Segmentation Policy Configuration Guide

Segmentation Policy PBR

Software-Defined Segmentation Policy

Table of Contents

Segmentation Policy PBR

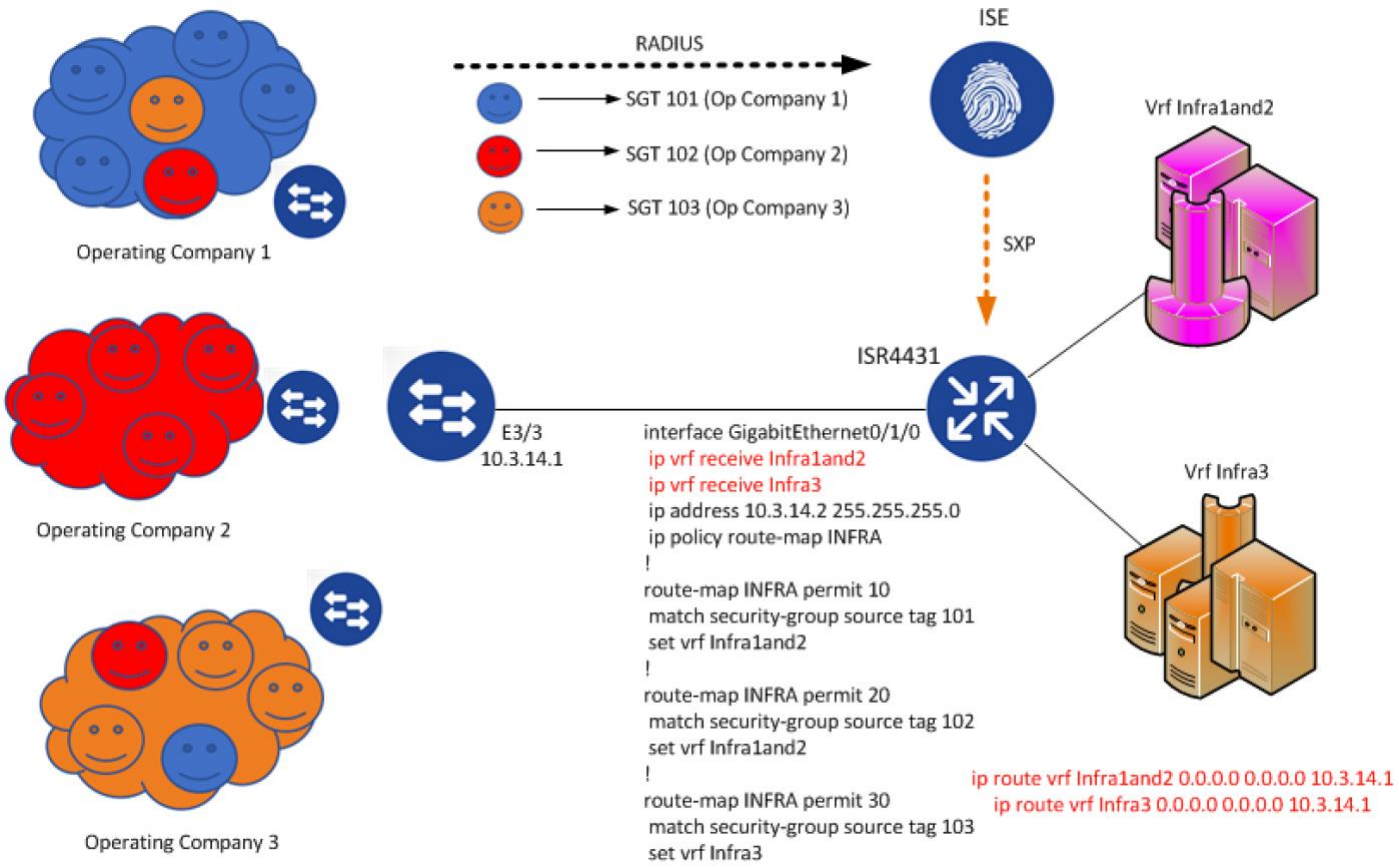
Introduction

Policy-Based Routing (PBR) provides a tool for forwarding and routing data packets based on policies defined by network administrators. In effect, it is a way to have the policy override routing protocol decisions. Policy-based routing includes a mechanism for selectively applying policies based on access list, packet size or other criteria. The actions taken can include routing packets on user-defined routes, setting the precedence, type of service bits, etc.

In this document we solve a customer problem of hundreds of operating companies moving into the same real estate campus with some companies sharing back-end infrastructure/server groups and others having their own with overlapping IP addresses. Over time the back-end infrastructure will be consolidated but in the interim, how can company traffic be routed to the correct destination without geographic constraint and extensive configuration?

