FLOW UX

Flow Visualization 2.0: Design Improvements

UX Design Document | Jibin Varghese

Design Improvements

Scalability and Usability

01 FILTERING AND GROUPING

Filtering Mechanism

Grouping Mechanism

02 CONFIGURATION IMPROVEMENTS

Configure using Tabular format.

Port Groups

03 ADVANCED VIZ UX IMPROVEMENTS

Multi Select Visual Configuration

Advanced Hover Interactions

TABLE OF CONTENT

- Filtering Mechanism
- Grouping Mechanism
- Configure using Tabular format.
- Port Groups
- Multi Select Visual Configuration
- Advanced Hover Interactions
- Other UX Improvements

Appendix

Meeting Notes

Important Links

PLEASE NOTE:

These are Wireframes (High-Fid-Closer-To-Actual).

Values are dummy.

Content and Visual Design are yet to be done.

For feedback and review

Specifically Configuration related use cases have been considered in below presented designs

FLOW UX

Filtering Mechanism

REQUIREMENT

Support Filtering and Search for Inbound / Outbound flows and AppTiers (Flow Policy Config Page)

Too many traffic lines in the Flow visualization creates clutter and makes it hard to create / update policies

USER STORY

As a user, I am configuring my policy, because of too many traffic lines in the Flow it is hard to create/ update policies and sometimes hinders performance.

IMPROVEMENTS

Flexibility to filter and search for Inbound / Outbound flows and AppTiers.

Filtering Mechanism to assist quick discoverability and usability.

Static lines to show connections and directional animated lines appears, only when the user hover or filter.

Identification tag on filter/search to keep user in context of search/filter type.

CASE#1

Filter using Subnets / IP Address

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 6 — Whitelist Only

Search Source, Port, Categories, etc.

+ Add Source

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

AppType Employee_Payroll

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

Set rules on app, instead.

Outbound Traffic 1 — Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Shows system identified type of search
In this example: Subnet

Inbound Traffic 6

Whitelist Only

192.168

Subnet/IP: 192.168

+ Add Source

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

Set rules on app, instead.

Outbound Traffic 1

Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Shows system identified type of search
In this example: Subnet

Inbound Traffic 6

Whitelist Only

192.168.12.1

Subnet/IP: 192.168.12.1

+ Add Source

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

Set rules on app, instead.

Outbound Traffic 1

Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Shows system identified type of search
In this example: Subnet

Inbound Traffic 6

Whitelist Only

192.168.12.1/22

Subnet/IP: 192.168.12.1/22

+ Add Source

Subnet/IP 192.168.12.1/22

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

Set rules on app, instead.

Outbound Traffic 1

Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

No Inbound source Found.

Inbound Traffic 6 Whitelist Only

192.168.12.7/12

+ Add Source

No Inbound Source Found

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

Set rules on app, instead.

Outbound Traffic 1 Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

CASE#2

Filter using Categories

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 6 — Whitelist Only

Search Source, Port, Categories, etc.

+ Add Source

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

AppType Employee_Payroll

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

Set rules on app, instead.

Outbound Traffic 1 — Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 6 — Whitelist Only

Empl

AppType: Employee_Payroll

+ Add Source

AppType Employee_Payroll

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

Set rules on app, instead.

Outbound Traffic 1 — Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 6 — Whitelist Only

Search Source, Port, Categories, etc.

+ Add Source

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

AppType Employee_Payroll

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

Set rules on app, instead.

Outbound Traffic 1 — Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

CASE#3

Filter using Destination Port

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Shows system identified type of search
In this example: Port

Inbound Traffic 6 Whitelist Only

80

Port: 80

+ Add Source

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

HTTP TCP 80

App Type: BusinessWebsite 3

Search Source, Port, Categories, etc.

+ Add Tier

AppTier App 3

Set rules on app, instead.

Outbound Traffic 1 Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

CASE# 4

Filter on AppTIer

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Shows system identified type of search
In this example: AppTier

Inbound Traffic 6 — Whitelist Only

+ Add Source

AppType Employee_Payroll

App Type: BusinessWebsite 3

App

AppTier: App

+ Add Tier

AppTier App 3

Set rules on app, instead.

Outbound Traffic 1 — Allow All

Search Source, Port, Categories, etc.

+ Add Destination

All Destinations

Explorations

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Search Source, Port, Categories, etc.

Inbound Traffic 6 — Whitelist Only

+ Add Source

Subnet/IP 192.168.12.1/21

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

AppType: BusinessWebsite 3 — Whole App

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

Outbound Traffic 1 — Allow All

+ Add Destination

All Destinations

Options

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Search Source, Port, Categories, etc.

Group by

Please Select

Apply

Inbound Traffic 6

Whitelist Only

AppType: BusinessWebs

affic 1

Allow All

+ Add Source

Subnet/IP 192.168.12.1/21

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

+ Add Tier

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Destination

All Destinations

Options

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	1st March 2019	Ravi, Raj, Ritesh
1.1	Revision	25th May 2019	-

MEETING NOTES:

Date	Notes	Reviewers	Status
24th April 2019	- Would need more grouping types. - VM as popup need to be user validated. - VM Popup columns need to reviewed and if required changed.	Ravi, Raj, Ritesh	-

FLOW UX

Grouping Mechanism

CASE# 1

Grouping using Category or Subnet Type

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Department HR and

Location San Jose

56 VMs

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Group by

Please Select

Apply

Click

Inbound Traffic

+ Add Source

Department HR and

Location San Jose

56 VMs

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic

Group by

Please Select

Apply

Type

CIDR Block

Categories

Services

VLAN

Cluster

Host

+ Add

Department HR and

Location San Jose

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Categories (2)

IP/Subnets (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Categories (2)

Department HR and

Location San Jose

56 VMs

AppType Some other Apptype

IP/Subnets (2)

Click

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Categories (2)

Department HR and

Location San Jose

56 VMs

AppType Some other Apptype

IP/Subnet (2)

Click

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Categories (2)

Department HR and

Location San Jose

56 VMs

AppType Some other Apptype

IP/Subnets (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Categories (2)

IP/Subnets (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

CASE#2

Group using Subnet Ranges

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Group by

Please Select

Apply

- Type
- CIDR Block
- Categories
- Services
- VLAN
- Cluster
- Host

Inbound Traffic

+ Add

Department HR and

Location San Jose

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

/22 (1)

/32 (1)

Other (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

CASE# 3

Group using Categories

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Group by

Please Select

Apply

- Type
- CIDR Block
- Categories
- Services
- VLAN
- Cluster
- Host

Inbound Traffic

Department

Location

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Assigned (1)

Unassigned (1)

Other (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

CASE# 4

Group using Destination Ports

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Group by

Please Select

Apply

- Type
- CIDR Block
- Categories
- Services
- VLAN
- Cluster
- Host

Click

Inbound Traffic

Department

Location

Sa

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Web (1)

SSH (1)

Custom (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

CASE# 5

Group using VLAN

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Group by

Please Select

Apply

- Type
- CIDR Block
- Categories
- Services
- VLAN
- Cluster
- Host

Inbound Traffic

Department

Location Sa

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

VLAN.1 (1)

VLAN.2 (1)

Other (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

CASE# 6

Group using Cluster

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Group by

Please Select

Apply

- Type
- CIDR Block
- Categories
- Services
- VLAN
- Cluster
- Host

Inbound Traffic

Department

Location

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Cluster 1 (1)

Cluster 2 (1)

Other (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

CASE# 7

Group using Host

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic

Group by

Please Select

Apply

Type

CIDR Block

Categories

Services

VLAN

Cluster

Host

Click

Department

Location

Sa

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.2/32

AppType Some other Apptype

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic

Whitelist Only

+ Add Destination

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

Host 1 (1)

Host 2 (1)

Other (2)

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

All Destinations

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	1st March 2019	Ravi, Raj, Ritesh
1.1	Revision	25th May 2019	-

