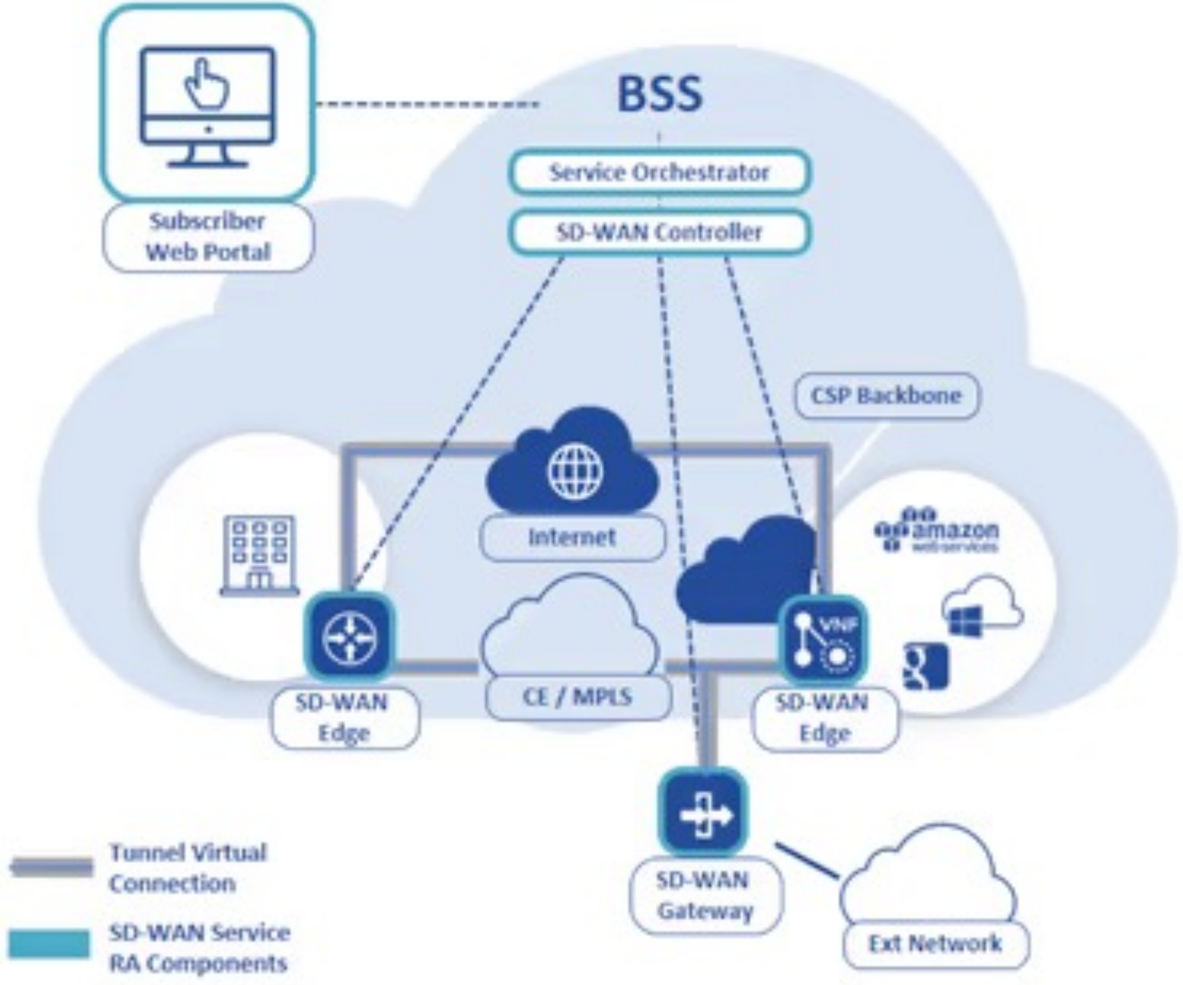


FRAMEWORK/ARCHITECTURE

- Many forms of SD-WAN, but all architectures include:
  - Controller function (pushing out policies & distributing routing info)
  - Virtual Overlay
    - Describes how SD-WAN sits above the network
    - Enables IT to remotely configure, monitor, and secure most aspects of WAN
  - Management console (reporting and policy configurations)
- Centralizes network control by abstracting and automating tasks traditionally programmed manually on each edge device
- Abstraction of transport layer from hardware to software → more elastic network