PBR is used to solve the problem but using source IP subnets within the matching criteria does not provide roaming capabilities for users. Additionally, providing the required number of SSIDs and IP pools for wireless connectivity is not scalable. The answer is to provide authentication with Identity Services Engine (ISE) and Authorization using Security Group Tags (SGTs) and using those SGTs in the PBR matching criteria to route to the correct back-end infrastructure/server group.

Figure 1: Example Setup



Summary of Operation

Employees of each operating company will authenticate with ISE and ISE will assign the appropriate SGT based on conditions configured in the ISE authorization table. So, the SGT classification is based on context using ISE and not purely based on the location/subnet of the user.

Operating Company 1 is coloured blue as are the employees of that company. As we are assigning the SGT based on context (like username, certificates, AD group etc), those employees can visit or roam to other company locations but still be classified with the blue SGT. You can see an Operating Company 1 employee is currently visiting Operating Company 3 but that person will still be classified with the blue SGT and hence gain access to the correct back-end infrastructure as explained below.

This classification information (IP address and SGT) is passed from ISE to the ISR4431 via Security Group Tag Exchange Protocol (SXP). When users attempt to access the back-end infrastructure, the ISR4431 will:

- receive the packets from the users
- initiate an internal SGT lookup based on the source IP address
- use the SGT as matching criteria within the route-map
- when matched, use the set attribute within the route-map to route the packets to the correct back-end infrastructure VRF.

The red text in the diagram is purely to provide routing information from/to the back-end infrastructure VRFs. Under the ISR4431 ingress interface, the 'ip vrf receive <VRF>' command inserts that interface IP address into the VRF routing tables and the default route in each VRF provides a next hop for return traffic. There will be other ways to route leak and/or redistribute the routes as necessary so it is encouraged to investigate the best way to handle network routing based on the customers particular needs.

Configuration

ISE Groups

Firstly, security groups need to be added into ISE to be used for classification. Navigate to Work Centers > TrustSec > Components > Security Groups and add the appropriate groups:

Security Groups

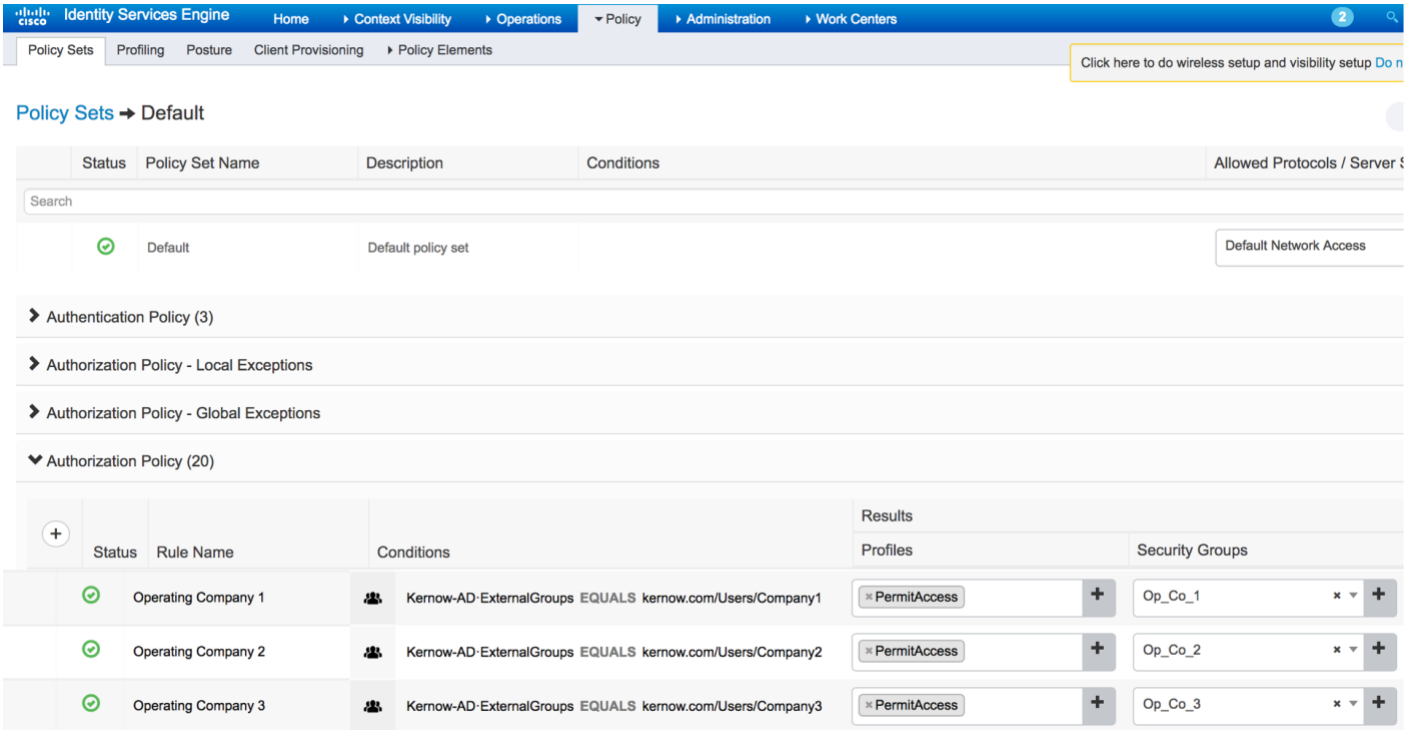
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit | Add | Import | Export | Trash | Push

