Cisco Expo 2012

Upravljanje operativnim informacijama Cisco TrustSec tehnologije

Milan Mesić, CCIE#22492 (Security)

linkedin.com/in/mmesic

Sadržaj

1. Upravljanje sigurnosnim informacijama
2. Cisco TrustSec
3. Izvori informacija
4. Tehnike prikupljanja informacija
5. Scenariji korištenja

Upravljanje sigurnosnim informacijama

- Prikupljanje, analiza i ocjenjivanje sigurnosti i događaja
- Brza identifikacija, prioretizacija i odgovor na kršenja korporativnih sigurnosnih propisa, vanjske napade i unutarnjih rizike
- Korelacija logova, uloga korisnika i mrežnih tokova
- Tko, što, gdje i kada
- Upravljanje aplikacijama, mrežom, IT operacijama, sigurnosti umreženog informacijskog sustava i poslovna analitika

Cisco TrustSec

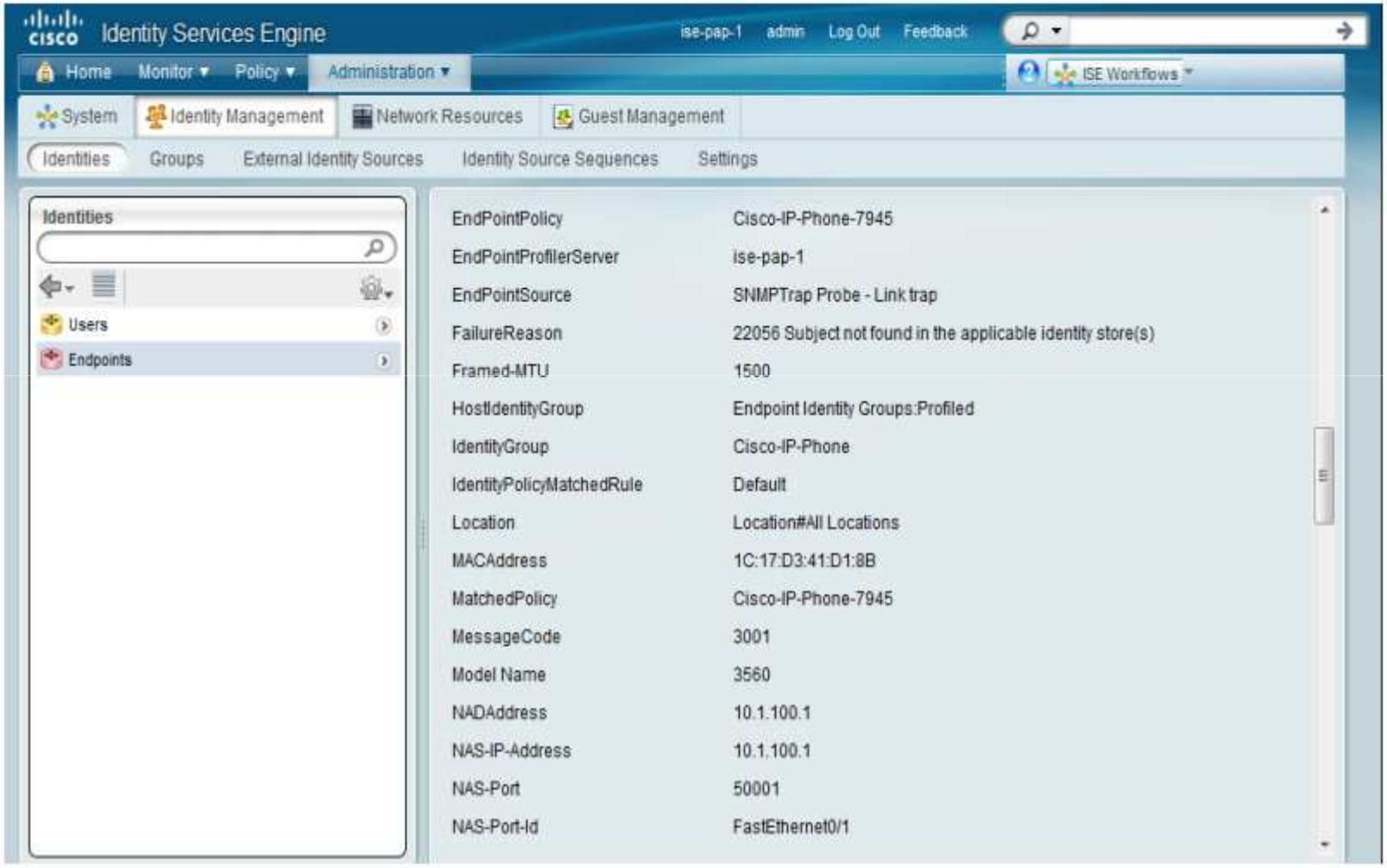
- Napredna kontrola pristupa mreži i upravljanje identitetima
- Integracija u mrežnu infrastrukturu (switchevi, wireless kontroleri)
- Velika količina korisnih podataka o događajima pristupa mreži
- Provjereno rješenje sa detaljno testiranom integracijom komponenti
- Funkcije za koje rješenja ostalih vendora zahtijevaju dodatne appliance i *overlay* uređaje – unutar TrustSec tehnologije switch radi samostalno
- Uz standardne IEEE 802.1X i VLAN kontrole podržava napredno upravljanje identitetima i kontrole njihovih prava
- Fleksibilna autentikacija, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), profiliranje uređaja i utvrđivanje sukladnosti uređaja

