OCTOBER 2023

Strategies For Getting Information From The Control Network

Elliott Middleton – Product Director - operations control

AVEVA

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Elliott Middleton

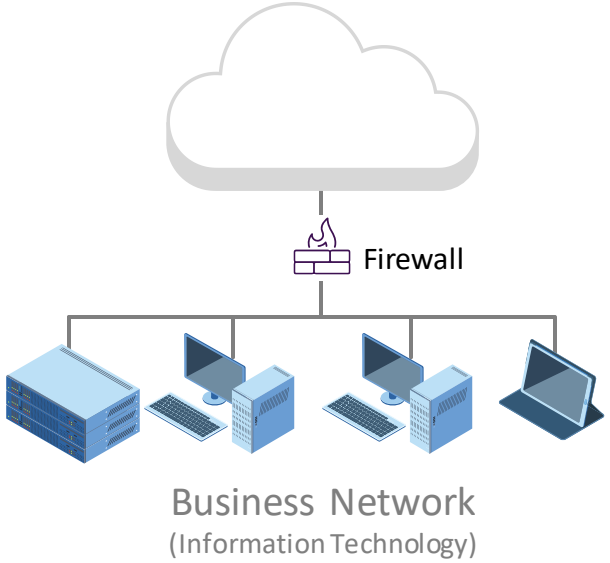
Product Director – operations control

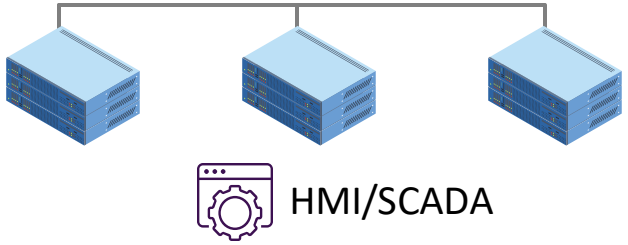
AVEVA

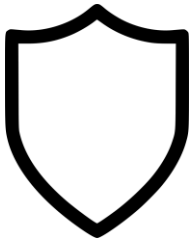
elliott.middleton@aveva.com

The Dilemma

Most of the Users







Safety Critical

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Reasons to Bridge Domains

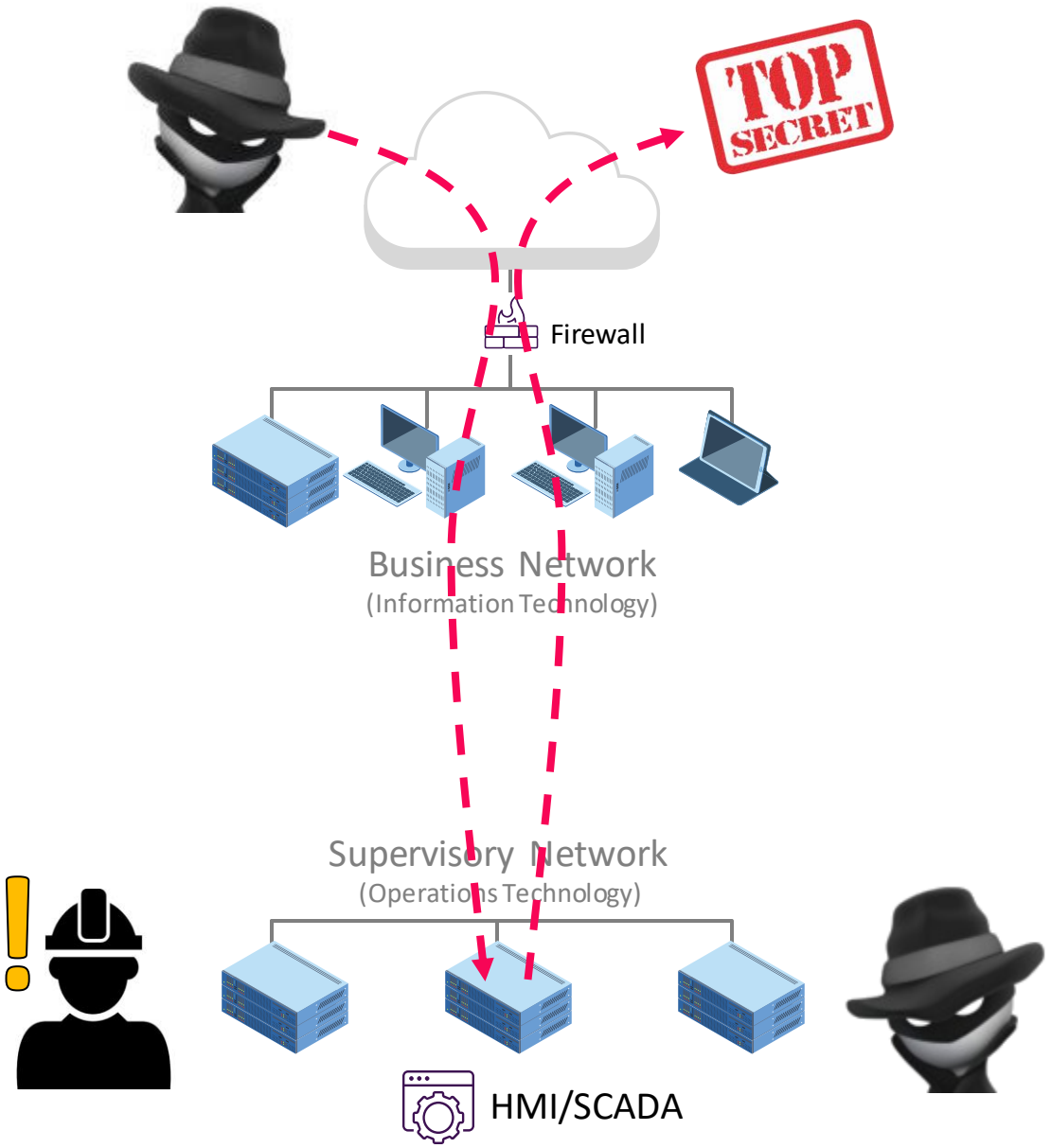
Make information more accessible

Fuel process improvement initiatives

Enable self-service analysis & reporting

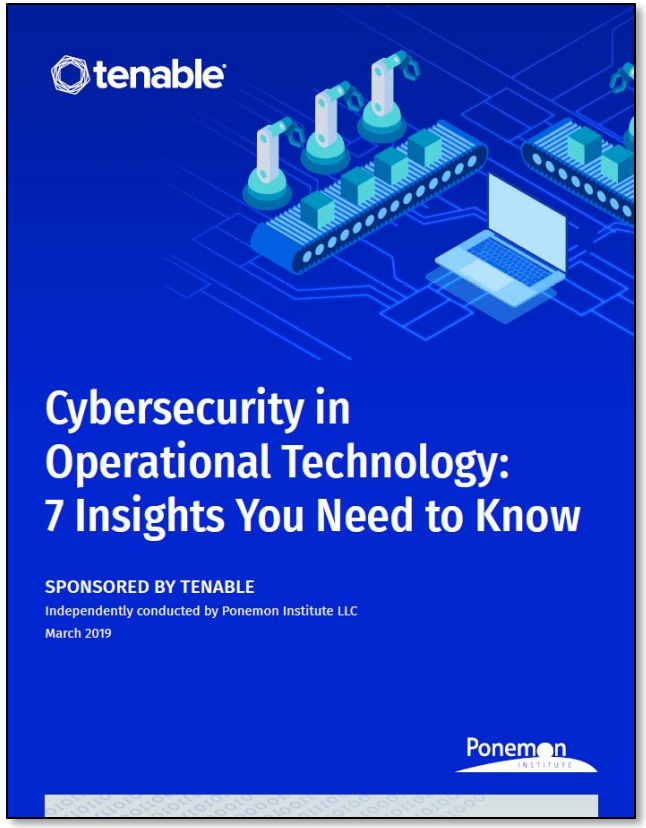
© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Threats



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Cybersecurity Threat



2019 Cybersecurity Survey

- Focused on operational technology (OT)
- At least one participant is an AVEVA Historian customer (Taiwan Semiconductor)
- 701 total participants

Highlights:

- ? experienced plant *downtime* in the last 24 months
- ? experienced a nation-state attack

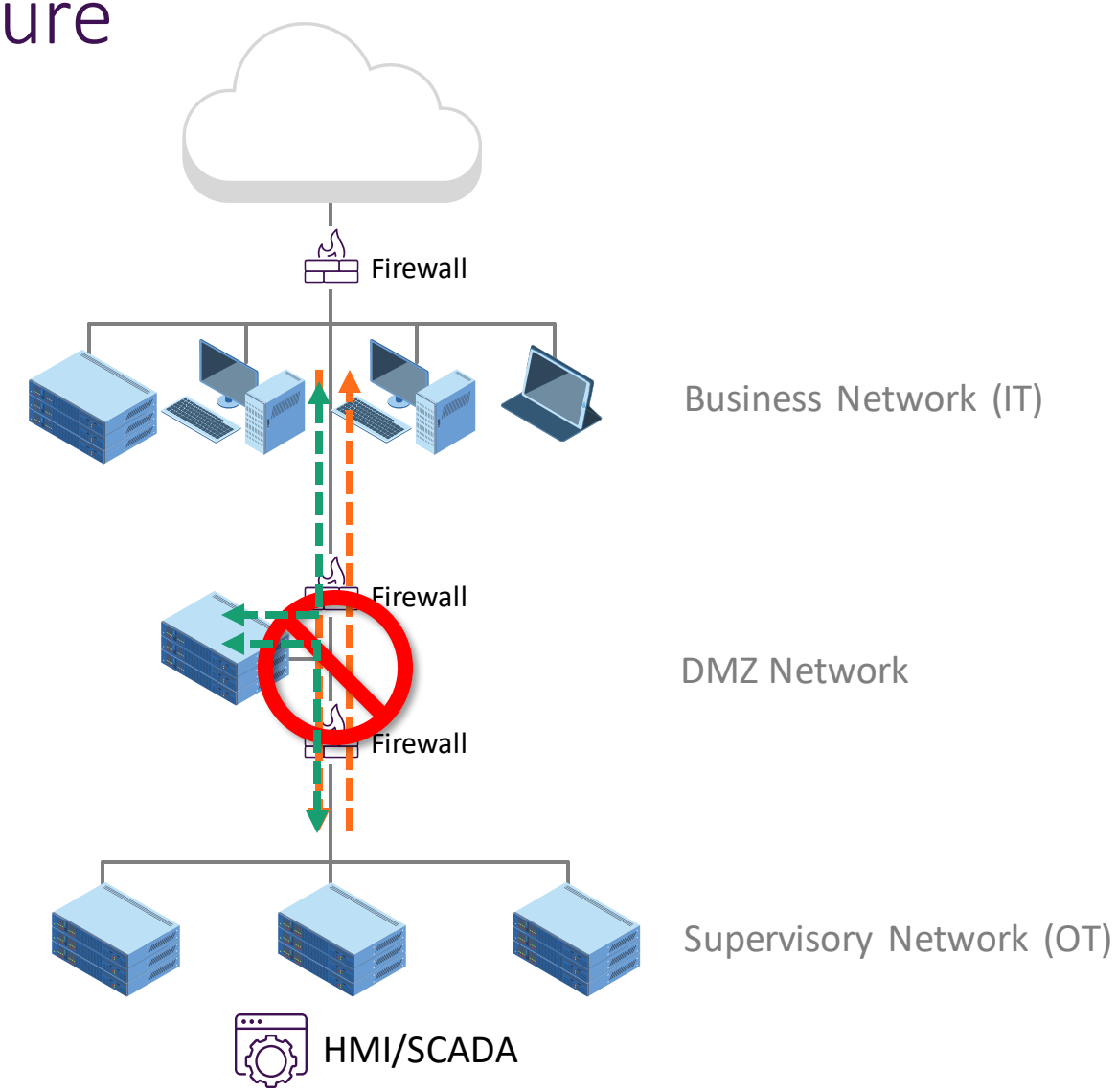
© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