Icon	Name	SGT (Dec / Hex)	Description
			Operating
	Op_Co_1	101/0065	Operating Company 1
	Op_Co_2	102/0066	Operating Company 2
	Op_Co_3	103/0067	Operating Company 3

ISE Authorization

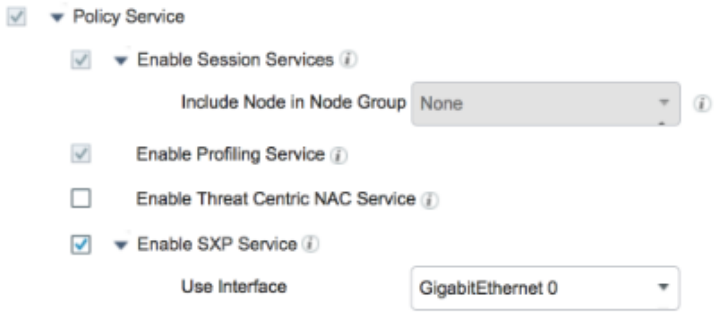
The SGT's are assigned by ISE within the authorization table. Navigate to Policy > Policy Sets and select the relevant policy set or select the default one. Expand the Authorization Policy table and add the relevant rules, example below uses conditions which include a username lookup to Active Directory groups with the relevant Security Group being assigned:



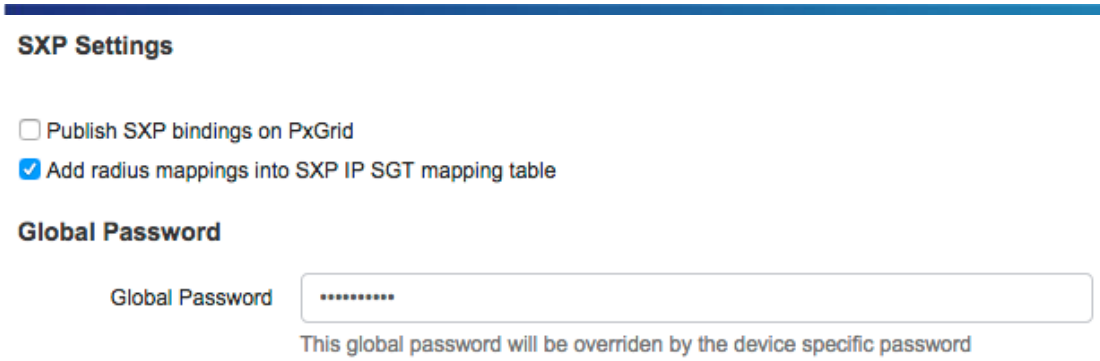
SXP from ISE to ISR4431

When users authenticate with ISE, an SGT will be assigned via the authorization table as explained above. The learned IP addresses of the clients along with the SGT's assigned for those client sessions will be stored within the ISE SXP mapping table. We need to enable SXP on ISE and then add an SXP connection to the ISR4431 to transfer that mapping information to the router for use in the lookup function.

