PAYCHEX®

Payroll | Benefits | HR | Insurance

Automating Firewall Rules for DevOps

The answer is Dynamic Objects

Agenda

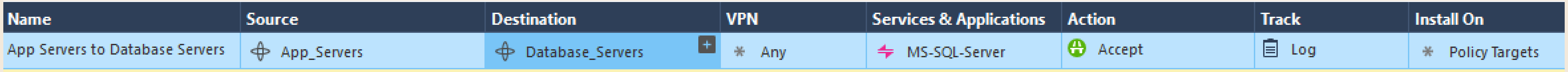
- Automation Challenges
- Rule Design
- Dynamic Objects

Automation Challenges

- Which policy/firewalls does a rule get added to?
- Where in the policy should the rule be added for efficiency?
  - Should I just be adding a source/destination/port to an existing rule?
- Competing actions against locked resources
- Need to push policy to activate the change
- Policy pushes take time
- Tagging is cool, but what about all of my other IP addresses that aren't virtual servers?

Rule Design

- Rules should be sociable
- Rules should be understood at a project’s inception
- Rules should be built as groups communicating to groups



Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
App Servers to Database Servers	App_Servers	Database_Servers	Any	MS-SQL-Server	Accept	Log	Policy Targets

The answer is Dynamic Objects

- No longer disable SecureXL if R80.10+
- Act like groups – they are a collection of IPs
- Do not require policy install to update
- Can be empty
- Manipulated on each gateway
- Are not locked
- Effective immediately
- Exist in a text file: $FWDIR/database/dynamic_objects.db

```
[admin@GATEWAY ~]# file $FWDIR/database/dynamic_objects.db
/opt/CPsuite-R80.30/fw1/database/dynamic_objects.db: ASCII text
```

Dynamic Objects – HERE’S THE CATCH

- Dynamic objects exist as RANGES ONLY

```
[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1           192.168.1.10
range 1 : 192.168.2.1           192.168.2.10

Operation completed successfully
```

- All commands must be crafted to manipulate ranges

Dynamic Objects - Add

- Add a single IP
- Add a network (you’re going to have to do some math)

```
[admin@GATEWAY ~]# dynamic_objects -o App_Servers -r 192.168.3.1 192.168.3.1 –a
[admin@GATEWAY ~]# dynamic_objects -o App_Servers -r 192.168.4.1 192.168.4.255 -a
[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1         192.168.1.10
range 1 : 192.168.2.1         192.168.2.10
range 2 : 192.168.3.1         192.168.3.1
range 3 : 192.168.4.1         192.168.4.255
```

Dynamic Objects - Add

- Intelligent enough to combine ranges when appropriate

```
[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1           192.168.1.10
range 1 : 192.168.2.1           192.168.2.4
range 2 : 192.168.2.6           192.168.2.10
[admin@GATEWAY ~]# dynamic_objects -o App_Servers -r 192.168.1.11 192.168.1.11 -a
[admin@GATEWAY ~]# dynamic_objects -o App_Servers -r 192.168.2.5 192.168.2.5 -a
[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1           192.168.1.11
range 1 : 192.168.2.1           192.168.2.10
```

Dynamic Objects - Delete

- Not intelligent

```
[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1           192.168.1.11
range 1 : 192.168.2.1           192.168.2.10
[admin@GATEWAY ~]# dynamic_objects -o App_Servers -r 192.168.2.5 192.168.2.5 -d

IP range does not exist
```

Dynamic Objects – How to Delete

- Delete the entire range and add back what you want (Do you see the problems?)

```
[admin@GATEWAY ~]# dynamic_objects -l
object name : dynobj_cpx
range 0 : 192.168.1.1          192.168.1.11
range 1 : 192.168.2.1          192.168.2.10
[admin@GATEWAY ~]# dynamic_objects -o dynobj_cpx -r 192.168.2.1 192.168.2.10 -d
[admin@GATEWAY ~]# dynamic_objects -o dynobj_cpx -r 192.168.2.1 192.168.2.4 -a
[admin@GATEWAY ~]# dynamic_objects -o dynobj_cpx -r 192.168.2.6 192.168.2.10 -a
[admin@GATEWAY ~]# dynamic_objects -l

object name : dynobj_cpx
range 0 : 192.168.1.1          192.168.1.11
range 1 : 192.168.2.1          192.168.2.4
range 2 : 192.168.2.6          192.168.2.10
```

Dynamic Objects – Handling Deletion problems

- Clone
- Management Push
- HA Push

Dynamic Objects - Clone

```
dynamic_objects -n App_Servers_CLONE
while IFS= read -r range; do
  dynamic_objects -o App_Servers_CLONE -r $range -a
done < <(dynamic_objects -l | awk -v pat= App_Servers '$0~pat' RS=|grep range | awk
'{print $4 " " $5}')

[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1           192.168.1.11
range 1 : 192.168.2.1           192.168.2.10

object name : App_Servers_CLONE
range 0 : 192.168.1.1           192.168.1.11
range 1 : 192.168.2.1           192.168.2.10
```

Dynamic Objects – Clone Commit

- Make your manipulations to the clone, then just replace the original (Remember, it’s just a text file)

```
[admin@GATEWAY ~]# dynamic_objects -o App_Servers_CLONE -r 192.168.2.1 192.168.2.10 -d
[admin@GATEWAY ~]# dynamic_objects -o App_Servers_CLONE -r 192.168.2.1 192.168.2.4 -a
[admin@GATEWAY ~]# dynamic_objects -o App_Servers_CLONE -r 192.168.2.6 192.168.2.10 -a

sed -i "s/App_Servers/DELETE_ME_NOW__/g" $FWDIR/database/dynamic_objects.db
sed -i "s/App_Servers_CLONE/App_Servers/g" $FWDIR/database/dynamic_objects.db
dynamic_objects -do DELETE_ME_NOW__

[admin@GATEWAY ~]# dynamic_objects -l

object name : App_Servers
range 0 : 192.168.1.1          192.168.1.11
range 1 : 192.168.2.1          192.168.2.4
range 2 : 192.168.2.6          192.168.2.10
```

PAYCHEX®
Payroll | Benefits | HR | Insurance

Dynamic Objects – Management Push

- Dynamic object actions can be performed on a management server - the tool exists.
- It’s just a text file
    - SCP the file from the gateway you want to update
    - Make the updates on the manager
    - SCP the file back
    - Need to run some sort of “activation”
- Also great for batch operations – if you use the same dynamic objects across multiple gateways, update once on manager and SCP to all the gateways

Dynamic Objects – HA Standby Push

- Running in HA? Similar idea
- It’s just a text file
  - Check if you’re on that Standby member (if Active, do nothing)
  - Make the updates on the standby member
  - SCP the file to the Active member
  - Run an “activation”

Dynamic Objects – BONUS

Dynamic Objects – Geo protection

- Dynamic objects as Geo protection exceptions was removed in R80.20…but we can work with that
- Create dynamic objects with the country IPs $FWDIR/tmp/geo_location_tmp/IpToCountry.csv
- Block access to these dynamic objects at the top of your rule base
- Need an exception? Just delete the IP from the range
- I can’t do that with Updatable Objects

Dynamic Objects

- Checkpoint has created a python API to facilitate some of these features
- https://github.com/CheckPointSW/dynobj