AVEVA

Best Practice Architecture

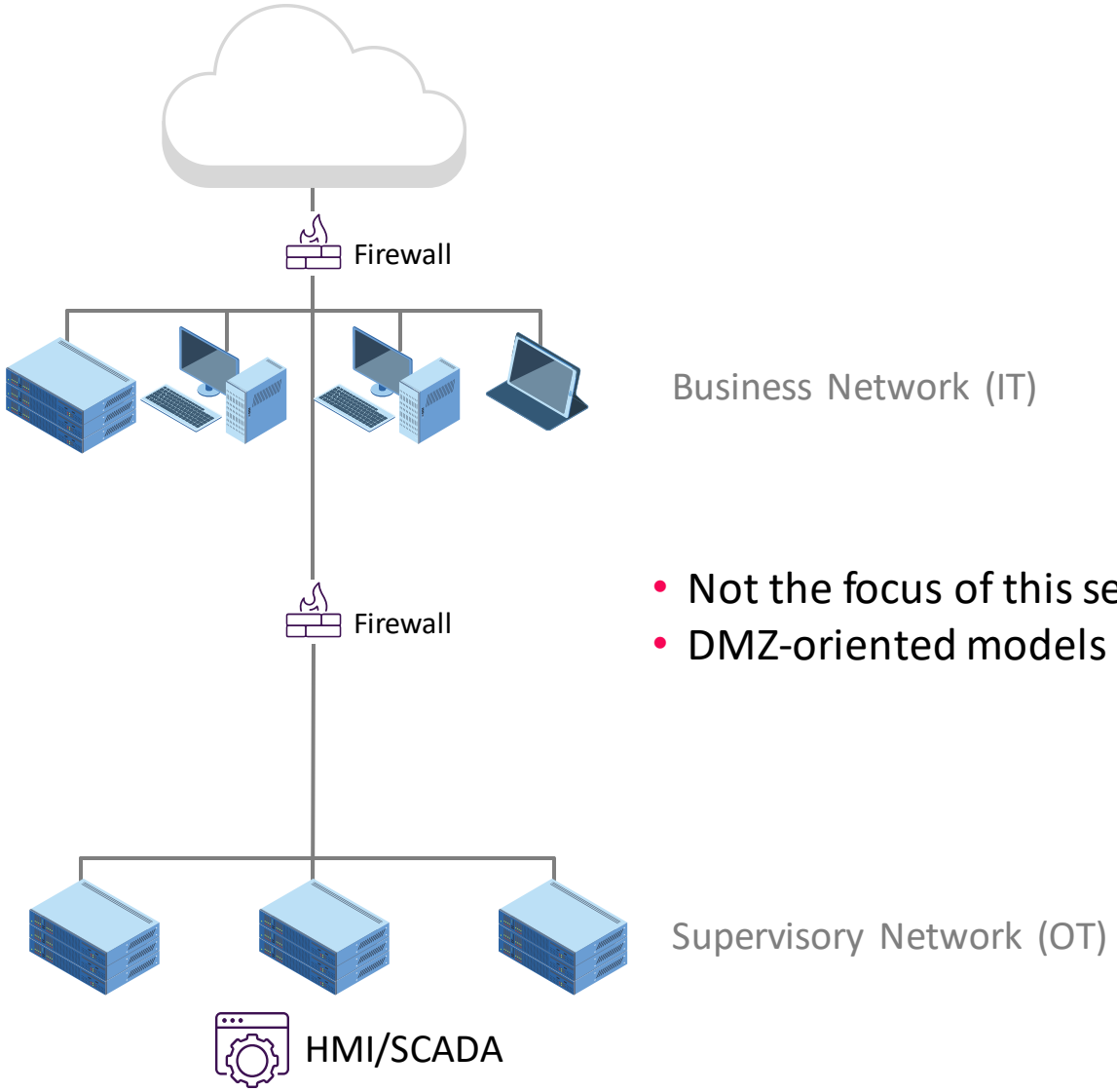
NERC-CIP
NIST

- No direct access between Supervisory/Business networks
- Only to adjacent network (DMZ)



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Common Architecture

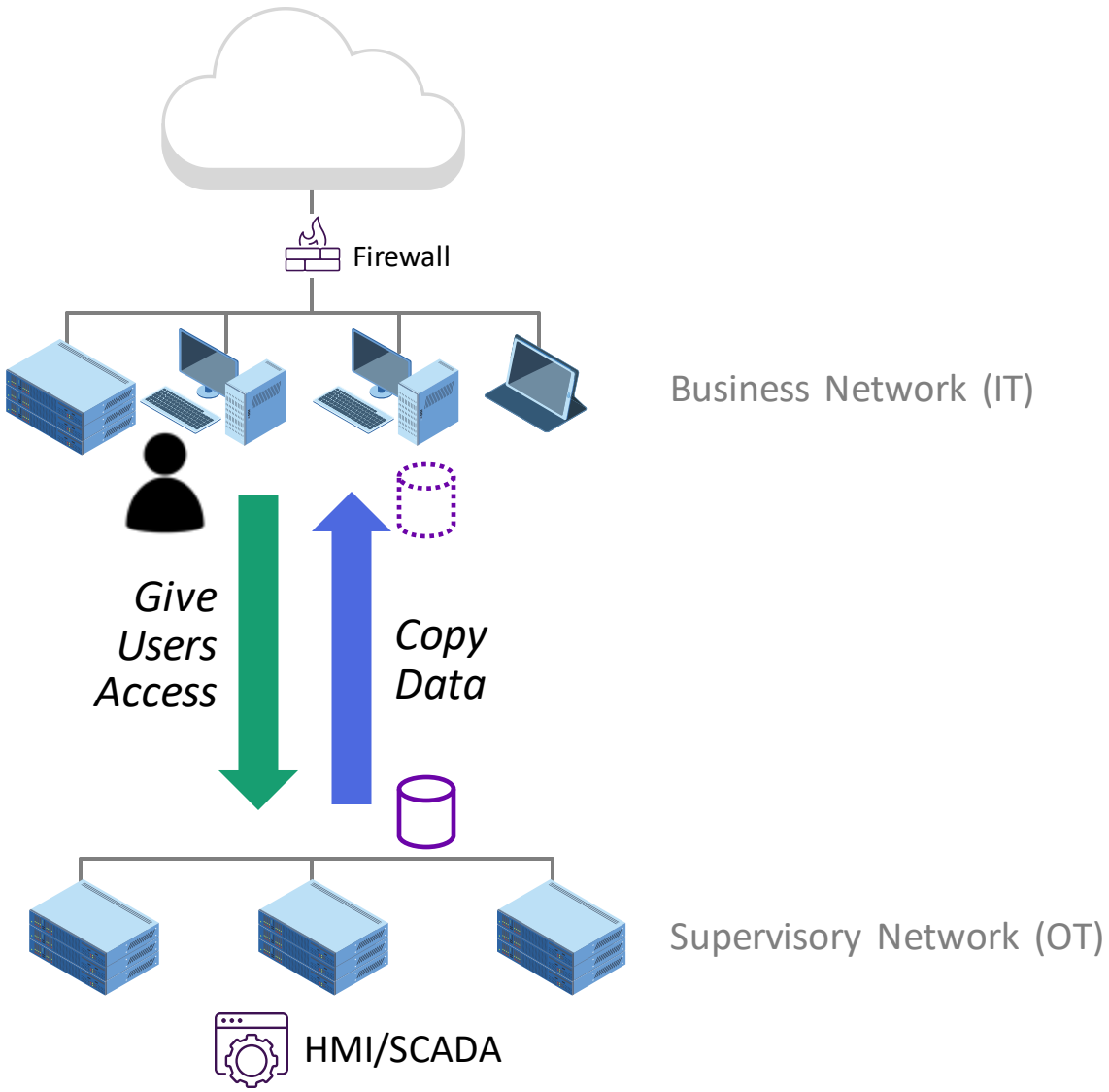


- Less isolation than dual firewalls
- Simpler to use & manage

- Not the focus of this session
- DMZ-oriented models can be adapted

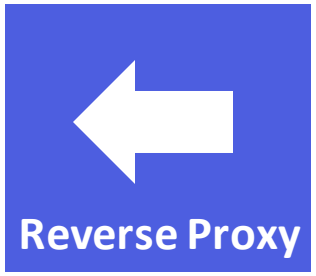
© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