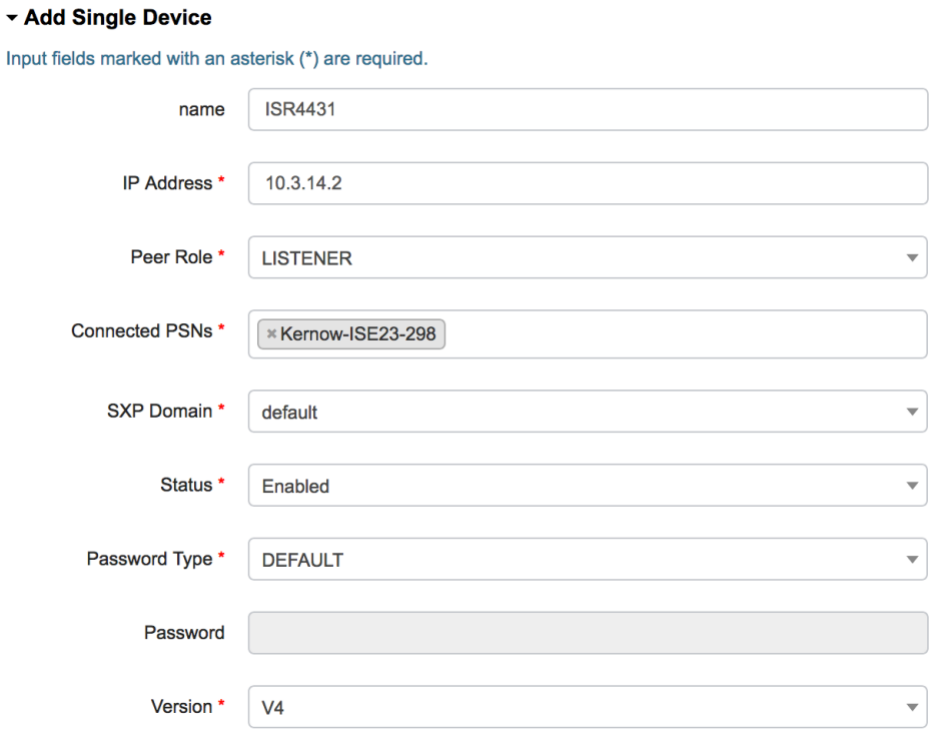
Enable SXP in ISE via Administration > System > Deployment > (Hostname)



Navigate to Work Centers > TrustSec > Settings > SXP Settings and enter a Global Password to be matched when adding the other end of the SXP connection on the Border device. Additionally, ensure 'Add radius mappings into SXP IP SGT mapping table' is enabled:



Now, under Work Centers > TrustSec > SXP > SXP Devices, we can add a new Device/Connection to the ISR:



We now need to access the ISR and add SXP configuration there:

Kernow-ISR4431#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Kernow-ISR4431(config)#cts sxp enable
Kernow-ISR4431(config)#cts sxp default source-ip 10.3.14.2
Kernow-ISR4431(config)#cts sxp default password <password to match the global SXP password set in ISE>
Kernow-ISR4431(config)#cts sxp connection peer 10.1.101.60 source 10.3.14.2 password default mode local listener

Kernow-ISR4431#show cts sxp connections brief
SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: 10.3.14.2
Connection retry open period: 120 secs

Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set

Peer_IP	Source_IP	Conn Status	Duration
10.1.101.60	10.3.14.2	**On**	0:01:59:37 (dd:hr:mm:sec)

Total num of SXP Connections = 1

Navigating back to ISE Work Centers > TrustSec > SXP > SXP Devices, we can also see the connection is ON/up:

PBR Configuration

For the route-maps to route traffic to the correct VRFs, the VRFs have to be present within the ISR4431. Create the VRFs (if not already added):

Kernow-ISR4431#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Kernow-ISR4431(config)#vrf definition Infra1and2
Kernow-ISR4431(config-vrf)#address-family ipv4
Kernow-ISR4431(config-vrf-af)#exit
Kernow-ISR4431(config-vrf)#exit
Kernow-ISR4431(config)#vrf definition Infra3
Kernow-ISR4431(config-vrf)#address-family ipv4

We will assume the routing within each VRF is successfully provisioned.

The route-map on the ISR4431 is configured to match source security group tags and route to the correct destination VRF based on the SGT value.

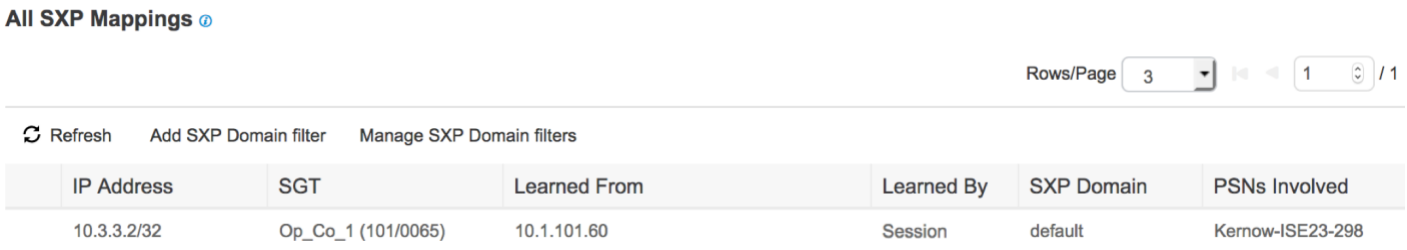
Kernow-ISR4431#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Kernow-ISR4431(config)#route-map INFRA permit 10
Kernow-ISR4431(config-route-map)#match security-group source tag 101
Kernow-ISR4431(config-route-map)#set vrf Infra1and2
Kernow-ISR4431(config-route-map)#exit