FLOW UX

Named ~~Port~~ Service Groups

USER STORY

#1

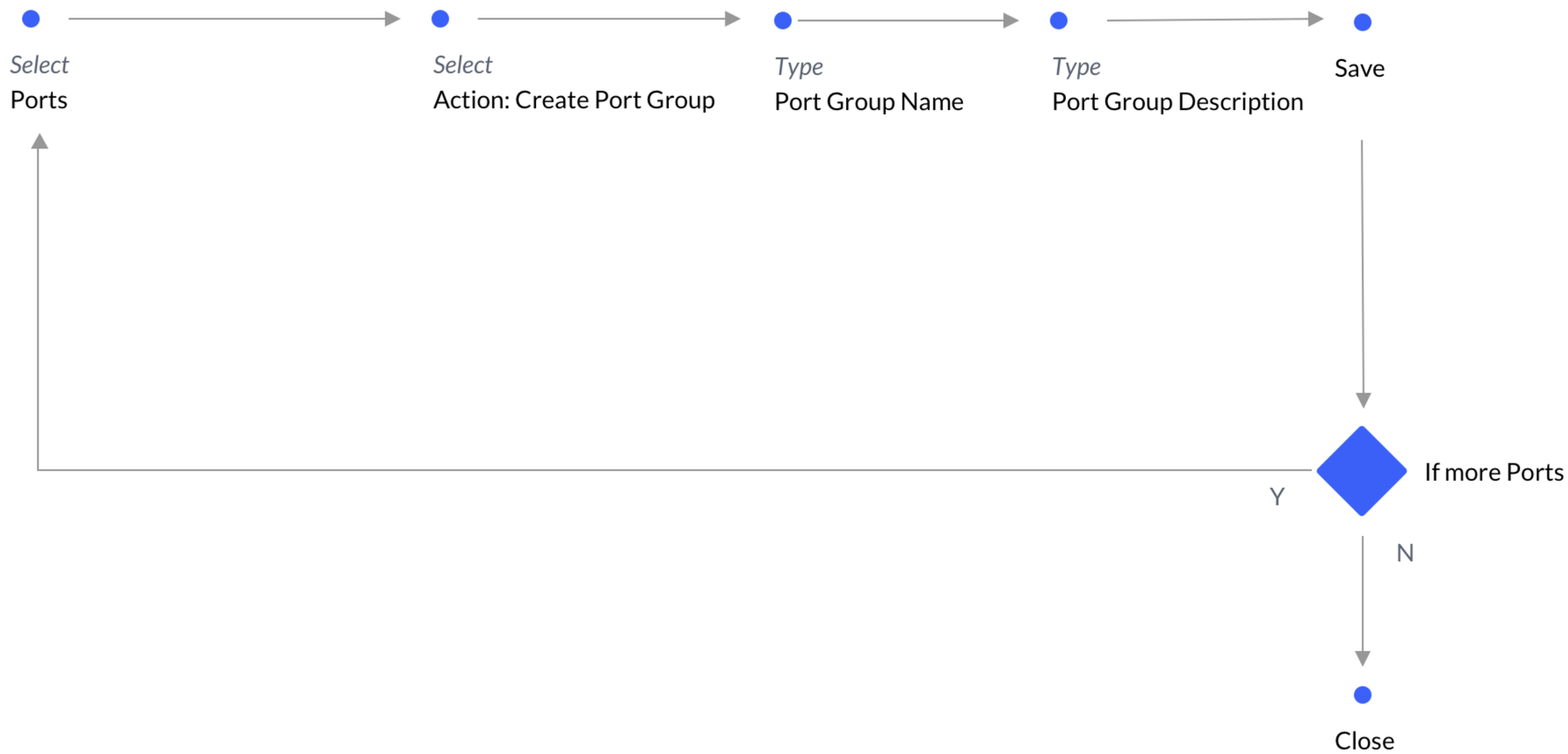
As a user, I should have a feasibility to group protocols and port numbers to a named service type like Web.

#2

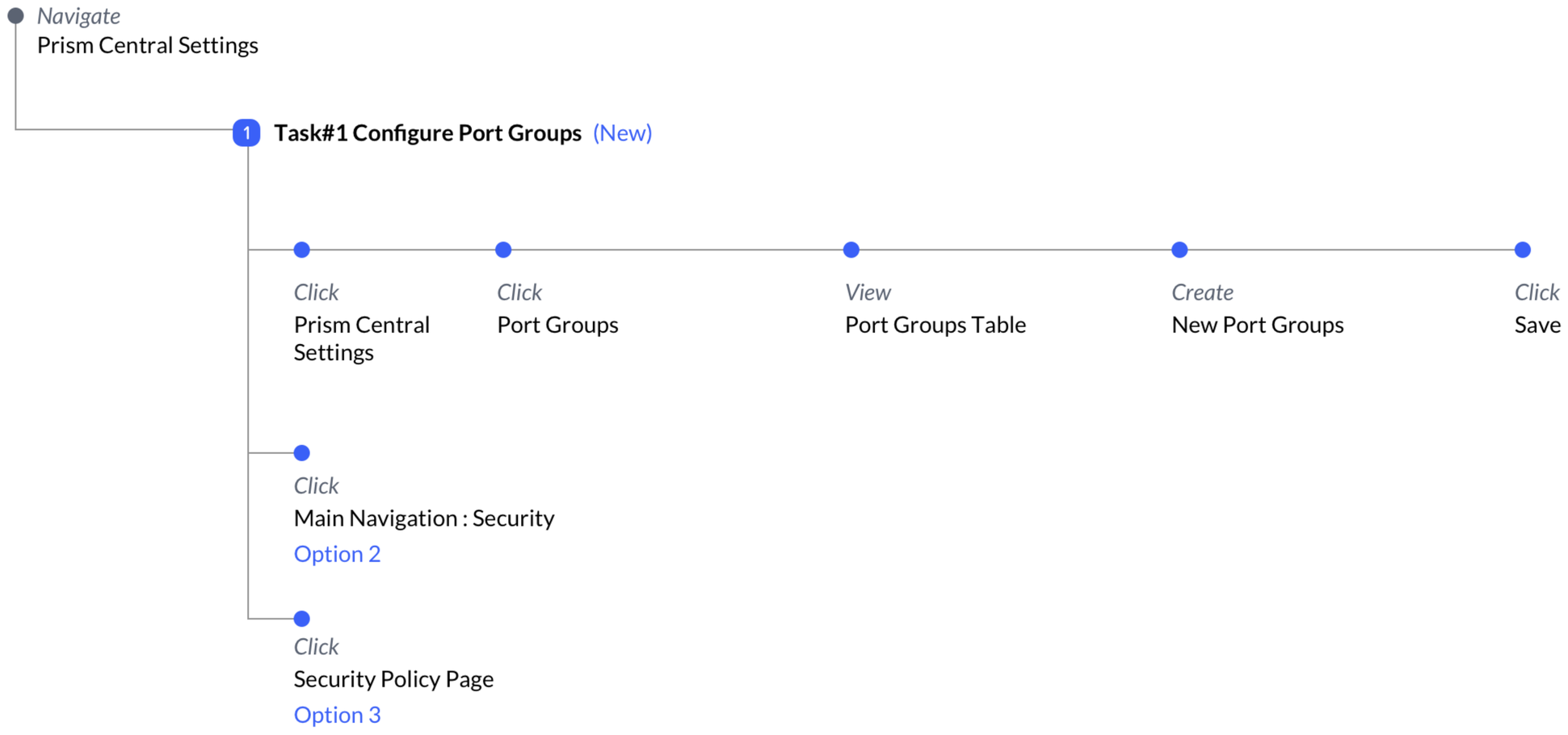
Modifying the port/protocol for this service should reflect in all the policies created using this.

TASK FLOW

1 Task#1 Configure Port Groups (New)



NAVIGATION FLOW



- Dashboard
- Bookmarks
- Browsing History

- Virtual Infrastructure
- Security
- Operations
- Policies
- Hardware
- Activity
- Adminstration
- Services

- Prism Central Settings

Options

Security

42 Security Policies

Summary
Security Planning
Security Policies
Services

+ Add Service | Actions

Service Dictionary

1 - 13 of 13

Service Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162

Options

Security

42 Security Policies

Summary
Security Planning
Security Policies

Services

+ Add Service | Actions

Services Dictionary

1 - 13 of 13

Service Name	Description	Protocol	Port
SSH System Default	Secure Shell	TCP	22
Telnet System Default	Telnet	TCP	23
SMTP System Default	Simple Mail Transfer Protocol	TCP	25
DNS System Default	Domain Name System	TCP	53
DHCP System Default	Dynamic Host Configuration Protocol	UDP	67
HTTP System Default	Hypertext Transfer Protocol	TCP	80
POP System Default	Post Office Protocol (POP) version 3	TCP	110
IMAP System Default	Internet Message Access Protocol	TCP	143
SNMP - TCP System Default	Simple Network Management Protocol	TCP	161
SNMP - UDP System Default	Simple Network Management Protocol	UDP	162
HTTPS System Default	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP System Default	Simple Network Management Protocol	UDP, TCP	162, 162
User_Defined_Port Custom	Creating custom user defined Port	TCP, TCP	443, 80

Security

42 Security Policies

Summary
Security Planning
Security Policies

Services

+ Add Service | Actions

Service Dictionary

1 - 14 of 14

Service Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162
User_Defined_Port	Custom user defined Port	TCP, TCP	443, 80

Security

42 Security Policies

Summary
Security Planning
Security Policies
Services

+ Add Service | Actions

Click

Service Dictionary

1 - 13 of 13

Service Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162

Security

42 Security Policies

Summary
Security Planning
Security Policies
Services

+ Add Service | Actions

Create Service Groups

Click

Service Dictionary

1 - 13 of 13

Service Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162

Security

42 Security Policies

- Summary
- Security Planning
- Security Policies
- Services

+ Add Service | Actions

Selected 1 out of 322 total VMs

1 - 13 of 13

				Port	
☐				21	⋮
☐				22	⋮
☐				23	⋮
☐				25	⋮
☐				53	⋮
☐				67	⋮
☑				80	⋮
☐				110	⋮
☐				143	⋮
☐				161	⋮
☐				162	⋮
☑	HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443	⋮
☐	SNMP	Simple Network Management Protocol	UDP, TCP	162, 162	⋮

Create Service Groups

Port Group Name: User_Defined_Port

Description: Custom user defined Port

Specify the Service Group details

Port Group	Protocol	Port	Actions
HTTP	TCP	80	⊗
HTTPS	TCP	443	⊗

Cancel | Save

Click

Security

42 Security Policies

Summary
Security Planning
Security Policies

Services

+ Add Service | Actions

Service Dictionary

1 - 14 of 14

Service Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162
User_Defined_Port	Custom user defined Port	TCP, TCP	443, 80

Click

Security

42 Security Policies

Summary
Security Planning
Security Policies

Services

+ Add Service | Actions

Service Dictionary

1 - 14 of 14

Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162
User_Defined_Port	Custom user defined Port	TCP, TCP	443, 80

Edit
Remove
Click

Security

42 Security Policies

Summary
Security Planning
Security Policies
Services

+ Add Port | Actions

Port Dictionary

1 - 14 of 14

Name	Description	Protocol	Port
FTP	File Transfer Protocol	TCP	21
SSH	Secure Shell	TCP	22
Telnet		TCP	23
SMTP		TCP	25
DNS		TCP	53
DHCP		UDP	67
HTTP		TCP	80
POP		TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162
User_Defined_Port	Custom user defined Port	TCP, TCP	443, 80

Delete this Service Group

Deleting **User_Defined_Service_Group** will affect **2 security policies**, If yes type 'DELETE'.