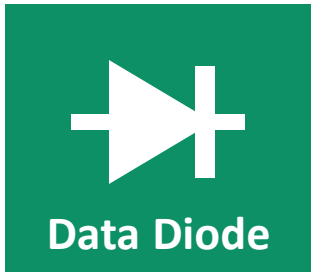
General Approaches



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Strategies to Bridge IT/OT

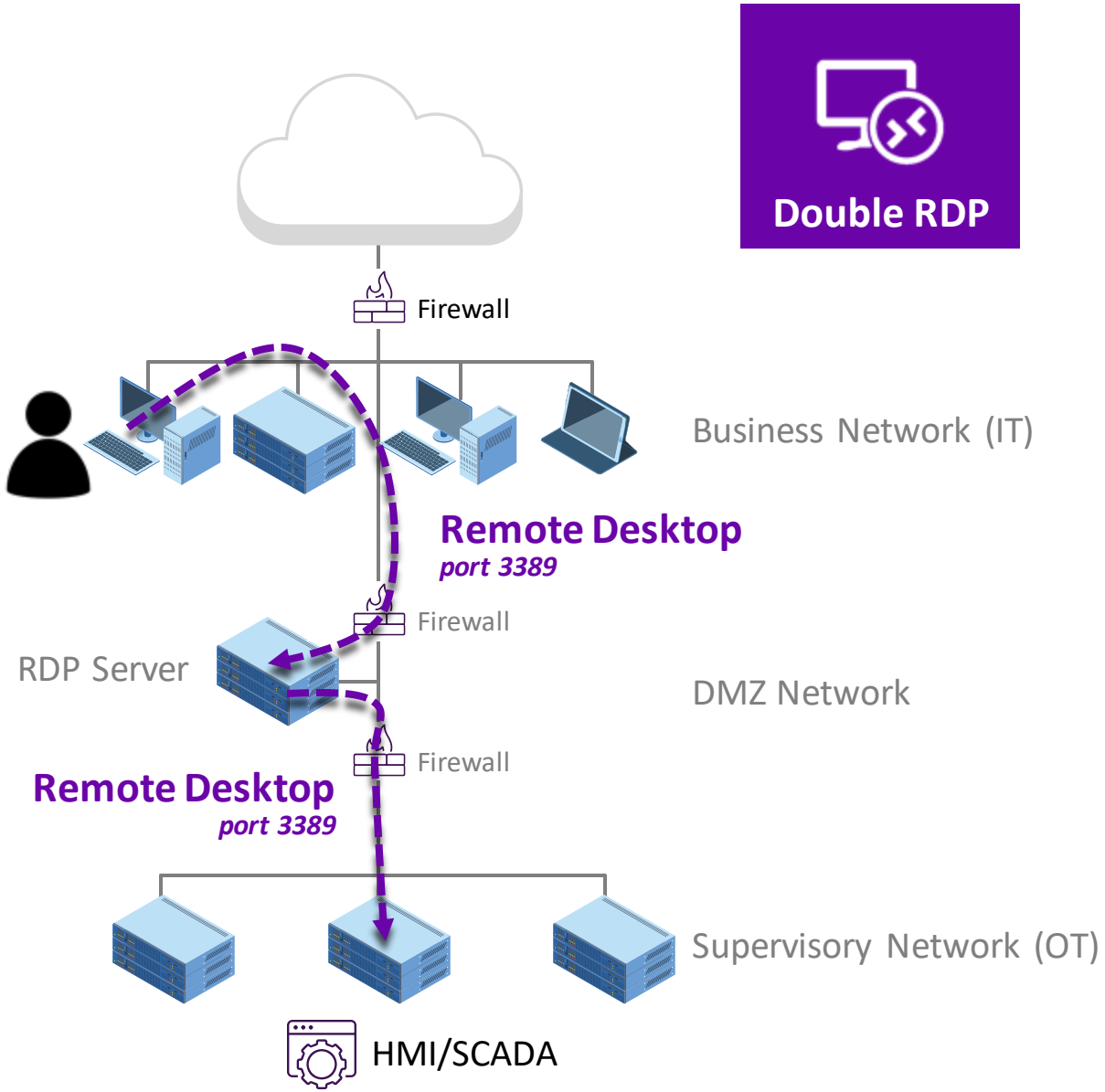




©2023 AVEVA Group plc and its subsidiaries. All rights reserved.

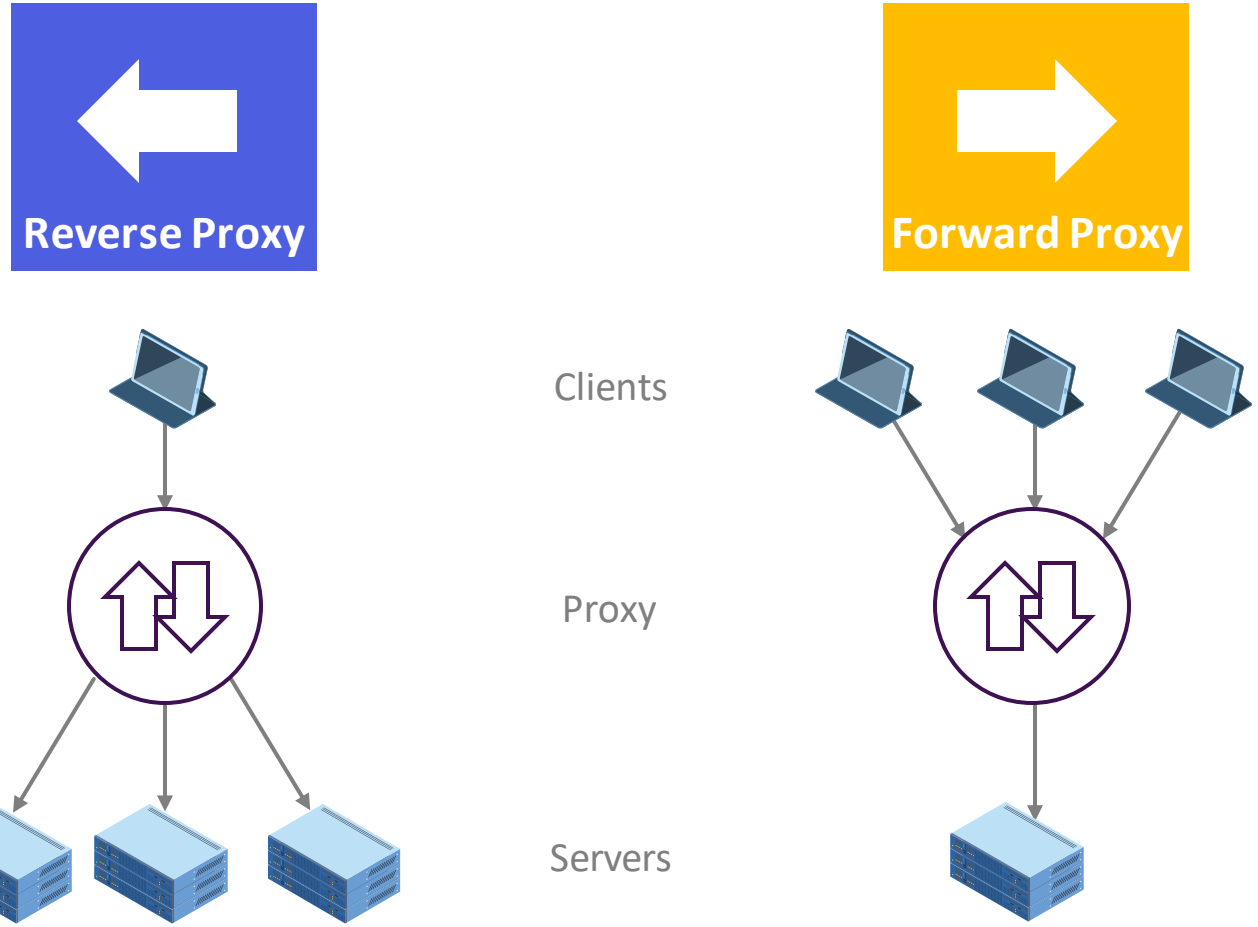
Double RDP

- Approach
  - RDP Server in DMZ
  - Open RDP to DMZ from IT network, to OT from DMZ
- Pros
  - Gives users access
  - Simple to define & manage
  - Secure protocol
- Cons
  - Requires inbound access to DMZ, OT
  - Multiple user logins to manage (2-3)
  - Only user access
  - Higher resource requirements than some options
  - Need care to restrict rights appropriately
- Example Threat: Compromised credentials, user error



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Web Proxies

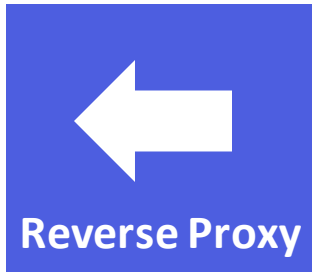


- In front of server
- Isolates servers

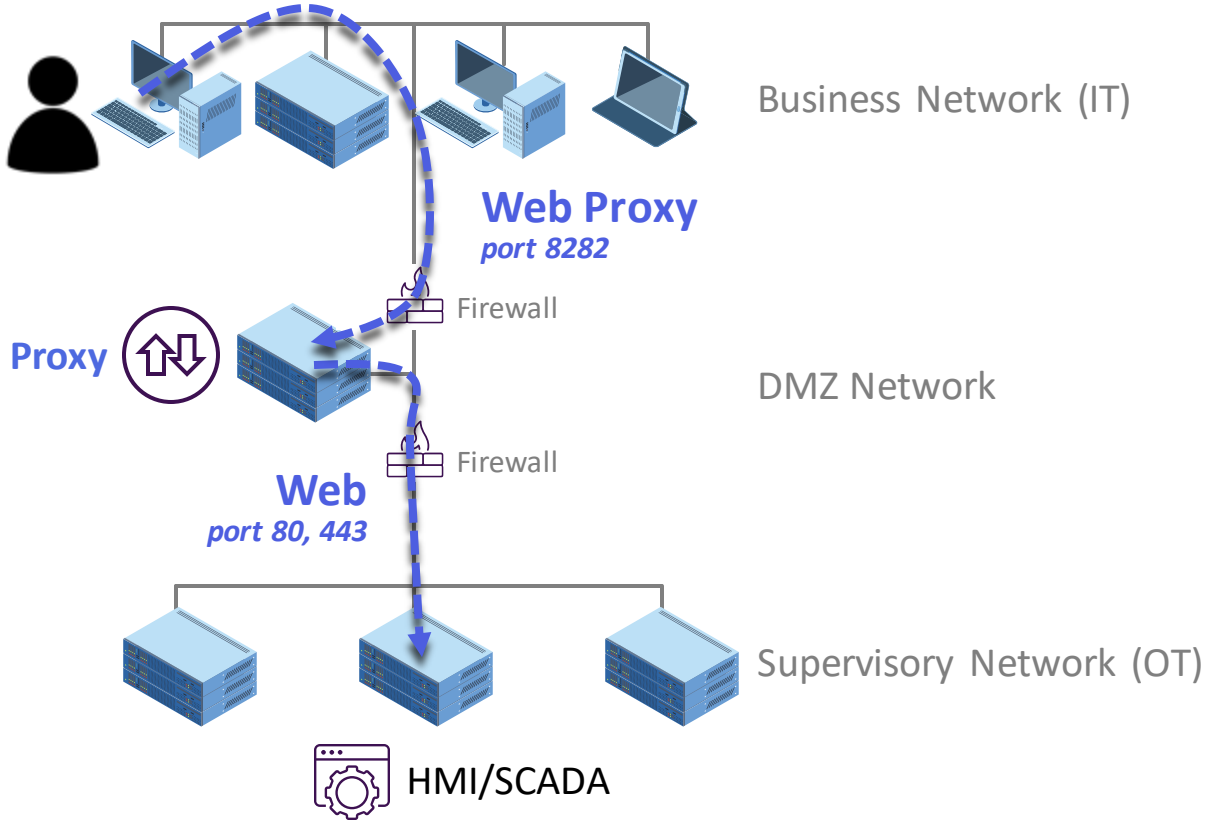
- In front of clients
- Protects clients

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Reverse Web Proxy



- Approach
  - Proxy server in DMZ
  - Open Web to DMZ from IT network
  - Open Web to OT from DMZ
- Pros
  - Simple browser access
  - More narrow access
  - Proxy is mostly transparent to users
- Cons
  - Requires inbound access to DMZ, OT
  - Certificate management for HTTPS
  - Manage proxy settings
- Example Threat: Log4Js

