Next-Gen Firewall Automation

NANOG 83

Presenter: Ken Celenza

>>> Introduction

Ken Celenza

- VP of Professional Services at Network to Code
  - Involved in dozens of network automation projects in the past several years
- Traditional network engineer by day, coder by night
- Converted full time network automator in 2016
- Over 20 years in the industry, primarily supporting enterprises

Manual Firewall Rule Management

Current Firewall Automation

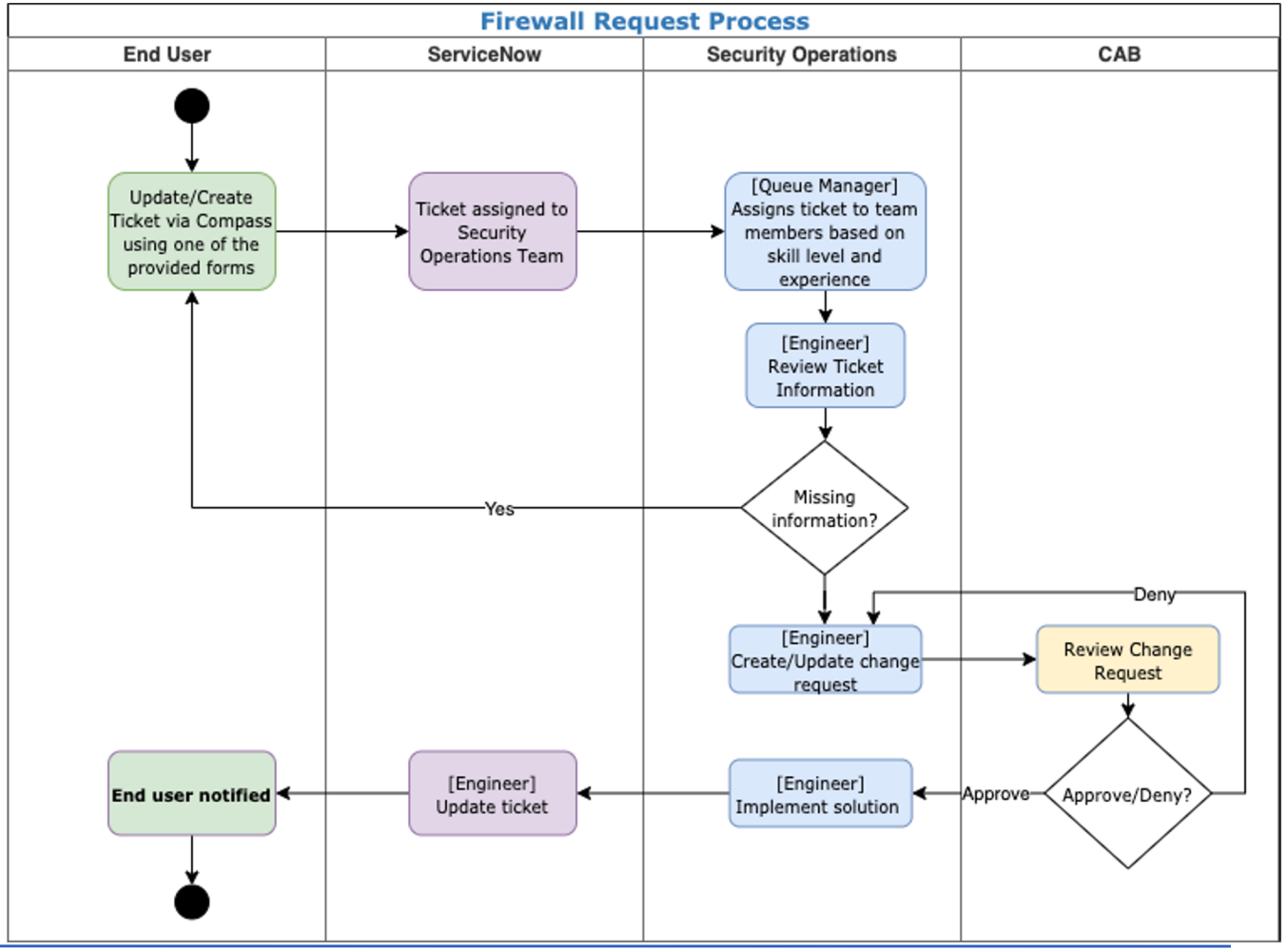
Next-Gen Firewall Automation

Demo


Manual Firewall Rule Management

Manual Workflow

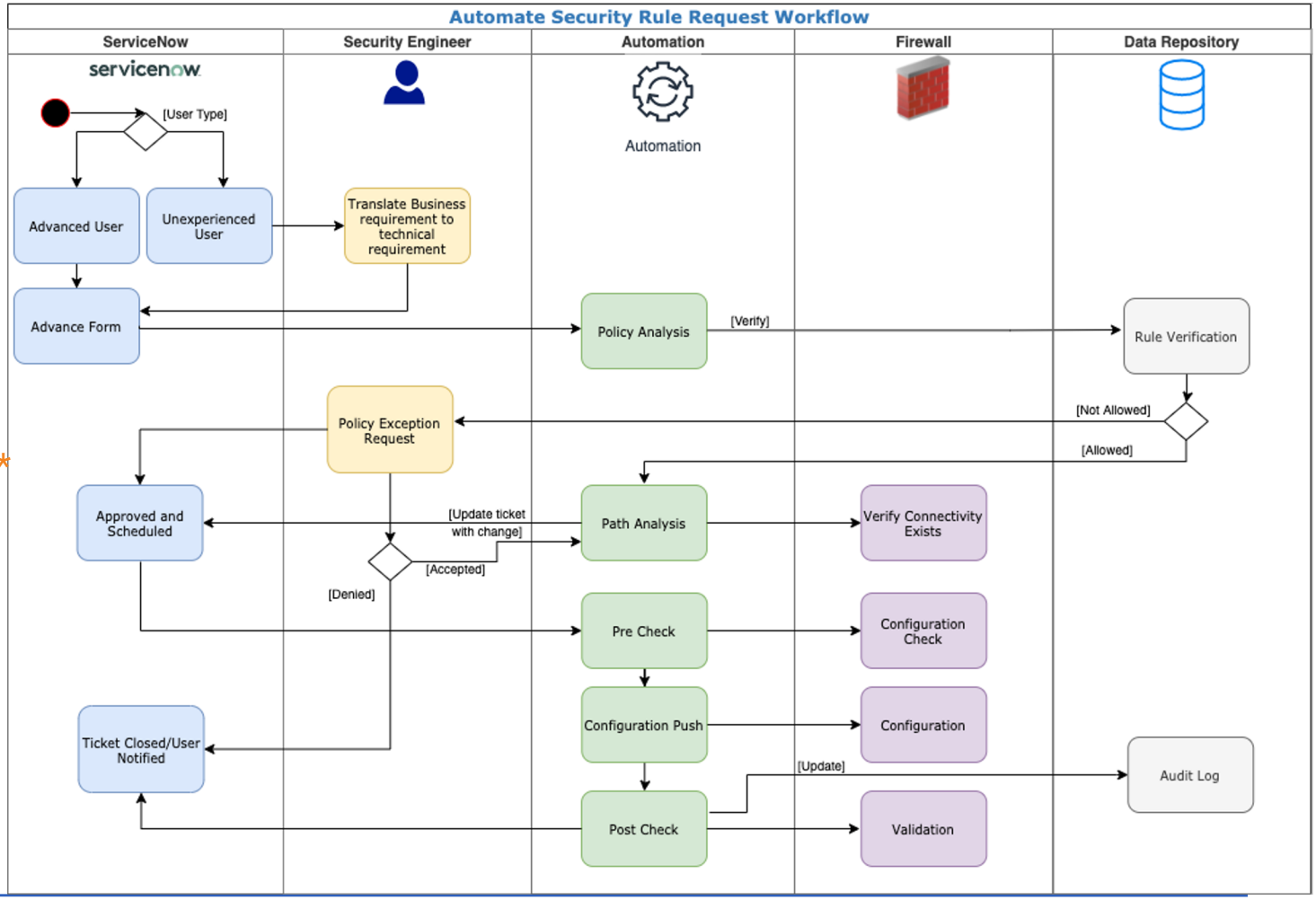
- User Makes Request
- Operator Review
- Validates, determines path
- CAB Review
- Implements
- Closes ticket




Current Firewall Automation

Automated Workflow

- User Makes Request
- Operator Review
- Pre-validation **
- CAB Review
- Pre-checks **
- Deploy Configuration **
- Post Checks **
- Closes ticket



