Network as an Enforcer (NaaE)

Cisco Services

`

NaaE Feature Guide

INTRODUCTION

Introduction

Overview of Network as an Enforcer

Cisco TrustSec is an end-to-end network infrastructure that provides a scalable architecture for enforcement of role-based access control, identity-aware networking, and data confidentiality that helps secure a network and its resources. Cisco TrustSec is a critical component of Enterprise Security architecture that envisions a comprehensive and agile security framework, which in turn allows enforcement of context-aware policies to meet new dynamic access control challenges of Bring your own device (BYOD) and mobility. Along wth the Enterprise Fabric and integration of services quality of service (QOS), Cisco Performance Routing (PFR), security in Cisco Intellignet WAN (IWAN), it will be the basis of security implementation going forward.

Traditionally, the access control policy is dependent on network topology. In today's world, the devices are used freely throughout the network, with dynamic IP addresses. Due to this, the rules associated with subjeCisco TrustSec and objeCisco TrustSec of a particular security group and the access control applied between several such security groups remain a challenge in a mobility network infrastructure.

In such scenarios, a Security Group Access Control List (SGACL) provides a state-less access-control mechanism based on the security association or security group tag (SGT) value rather than IP addresses.

The Cisco TrustSec SGACL feature provides CLI commands for local configuration, remote download, debugging, and troubleshooting. CLI commands are available to enable and disable this feature, show configuration information, perform tests, and enable debugging.

Note:

The Debug CLI is intended for developers who appreciate shorter commands and direct control of each feature. Therefore, debug CLI commands pertaining to this feature are defined directly under debug RBM.

Key Benefits

The following are the main benefits of SGACL:

- State-less access control
- Filtering traffic based on class match

Regardless of the enforcement device and IP topology, a single business-relevant policy can be defined from a centralized policy server. Additionally, the duties between operations defining the security policy can be separated and updated on the device in a short period of time so that network operations do not override security policy via CLI changes.

Audience

This feature guide is intended for Cisco equipment providers, partners, and networking teams who are technically knowledgeable and familiar with Cisco network devices and Cisco IOS software and features.

Scope

In the initial phase, the SGACL feature is supported in the egress

direction, on par with the existing feature support on devices.

The SGACL feature is bundled with Cisco ASR 1000 Series Aggregation Services Router and Cisco 4000 Series Integrated Services Router images with strong cryptography features (k9). It is a part of the images that have the Cisco TrustSec subsystem bundled in.

Plan

Guidelines and Limitations

- Performance is lower than the security (IP) access control list (ACL).
  The SGACL increments more counters compared to the security ACL, there is a noticeable performance drop with each lookup. SGACL performs more ternary content addressable memory (TCAM) and DRAM lookups (SGT, detination group tag (DGT), cell, and TCAM lookups) – one lookup vs. maximum of four lookups.

- In case of a dynamic policy, Cisco TrustSec platform independent (PI) downloads policies (policies for a single SGT) one at a time and gives it to platform dependent (PD). In case of a static policy, whenever enforcement is enabled after disablement, PI downloads all the policies to PD. PI must make sure that the entire bandwidth of the CPU is not used during the performance of this task.

- SGACL enforcement is precluded on the management GigabitEthernet interface, named GigabitEthernet0. This is largely because the management interface is deemed as ingress for router management, and is not considered as a router-forwarding port. Also, this interface is often used as a failsafe option to connect to a router even if the forwarding interfaces are not functional. In addition, the management interface is a conduit for exchange of forwarding-state information between Active and Standby ESPs which allows the forwarding plane of the Standby ESP to be visible to the Active ESP. Any form of access control on the interface impaCisco TrustSec this communication and renders the Active device blind to the forwarding plane of the Standby device.

- Dynamic SGACL messages that are larger than ~6 KB in characters is impacted by an infrastructure check. This in turn limits the size of a SGACL to be successfully downloaded and enforced. This issue with the dynamic SGACL download size is applicable for all Cisco Denali IOS XE 16.3.1 switches and router platforms.