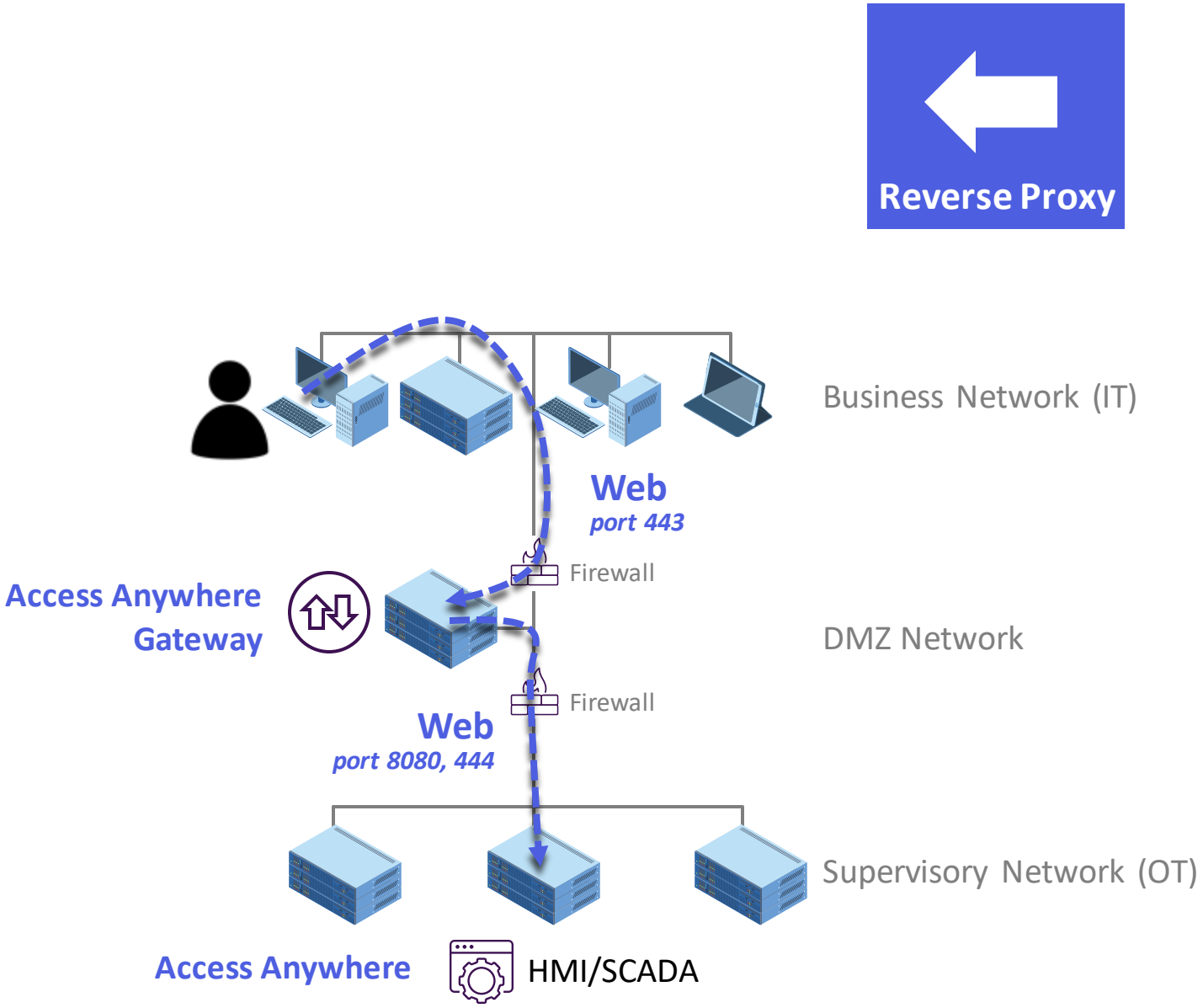


© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Reverse Web Proxy

With Access Anywhere Gateway

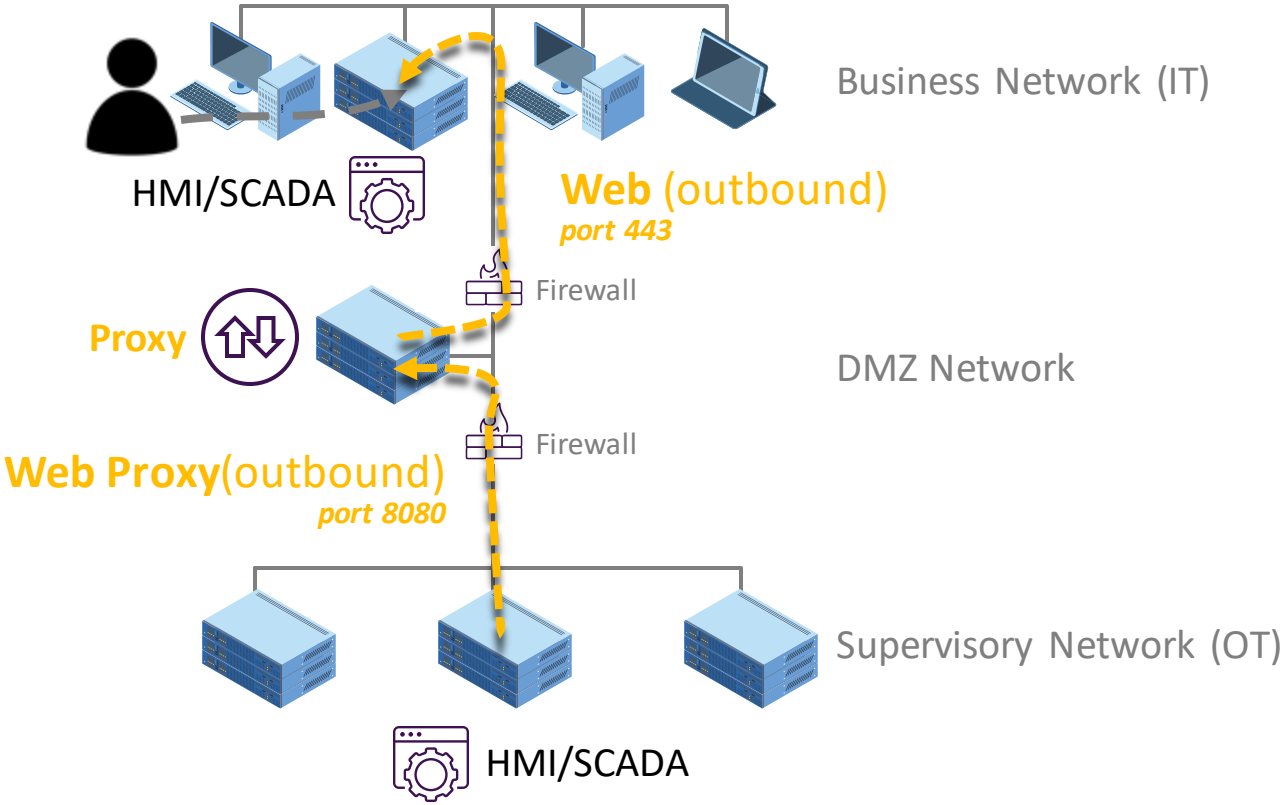
- Approach
  - Proxy server in DMZ
  - Open Web to DMZ from IT network
  - Open Web to OT from DMZ
- Pros
  - Simple browser access
  - More narrow access
  - Proxy is mostly transparent to users
- Cons
  - Requires inbound access to DMZ, TO
  - Certificate management for HTTPS
  - ~~Manage proxy settings~~
- Example Threat: Log4Js



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Forward Web Proxy

- Approach
  - Mirror to on-premises
  - Proxy server in DMZ for publishing
- Pros
  - No access to DMZ, OT required
  - Simple, broader access possible
  - Single Sign On (SSO) common
- Cons
  - Cost to maintain mirrored system
  - Manage “allow list” to limit access