Izvori informacija : ISE monitoring

Izvori informacija : ISE monitoring : **Profilirani uređaji**

- Probe:
  - NetFlow
  - DHCP
  - DHCP SPAN
  - HTTP
  - RADIUS
  - NMAP *(ISE 1.1 - 19.03.)*
  - DNS
  - SNMP Query
  - SNMP Trap
  - IOS Sensor *(ISE 1.1 - 19.03.)*

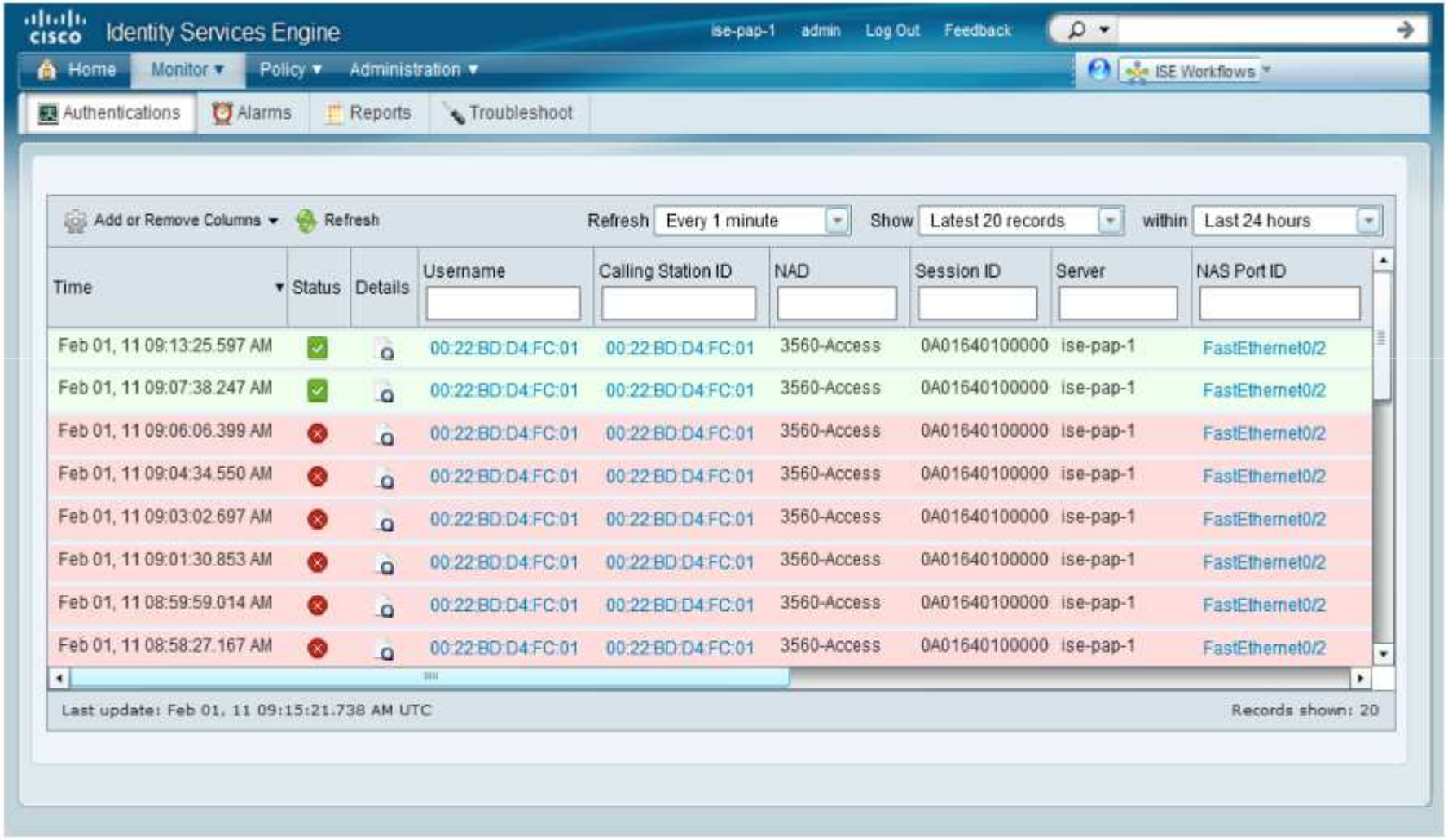
Izvori informacija : ISE monitoring : **Profilirani uređaji**



