



DYNICS CYBERSECURITY CONSOLE



RECENT DEVELOPMENTS

- **Rule Priority and Ordering**
- **Clone Rulesets and Aliases**
- **Use Network-Based Rules**
- **Improve integration with ICS360.IAM**
- **Numerous Performance / Reliability Improvements**

RULE PRIORITY

ICS360.DCC Dynics Cybersecurity Console version 8352cea develop

Deployments Rulesets Aliases Networks

Order View Save Order

Priorities

Protocol	Source	Port	Destination	Port	Gateway	Network	Description
TCP	Any	*	ICS360.Defender	53 - 53	*	WAN	Allow DNS Queries from WAN
ICMP	Any	*	ICS360.Defender	*	*	WAN	Allow WAN Pings
Any	Any	*	Any	*	*	WAN	Disallow All Traffic

Rows per page: All 1-3 of 3

ICS360.DCC Dynics Cybersecurity Console version 8352cea develop

Deployments Rulesets Aliases Networks

Order View Save Order

Priorities

Protocol	Source	Port	Destination	Port	Gateway	Network	Description
TCP	Any	*	ICS360.Defender	53 - 53	*	WAN	Allow DNS Queries from WAN
Any	Any	*	Any	*	*	WAN	Disallow All Traffic
ICMP	Any	*	ICS360.Defender	*	*	WAN	Allow WAN Pings

Rows per page: All 1-3 of 3



CLONE RULES AND ALIASES

The screenshot shows the Dynics Cybersecurity Console interface. On the left is a navigation sidebar for 'ICS360.DCC' with menu items: Collections, User Groups, Users, Device Groups, Devices, Firewalls (highlighted), and Licensing. The main content area is titled 'Dynics Cybersecurity Console' with version '8352cea develop'. It features tabs for Deployments, Rulesets (active), Aliases, and Networks. Below the tabs are icons for Table View, a checkmark, a trash can, a clone icon, and a list icon. A blue banner indicates 'selected 2 of 3 rules' and a 'Clone selected items' button is visible. A 'Priorities' dialog box is open, displaying a table of firewall rules.

	Protocol	Source	Port	Destination
<input type="checkbox"/>	Filter...	Filter...	Filter...	Filter...
<input checked="" type="checkbox"/>	TCP	Any	*	ICS360.Defender
<input checked="" type="checkbox"/>	Any	Any	*	Any
<input type="checkbox"/>	ICMP	Any	*	ICS360.Defender











Network Rules






Why do we write rules the way we do?

Firewall / Rules / WAN

Floating **WAN** LAN DYNICS_VPN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP <i>echorep, echoreq</i>	*	*	This Firewall	*	*	none			    
<input type="checkbox"/>	✓ 19 / 1.21 MiB	IPv4 TCP	*	*	This Firewall	22 - 443	*	none			    