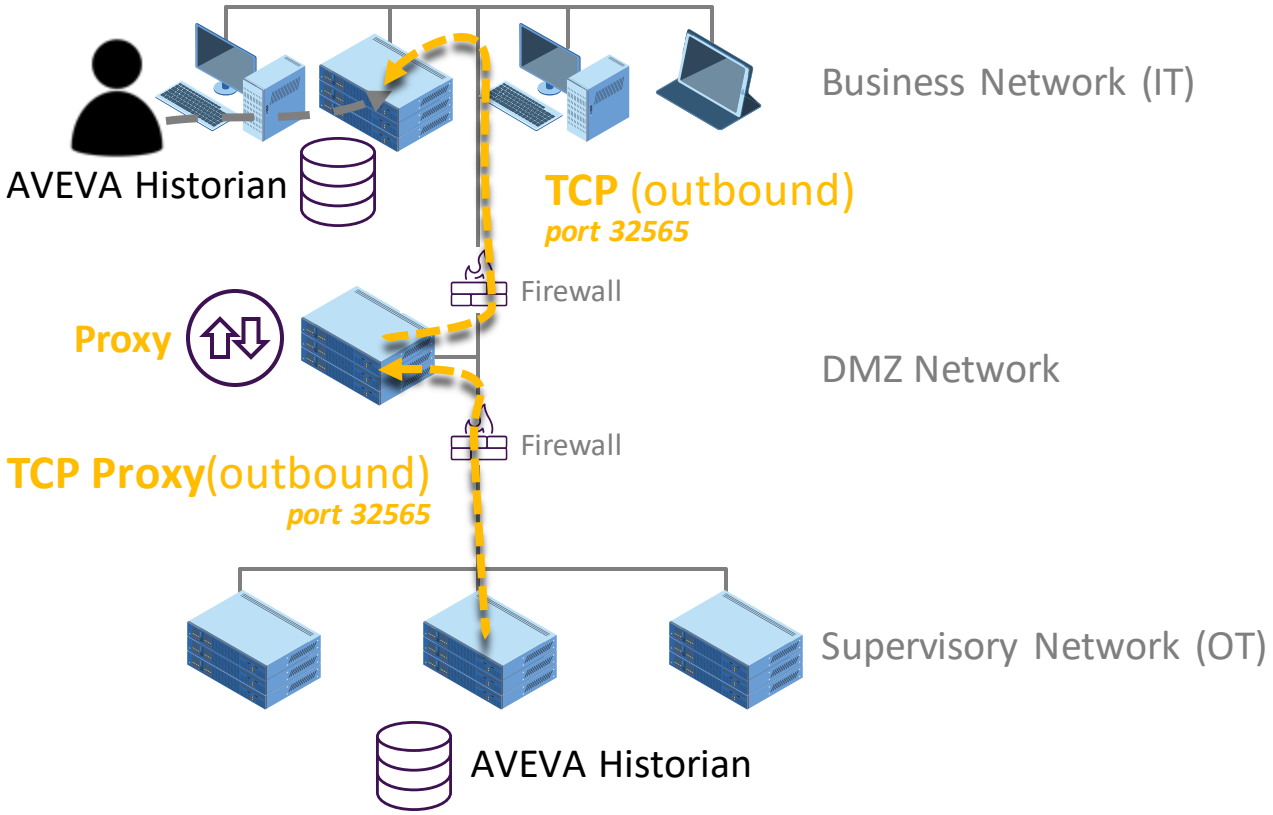


© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Forward Web Proxy

With AVEVA Historian 2023 R2

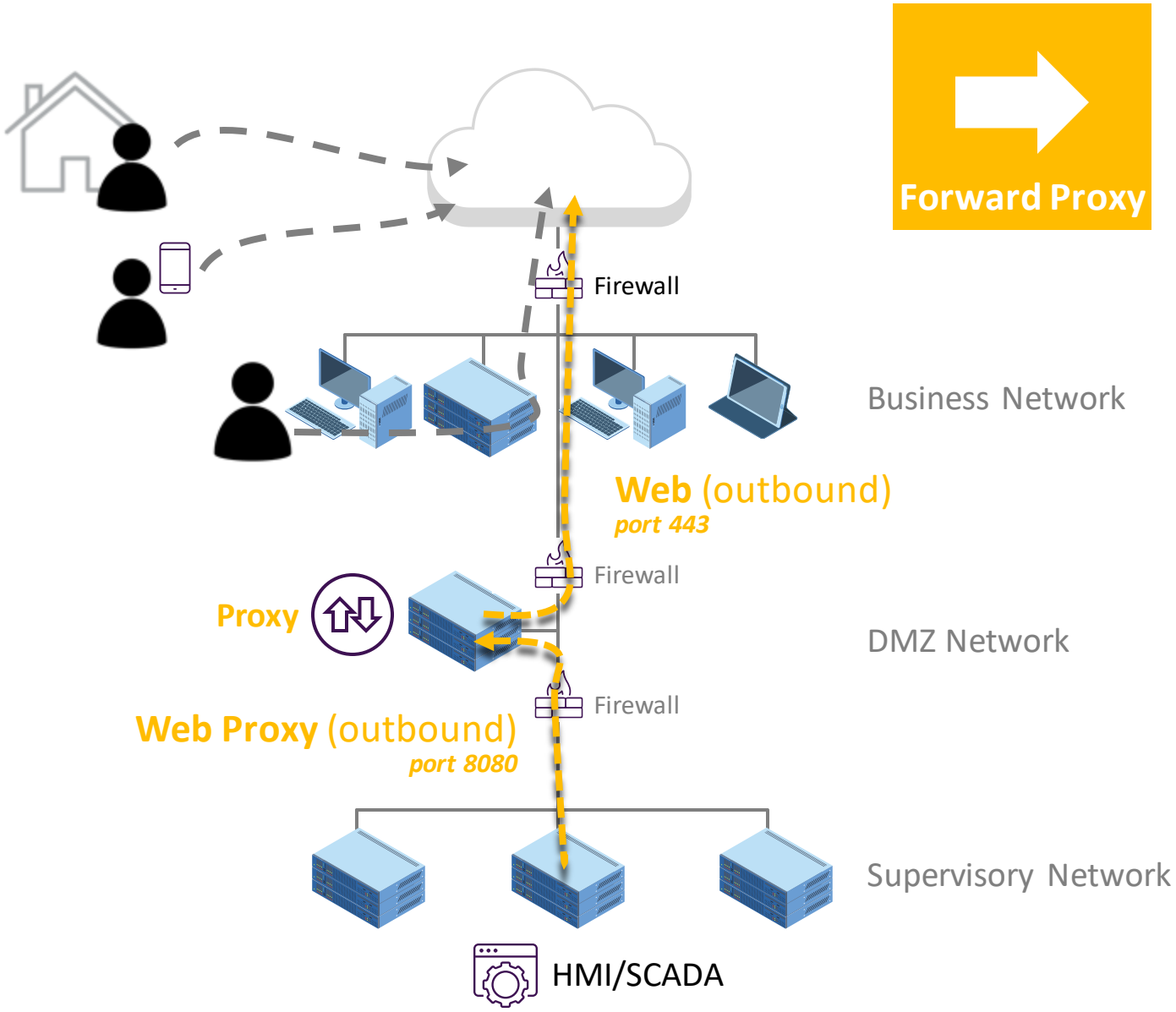
- Approach
  - Mirror to on-premises
  - Proxy server in DMZ for publishing
- Pros
  - No access to DMZ, OT required
  - Simple, broader access possible
  - Single Sign On (SSO) common
- Cons
  - Cost to maintain mirrored system
  - Manage “allow list” to limit access



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Forward Web Proxy

- Approach
  - Publish data to Cloud
  - Proxy server in DMZ for publishing
- Pros
  - No access to DMZ, OT required
  - Simple, broader access possible
  - Might use SSO
- Cons
  - Requires additional cloud subscription
  - Manage “allow list” to protect against malware, exfiltration, updates
- Example Threat: malicious site

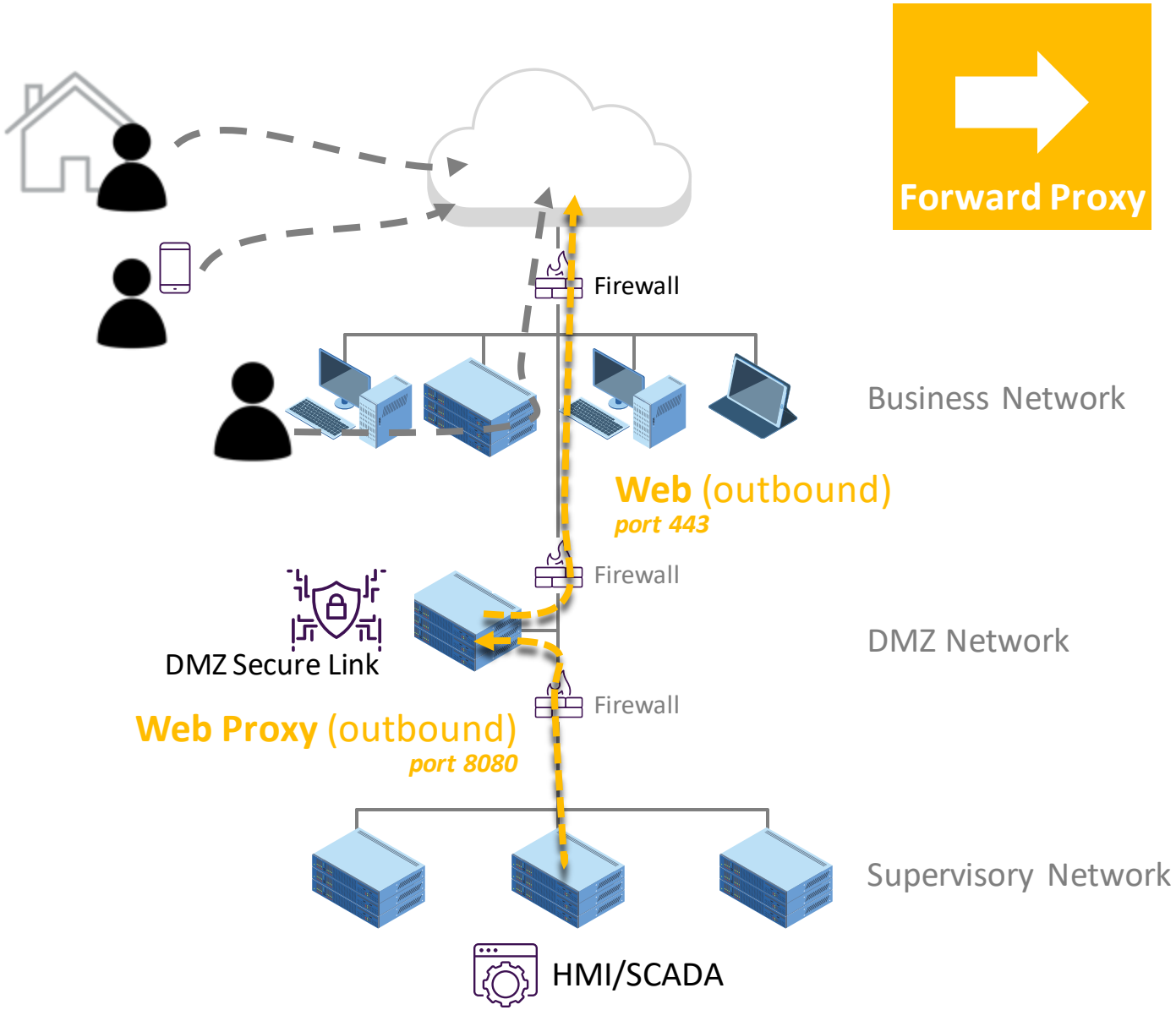


© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Forward Web Proxy

With DMZ Secure Link

- Approach
  - Publish data to Cloud
  - Proxy server in DMZ for publishing
- Pros
  - No access to DMZ, OT required
  - Simple, broader access possible
  - Might use SSO
- Cons
  - Requires additional cloud subscription
  - ~~Manage "allow list" to protect against malware, exfiltration, updates~~
- ~~Example Threat: malicious site~~