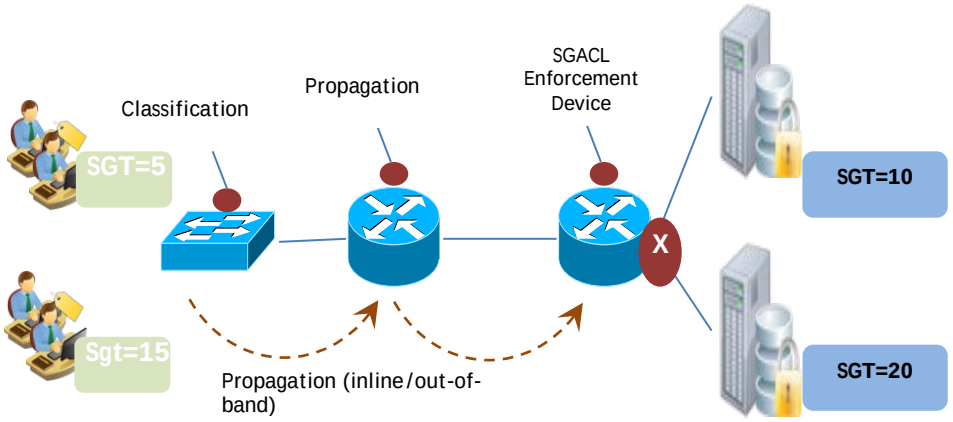
- There is no validation of SGACL enforcement on port channel interfaces.

- Connectivity to a Cisco ISE server should be through a non-VRF-enabled interface, if it is configured to be reachable.

Install /Deploy

Deploying Network as an Enforcer

Figure 1: Cisco TrustSec Solution Deployment



TrustSec devices are categorized into the following types or roles:

Classification Device

In a network, this is the device in which, a user or resource is assigned an SGT and bound to the device source IP address. Typically, the classification occurs at the point where a user or resource is attached to the network. There are multiple ways in which SGT is assigned. This includes the dynamic (AAA) and static (CLI) methods.

Propagation Device

In a network, this is the device that is responsible for carrying forward or propagating SGT in a hop-by-hop basis. The propagation method can be inline or out-of-band. Inline propagation methods include SGT tagging over Ethernet, IPSec, GRE, LISP, VxLAN, and so on. Out-of-band propagation is via SXP.

Enforcement Device

In a network, this is the device that enforces security group-based access control lists or service such as QoS, policy-based routing, and so on. While TrustSec monitoring and troubleshooting node (MnT) captures details related to the enforcement of SGT-based access control and services, certain troubleshooting scenarios cannot be viewed in silo. Therefore, an attempt has been made to capture the actions of non-SGT-based features, such as, IP ACL, along with other SGT- based features.

Security Group, Security Group Tag and SGACL

Security Group

A security group is defined by the administrator in the policy management station, such as, Cisco identity services engine (ISE). A security group is a flexible grouping of users, end-point devices, and resources that share access control policies. SubjeCisco TrustSec (users, devices, and resources) are mapped to a security group using attribute-based rules. The rules are flexible and can consider attributes from multiple domains, such as identity, location, type of access, time of day, and end-point device posture.

Security Group Tag

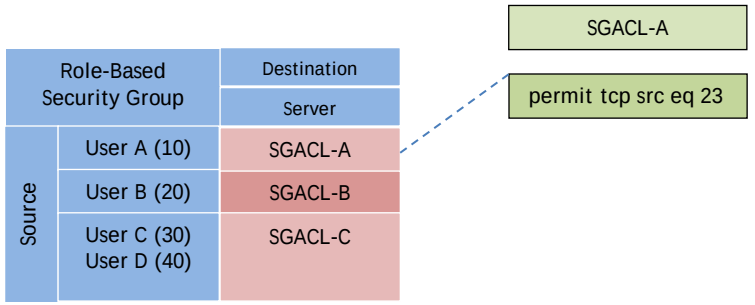
Network device software does not consider the method by which security groups are assigned. Only the visible representation of security groups is considered. Security groups are represented on the network device using a 16-bit number known as SGT. Each security group is assigned a unique SGT (the range is from 2 to 65534) by the policy management application. When the SGT is used to refer to the security group of a packet's destination, it is called Destination Group Tag (DGT).