** Automated

>>> Pros

Current Firewall Automation

- Configuration is Normalized and Standardized
- Form validation ensures reasonable quality of data
- Enables customers to self-provision
- Reduce time to market
- Provides traceability of configuration pushes
- Reduces monotonous tasks and associated fatigue

>>> Cons

Current Firewall Automation

- Requires expert knowledge of how applications and networks work
- There is not an intended state or a SoT of the infrastructure
- Rule creation is difficult to track
  - When viewing a rule, it is difficult to understand when & how it was created
- Rule ownership is difficult to track, often presumed to be security team
- Traversing multiple security points complicates rule sets, design, and automation
- Firewall rules grow at exponential rate, but are rarely removed


Next-Gen Firewall Automation

>>> Application Centric Firewall Automation

It is a Source of Truth that models applications and the network relationship between them

>>> Application Dictionary - Proposal

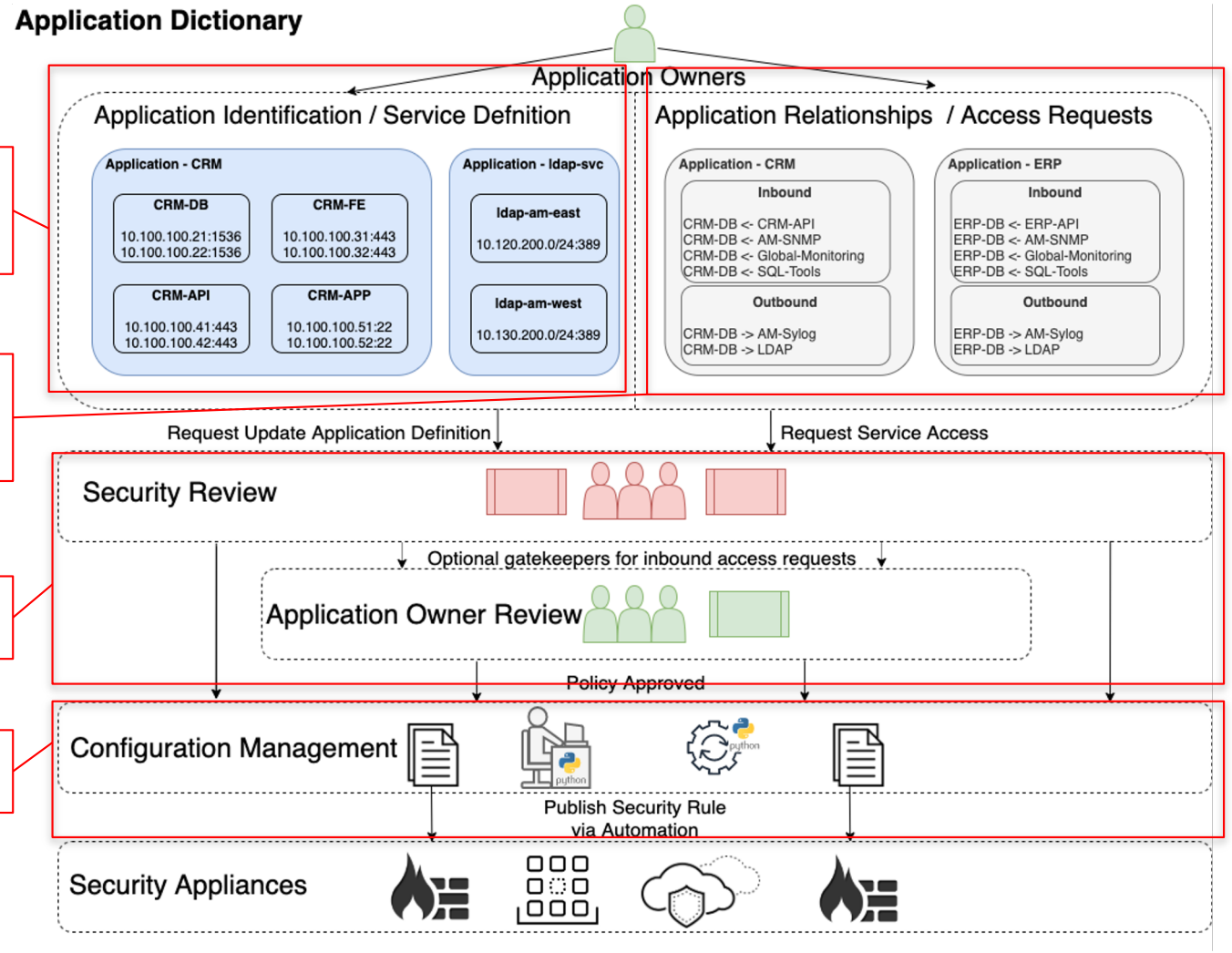
- Request by business needs, using application names, not IP protocols
  - Please allow *"CRM-API -> CRM-DB"*
  - Please allow ~~*"10.1.100.41 & 42 -> 10.10.100.21 & 22 : tcp/1536"*~~
- Assign metadata to application
  - Application owner
  - Confidentiality of data
  - Encryption
  - Authentication
- Manage non-firewall control points
- Rule optimization, remove duplicate/unnecessary rules
- Provide full firewall rule configuration