Type DELETE

Cancel | Delete

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

Click

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic Whitelist C

Traffic Whitelist Only

Subnet 10.

Subnet 10.

+ Add Source

+ Add Destination

Option

Create Inbound Rule

1 Inbound Source

AppType BusinessWebsite

Option Created for On-the-Fly creation of Ports in Port Dictionary

Specify the Service details

+ Add

Service Name	Description	Protocol	Port	Actions
User_Defined				

User_Defined_Port

Click

Redirect through service chain

East West Firewall

Cancel Save

Inbound Traffic Whitelist C

Traffic Whitelist Only

Subnet 10.

Subnet 10.

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source — AppType BusinessWebsite

Specify the Service details + Add

Port Name	Description	Protocol	Port	Actions
User_Defined_Port	User Defined Port..	TCP,TCP	80,443	

☐ Redirect through service chain

East West Firewall

Cancel Save

Click

Appendix

ENTRY POINT

Port Groups Configuration can be placed either on:

OPTION 1	Prism Central Settings Page : If its going to be used for multiple product offerings	✓
OPTION 2	Security Policies Page: If we wish to keep the port groups on Security Policies only.	✗
OPTION 3	On redesigned Navigation: Security Page If we wish to keep the port groups for flow related services like but not anywhere else.	✓

Settings

Options

Connect to Citric Cloud

Prism Central Registration

Pulse

Reck Configuration

Network

HTTP Proxy

Name Servers

Network Configuration

Network Switch

NTP Servers

SNMP

Flow

Service Groups

Security

Cluster Lockdown

SSL Certificate

Authentication

Role Mapping

Prism Central Settings

Choose an item on the left to configure

- Dashboard
- Bookmarks
- Browsing History

- Virtual Infrastructure
- Security
- Operations
- Policies
- Hardware
- Activity
- Adminstration
- Services

- Prism Central Settings

Options

Security

42 Security Policies

Summary
Security Planning
Security Policies

Service Groups
Subnet Groups

+ Add Port | Actions

Service Group Dictionary

1 - 13 of 13

Service Name	Description	Protocol	Port
User_Defined_Custom_Port	User Defined Custom Port	TCP	112
SSH	Secure Shell	TCP	22
Telnet	Telnet	TCP	23
SMTP	Simple Mail Transfer Protocol	TCP	25
DNS	Domain Name System	TCP	53
DHCP	Dynamic Host Configuration Protocol	UDP	67
HTTP	Hypertext Transfer Protocol	TCP	80
POP	Post Office Protocol (POP) version 3	TCP	110
IMAP	Internet Message Access Protocol	TCP	143
SNMP - TCP	Simple Network Management Protocol	TCP	161
SNMP - UDP	Simple Network Management Protocol	UDP	162
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	443
SNMP	Simple Network Management Protocol	UDP, TCP	162, 162

Options

Security Policies

3 Policies

Summary

Create Security Policy | Export & Import | Port Groups

Click

Name	Policy Type	Policy	Status
Type to filter...			
Secure MySQL	App Policy	App Policy for MySQL Application: AppTier App; AppType MySQL; Environment Production; AppType Employee Payroll; 2 more	Enforced
Dev Prod Isolation	Isolation Policy	Isolate Test and Production Workloads: Environment Development; Environment Production	Monitoring
My VDI Policy	VDI Policy	Policy for VDI Environment: Subnet/IP 192.168.10.1/24; Subnet/IP 192.168.12.1/24; ADGroups; AppType Employee Payroll; 3 more	Monitoring

Options

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

This option may delink Port & Service Group creation but easy and less columns.

Option

Create Inbound Rule

1 Inbound Source ····· AppType BusinessWebsite

Specify the Port details

+ Add Rule

Protocol	Port	Actions
TCP		

- HTTP TCP 80
- FTP TCP 21
- User_Defined TCP 80, 443

Cancel

Save

Click

Inbound Traffic

Whitelist C

Traffic

Whitelist Only

Subnet 10.

Subnet 10.

+ Add Source

+ Add Destination

Security

42 Security Policies

Summary
Security Planning
Security Policies

Services

+ Add Service

Service Dictionary

1 - 13 of 13

Create Service Groups

To create Service Groups please select from available service or add new service.

Service Name

User_Defined_Service

Description

Custom user defined Service

Specify the Service Group details

+ Add Service

Service	Protocol	Port	Actions
Service	Any		

Cancel

Create

OPEN QUESTIONS

Since port groups is used in other context in different product. What should port groups be reffered as?
Service Groups

Should user be restricted only to user defined ports in port group?
No he should be able to create port groups on the fly.

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	1st March 2019	Ravi, Raj, Ritesh
1.1	Revision	30th May 2019	-
2.0	Revision, addition of few cases	4th June 2019	Abhishek, Ritesh, Raj, Ravi
2.1	Revision, Renaming as Service Groups, Entry Point	11th June 2019	Ravi Samprathi

FLOW UX

Configuration using Tabular View

OBJECTIVE

Many customers are used to **more traditional** (yet advanced / easy to use) FW Rules configuration.

These traditional way are mostly **a tabular view** (list view)

Though Visualization is a USP, however an **alternative** is required.

PRD

Selling to Security Admins require a more traditional view of the configuration.

There are known issues with mixing configuration and visualization in terms of max Inbound rules that can be configured (378).

Many customers are used to more traditional (yet advanced / easy to use) FW Rules configuration.

Tabular format for is one of the ways to address rule configuration - there could be other ways to address configuring firewall rules without traffic Flow visualization (this ask is about ease of rule configuration not a specific way of doing it). Tabular form is however most prevalent and easy to understood option

Reference:
Flow Visualization Improvements | Created by Abhishek Tiwari
https://confluence.eng.nutanix.com:8443/x/KIDuAQ

USER STORY

As a security admin, traditionally I am used to configure FW rules on more flat / tabular mode with using 5 tuple method
Src-Src port - Dest- Dest Ports - Protocol.

As an user I wish configuration mode that supports this traditional configuration style.

IMPROVEMENTS

Addition of Tabular Mode for configuration.

Tabular mode ideated to be **a middle ground** between traditional configuration and existing flow visualization.

User can **switch between Visualization-Tabular View** as it will facilitate Preview-Configuration Approach.

NAVIGATION FLOW

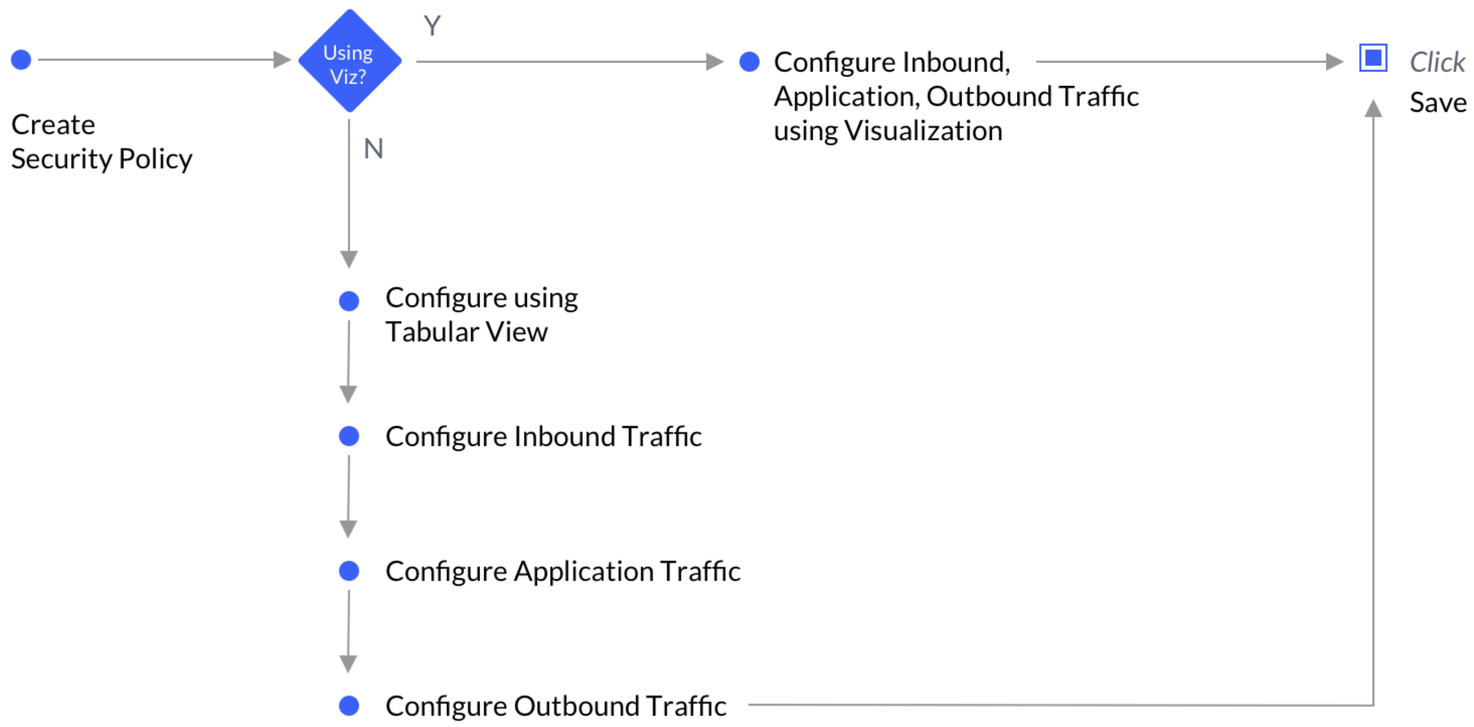
Login
Prism Central

1 Task#1 Configure Security Policy using table (New)

Navigate	*Click*	*Create*	*Type*	*Click*
Main Menu	Security Policies	New Security Policy	Add Policy Details	Tabular View

TASK FLOW

1 Task#1 Configure Security Policy using Table (New)



Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Tabular Control on Panel to open popup.