 Add  Add  Delete  Save  Separator

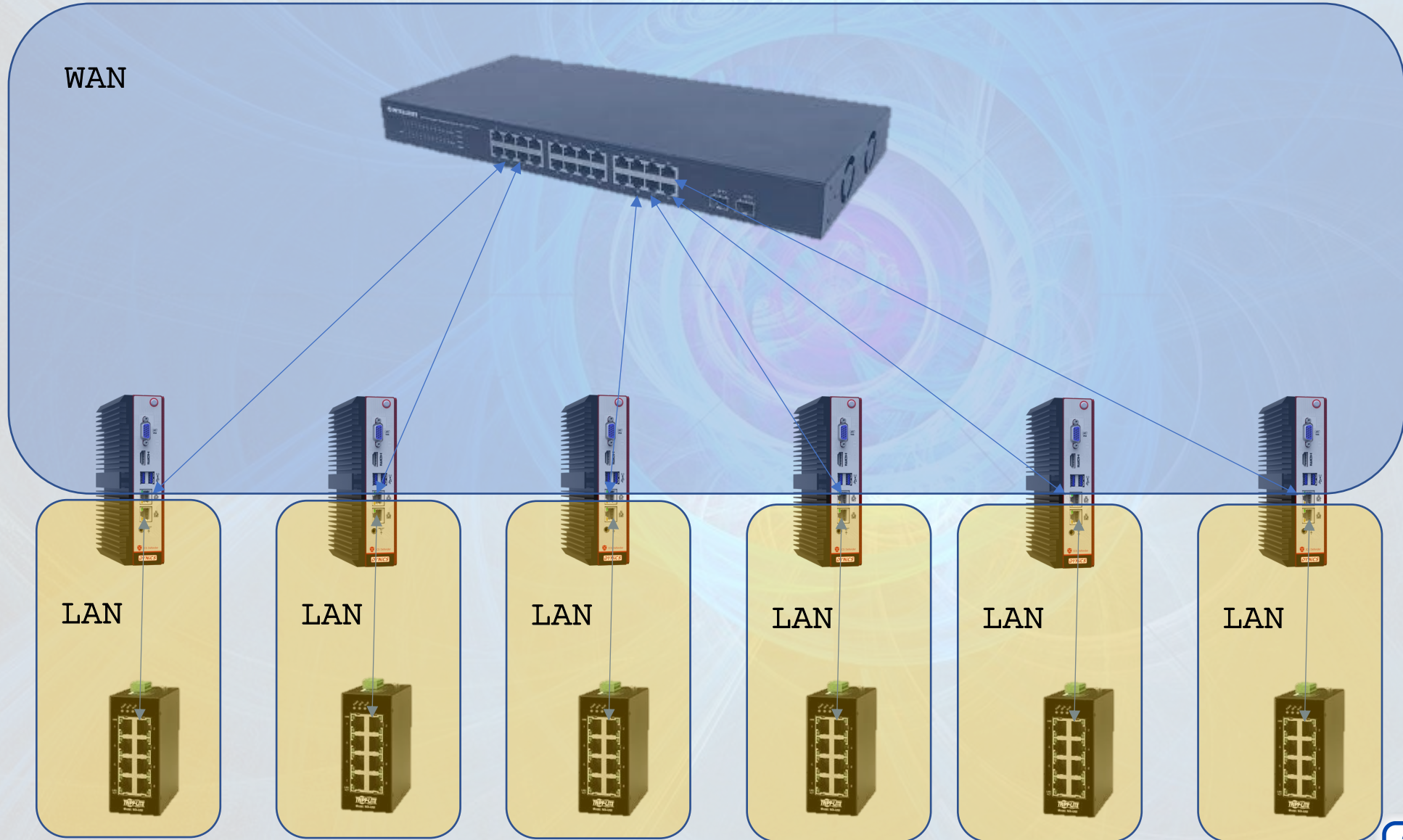


WAN

LAN



BUT WHAT IF I'M MANAGING MULTIPLE FIREWALLS?



YOU DEFINE A NETWORK!

Deployments Rulesets Aliases **Networks**

Network: PLANTFLOOR Save Changes

Network includes interfaces that match any of the following criteria:

↳ One of the following: 🗑️

- ↳ Name is PLANTFLOOR 🗑️
- ↳ Name is WAN 🗑️
- ↳ IP Address in 192.168.3.0 / 24 🗑️

[+ Add](#)

Interfaces

Device	Interface	IP Address	MAC Address	Networks
ICS360.Defender 67fc4d	WAN	192.168.3.128	00:0c:29:a5:22:79	▼
ICS360.Defender 984f4d	WAN	192.168.3.130	00:0c:29:a6:36:17	▼