>>> Firewall Complications of a Modern Network

- DNS and IP addresses are no longer the only source or destination
  - Identity based access, e.g. LDAP groups
  - Container security
  - SaaS services
  - Application identification
- Network Address Translation (NAT) and Virtual IPs (VIPs)
- Edge Enforcement
  - Container security enforcement
  - Cloud enforcement, e.g. AWS security groups
  - Hypervisors enforcement
  - Firewalld and IPTables

>>> Solution

- Application Owners Define their Application
- User request access from application to application
- Security Review
- Automation Deploys



Example Rule Created From SoT

Access Request

CRM-API	->	**CRM-DB**
CRM-API	->	**Splunk-Svc**
CRM-DB	->	**Splunk-Svc**

Application Definition

CRM-API		**Splunk-mgmt**
10.100.100.41:443		10.100.200.51:443
10.100.100.42:443		10.100.200.51:443
CRM-DB		**Splunk-Svc**
10.100.100.21:1536		10.100.200.51:514
10.100.100.22:1536		10.100.200.51:514

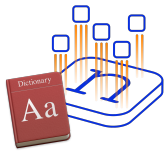
Firewall Rules

Function	Source IP	Destination IP	Destination Port
CRM-API - CRM-DB	10.100.100.41 10.100.100.42	10.100.100.21 10.100.100.22	1536
CRM-API - Splunk-Svc	10.100.100.41 10.100.100.42	10.100.200.51 10.100.200.52	514
CRM-DB - Splunk-Svc	10.100.100.21 10.100.100.22	10.100.200.51 10.100.200.52	514

