TrustSec Configuration Guide

TrustSec with Meraki MS320 Switch Configuration Guide
## Table of Contents

**TrustSec with Meraki MS320 Switch**

- Introduction .......................................................................................................................... 3
- Summary of Operation ......................................................................................................... 3
- Configuration ...................................................................................................................... 4
  - Meraki Dashboard Configuration ......................................................................................... 4
  - Switch Summary .................................................................................................................. 4
  - Switch Ports ....................................................................................................................... 5
  - Access Policy .................................................................................................................... 7
  - DHCP Server Configuration ............................................................................................... 8
  - Routing and DHCP Configuration (Not Added) ................................................................. 8
  - OSPF Configuration (Not Added) ...................................................................................... 9
- ASR Trunk Port Configuration ............................................................................................. 9
- ISE Authorization Table ...................................................................................................... 9
- Operation ............................................................................................................................ 10
  - Connect / Authenticate Client ............................................................................................ 10
  - SXP Mapping and Propagation ......................................................................................... 10
  - TrustSec Enforcement .................................................................................................... 11
Introduction

This use case is for customers that wish to utilize Meraki access switches but want to use TrustSec group based policy enforcement.

At the time of writing this guide, the Meraki access switches do not support TrustSec classification, propagation or enforcement. However, the Meraki switches can still be used in a TrustSec deployment by making use of Trustsec functions within other network components.

Summary of Operation

The latest Meraki firmware supports RADIUS Authentication and Accounting. This allows the Meraki access switches to send RADIUS authentication and accounting messages to ISE which provides the capability to build complete sessions for authenticating clients.

If a client successfully authenticates to ISE via a Meraki access switch, ISE can be configured to assign a Security Group Tag to the learned client IP address, known as an IP:SGT mapping. ISE can send this mapping to TrustSec enforcement points in the network via Security Group Tag Exchange Protocol (SXP).
The enforcement points then have the ability to enforce policy based on the source group information sent via ISE and the destination group information learned via any supported methods.

As can be seen, the Meraki access switch only takes part in RADIUS messaging, it does not play a part in TrustSec classification, propagation or enforcement. The TrustSec functions within other network components allows the Meraki access switches to be deployed and used within this architecture.

Configuration

Meraki Dashboard Configuration

Switch Summary
Port 1 is purely for management.  
Port 2 is the uplink trunk to the network (ASR).  
Port 3 is the access port where the 802.1x client is connected.

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Type</th>
<th>VLAN</th>
<th>Current traffic</th>
<th>Sent ↓</th>
<th>Received ↑</th>
<th>Total bytes</th>
<th>RSTP state</th>
<th>PoE usage</th>
<th>Link</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>trunk</td>
<td>native 1</td>
<td>-</td>
<td>3.6 MB</td>
<td>Forwarding</td>
<td>-</td>
<td>S-4930-DC</td>
<td>Auto negotiate (1 Gbps)</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>trunk</td>
<td>native 1</td>
<td>-</td>
<td>202.9 MB</td>
<td>Forwarding</td>
<td>-</td>
<td>-</td>
<td>1 Gigabit full duplex</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>UCS vmnic 8</td>
<td>access</td>
<td>10</td>
<td>-</td>
<td>933.3 KB</td>
<td>Disabled</td>
<td>-</td>
<td>1 Gigabit full duplex</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Switch ports: Kernow-Meraki/2

Name:

Tags: eg. "email-alerts phone"

Enabled:

RSTP:

STP guard:

PoE:

Link:

Port schedule:

Isolation:

Type:

Native VLAN:

Allowed VLANs: 1,10
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch ports</td>
<td>Kernow-Meraki/3</td>
</tr>
<tr>
<td>Name</td>
<td>UCS vmnic 8</td>
</tr>
<tr>
<td>Tags</td>
<td>eg. &quot;email-alerts phone&quot;</td>
</tr>
<tr>
<td>Enabled</td>
<td>enabled</td>
</tr>
<tr>
<td>RSTP</td>
<td>disabled</td>
</tr>
<tr>
<td>PoE</td>
<td>disabled</td>
</tr>
<tr>
<td>Link</td>
<td>1Gbps (auto)</td>
</tr>
<tr>
<td>Port schedule</td>
<td>Always on</td>
</tr>
<tr>
<td>Isolation</td>
<td>disabled</td>
</tr>
<tr>
<td>Type</td>
<td>access</td>
</tr>
<tr>
<td>Access policy</td>
<td>For ISE</td>
</tr>
<tr>
<td>VLAN</td>
<td>10</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td></td>
</tr>
</tbody>
</table>
**Access Policy**

As can be seen in the port 3 configuration above, the access policy is set as ‘For ISE’. This policy is added in the dashboard as follows where 10.1.101.41 is the IP address of the Identity Services Engine (ISE).

The ISE RADIUS server is added for authentication and accounting is enabled:

<table>
<thead>
<tr>
<th>Name</th>
<th>For ISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS servers</td>
<td>10.1.101.41</td>
</tr>
<tr>
<td>Port</td>
<td>1812</td>
</tr>
<tr>
<td>Secret</td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td></td>
</tr>
</tbody>
</table>
DHCP Server Configuration

DHCP servers

DHCP servers running on layer 3 switches in this network can be configured on the Routing and DHCP page.