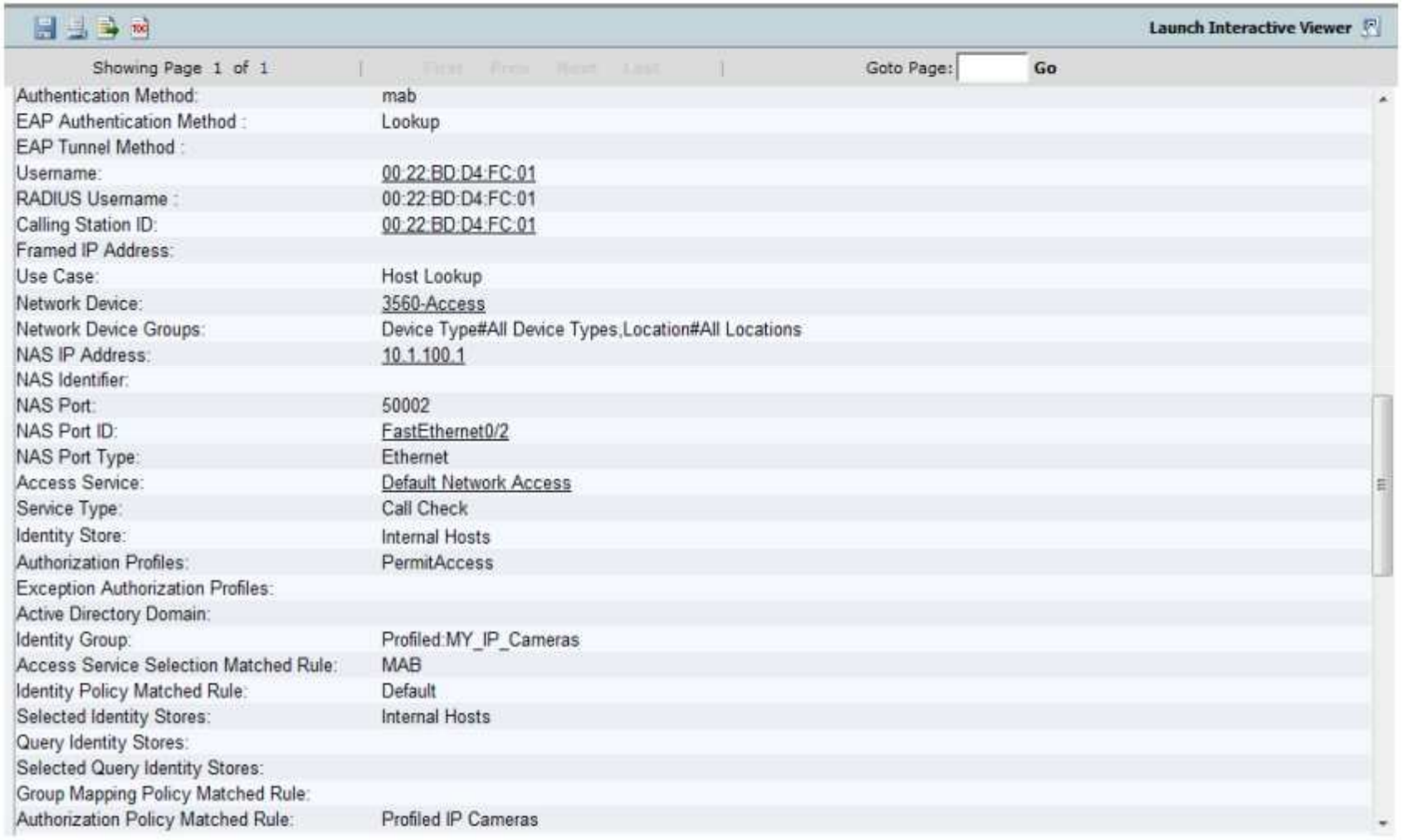
Izvori informacija : ISE monitoring : **Autentikacija i autorizacija**