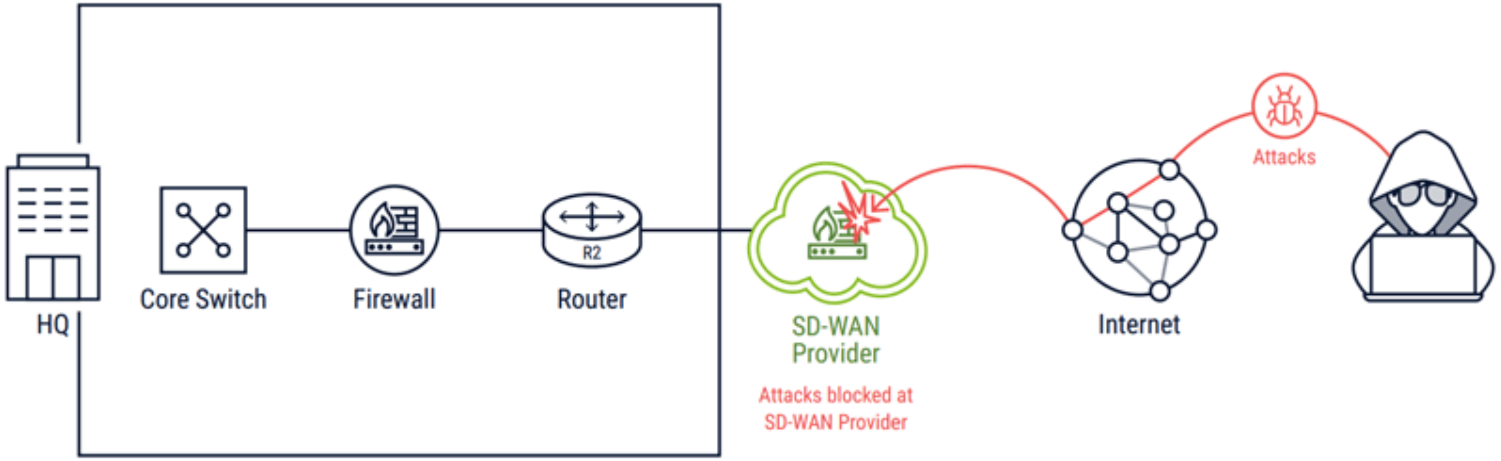
EDGE APPLIANCES ARCHITECTURE

- Virtual overlay stretches from location to location
- Appliances installed at each site → retrieves configuration profiles from the SD-WAN controller
- SD-WAN devices configure themselves and join/construct virtual overlay with the other devices
- Each device runs policy-based routing algorithms that steer traffic to the most appropriate link