Kernow-ISR4431(config)#route-map INFRA permit 20
Kernow-ISR4431(config-route-map)#match security-group source tag 102
Kernow-ISR4431(config-route-map)#set vrf Infra1and2
Kernow-ISR4431(config-route-map)#exit

```
Kernow-ISR4431(config)#route-map INFRA permit 30
Kernow-ISR4431(config-route-map)#match security-group source tag 103
Kernow-ISR4431(config-route-map)#set vrf Infra3
```

```
Kernow-ISR4431#show route-map INFRA
route-map INFRA, permit, sequence 10
  Match clauses:
    security-group source tag 101
  Set clauses:
    vrf Infra1and2
  Policy routing matches: 0 packets, 0 bytes
route-map INFRA, permit, sequence 20
  Match clauses:
    security-group source tag 102
  Set clauses:
    vrf Infra1and2
  Policy routing matches: 0 packets, 0 bytes
route-map INFRA, permit, sequence 30
  Match clauses:
    security-group source tag 103
  Set clauses:
    vrf Infra3
  Policy routing matches: 0 packets, 0 bytes
```

When a user connects and authenticates with ISE, an SGT is assigned and the associated IP to SGT mapping can be found under Work Centers > TrustSec > SXP > All SXP Mappings:



In this case, a user within Operating Company 1 has been assigned an IP address of 10.3.3.2 via DHCP and SGT Op_Co_1 (SGT 101) via the ISE authorization table. As there is an SXP connection active from ISE to the ISR, that mapping will get sent to the ISR:

```
Kernow-ISR4431#show cts role-based sgt-map 10.3.3.2
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
========================================
10.3.3.2                101     SXP
```

Now, when that client/user (10.3.3.2) sends traffic towards the servers, the ISR will:

- Receive those packets sourced from 10.3.3.2
- Instigate an internal SGT lookup based on the source IP
- Use that SGT as a match in the route-map called INFRA
- Route the packets to a VRF based on the set attribute within the route-map

In our case, the user in Operating Company 1 will be routed to the Infra1and2 VRF:

```
Kernow-ISR4431#show route-map INFRA
route-map INFRA, permit, sequence 10
  Match clauses:
    security-group source tag 101
  Set clauses:
    vrf Infra1and2
  Policy routing matches: 757 packets, 73786 bytes
route-map INFRA, permit, sequence 20
  Match clauses:
    security-group source tag 102
  Set clauses:
    vrf Infra1and2
  Policy routing matches: 0 packets, 0 bytes
route-map INFRA, permit, sequence 30
  Match clauses:
    security-group source tag 103
  Set clauses:
    vrf Infra3
  Policy routing matches: 0 packets, 0 bytes
```

Similarly, if a user from Operating Company 3 connects and authenticates, SGT Op_Co_3 (SGT 103) will be assigned and traffic sent towards the servers will be routed to the Infra3 VRF

```
Kernow-ISR4431#show route-map INFRA
route-map INFRA, permit, sequence 10
  Match clauses:
    security-group source tag 101
  Set clauses:
    vrf Infra1and2
  Policy routing matches: 757 packets, 73786 bytes
route-map INFRA, permit, sequence 20
  Match clauses:
    security-group source tag 102
  Set clauses:
    vrf Infra1and2
  Policy routing matches: 1 packets, 82 bytes
route-map INFRA, permit, sequence 30
  Match clauses:
    security-group source tag 103
  Set clauses:
    vrf Infra3
  Policy routing matches: 15 packets, 1470 bytes
```

References

PBR for SGT was released in the following versions:

Platform	Feature	Release	URL
ASR	SGT Based PBR	3.16s	https://www.cisco.com/c/en/us/td/docs/routers/asr1000/release/notes/asr1k_rn_rel_notes/asr1k_feats_important_notes_316s.html
ISR	SGT Based PBR	15.6(1)T	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-mt/iri-15-mt-book/iri-sgt-based-pbr.html
ASA	Policy Based Routing support for Identity Firewall and Cisco Trustsec	9.5(1)	https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/release/notes/asarn95.html#reference_AFFBD30E162448BCA88376D187C2E412