- Metoda autentikacije (802.1X, MAB, web)
- Username
- NAD, NAS Port ID
- Identity store
- Authorization policy match
- …

Izvori informacija : ISE monitoring : **Autentikacija i autorizacija**



Izvori informacija : ISE monitoring : **Autentikacija i autorizacija**



Izvori informacija : ISE monitoring : **Posture services**

- Ocjenjivanje sukladnosti krajnjih uređaja (*assessment*)
- Granulacija i filtriranje prava pristupa u ovisnosti o sukladnosti (*policy enforcement*)
- Windows i MacOS klijenti
- Izvor informacija o nesukladnosti (ili sukladnosti) krajnjih uređaja koji se spajaju na mrežu
- Uključuje informaciju o utvrđenom uzroku nesukladnosti

Izvori informacija : ISE monitoring : **Posture services**

Search Result

	Time	Status	Username	MAC Address	Failure Reason
○	2011-03-30 05:52:36.804	✔	contractor1	00:10:18:88:22:24	
○	2011-03-30 05:52:36.804	⊘	contractor1		
◉	2011-03-30 05:52:03.305	✖	contractor1	00:10:18:88:22:24	
○	2011-03-30 05:52:03.305	⊘	contractor1		

Diagnosis and Resolution

Diagnosis

Details of policy(s) for Mac Address - 00:10:18:88:22:24

Posture policy - **Contractor_Windows AV Installed and Curren** - has Failed

Here is the list of requirements that failed and associated conditions, also the remediations that can be applied

Requirements	Status	Passed Conditions	Failed Conditions	Skipped Conditions	Remediations
Guest_AV Installed[Mandatory]	Passed	av_inst_ANY_vendo	None	None	LocalCheck(Predefined local check)
Guest_AV Current[Mandatory]	Failed	None	av_def_AN	None	LocalCheck(Predefined local check)

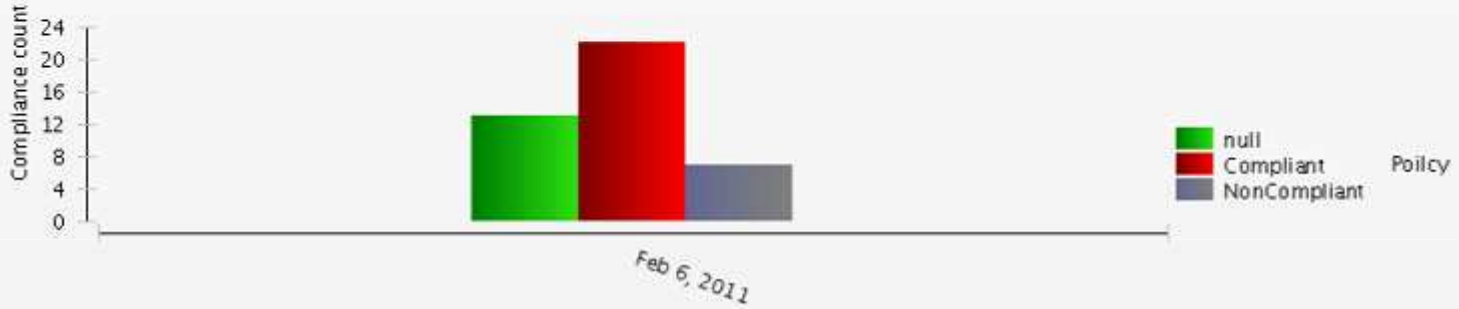
Izvori informacija : ISE monitoring : **Posture services**

Posture > Posture Trend

Date : February 06,2011

(Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on February 6, 2011 5:28:38 AM UTC