Inbound Traffic 1 Whitelist Only

+ Add Source

App Type: Business Website 3

AppTier BusinessWebsite

Set rules on app, instead.

Outbound Traffic Allow All

+ Add Destination

Inbound Traffic 1

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Sour

d Destination

Add Inbound Rules

Inbound Rules 8

Actions + Add Rule 1 – 7 of 200

Source	Destination	Portocol	Port	Service Chain
Type to filter...				
192.180.12.1/11	AppTier	TCP	80	No

AppTier: Web
AppTier: DB
AppTier: App
default

HTTP TCP 80
FTP TCP 21
User_Defined TCP 80, 443

Cancel Save

Create App Security Policy

Inbound Rule Popup.

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 1

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Sour

d Destination

Add Inbound Rules

Inbound Rules 8

Actions + Add Rule 1 – 7 of 200

Source	Destination	Protocol	Port	Service Chain
Type to filter...				
Subnet 192.23.23.103/56	AppTier Web	TCP	80	No
Subnet 192.23.23.106/87	AppTier App	TCP	25	No
Subnet 10.28.32.40/10	AppTier Web	UDP	12	No
Subnet 10.28.32.32/2	AppTier Web	TCP	20	No
Subnet 10.28.32.43/12	AppTier Web	UDP	11	No
Subnet 10.28.32.51/32	AppTier Web	UDP,TCP	10,80	No
Subnet 10.28.32.52/14	AppTier Web	UDP	44	No
192.180.12.1/11	AppTier	TCP	80	No

AppTier: Web
AppTier: DB
AppTier: App
default

HTTP TCP 80
FTP TCP 21
User_Defined TCP 80, 443

Cancel Save

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 1 Whitelist Only

+ Add Source

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

App Type: Business Website 3

Click

+ Add Tier

AppTier Web 3

AppTier App 2

AppTier DB 2

Set rules on app, instead.

Outbound Traffic Allow All

+ Add Destination

All Destination

Create App Security Policy

Inbound Rule Popup.

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 1

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Sour

d Destination

Add Microsegmentation Rules

AppType: Business Website 3

Actions + Add Rule 1 – 7 of 200

Source	Destination	Protocol	Port	Link Source VMs	Service Chaining
Type to filter...					
AppTier Web	AppTier App	TCP	80	Yes	Yes
AppTier App	AppTier DB	TCP	20	No	No
AppTier App	AppTier Web	TCP	34	No	No

Cancel Save

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 3 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: MyApp 3

AppTier Web 3

AppTier App 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Allow All

Click

+ Add Destination

All Destination

Create App Security Policy

Inbound Rule Popup.

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 1

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Sour

d Destination

Add Inbound Rules

Outbound Rules 1

Actions + Add Rule 1 – 7 of 200

Source	Destination	Portocol	Port	Service Chain
Type to filter...				
AppTier Web	Destination Any	Any	Any	Yes

Cancel Save

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 3 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: MyApp 3

AppTier Web 3

AppTier App 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic 1 Whitelist Only

All Destination

+ Add Destination

Explorations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View

Next

User can use Tabular View for traditional way of flow rule configuration.

Inbound Traffic Whitelist Only

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Inbound Rule

- (•) Allow All
  Allow all inbound traffic
- ( ) Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Use Default Save

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ◉ Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

No Inbound Rules have been created

+ Inbound Rule

Click

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Add Inbound Rule

Source

192.168.20.1/1

Apply Rule on App Tier

Destination

AppType: BusinessWebsite

Configure Manually Use Port Groups

Click

Specify the protocol details

+ Add Rule

Protocol	Port	Actions
Any	Eg: 'Any', 80, 20-26	

Cancel Save

d Rule

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Add Inbound Rule

Source

192.168.20.1/1

Apply Rule on App Tier

Destination

AppType: BusinessWebsite

New Feature- Port Groups

Configure Manually

Use Port Groups

Click

Port Group

Web_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Cancel Save

d Rule

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ● Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Similarly adding multiple Rules

Inbound Rules 3

Actions + Add Rule

	Source		Destination		Protocol	Port	Service Chain	
☐	Subnet	192.168.12.1/24	AppTier	Web	TCP	80	Yes	⋮
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	No	⋮
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	No	⋮

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ● Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Similarly adding multiple Rules

Inbound Rules 3

Actions ⌄ + Add Rule

Delete
Clone
Disable

	Source		Destination		Protocol	Port		
☐	Subnet	192.168.12.1/24	AppTier	Web	TCP	80		⋮
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	No	⋮
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	No	⋮

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Click

Application Traffic

- (•) Set rules on **AppType: BusinessWebsite**
  Secure the whole application
- ( ) Set rules on AppTiers of **AppType: BusinessWebsite**
  Secure and create rules on application tiers

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Application Traffic

- ○ Set rules on **AppType: BusinessWebsite**
  Secure the whole application
- ◉ Set rules on AppTiers of **AppType: BusinessWebsite**
  Secure and create rules on application tiers

AppType: Business Website 3 Actions + Add Rule

	Source	Destination	Protocol	Port	Link Source VMs	Service Chaining
☐	AppTier Web	AppTier App	TCP	80	Yes	Yes
☐	AppTier App	AppTier DB	TCP	20	No	No
☐	AppTier App	AppTier Web	TCP	34	No	No

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

+ Add Rule

Add Microsegmentation Rule

Source

AppTier: App

Can Source VMs Talk to each other? Yes No

Destination

AppTier: DB

Configure Manually Use Port Groups

Specify the protocol details

+ Add Rule

Protocol	Port	Actions
TCP	20	

Cancel Save

Click

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Application Traffic

- ○ Set rules on whole Application
  Secure the application as a whole
- ◉ Set rules on AppTiers of MyApp Application
  Secure and create rules on Application Tiers

Microsegmentation Rule

+ Add Rule

Source	Destination	Protocol	Port	Link Source VMs	Action
AppTier Web	AppTier App	TCP	80	Yes	Allow
AppTier App	AppTier DB	TCP	20	No	Allow
AppTier App	AppTier Web	TCP	34	No	Allow

Clicking the Dots provides user option to edit or delete the records.

Edit
Remove

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

Click

Outbound Rule

- (•) Allow All
  Allow all inbound traffic
- ( ) Whitelist Only (Recommended)
  Allow only whitelisted inbound traffic mentioned in table below.

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

Inbound Traffic | Application Traffic | Outbound Traffic

User can Preview the table configuration using “Visualization View” or vica versa.

Outbound Rule

- ○ Allow All
  Allow all inbound traffic
- ◉ Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Outbound Rule 3 Actions + Add Rule

Source	Destination	Protocol	Port	Service Chain
AppTier Web	Destination Any	Any		Yes

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

User can return to previous Tabular Mode

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: Business Website 3

AppTier Web 3

AppTier App 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

All Destination

+ Add Destination

Options

OTHER EXPLORATIONS

Some other Explorations to view different grouped rules.

Create App Security

Option 1
Side Summary Navigation Bar

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

- **Inbound Rule**
  Whitelist Only
- **Application Rules**
  Apptype: BusinessWebsite
- **Outbound Rules**
  Allow All

[Exploration] Ideas is to give a quick summary.

Inbound Rule

- (•) **Allow All**
  Allow all inbound traffic
- ( ) **Whitelist Only**
  Allow only whitelisted inbound traffic mentioned in table below.