SGACL

A Security Group access Control List (SGACL) is a policy enforcement mechanism through which users can control the operations that will be performed based on the security group's assignment of users and destination resources. Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with the source security group number on one axis and the destination security group number on the other axis. Each cell in the matrix can contain an ordered list of SGACLs that specify the permissions that should be applied to packets originating from the source security group and destined for the destination security group.

Figure 2 shows an example of Cisco TrustSec permissions matrix for a simple domain with three user roles and one destination resource. Three SGACL policies perform control access on the destination server based on the role of the user.

Figure 2: A Cisco TrustSec Permission Matrix



SGACL Monitor Overview

When SGACL monitor mode is enabled, all the traffic is permitted. However, the statistics of traffic flow (permit/deny) hitting particular

cells is still maintained. This provides insight into the effect of deploying certain policies before actually enforcing them in a production environment. These monitor mode counters are maintained for both datapath and software-enforced traffic in a manner that is similar to the regular counters. When monitor mode is enabled along with SGACL logging, the action that is shown is the one in the access control entry and not permitted.

Testing the Deployment

Testing the SGACLs, basic infrastructure requires Cisco ISE setup connected with Unit Under Test (UUT) (ASR1K/ISR-G3/3850) devices. Switch or router devices should act as a host device to generate traffic along with the SGT tag and send it to UUT.

You can test the following:

- Branch router with Dynamic Multipoint Virtual Private Network (DMVPN) GRE tunnel, where enforcement is applied on both the tunnel interface and the WAN interface.
- Branch router with enforcement on LAN interface, which applies a policy to return traffic from an enterprise.

Configure

Configuring a SGACL on Cisco ASR Router and a Cisco Catalyst Switch:

	Command or Action	Purpose

Step 1	**cts role-based enforcement**
	
	no cts role-based enforcement
	
	Example:
	`Device(config)# Cisco TrustSec role-based enforcement`
	
	For Cisco Catalyst 3850 Series Switches:
	`Device(config-if)# Cisco TrustSec role-based enforcement vlan-list 31-35, 41`
		Enables SGACL enforcement. On configuring this command, SGACL enforcement is automatically enabled on every L3 interface, except for tunnel interfaces.
		
		Disables SGACL enforcement.
		
		Note: To apply ACL in order to switch traffic within a VLAN in Cisco Catalyst 3850 Series Switches, you must enable SGACL policy enforcement on specific VLANs, or to traffic that is forwarded to an switch virtual interface (SVI) associated with a VLAN.

Step 2	**ip access-list role-based *sgacl-name*** Example: `Device(config)# ip access-list role-based test_acl`	Defines IPv4 SGACL. ***Note***: The local admin can define SGACLs as a fallback policy in the absence of a dynamic downloaded policy from ISE.
Step 3	***sequence_number*** **{permit|deny} protocol-num [option *option_name*] [precedence *precedence*] [tos**	Defines an ACE for an IPv4 SGACL.

	***tos*] [log] [fragments]** For Cisco Catalyst 3850 Series Switches: ***sequence_number* {permit|deny} icmp [*icmp-type* [*icmp-code*] [precedence *precedence*] [tos *tos*] [log] [fragments]** Example: `Device(config-rb-acl)# 12 permit icmp 1 1 precedence 2 tos 4 log`	Apart from ICMP, an ACE can be defined for TCP, UDP, and other IPs.
Step 4	**cts role-based permissions from {*security-group-tag* | unknown} to {*destination-group-tag* | unknown} [ipv4] *rbacl_name*** **cts role-based permissions default *rbacl_name*** Example: `Device(config)# cts role-based permissions from 10 to 12 ipv4 test_acl`	Defines, replaces, or deletes the list of RBACLs for a given SGT-DGT pair. This policy will be in effect as long as there is no dynamic policy for the same SGT-DGT pair.
Step 5	**cts refresh policy { peer *peer_id* | sgt *sgt_number* | default | unknown}**	(Not applicable for Cisco Catalyst 3850 switches.)