Day	Hit Count	Policy	Status	Type
February 6, 2011	2	Guest_AV Current	Passed	Mandatory
February 6, 2011	2	Guest_AV Current	Failed	Mandatory
February 6, 2011	22	Screen Saver On and Secure	Passed	Mandatory
February 6, 2011	4	Screen Saver On and Secure	Failed	Mandatory
February 6, 2011	21	AV Installed	Passed	Mandatory
February 6, 2011	21	AV Current	Passed	Mandatory
February 6, 2011	2	Guest_AV Installed	Passed	Mandatory

Izvori informacija : SGT (security group tag) ACL logging

```
%ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 10, Source IP:
1.1.1.1, Destination IP: 1.1.1.2, Source Port: 1111,
Destination Port: 2222, Source Interface: Ethernet4/1,
Protocol: tcp, Hit-count = 2#
```

- Ne sadrži destination group tag (DGT)
- IP-SGT mapping se može dobiti pomoću

  show cts role-based sgt-map

Izvori informacija : **OAL**

- Optimized Access-list Logging
- Različito od tradicionalnog IOS ACL logginga
- Hit notifikacija se šalje u određenim intervalima
- Uvedeno kao opcija na 6500/7600
- Na Nexus 7000 jedino OAL

Izvori informacija : OAL

```
RP_7k2# show log ip access-list cache
Source IP         Destination IP    S-Port  D-Port    Interface   Protocol   Hits
------------------------------------------------------------------------------
11.0.0.2         10.0.0.2          0       0         Ethernet2/11     (1)ICMP    5
10.0.0.2         11.0.0.2          0       0         Ethernet2/10     (1)ICMP    5

Number of cache entries: 2
------------------------------------------------------------------------------
RP_7k2#
```

```
RP_7k2(config)# show log ip access-list status
Max flow        = 8000
Alert interval  = 300
Threshold value = 0
RP_7k2(config)#
```

Izvori informacija : OAL

```
switch(config)# logging level acllog 3
switch(config)# acllog match-log-level 3
switch(config)# logging logfile [name] 3
```

```
2010 Nov 16 18:08:14 RP_7k2 %ACLLOG-3-ACLLOG_FLOW_INTERVAL: Source IP: 10.0.0.2,
Destination IP: 11.0.0.2, Source Port: 0, Destination Port: 0, Source Interface
: Ethernet2/10, protocol: "ICMP"(1),  Hit-count = 5
2010 Nov 16 18:08:17 RP_7k2 %ACLLOG-3-ACLLOG_FLOW_INTERVAL: Source IP: 11.0.0.2,
Destination IP: 10.0.0.2, Source Port: 0, Destination Port: 0, Source Interface
: Ethernet2/11, protocol: "ICMP"(1),  Hit-count = 5
```

Izvori informacija : NetFlow Security Group Tag (SGT)

```
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
exit
flow record rm_1
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match flow direction
match flow cts source group-tag
match flow cts destination group-tag
collect routing source as
collect routing destination as
collect routing source as peer
collect routing destination as peer
collect routing next-hop address ipv4
collect routing next-hop address ipv4 bgp
collect ipv4 source prefix
collect ipv4 source mask
collect ipv4 destination prefix
collect ipv4 destination mask
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor mm_1
record rm_1
exporter EXPORTER-1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

Tehnike prikupljanja informacija: ISE API

- Representational State Transfer (REST) Application Programming Interfaces (APIs)
- Dvije verzije na razini HTTP:
  - HTTP GET – jednostavnije korištenje
  - HTTP PUT – veća fleksibilnost kod upita koji sadrže veći broj parametara
- Informacije dostupne kroz API:
  - Broj aktivnih sessiona
  - Tip aktivnih sessiona
  - Autentikacijskih status aktivnih sessiona (sažeta ili detaljna lista)
  - MAC adrese koje se koriste
  - NAS IP adrese koje se koriste
  - Verzije nodeova i njihovi tipovi
  - Razlozi autentikacijskih pogrešaka

Tehnike prikupljanja informacija: ISE API

- Primjer HTTP GET upita i odgovora (sažeta lista):

  https://ise-1.demo.local/ise/mnt/api/Session/ActiveList

```
<activeSessionList noOfActiveSession="1">
 <activeSession>
   <user_name>user2</user_name>
   <calling_station_id>00:10:18:57:3A:44</calling_station_id>
   <nas_ip_address>10.1.250.2</nas_ip_address>
   <acct_session_id>00000366</acct_session_id>
   <audit_session_id>0A01FA0200000176A3FCBF6E</audit_session_id>
   <server>ise-1</server>
  </activeSession>
</activeSessionList>
```

Tehnike prikupljanja informacija: ISE API

- Primjer HTTP GET upita i odgovora (detaljan ispis):

  https://ise-1.demo.local/ise/mnt/api/Session/MACAddress/00:10:18:57:3A:44