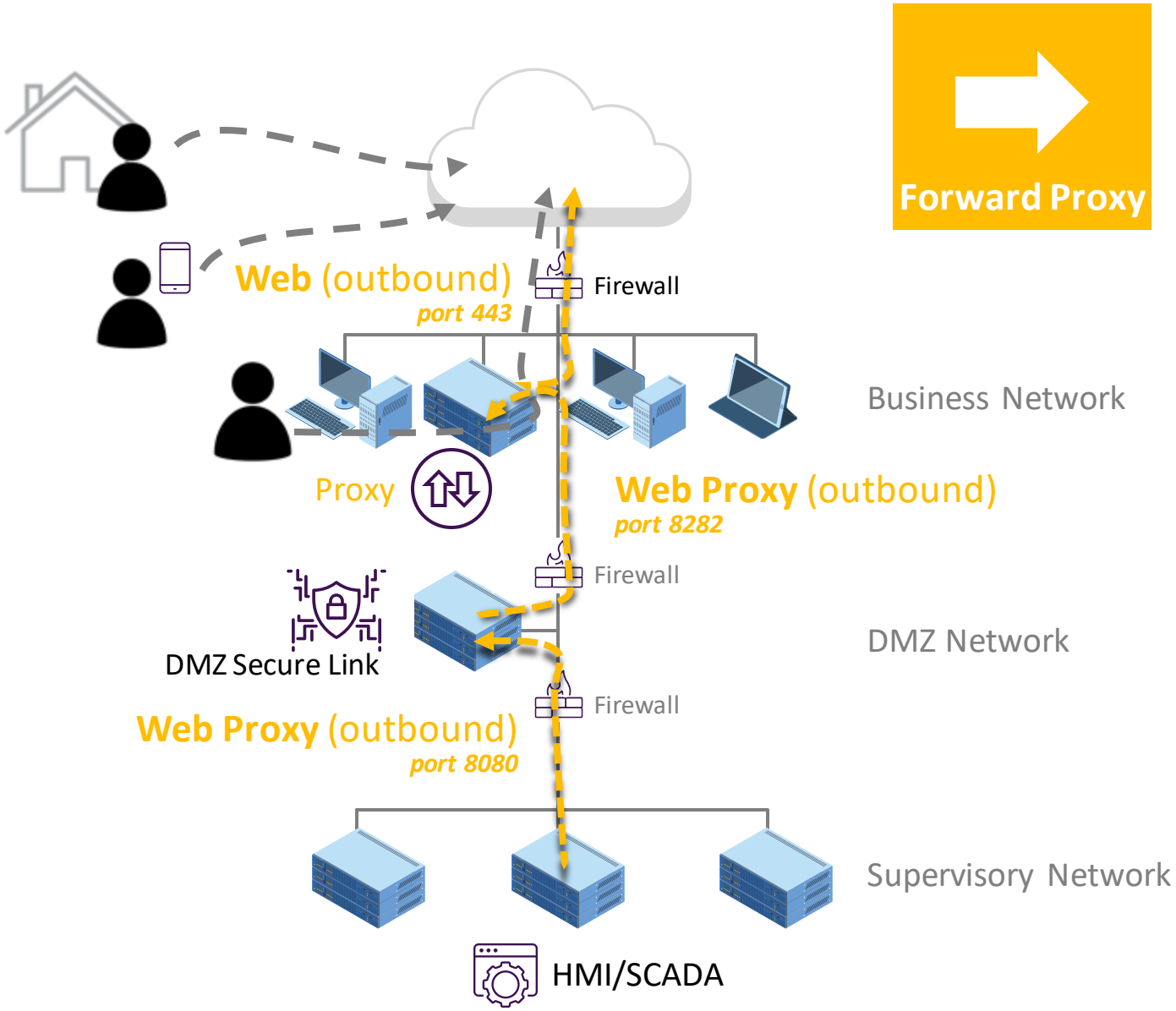


© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Forward Web Proxy

With DMZ Secure Link

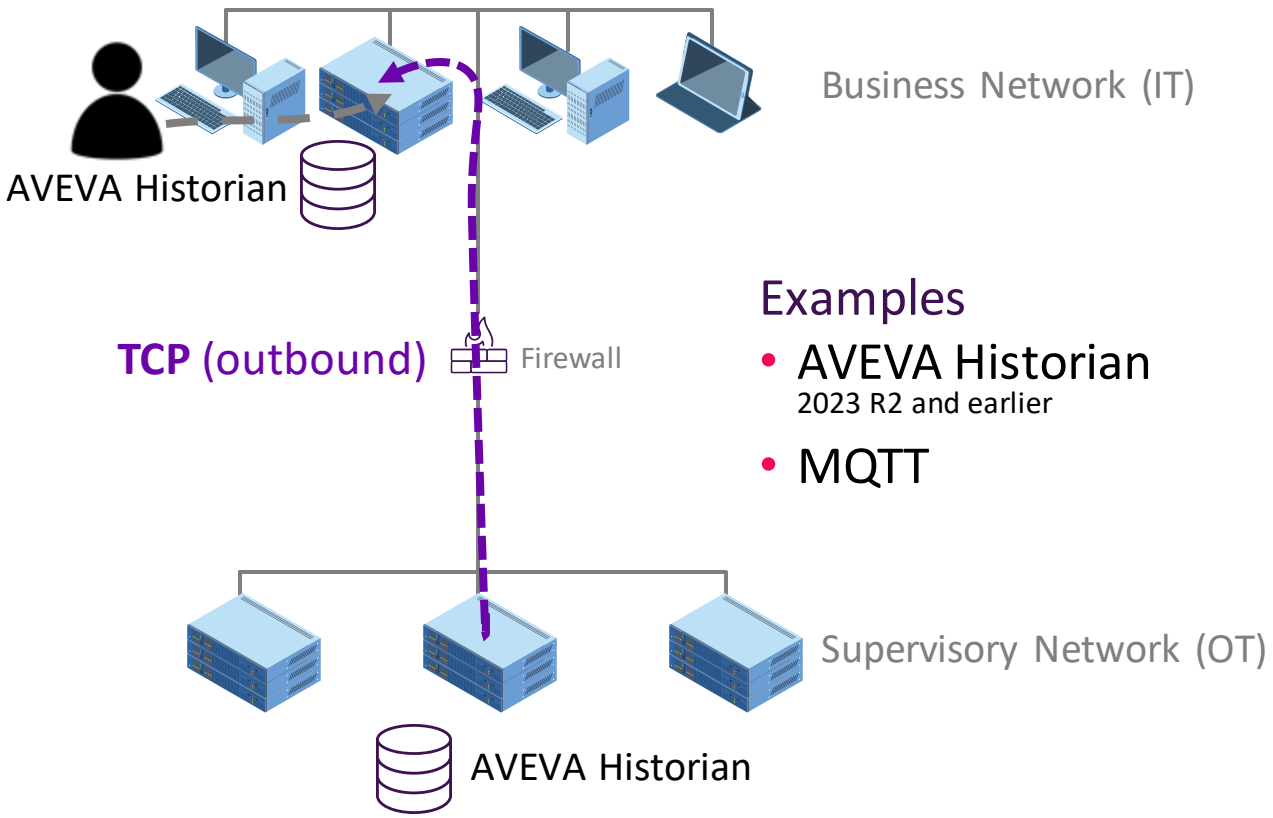
- Approach
  - Publish data to Cloud
  - Proxy server in DMZ for publishing
- Pros
  - No access to DMZ, OT required
  - Simple, broader access possible
  - Might use SSO
- Cons
  - Requires additional cloud subscription
  - ~~Manage "allow list" to protect against malware, exfiltration, updates~~
- ~~Example Threat: malicious site~~



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Simple Firewall (no DMZ)

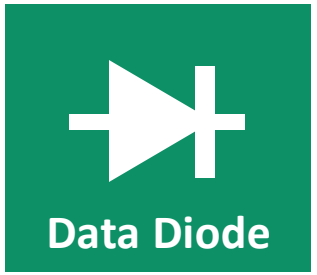
- Approach
  - Mirror to on-premises (IT) system
  - Connections *from* OT to IT only
- Pros
  - Simple user access
  - Single Sign On (SSO) common
- Cons
  - Less protection for OT
  - Cost to maintain mirrored system



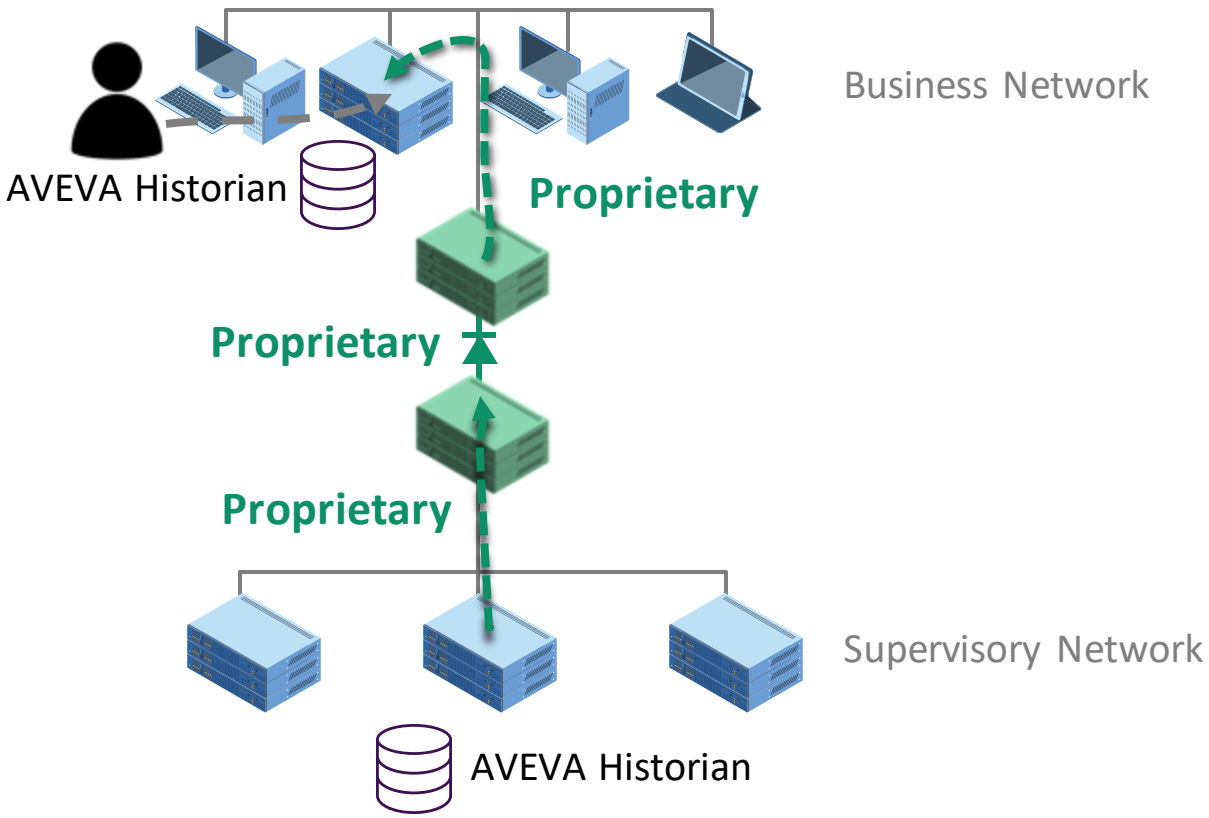
Examples
- AVEVA Historian
  2023 R2 and earlier
- MQTT

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

“Data Diode”



- Approach
  - Dual computers (vs. firewalls)
  - Connected with 1-way optical network
  - Proprietary mirroring
- Pros
  - Simple user access
  - Guaranteed 1-way “push”
- Cons
  - Unreliable delivery
  - Cost, proprietary solution
  - Cost to maintain mirrored systems
- Example Threat: Direct OT network & physical access



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Summary of Strategies

	Double RDP	Reverse Proxy	Forward Proxy	Data Diode
+	• Flexible access • Simple to setup • Secure protocol	• Simple browser • Narrow access • Nearly transparent	• Simple access • No DMZ/OT access • SSO possible	• Simple access • True one-way • SSO possible
−	• Inbound access • Multiple logins • More resources • Limit rights	• Inbound access • Certificate issues • Manage proxy	• Mirrored system • Manage allow list	• Mirror system • Cost • Proprietary • Unreliable delivery

©2023 AVEVA Group plc and its subsidiaries. All rights reserved.