Click

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

- Inbound Rule
  Whitelist Only
- Application Rules
  Apptype: BusinessWebsite
- Outbound Rules
  Allow All

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ● Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

No Inbound Rules have been created

+ Inbound Rule

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

- **Inbound Rule**
  Whitelist Only
- **Application Rules**
  Apptype: BusinessWebsite
- **Outbound Rules**
  Allow All

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ● Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Inbound Rules 3

Actions + Add Rule

	Source		Destination		Protocol	Port	Service Chain	
☐	Subnet	192.168.12.1/24	AppTier	Web	TCP	80	Yes	⋮
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	No	⋮
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	No	⋮

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

- **Inbound Rule**
  Whitelist Only
- **Application Rules**
  Apptype: BusinessWebsite
- **Outbound Rules**
  Allow All

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ● Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Inbound Rules 3

Actions + Add Rule 1 – 7 of 200

	Source	Destination	Protocol	Port	Service Chain
	Type to filter...				
	192.180.12.1/11	AppTier	TCP	80	No
	Subnet 192.23.23.103/56	AppTier Web	TCP	80	No
	Subnet 192.23.23.106/87	AppTier App	TCP	25	No
	Subnet 10.28.32.40/10	AppTier Web	UDP	12	No
	Subnet 10.28.32.32/2	AppTier Web	TCP	20	No
	Subnet 10.28.32.43/12	AppTier Web	UDP	11	No
	Subnet 10.28.32.51/32	AppTier Web	UDP,TCP	10,80	No
	Subnet 10.28.32.52/14	AppTier Web	UDP	44	No

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

- **Inbound Rule** — Whitelist Only
- **Application Rules** — Apptype: BusinessWebsite
- **Outbound Rules** — Allow All

Inbound Traffic

- ○ Allow All
  Allow all inbound traffic
- ● Whitelist Only
  Allow only whitelisted inbound traffic mentioned in table below.

Inbound Rules 3

Actions + Add Rule 1 – 7 of 200

Source	Destination	Protocol	Port	Service Chain	
Type to filter...					
192.180.12.1/11	AppTier	TCP	80	No	
Subnet 192.23.23.103/56				No	
Subnet 192.23.23.106/87				No	
Subnet 10.28.32.40/10				No	
Subnet 10.28.32.32/2	AppTier	Web		No	
Subnet 10.28.32.43/12	AppTier	Web	UDP	11	No
Subnet 10.28.32.51/32	AppTier	Web	UDP,TCP	10,80	No
Subnet 10.28.32.52/14	AppTier	Web	UDP	44	No

AppTier: Web
AppTier: DB
AppTier: App
default

TCP
UDP
ICMP

Port Groups

Web_Port_1 TCP, UDP

Options

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Visualization View Next

- **Inbound Rule**
  Whitelist Only
- **Application Rules**
  Apptype: BusinessWebsite
- **Outbound Rules**
  Allow All

Inbound Traffic

- ○ **Allow All**
  Allow all inbound traffic
- ● **Whitelist Only**
  Allow only whitelisted inbound traffic mentioned in table below.

Inbound Rules 3

Actions + Add Rule

	Source		Destination		Protocol	Port	Service Chain
☐	Subnet	192.168.12.1/24	AppTier	Web	TCP	80	●
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	●
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	○
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	●
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	●
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	○
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	○
☐	Subnet	192.168.12.1/25	AppTier	Web	TCP	62	○
☐	Subnet	192.168.12.1/26	AppTier	App	TCP	43	○

Options

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	20th March 2019	Ritesh Jain
2.0	Revision	14th May 2019	-

MEETING NOTES:

Date	Notes	Reviewers	Status
14th May 2019	- Addition of service chaining tab. - Removal of Action tab: Allow, Block Option from tabular view. - Table Organisation with multiple action options. - Making Application name available for Application Traffic view.	Ritesh Jain	Revised. Available in Version 2.0
14th May 2019	- Actual need for tabular configuration? - What is good and not so good with traditional way of configuration? - To help users, Can quick summary be given of defaults?	Design Team	-

FLOW UX

Multi Select Advanced Configuration

REQUIREMENT

Support Filtering and Search for Inbound / Outbound flows and AppTiers (Flow Policy Config Page)

Too many traffic lines in the Flow visualization creates clutter and makes it hard to create / update policies

USER STORY

As a user, I am configuring my policy, because of too many traffic lines in the Flow it is hard to create/ update policies and sometimes hinders my performance.

IMPROVEMENTS

Flexibility to filter and search for Inbound / Outbound flows and AppTiers.

Filtering Mechanism to assist quick discoverability and usability.

Static lines to show connections and directional animated lines appears, only when the user hover or filter.

Identification tag on filter/search to keep user in context of search/filter type.

Multi Selection

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic Whitelist Only

Add Source By: Subnet

192.168.12.1/24

Add

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 — Whitelist Only

Subnet 10.1.2.3/33

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic — Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 — Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic — Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppType BusinessWebsite

Configure Manually

Use Port Groups

Specify the protocol details

+ Add Rule

Protocol	Port	Actions
Any	Eg: 'Any', 80, 20-26	

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppType BusinessWebsite

Configure Manually

Use Port Groups

Using Port Groups helps as aggregated port groups.

Port Group

Custom_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

4 Inbound Source

AppType BusinessWebsite

Configure Manually

Use Port Groups

Using Port Groups helps as aggregated port groups.

Port Group

Web_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

TCP Port 80

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 5 — Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic 1 — Allow All

All Destinations

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

This policy allows

5	0	All
Inbound Connection(s)	Internal Connection(s)	Outbound Connection(s)

Apply Now Save & Monitor

Inbound Traffic 5 Whitelist Only

- Subnet/IP 192.168.12.1/24
- Subnet/IP 192.168.12.1/25
- Subnet/IP 192.168.12.1/25
- Subnet/IP 192.168.12.1/25
- Subnet/IP 192.168.12.1/25

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic 1 Allow All

All Destinations

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	1st March 2019	-

OTHER EXPLORATIONS

Multiselect on AppTier

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic Whitelist Only

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic Whitelist Only

Add Source By: Subnet

192.168.12.1/24

Add

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet 10.1.2.3/33

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 — Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic — Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

All Destination 10.1.2.3/33

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

Select a tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

All Destination 10.1.2.3/33

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

All Destination 10.1.2.3/33

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

All Destination

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

All Destination 10.1.2.3/33

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppTier App

Configure Manually Use Port Groups

Specify the protocol details

+ Add Rule

Protocol	Port	Actions
Any	Eg: 'Any', 80, 20-26	

Redirect through service chain

East West Firewall

Cancel Save

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppTier App

Configure Manually

Use Port Groups

Using Port Groups helps as aggregated port groups.

Port Group

Web_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppTier App

Configure Manually

Use Port Groups

Using Port Groups helps as aggregated port groups.

Port Group

Web_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppTier Web

Configure Manually

Use Port Groups

Using Port Groups helps as aggregated port groups.

Port Group

Web_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

Can VM in this tier talk to each other?
Yes No

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1

Whiteli

ffic

Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

+ Add Destination

Create Inbound Rule

1 Inbound Source

AppTier Web

Configure Manually

Use Port Groups

Using Port Groups helps as aggregated port groups.

Port Group

Web_Port_1

Each Inbound Source will be talk on Ports defined in Web_Port_1.

Redirect through service chain

East West Firewall

Cancel

Save

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

FLOW UX

Hover States

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 2

Whitelist Only

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

+ Add Source

App Type: BusinessWebsite

App Tier Appserver

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

No Animated Lines in Static state.

Outbound Traffic 1

Allow All

All Destination

Show Discovered Traffic

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 2

Whitelist Only

Animated Lines show on contextual Hover.

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

+ Add Source

App Type: BusinessWebsite

App Tier Appserver

Hover

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

Outbound Traffic 1

Allow All

All Destination

Show Discovered Traffic

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 2

Whitelist Only

Outbound Traffic 1

Allow All

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

+ Add Source

Protocol/ Port TCP 80

Hover

App Type: BusinessWebsite

App Tier Appserver

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

All Destination

Show Discovered Traffic

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Inbound Traffic 2

Whitelist Only

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

+ Add Source

App Type: BusinessWebsite

App Tier Appserver

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

Outbound Traffic 1

Allow All

All Destination

Hover

Show Discovered Traffic

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Hover

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Click

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Click

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Hover

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier App 3

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic Whitelist Only

+ Add Destination

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	20th March 2019	-

FLOW UX

VM Pop Up

REQUIREMENT

Clicking on VMs tag for the category boxes in security page takes user out of context from the security page.

USER STORY	As a user, I wish to view VMs which are part of particular category while am configuring my policy.
IMPROVEMENTS	Pop Up with required VM details Introduced.

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 6 — Whitelist Only

Subnet/IP 192.168.12.1/21

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

+ Add Source

App Type: BusinessWebsite 3

AppTier App 3

Click

AppTier Web 2

AppTier DB 2

+ Add Tier

Set rules on app, instead.

Outbound Traffic 1 — Allow All

All Destinations

+ Add Destination

Show Discovered Traffic

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 6

Whiteli

ffic 1

Allow All

Subnet/IP 192.168.12.1/21

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

+ Add Source

+ Add Destination

Virtual Machines: App

Required Columns can be changed.

List of Virtual Machines

Name	Host	Hypervisor	Project	IP Address	Power State
VM_Test1	Host1	AHV	default	10.51.121.12	On
VM_Test2	Host1	AHV	default	10.51.121.13	On
VM_Test3	Host1	AHV	default	10.51.121.14	On

Close

Explorations

Inbound Traffic 6

Whiteli

ffic 1

Allow All

Subnet/IP 192.168.12.1/21

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

+ Add Source

+ Add Destination

Options

Virtual Machines: App

Required Columns can be changed.