Rows per page: 10 1-2 of 2 < >

AND THEN USE IT

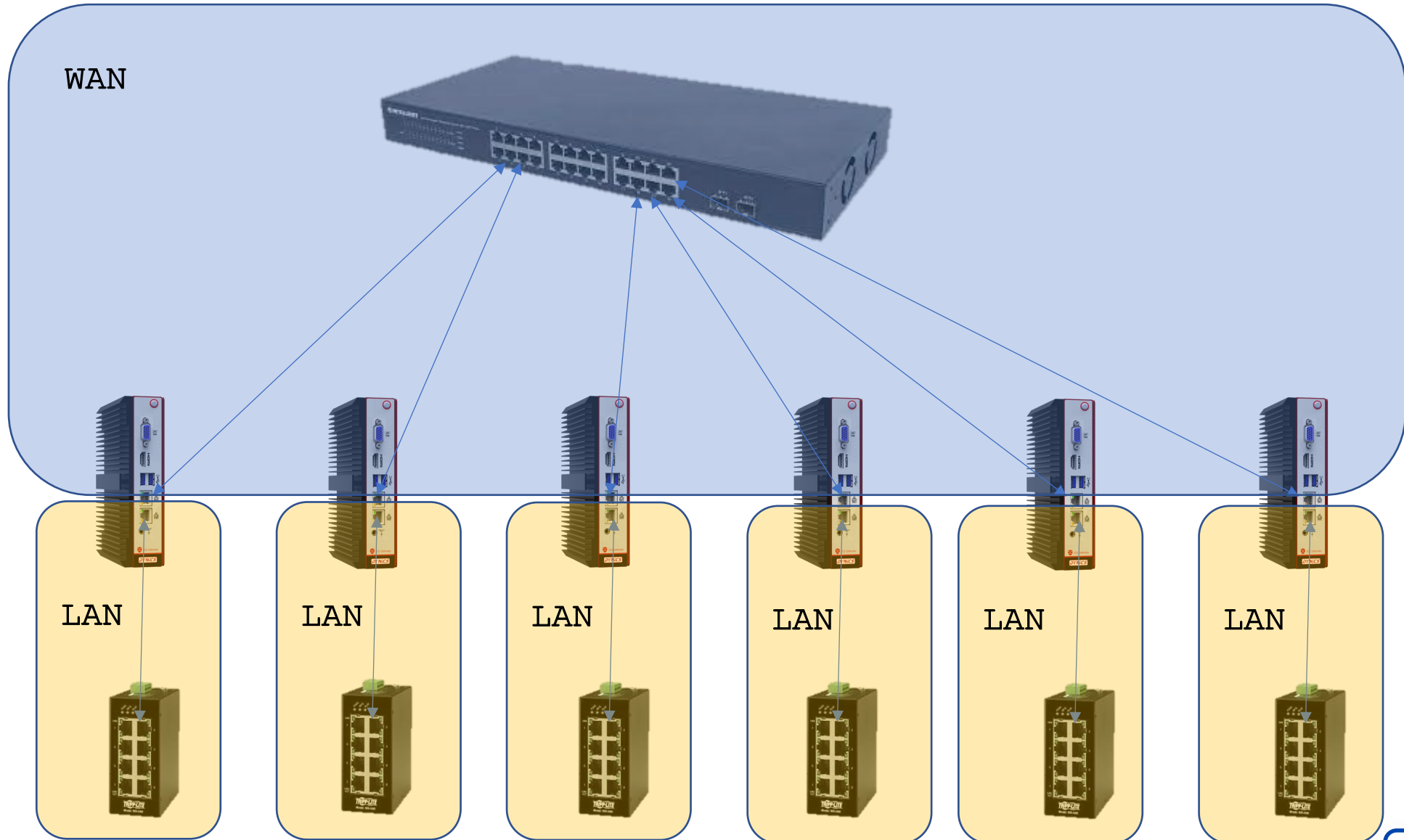
New Rule

	Source	Destination	Firewall Rule
Action	Pass		▼ ?
Network(s)	PLANTFLOOR		▼ ?
Address Family	IPv4		▼ ?
Protocol	TCP		▼ ?
ICMP Type	Any		▼
Log	<input type="checkbox"/> ?		
Description	Enter description		

0 / 255

 Save  Cancel

AND THAT RULE GOES EVERYWHERE



WHAT'S UP NEXT?

- **Firmware / Package updates through DCC**
- **Importing Rules from existing Defenders**
- **LDAP/AD Support**
- **Deployment Previews**

Thanks for your time, any questions?

Joshua Jacobson
Senior Software Engineer