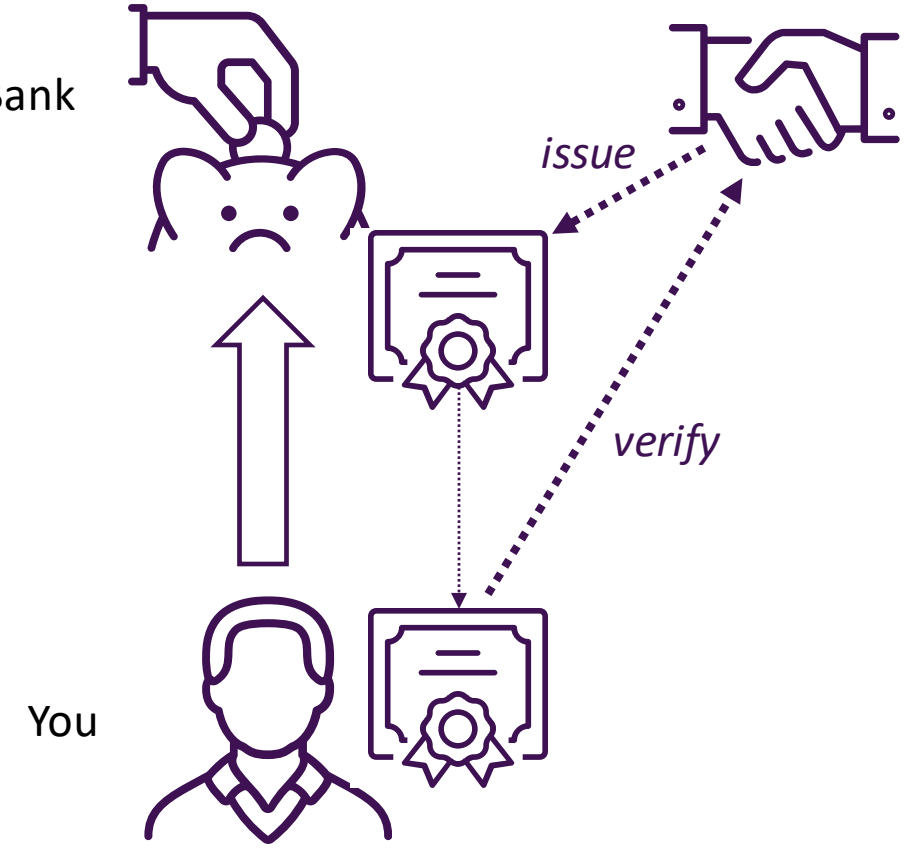
Other Challenges

© 2023 AVEVA Group Limited and its subsidiaries. All rights reserved.

Certificate Basics

1 Your Bank

Trusted Authority 2



Threats

- Eavesdropping
- Tampering
- Impersonating

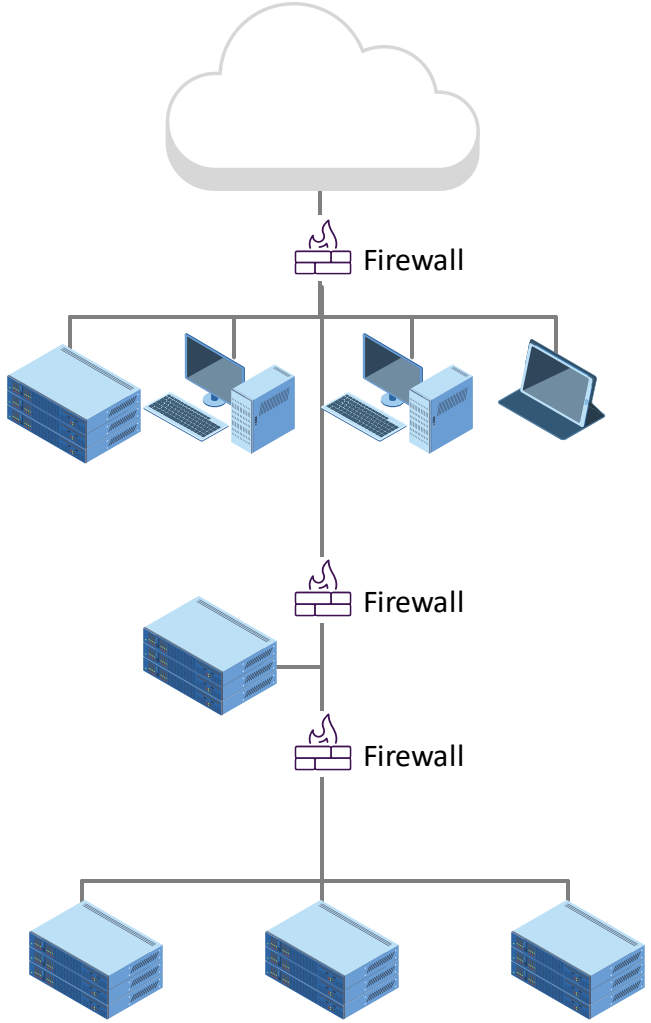
Challenges

- Authority
- Expiration
- Revocation

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Certificate Challenges

Trusted Authority



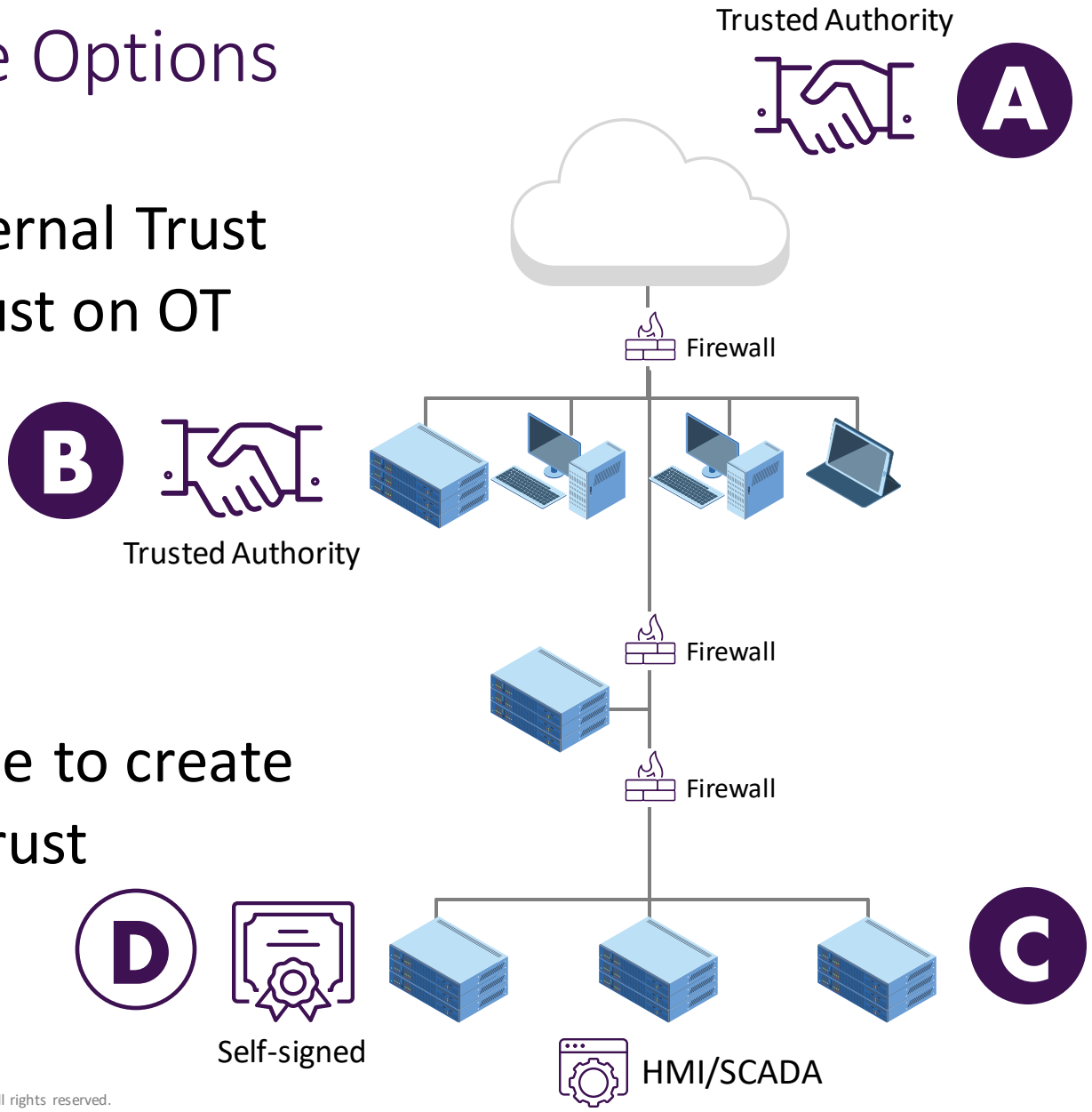
Challenges

- Where to place authority?
- How to handle expiration
- Access to revocation list

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Certificate Options

- Pro: Internal Trust
- Con: Trust on OT



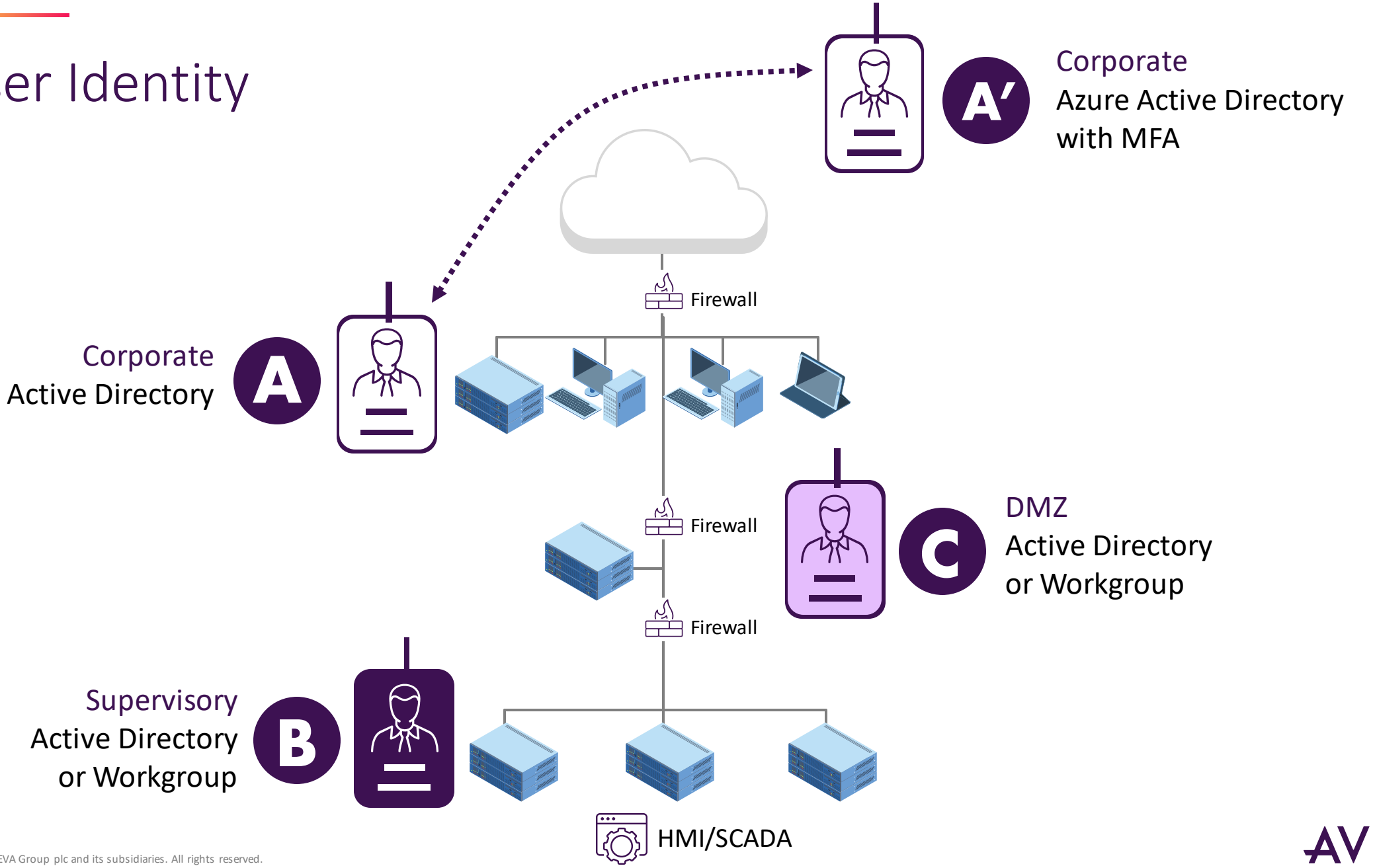
- Pro: Wide Trust
- Con:
  - Cost
  - Trust on OT