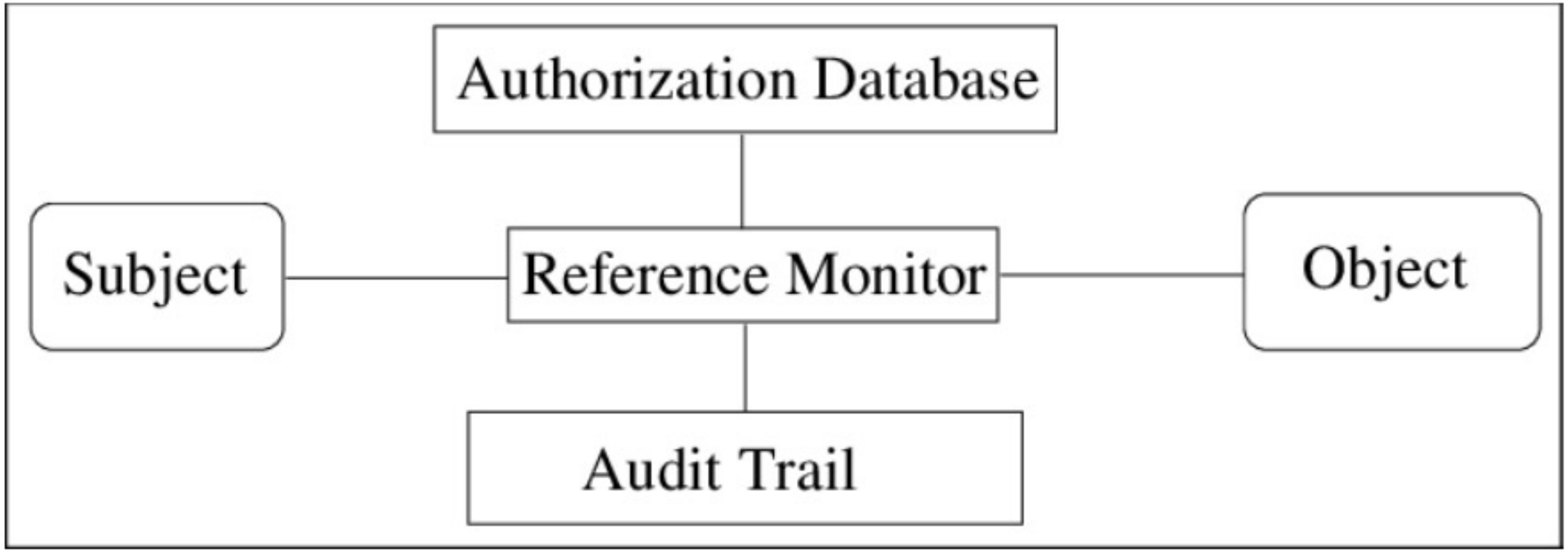


SECURITY BENEFITS

- Security is centralized and scalable
  - The SD-WAN controller can create and distribute security policies for the entire organization that can be enforced and maintained centrally
  - Suspicious activity will automatically be redirected and reported to admins
- Zero-touch provisioning: Method to automatically configure devices quickly to deploy at a new remote location
  - Advantage: Policies automatically distributed to all devices connected to SD-WAN
- Encrypted overlay network → Encrypts traffic over entire network
- Other advanced security services can be implemented on top of it

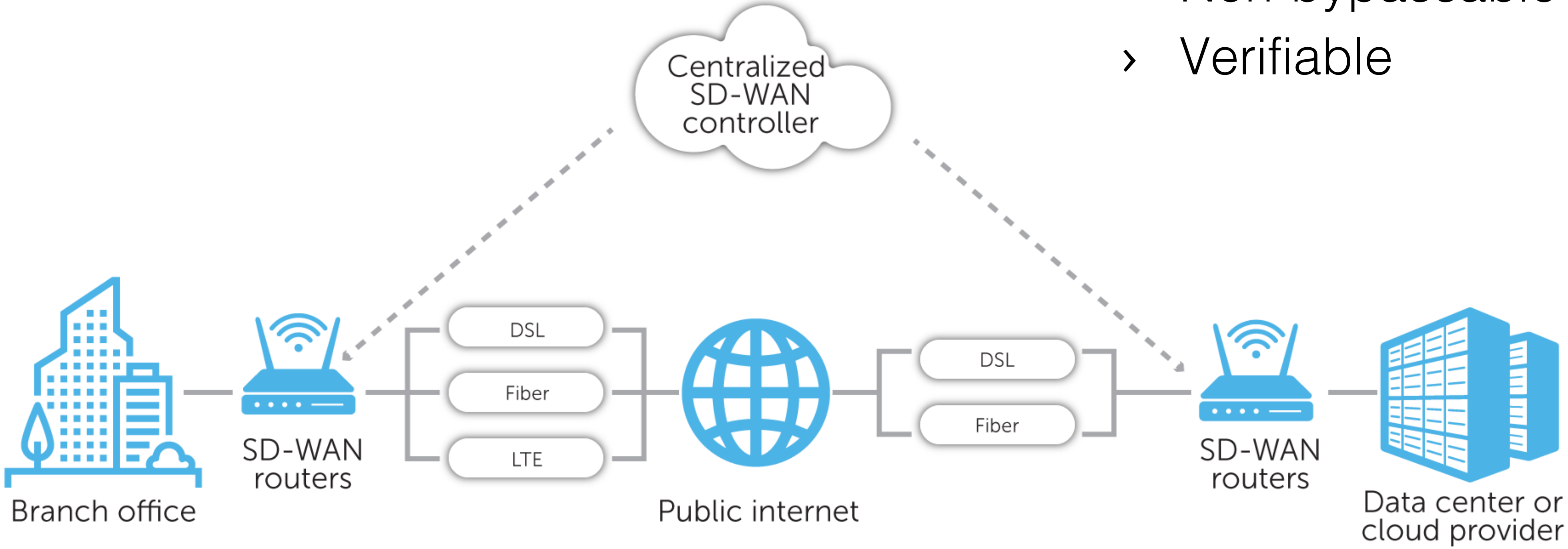


REFERENCE MONITOR



Element	Item
Subjects	The user such as the remote sites in the network.
Objects	Services or data in data center.
Authorization database	SD-WAN manager will store all the information of the remote site. Only the remote site with right token can permission connect to the SD-WAN network. Those sites will store as a record in database.
Audit trail	Only record the recently security-relevant event.