Automation Stack Components

Nautobot: Open Source SoT Automation Platform

Application Dictionary: Primary Nautobot Plugin



Firewall Model: Nautobot Plugin providing firewall rule data model

Capirca: Google Open Source ACL generation Python library

Nornir: Open Source Configuration Management Python library

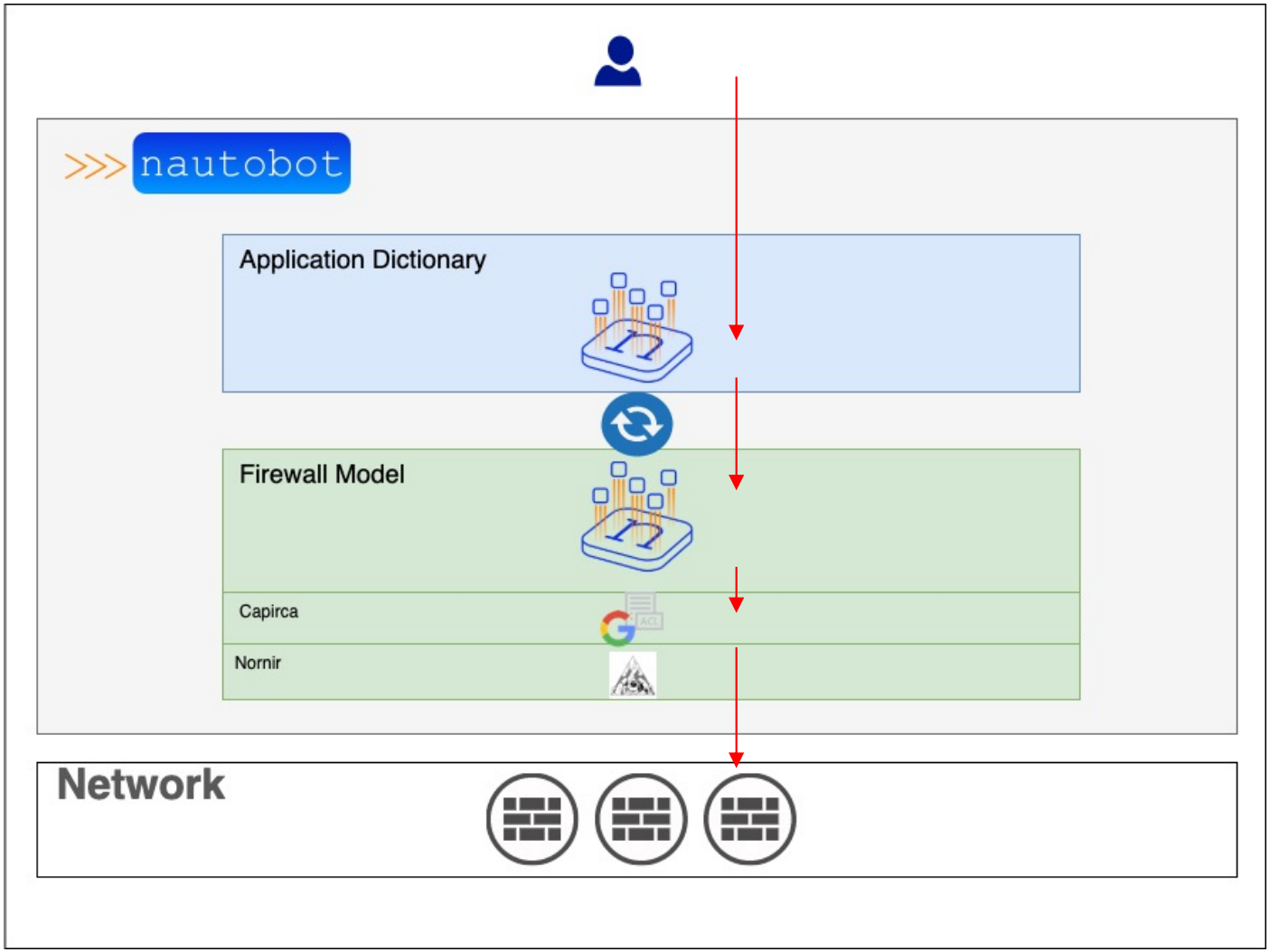
>>> Design

1. User makes request

2. App-Dictionary Syncs with Firewall Model

3. Capirca Generates Config

4. Deploy with Nornir

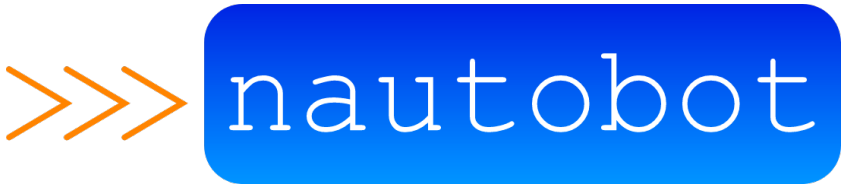



Demo