Email alerts

Do not send email alerts

Default DHCP server policy

Allow DHCP servers

Note: Switches with configured DHCP servers are always allowed.

Blocked DHCP servers

<table>
<thead>
<tr>
<th>Description</th>
<th>MAC</th>
<th>VLAN</th>
<th>Subnet</th>
<th>IP</th>
<th>Last seen</th>
<th>Recent packet</th>
<th>Policy</th>
<th>Seen by</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:b7:48:7e:5a:15</td>
<td>e8:b7:48:7e:5a:15</td>
<td>10</td>
<td>10.1.0/24</td>
<td>10.1.100.2</td>
<td>18 hours</td>
<td>view</td>
<td>allowed</td>
<td>Kernow-Meraki</td>
</tr>
</tbody>
</table>

Routing and DHCP Configuration (Not Added)

Routing and DHCP

Interfaces and static routes

This section includes all existing static routes and L3 interfaces configured in your network.

Add a static route  Add an interface  Move

You have not configured any static routes or L3 interfaces.

Warm spares

This section displays any warm spares that you've configured within the network. This feature adds L3 redundancy to non-stacking gateway switches.

Add a new warm spare

You have not configured any warm spares.
OSPF Configuration (Not Added)

Open Shortest Path First (OSPF) routing

OSPF  Disabled

ASR Trunk Port Configuration

The following configuration resides on the ASR router interface connected to the Meraki MS320 switch:

```
interface GigabitEthernet0/1/5
  description Connected to Meraki MS320 port 2
  no ip address
  negotiation auto

interface GigabitEthernet0/1/5.1
  encapsulation dot1Q 10
  ip address 10.6.1.1 255.255.255.0
  ip helper-address 10.1.100.2
```

ISE Authorization Table

ISE contains the following authorization table entry.
The condition checks if the user logging into the network is a member of the TSEngineering group in AD. If yes then permit access and assign the TSEngineering security group.

```
Authorization Policy
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions (Identity groups and other conditions)</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>TSEng</td>
<td>Kernow-AD:ExternalGroups EQUALS kernow.com/Users/TSEngineering</td>
<td>PermitAccess AND TSEngineering</td>
</tr>
</tbody>
</table>
```
**Operation**

**Connect / Authenticate Client**

When the client is connected/authenticated, ISE shows the following entry in the Live Log:

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Details</th>
<th>Network Device</th>
<th>Identity</th>
<th>Endpoint ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 27, 2017</td>
<td></td>
<td></td>
<td>Kernow-MerakiMS320</td>
<td>KERNOWiseng1</td>
<td>00:50:56:8F:69:6F</td>
</tr>
</tbody>
</table>

So, the TSeng authorization table entry has been hit/selected and therefore the TSEngineering security group has been assigned.

**SXP Mapping and Propagation**

After a successful authentication, ISE tracks the IP:SGT mapping of the user. Static mappings have also been added to ISE for the DC servers. All these mappings are placed in the ISE SXP table:
With an SXP connection deployed between ISE and the N7k, the mappings are propagated to the N7k:

```
Kernow-N7k# show cts role-based sgt-map

<table>
<thead>
<tr>
<th>IP ADDRESS</th>
<th>SGT</th>
<th>VRF/VLAN</th>
<th>SGT CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.100.3</td>
<td>11(11_Dev_Srvrs)</td>
<td>vrf:1</td>
<td>Learnt from SXP peer:10.3.3.1</td>
</tr>
<tr>
<td>10.1.100.4</td>
<td>14(14_PCI_Srvr)</td>
<td>vrf:1</td>
<td>Learnt from SXP peer:10.3.3.1</td>
</tr>
<tr>
<td>10.1.140.2</td>
<td>19(19_Prod_srvr)</td>
<td>vrf:1</td>
<td>Learnt from SXP peer:10.3.3.1</td>
</tr>
<tr>
<td>10.6.1.10</td>
<td>17(TSEngineering)</td>
<td>vrf:1</td>
<td>Learnt from SXP peer:10.1.101.42</td>
</tr>
</tbody>
</table>
```

**TrustSec Enforcement**

Once the N7k learns of mappings, it downloads the TrustSec policy from ISE for groups it needs to protect. The TrustSec policy matrix in ISE includes a policy to deny traffic from the TSEngineering group to the PCI_Srvr group:

![Production Matrix](image)

The N7k shows this policy in residence once it has been downloaded from ISE:

```
Kernow-N7k# show cts role-based policy sgt 17 dgt 14

sgt:17(TSEngineering)
dgt:14(14_PCI_Srvr) rbac:Deny IP
deny ip
```

Kernow-N7k#
The policy is active on the N7k with counters showing traffic being denied from the TSEngineering group to the PCI_Srvr group. This is blocking the user logged onto the network (via dot1x on the Meraki switch) from accessing the PCI Servers in the DC:

Kernow-N7k# show cts role-based counters sgt 17 dgt 14

RBACL policy counters enabled
Counters last cleared: Never

sgt:17(TSEngineering) dgt:14(14_PCI_Srvr) [6]
   rbacl:Deny IP
      deny ip [6]
Kernow-N7k#

Hence the Meraki access switch can be used in a TrustSec deployment even though the switch itself does not support TrustSec capabilities today.