List of VMs

Name	IP	Cluster	Status
aparche-db-01	10.0.0.1	puppyfood	On
aparche-db-02	10.0.0.2	puppyfood	On
oracle-zwx	220.5.23.1	stark	On
aparche-db-04	10.0.0.4	puppyfood	Off

Show VM Details

Close

Create App Security Policy

‹ Back

1 Finished Step 2 Current Step 3 Unfinished Step

Next

Inbound Traffic 6

Whiteli

ffic 1

Allow All

Subnet/IP 192.168.12.1/21

Subnet/IP 192.168.12.1/22

Subnet/IP 192.168.12.1/23

Subnet/IP 192.168.12.2/32

Subnet/IP 192.168.24.2/2

Subnet/IP 192.168.18.5/12

+ Add Source

ations

+ Add Destination

Options

Virtual Machines: App

Required Columns can be changed.

List of VMs

Name	IP
aparche-db-01	10.0.0.1
aparche-db-02	10.0.0.2
oracle-zwx	220.5.23.1
aparche-db-04	10.0.0.4

Show VM Details

Close

REVISIONS

Version	Changes	Date	Reviewed By
1.0	Initial Draft	4th March 2019	Ravi Samprathi
1.1	IP Address Column Added to PopUp	20th March 2019	Ravi Samprathi

FLOW UX

Control Bar Options

Inbound Traffic 1 Rule

Whitelist Only

Subnet/IP 192.168.12.1/21

Inbound Traffic 1 Rule

Whitelist Only

Search Categories, Subnets, Ports etc.

Search Bar appears below on Click

Subnet/IP 192.168.12.1/21

Inbound Traffic 1 Rule

Whitelist Only

Subnet/IP 192.168.12.1/21

Inbound Traffic 1 Rule

Whitelist Only

Subnet/IP 192.168.12.1/21

Inbound Traffic 1 Rule

Whitelist Only

Group By

Apply

Filter/Group By appears below on Click

Subnet/IP 192.168.12.1/21

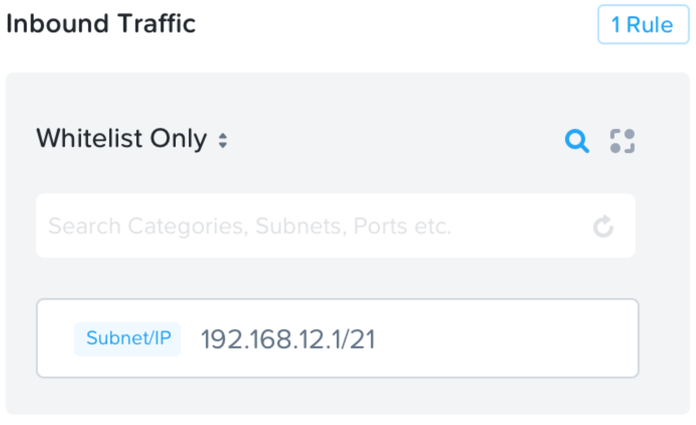
Inbound Traffic 1 Rule

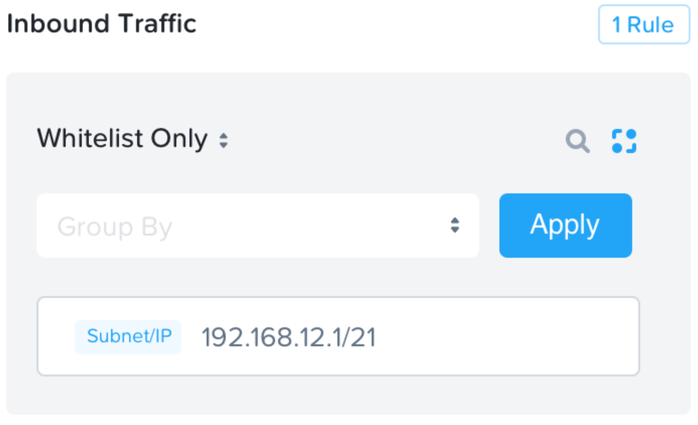
Whitelist Only

Subnet/IP 192.168.12.1/21

Option 1

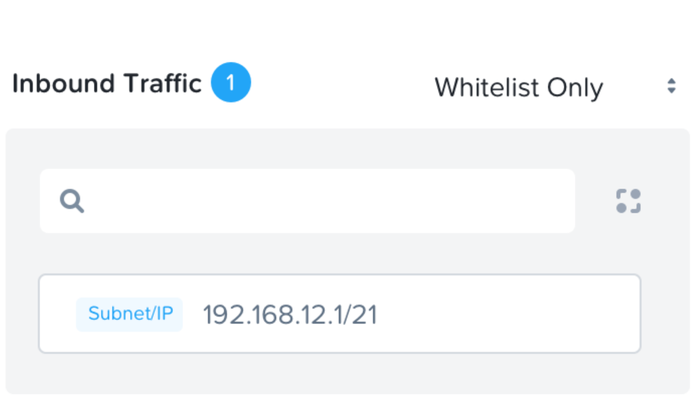
Less Noise.
Consistent Interaction across controls.
Flexibility for more control.
On Demand Actions.

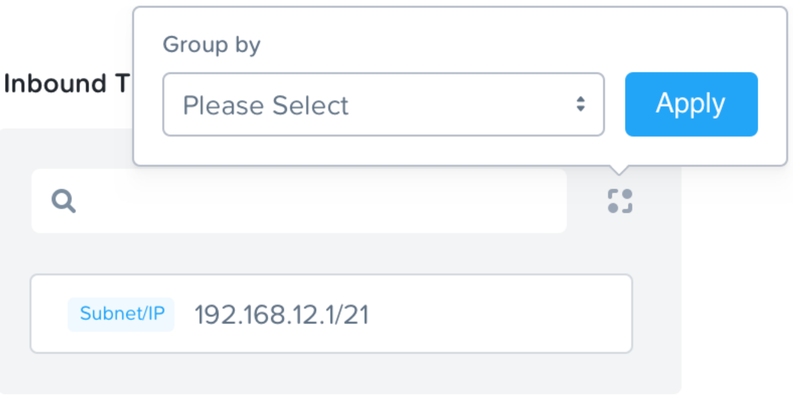




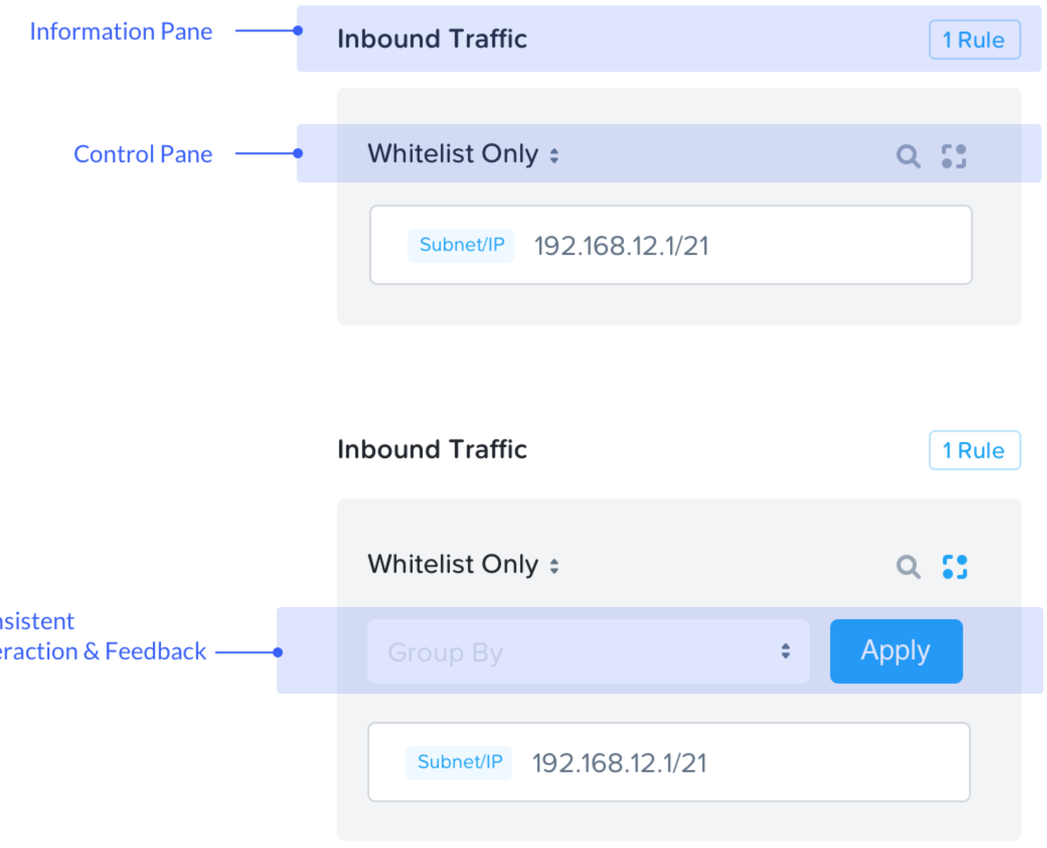
Option 2

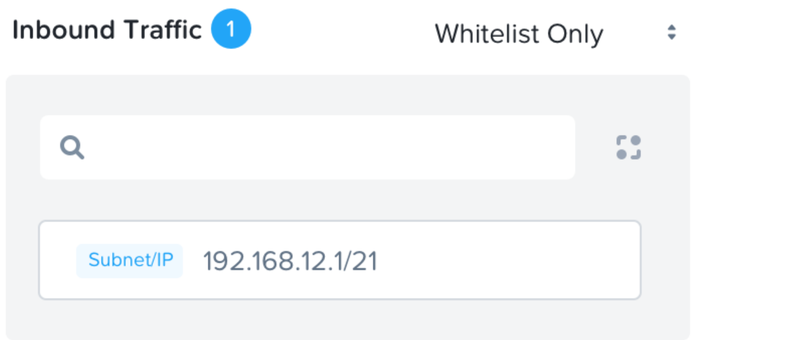
Search heavy view.
Inconsistent Control Panel
Easy and Quick Search