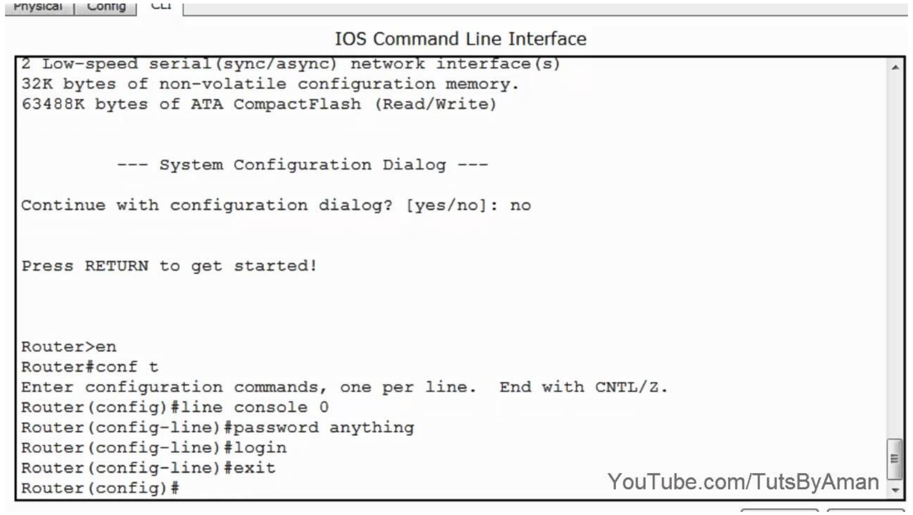
- Tamperproof
- Non-bypassable
- Verifiable



ADVANTAGES

- High performance with low cost
- Simple infrastructure and centralized control
- Line Rate Detection such as SLA finds the optimal line guaranteed transfer speed
- Protect data druing transformation with end-to-end encryption (E2EE)

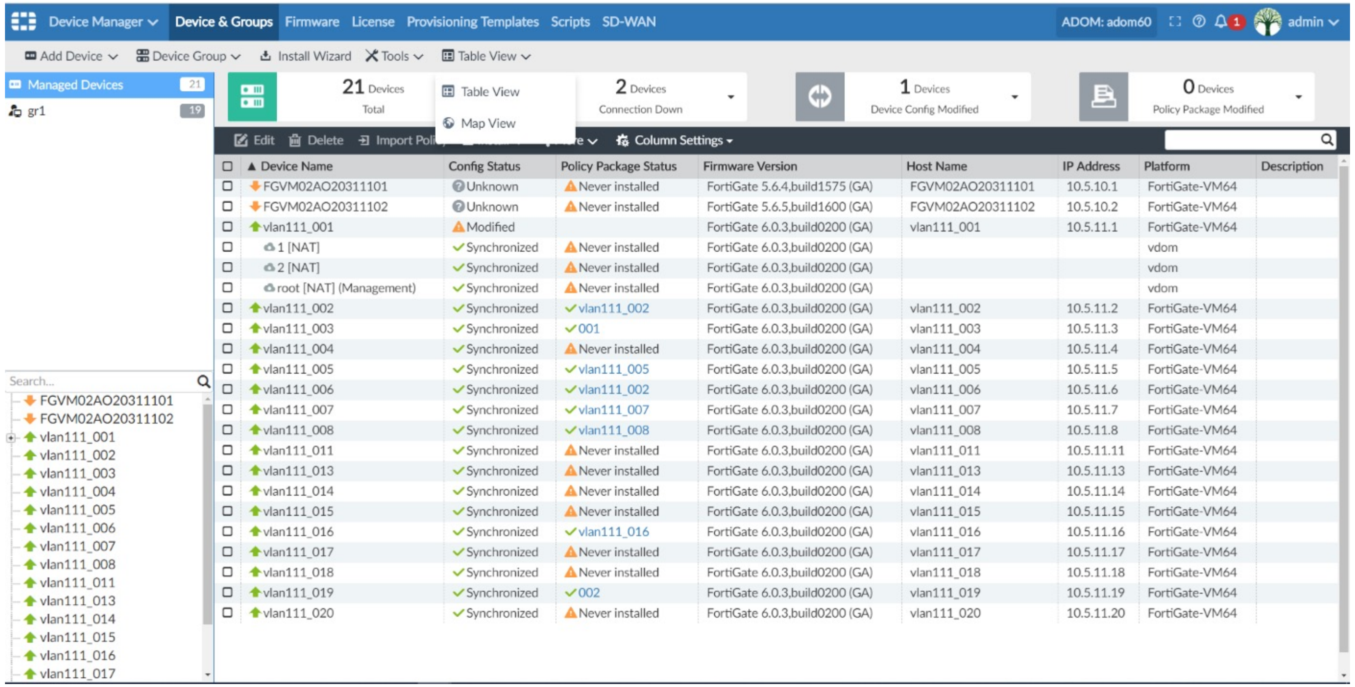
EXAMPLE: ADD NEW SITE IN TRADITIONAL WAN