	Example: `Device(config)# cts refresh policy peer 1`	Refreshes the SGACL policies downloaded to the router from the authentication server.

Configuring RADIUS Change of Authorization

	Command or Action	Purpose
Step 1	**enable** Example: `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** Example: `Device#configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** Example: `Device(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**aaa server radius dynamic-author** Example: `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as an AAA server to facilitate interaction with an

		external policy server.
Step 5	**client {*ip-address* | *name* [vrf *vrf-name*]} server-key [0 |7] *string*** Example: `Device(config-locsvr-da-radius)# client 10.0.0.1`	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 6	**port *port-number***	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. Note : The default port for packet of disconnect is 1700. Port 3799 is required to interoperate with ACS 5.1.
Step 7	**ignore session-key** Example: `Device(config-locsvr-da-radius)# ignore session-key`	(Optional) Configures the device to ignore the session key.
Step 8	**ignore server-key** Example:	(Optional) Configures the device to ignore the server key.

	`Device(config-locsvr-da-radius)# ignore server-key`	

Configuring SGACL Monitoring and Logging

This task can be performed only on Cisco Catalyst 3850 Series switches.

	Command or Action	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**cts role-based monitor {all | enable | permission}** Example: `Device(config)# cts role-based monitor all`	Selects monitor mode.
Step 3	**cts role-based monitor permissions {default | from}** Example: `Device(config)# cts role-based monitor`	Selects the Permission list.

	`permissions default`	
Step 4	**cts role-based monitor permissions from {*security-group-tag* | unknown} to {*destination-group-tag* | unknown} [ipv4]** Example: `Device(config)# cts role-based permissions from 10 to 12 ipv4`	Configures the device to monitor the filtered traffic with the specified SGT and DGT.
Step 5	**cts role-based enforcement logging-interval *seconds*** Example: `Device(config)# cts role-based enforcement logging-interval 10`	Configures logging interval. The range is from 1 to 86400 seconds.

Monitor

Use the following commands to monitor the deployment:

`Device# show cts role-based permissions [from {sgt|unknown}] [to {dgt|unknown}] [ipv4] [details]`	To display the contents of the permission matrix.
`Device# show cts rbacl rbacl_name`	To look at the ACEs of an Role-Based ACL that is effectively applied to one or more cells.
`Device# show cts role-based counters ipv4`	To display counter logs applicable only for Cisco Catalyst 3850 Series switches.

Display configured SGACL policy

Device#show cts role-based permissions [from {*sgt*|unknown}] [to {*dgt*|unknown}] [ipv4] [details]

The following is a sample console output:

```
Device#show cts role-based permissions ?
  default             Default Permission list
  from                Source Group
  to                  Destination Group
  ipv4                Protocol Version - IPv4
  |                   Output modifiers
  <cr>
```

```
r101#show cts role-based permissions from ?
  <0-65533>            Security Group Tag
  unknown              Unknown Source Group

r101#show cts role-based permissions from 3 ?
  to                  Destination Group
  ipv4                Protocol Version - IPv4
  |                   Output modifiers
  <cr>

r101#show cts role-based permissions from 3
Role-based permissions from group 3 to group 5:
        srb3
        srb5
Role-based permissions from group 3 to group 7:
        srb4

r101#show cts role-based permissions to ?
  <0-65533>            Security Group Tag
  unknown              Unknown Destination Group

r101#show Cisco TrustSec role-based permissions to 5 ?
  ipv4                 Protocol Version - IPv4
  |                    Output modifiers
  <cr>

r101#show cts role-based permissions to 5
Role-based permissions from group 2 to group 5:
        srb2
        srb5
Role-based permissions from group 3 to group 5:
        srb3
```

```
        srb5

r101#show cts role-based permissions from 2 to 5
Role-based permissions from group 2 to group 5:
        srb2
        srb5

r101#show cts role-based permissions
Role-based permissions from group 2 to group 5:
        srb2
        srb5
Role-based permissions from group 3 to group 5:
        srb3
        srb5
Role-based permissions from group 3 to group 7:
        srb4
```