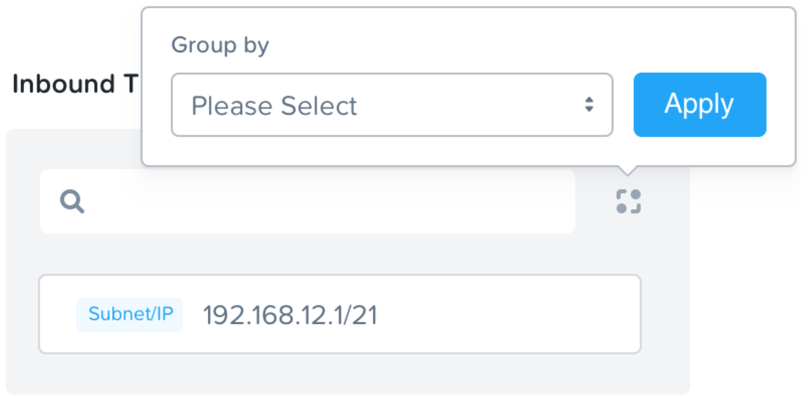


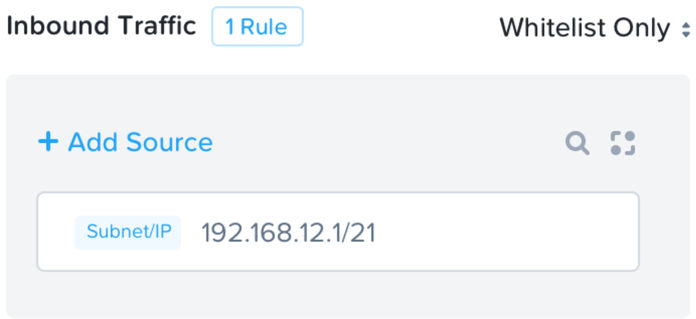


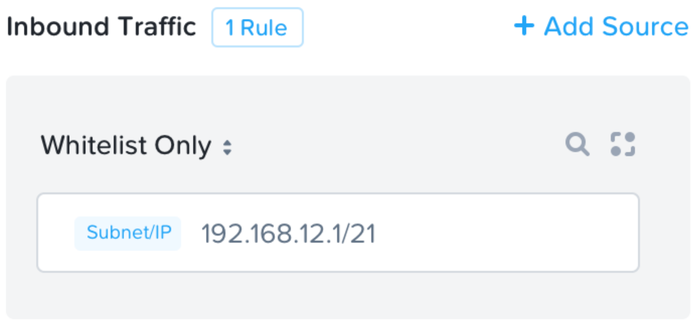
Less Noise.
Consistent Interaction across controls.
Flexibility for more control.
On Demand Actions.