- Pro: Simple to create
- Con: No trust

- Pro: Internal Trust
- Con: Trust on IT

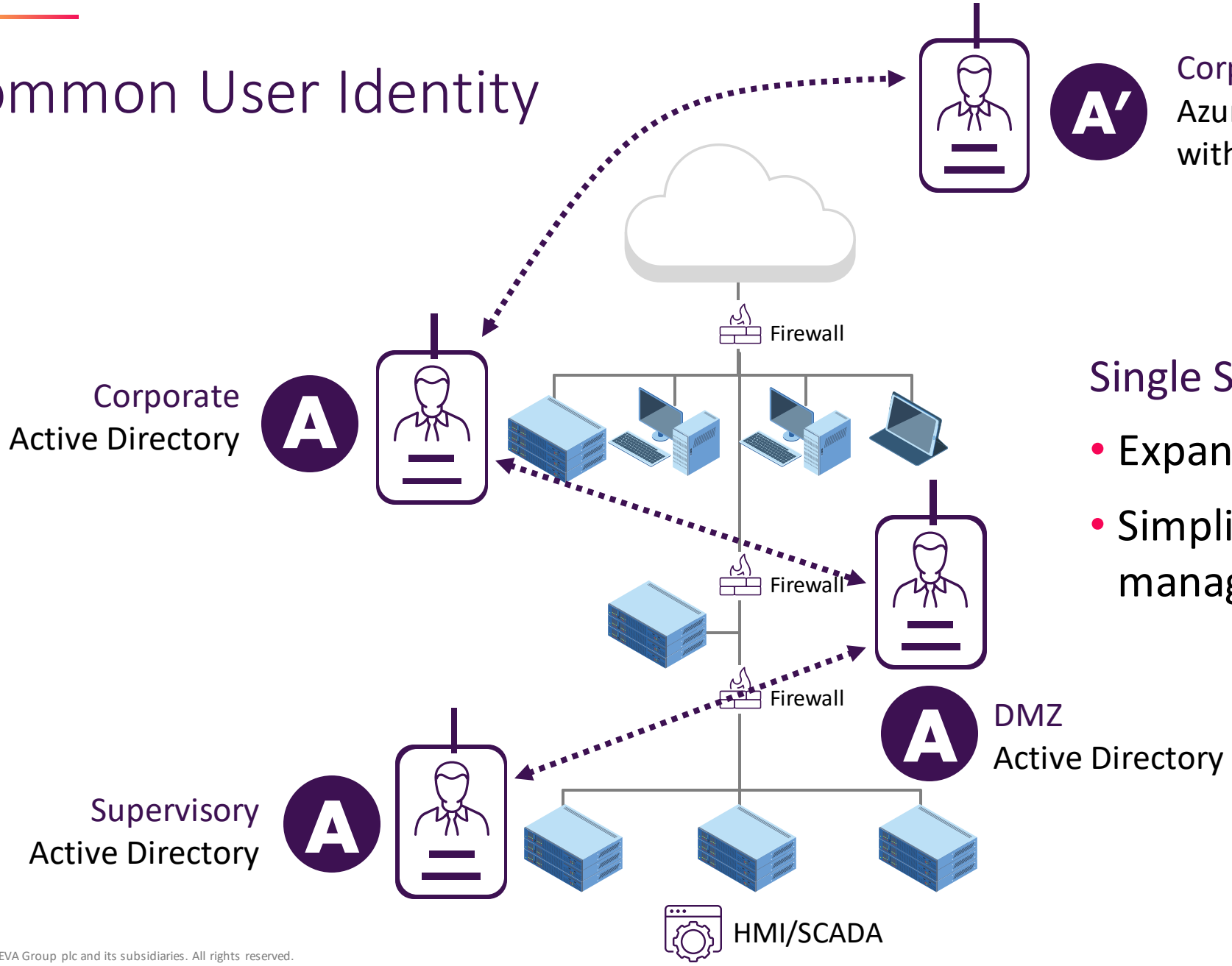
© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

User Identity



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Common User Identity

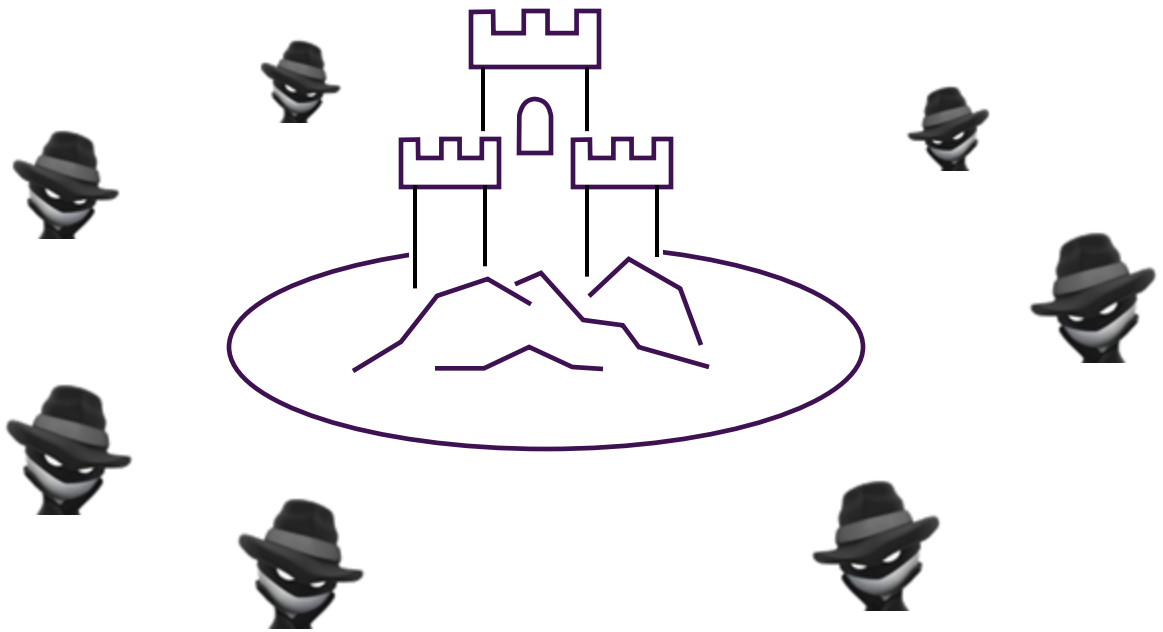


Single Sign-On (SSO)

- Expands connectivity needs
- Simplified identity management

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Security Models



- “Castle & Moat”
  - All the threats are outside
  - Focus on securing the perimeter
  - Trust insiders
- Reality
  - Insiders can be compromised
  - “Good guys” can make mistakes

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

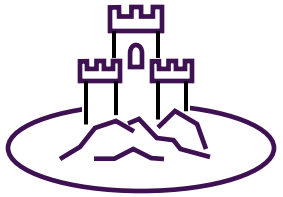
Security Models

- "Castle & Moat"
  - All the threats are outside
  - Focus on securing the perimeter
  - Trust insiders
- Reality
  - Insiders can be compromised
  - "Good guys" can make mistakes
- "Zero Trust"
  - Treat every system as if it is exposed to the Internet
  - Block/deny by default

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

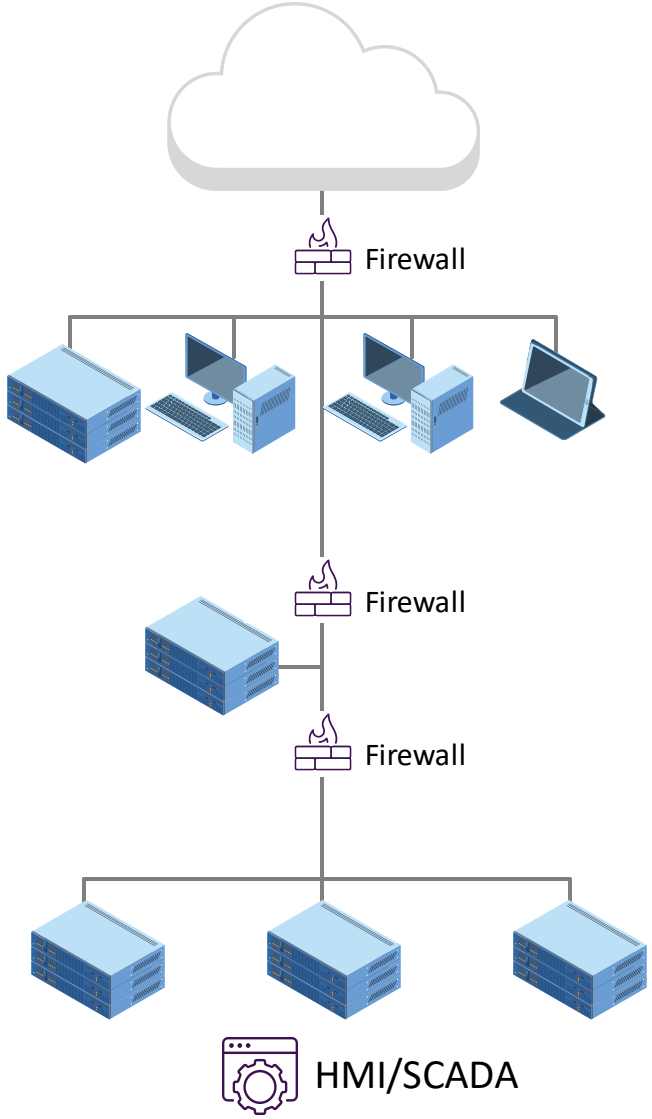
Recommendations for Operations

- Begin “Zero Trust” on IT network



- Continue protecting the OT perimeter

- Expand “Zero Trust” to OT network



© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Reasons to Bridge Domains

Make information more accessible

Fuel process improvement initiatives

Enable self-service analysis & reporting

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Questions?

Please wait for the microphone.

State your name and company.

Please remember to…

Navigate to this session in the mobile app to complete the survey.

Strategies For Getting Information From The Control Network

Thank you!

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

AVEVA

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a world leader in industrial software, providing engineering and operational solutions across multiple industries, including oil and gas, chemical, pharmaceutical, power and utilities, marine, renewables, and food and beverage. Our agnostic and open architecture helps organizations design, build, operate, maintain and optimize the complete lifecycle of complex industrial assets, from production plants and offshore platforms to manufactured consumer goods.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. The company is headquartered in Cambridge, UK.

Learn more at www.aveva.com

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

AVEVA