Display the ACEs Effectively Applied to the Matrix Cell

Device#show cts rbacl ?

```
   WORD     Show RBACL list by name
   |        Output modifiers

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
name =Deny_All-02
IP protocol version = IPV4
refcnt = 10
flag = 0x40000000
stale = FALSE
RBACL ACEs:
deny ip log

name =IT_ACL-06
IP protocol version = IPV4
refcnt = 2
flag = 0x40000000
stale = FALSE
RBACL ACEs:
permit ip log

name =Local_HR_ACL-01
IP protocol version = IPV4
refcnt = 2
flag = 0x40000000
stale = FALSE
RBACL ACEs:
```

```
permit ip log

name =LOCAL_IT_ACL-01
IP protocol version = IPV4
refcnt = 2
flag = 0x40000000
stale = FALSE
RBACL ACEs:
permit ip log

name =Permit IP-00
IP protocol version = IPV4
refcnt = 1
flag = 0x40000000
stale = FALSE
RBACL ACEs:
permit ip
```

Display the Counter Logs

Device# show Cisco TrustSec role-based counters ipv4

```
Role-based IPv4 counters
From  To     SW-Denied          HW-Denied          SW-Permitt         HW-Permitt         SW-Monitor
HW-Monitor
1000  3000     0                  0                  0                  0                  0
0
1001  3000     0                  0                  0                  0                  0
0
2000  3000     0                  0                  0                  0                  0
0
2001  3000     0                  0                  0                  0                  0
0
3000  3000     0                  0                  0                  0                  0
0
3001  3000     0                  0                  0                  0                  0
0
4000  3000     0                  0                  0                  0                  0
0
4001  3000     0                  0                  0                  0                  0
0
1000  3001     0                  0                  0                  0                  0
0
1001  3001     0                  0                  0                  0                  0
0
2000  3001     0                  0                  0                  0                  0
0
2001  3001     0                  0                  0                  0                  0
```

`

NaaE Feature Guide

Introduction	Plan	Configure	Install/Deploy	Monitor	Troubleshoot	Resources

```
0
3000  3001     0                0                0                0                0
0
3001  3001     0                0                0                0                0
0
4000  3001     0                0                0                0                0
0
4001  3001     0                0                0                0                0
0
```

Troubleshoot

In the specific case of failure in programming a cell in PD, generate a syslog message is generated and will keep the object is kept in error state. Use the **show platform software object fp active error** command to view the failed objeCisco TrustSec. For each of these objeCisco TrustSec, SGT and DGT details are displayed along with other Information. This helps in identifying the cell and policy that failed in programming.

In general, failure to program occurs if TCAM is full (which can be due to high scale of SGACL combined with other features that also use TCAM). In such a scenario, even reprogramming might fail. Sometimes, editing the failed cell content (from the CLI, in the context of static policy, and in Cisco ISE, in the context of dynamic policy) will cause PI to attempt invoking PD to program again.

Use the **show cts role-based permissions command** to display the status of an SGACL and to verify the monitor mode.

The following is a sample output of the **show cts role-based permissions** command**:**

```
Device#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 6:SGT_6 to
group 6:SGT_6 (configured, monitored):
        sgacl_1
IPv4 Role-based permissions from group 10 to group
11 (configured, monitored):
        sgacl_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : TRUE
```

Resources

For more information on Cisco TrustSec refer to the Cisco TrustSec Switch Configuration Guide.

TOMORROW
starts here.