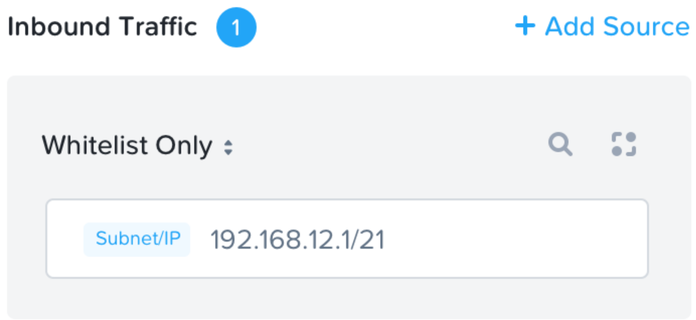


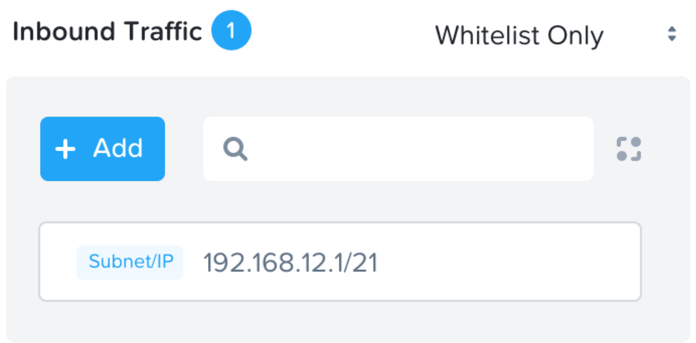


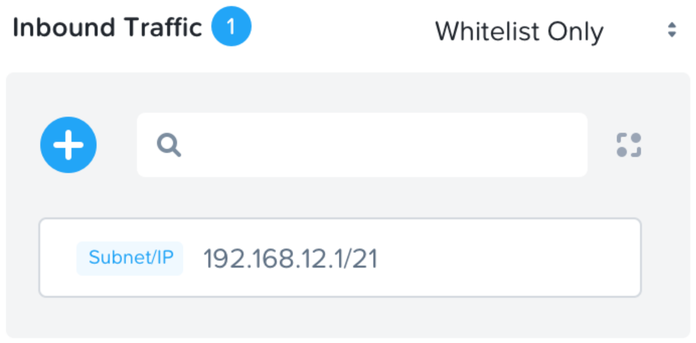


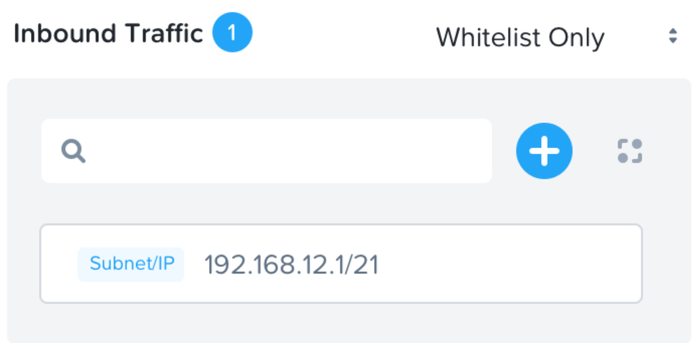

Inbound Traffic
1 Rule
Whitelist Only
+ Add Source
Subnet/IP
192.168.12.1/21

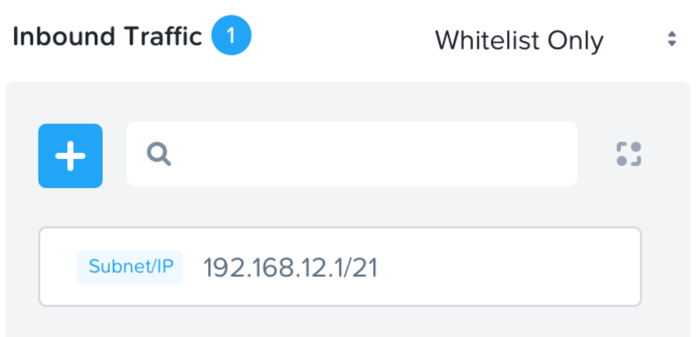

Inbound Traffic
1 Rule
+ Add Source
Whitelist Only
Subnet/IP
192.168.12.1/21

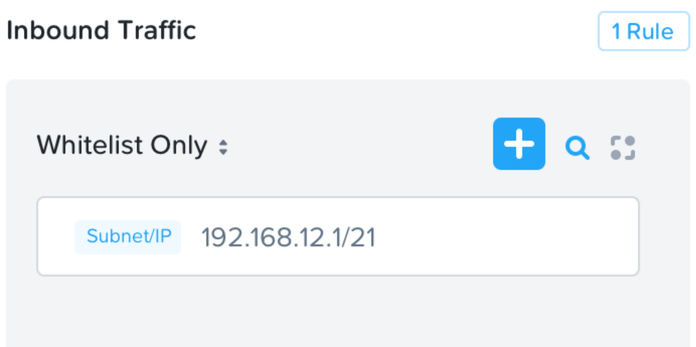

Inbound Traffic
1
+ Add Source
Whitelist Only
Subnet/IP
192.168.12.1/21

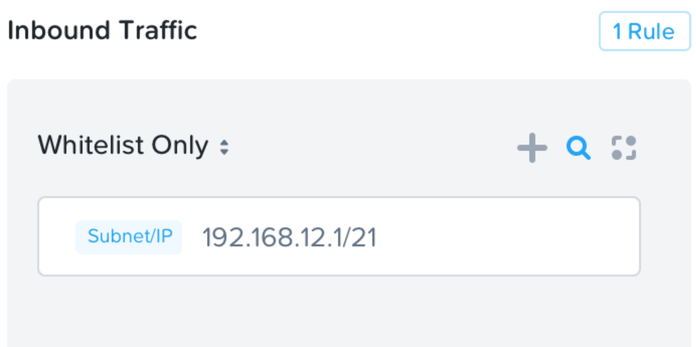

Inbound Traffic
1
Whitelist Only
+ Add
Subnet/IP
192.168.12.1/21

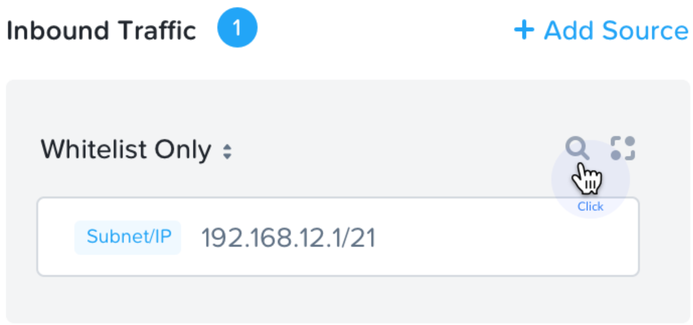

Inbound Traffic
1
Whitelist Only
Subnet/IP
192.168.12.1/21

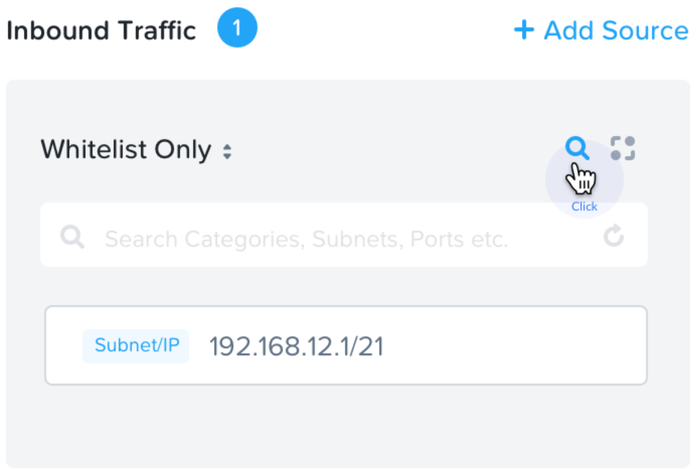

Inbound Traffic
1
Whitelist Only
Subnet/IP
192.168.12.1/21

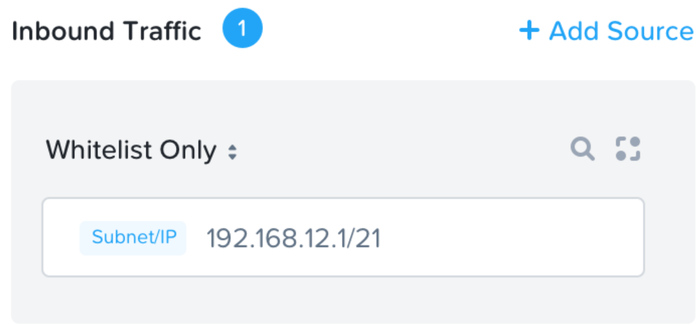

Inbound Traffic
1
Whitelist Only
Subnet/IP
192.168.12.1/21

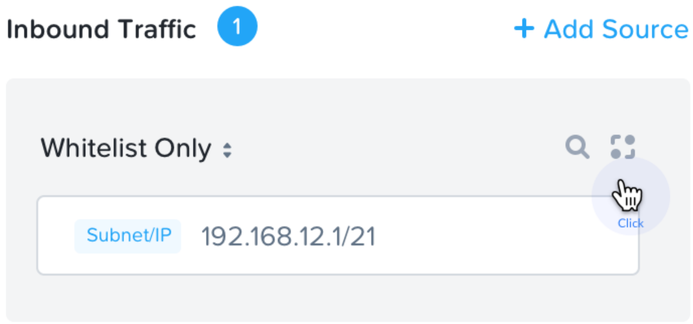

Inbound Traffic
1 Rule
Whitelist Only
Subnet/IP
192.168.12.1/21

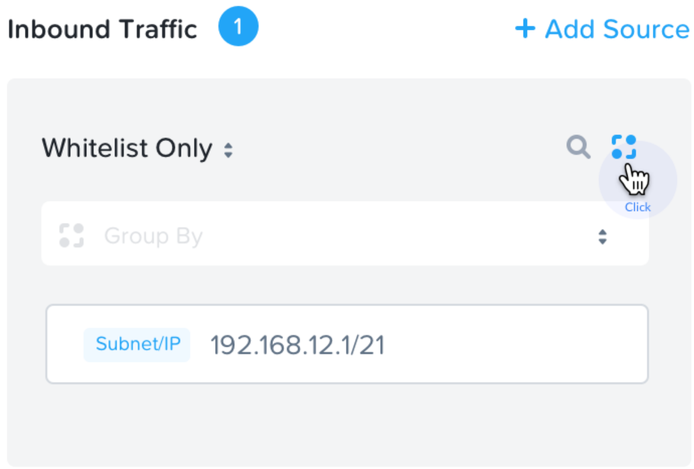

Inbound Traffic
1 Rule
Whitelist Only
Subnet/IP
192.168.12.1/21


Inbound Traffic 1
+ Add Source
Whitelist Only
Click
Subnet/IP 192.168.12.1/21


Inbound Traffic 1
+ Add Source
Whitelist Only
Click
Search Categories, Subnets, Ports etc.
Subnet/IP 192.168.12.1/21


Inbound Traffic 1
+ Add Source
Whitelist Only
Subnet/IP 192.168.12.1/21


Inbound Traffic 1
+ Add Source
Whitelist Only
Click
Subnet/IP 192.168.12.1/21


Inbound Traffic 1
+ Add Source
Whitelist Only
Click
Group By
Subnet/IP 192.168.12.1/21

Feature: Pin and Freeze

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Next

Inbound Traffic 1 Whitelist Only

Subnet/IP 192.168.12.1/24

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

Subnet/IP 192.168.12.1/25

+ Add Source

App Type: BusinessWebsite 1

AppTier BusinessWebsite

Set rules on app tier, instead.

Outbound Traffic Whitelist Only

+ Add Destination

FLOW UX

Visual Consitency

Inbound Traffic 4 Whitelist Only

+ Add Source

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

App Type: BusinessWebsite 3

App Tier Appserver

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

Outbound Traffic 1 Allow All

+ Add Source

All Destination

Show Discovered Traffic

Create App Security Policy

‹ Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Set Rules to & from App | Set Rules within App

Inbound Traffic 2

Whitelist Only

+ Add Source

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

App Type: BusinessWebsite

App Tier Appserver

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

Outbound Traffic 1

Allow All

+ Add Source

All Destination

Show Discovered Traffic

Create App Security Policy

Back

1 Define Policy 2 Secure Application 3 Review

Tabular View Next

Set Rules to & from App | Set Rules within App

Inbound Traffic 2 — Whitelist Only

Outbound Traffic 1 — Allow All

+ Add Source

Subnet 10.1.2.3/33

Subnet 10.1.2.4/34

Subnet 10.1.2.5/35

Subnet 10.1.2.6/37

App Type: BusinessWebsite

App Tier Appserver

App Tier Webserver

App Tier DBserver

Set rules on app tiers, instead.

+ Add Source

All Destination

Show Discovered Traffic

Appendix

MEETING NOTES:

Date	Notes	Reviewers	Status
16th May 2019	Thanks Abhishek for your inputs during sync up and Ritesh for detailed discussion today. Filtering and Grouping Filtering may use, LPM - Long Prefix Match. - Abhishek Suggested Group by: Subnet, categories, VLAN, Host, Cluster, Internal or External. - Abhishek Internal or External will be equivalent to Subnet Vs Categories for group by. - Ritesh. CIDR grouping may only make most sense for group by mechanism and we could ignore others. -Ritesh Filtering mechanism at individual section better than overall global search. - Ritesh Tabular View Tabular format will make it easy to configure without too many clicks. (User research - Qualcomm) - Abhishek Overall objective is to reduce no. of clicks and provide a more traditional approach as an alternative. - Abhishek UX Option 2, with an integrated table view on visualization a better approach. Ritesh to dive deeper and confirm. Option 2 Iterations and further screens to be created post-confirmation. Flexibility to view all the 5 tuples together, Importing rules from an external file, etc. features need to be discussed and captured as requirements.	Abhishek, Ritesh	-

MEETING NOTES:

Date	Notes	Reviewers	Status
16th May 2019	Port Groups Placing of Option of Port Groups (Port Dictionary) to decided. Suggestions of Placement: Prism Central Settings / Port Groups dedicated view / Security Policy. Ideally, Port groups can be flexible and the construct can be used anywhere in PC. - Ritesh DR uses "port groups" as a term, we would need an evaluation, if Port Group (Flow) is similar to Port Group (DR). _____	Ravi, Raj, Ritesh	-

Links

UX Documents
https://drive.google.com/drive/folders/11xIkNT_Aah-0qCfcjUHekw5cSK77yDfj
https://confluence.eng.nutanix.com:8443/display/NET/Usability+issues+with+current+Flow+Security+Policy+Model

Flow Visualization Improvements
https://confluence.eng.nutanix.com:8443/display/NET/Flow+Visualization+Improvements

Qualcomm Flow Workshop
https://confluence.eng.nutanix.com:8443/display/NET/Qualcomm+Flow+Workshop

Confluence Flow
https://confluence.eng.nutanix.com:8443/display/NET/Flow+Visualization+Improvements

Advanced Setting UX Mockup
https://sketch.cloud/s/EGvko

Ports and Description
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

UX Requirements
https://confluence.eng.nutanix.com:8443/pages/viewpage.action?pageId=39062033

Design Plan
https://confluence.eng.nutanix.com:8443/display/NET/Flow+5.12%2C+5.13+Engineering+Plan

List of Ports
http://www.pearsonitcertification.com/articles/article.aspx?p=1868080

Feedbacks and Suggestions:

Jibin Varghese
jibin.varghese@nutanix.com