IOS Command Line Interface

```
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password anything
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

EXAMPLE: ADD NEW SITE IN SD-WAN (ZERO TOUCH)



☐	▲ Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
☐	FGVM02AO20311101	Unknown	Never installed	FortiGate 5.6.4,build1575 (GA)	FGVM02AO20311101	10.5.10.1	FortiGate-VM64	
☐	FGVM02AO20311102	Unknown	Never installed	FortiGate 5.6.5,build1600 (GA)	FGVM02AO20311102	10.5.10.2	FortiGate-VM64	
☐	vlan111_001	Modified		FortiGate 6.0.3,build0200 (GA)	vlan111_001	10.5.11.1	FortiGate-VM64	
☐	1 [NAT]	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)			vdom	
☐	2 [NAT]	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)			vdom	
☐	root [NAT] (Management)	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)			vdom	
☐	vlan111_002	✓ Synchronized	✓ vlan111_002	FortiGate 6.0.3,build0200 (GA)	vlan111_002	10.5.11.2	FortiGate-VM64	
☐	vlan111_003	✓ Synchronized	✓ 001	FortiGate 6.0.3,build0200 (GA)	vlan111_003	10.5.11.3	FortiGate-VM64	
☐	vlan111_004	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_004	10.5.11.4	FortiGate-VM64	
☐	vlan111_005	✓ Synchronized	✓ vlan111_005	FortiGate 6.0.3,build0200 (GA)	vlan111_005	10.5.11.5	FortiGate-VM64	
☐	vlan111_006	✓ Synchronized	✓ vlan111_002	FortiGate 6.0.3,build0200 (GA)	vlan111_006	10.5.11.6	FortiGate-VM64	
☐	vlan111_007	✓ Synchronized	✓ vlan111_007	FortiGate 6.0.3,build0200 (GA)	vlan111_007	10.5.11.7	FortiGate-VM64	
☐	vlan111_008	✓ Synchronized	✓ vlan111_008	FortiGate 6.0.3,build0200 (GA)	vlan111_008	10.5.11.8	FortiGate-VM64	
☐	vlan111_011	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_011	10.5.11.11	FortiGate-VM64	
☐	vlan111_013	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_013	10.5.11.13	FortiGate-VM64	
☐	vlan111_014	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_014	10.5.11.14	FortiGate-VM64	
☐	vlan111_015	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_015	10.5.11.15	FortiGate-VM64	
☐	vlan111_016	✓ Synchronized	✓ vlan111_016	FortiGate 6.0.3,build0200 (GA)	vlan111_016	10.5.11.16	FortiGate-VM64	
☐	vlan111_017	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_017	10.5.11.17	FortiGate-VM64	
☐	vlan111_018	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_018	10.5.11.18	FortiGate-VM64	
☐	vlan111_019	✓ Synchronized	✓ 002	FortiGate 6.0.3,build0200 (GA)	vlan111_019	10.5.11.19	FortiGate-VM64	
☐	vlan111_020	✓ Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_020	10.5.11.20	FortiGate-VM64	

FGVM02AO20311101
FGVM02AO20311102
vlan111_001
vlan111_002
vlan111_003
vlan111_004
vlan111_005
vlan111_006
vlan111_007
vlan111_008
vlan111_011
vlan111_013
vlan111_014
vlan111_015
vlan111_016
vlan111_017

LIMITATIONS

- The problem of lost packages still exists

- Although SD-WAN give user a high performance, the quality is still not good as MPLS. It is better using MPLS when sensitive to the quality such as IP voice or video stream

- Lack on-site security functions

- In most cases, they only provide an advantage when accessing cloud-based applications. They do not provide any on-site security functionality.

REFERENCE

- https://www.techtarget.com/searchnetworking/tip/What-SD-WAN-devices-do-I-need-in-an-SD-WAN-deployment
- https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/essentials-sd-wan-architecture/
- https://www.infinitylabs.in/blog/sd-wan-for-operational-technology-ot/#:~:text=SD%2DWAN%20comes%20across%20as,of%20ownership%2C%20and%20improves%20security.
- https://www.iiot-world.com/ics-security/cybersecurity/defending-ot-networks-with-secure-sd-wan/
- https://bluecatnetworks.com/blog/extend-sd-wan-benefits-with-enterprise-grade-dns/
- https://www.routexp.com/2019/01/sd-wan-vs-traditional-wan-architecture.html
- https://www.aryaka.com/blog/sd-wan-pros-cons-deployment-right/