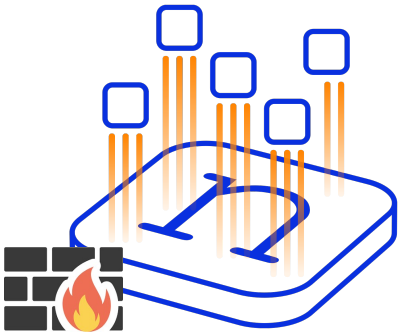
>>> Demo

Let's add an application and deploy configs

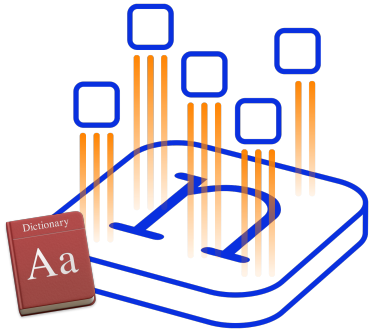
Availability



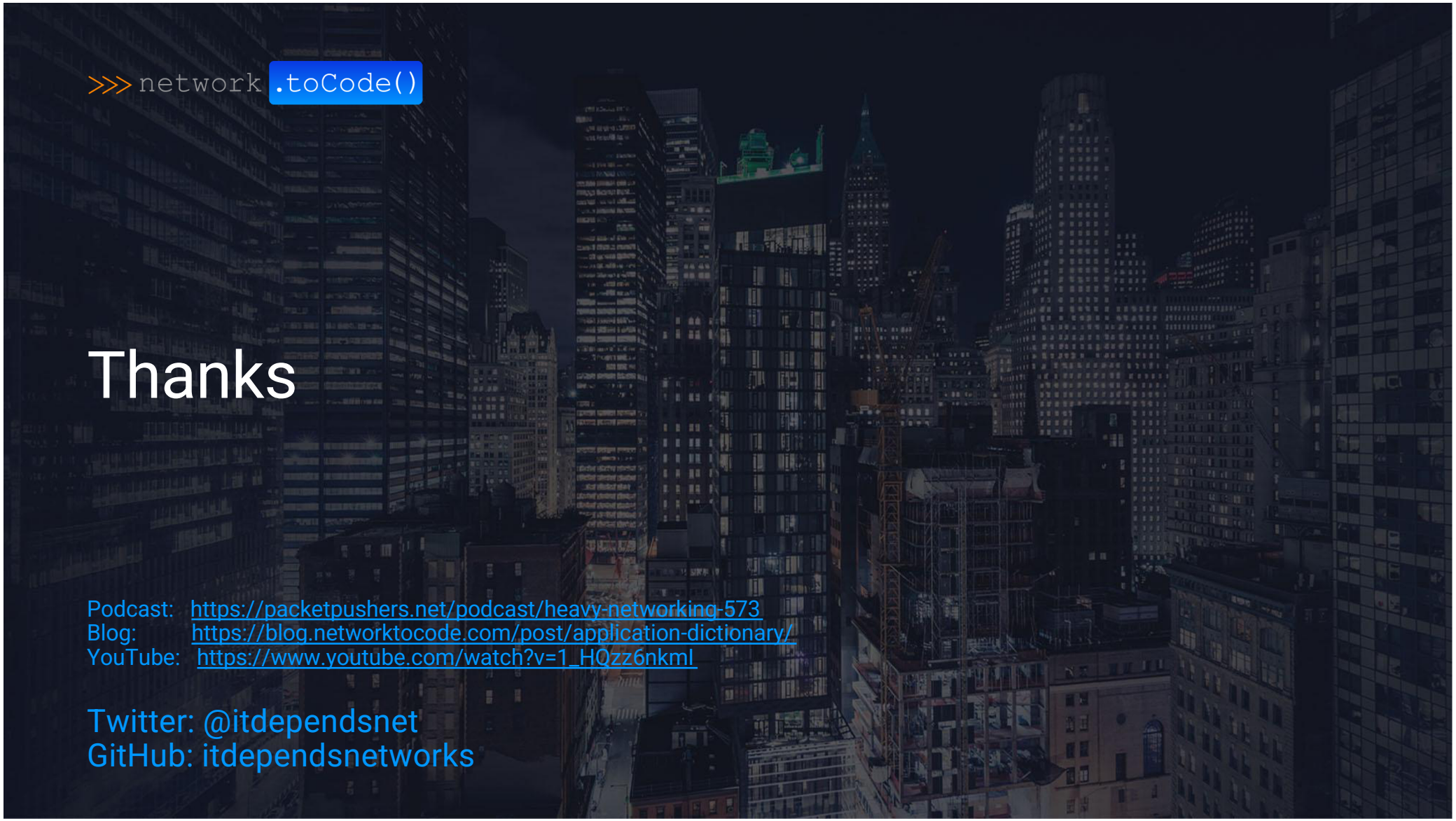
Nautobot
Open Source - Currently



Nautobot Firewall Model
Open Source – Q4 2021



Nautobot Application Dictionary
Open Source – Q1 2022



Thanks

Podcast: https://packetpushers.net/podcast/heavy-networking-573
Blog: https://blog.networktocode.com/post/application-dictionary/
YouTube: https://www.youtube.com/watch?v=1_HQzz6nkmI

Twitter: @itdependsnet
GitHub: itdependsnetworks