```
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>user2</user_name>
<nas_ip_address>10.1.250.2</nas_ip_address>
<calling_station_id>00:10:18:57:3A:44</calling_station_id>
<nas_port>50001</nas_port>
<network_device_name>3k-
access</network_device_name>
<acs_server>ise-1</acs_server>
<authen_protocol>EAP-MSCHAPv2</authen_protocol>
<framed_ip_address>169.254.241.229</framed_ip_addres
s>
–
<network_device_groups>
Device Type#All Device Types#Wired,Location#All
Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2011-03-
17T23:23:06.841Z</auth_acs_timestamp>
<authentication_method>dot1x</authentication_method>
```

```
<execution_steps>
11001,11017,15008,15048,15048,15004,11507,12500,126
25,11006,11001,11018,12301
,12300,12625,11006,11001,11018,12302,12318,12800,12
805,12806,12807,12810,1230
5,11006,11001,11018,12304,12305,11006,11001,11018,1
2304,12305,11006,11001,110
18,12304,12318,12812,12804,12801,12802,12816,12310,
12305,11006,11001,11018,12
304,12313,11521,12305,11006,11001,11018,12304,11522
,11806,12305,11006,11001,1
1018,12304,11808,15041,15006,15013,24430,24416,2440
2,22037,11824,12305,11006,
11001,11018,12304,11810,11814,11519,12314,12305,110
06,11001,11018,12304,12306
,11503,24423,15036,15004,15016,11002
</execution_steps>
<audit_session_id>0A01FA0200000176A3FCBF6E</audit
_session_id>
<nas_port_id>GigabitEthernet0/1</nas_port_id>
<auth_id>1300156207684327</auth_id>
….
```

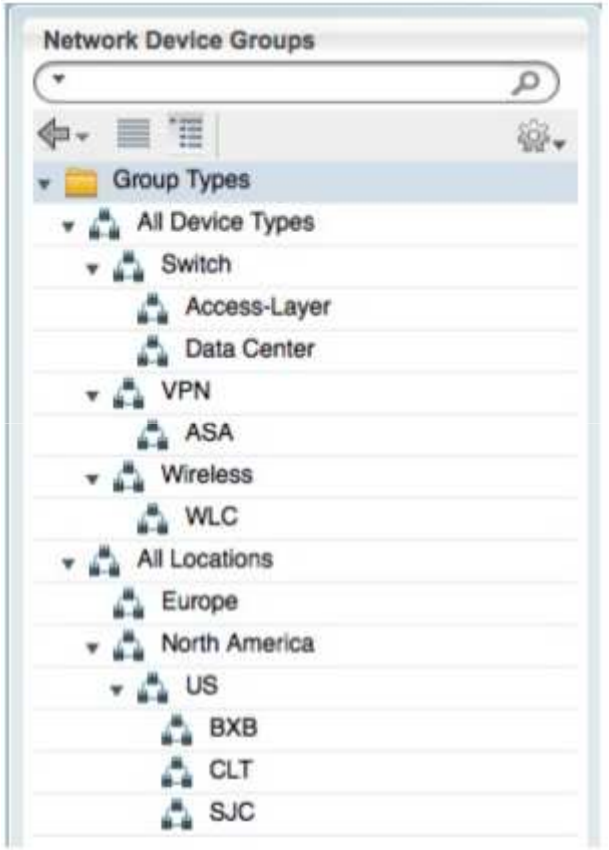
Tehnike prikupljanja informacija: ISE API

- Primjer HTTP PUT upita (veća fleksibilnost kod slanja parametara):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="acctRequest" type="mnTRESTAcctRequest"/>
 <xs:complexType name="mnTRESTAcctRequest">
  <xs:complexContent>
   <xs:extension base="mnTRESTRequest">
    <xs:sequence>
     <xs:element name="duration" type="xs:string" minOccurs="0"/>
    </xs:sequence>
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>
 <xs:complexType name="mnTRESTRequest" abstract="true">
  <xs:sequence>
   <xs:element name="valueList">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="value" type="xs:string" maxOccurs="unbounded"/>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="searchCriteria" type="xs:string"/>
  </xs:sequence>
 </xs:complexType>
</xs:schema>
```

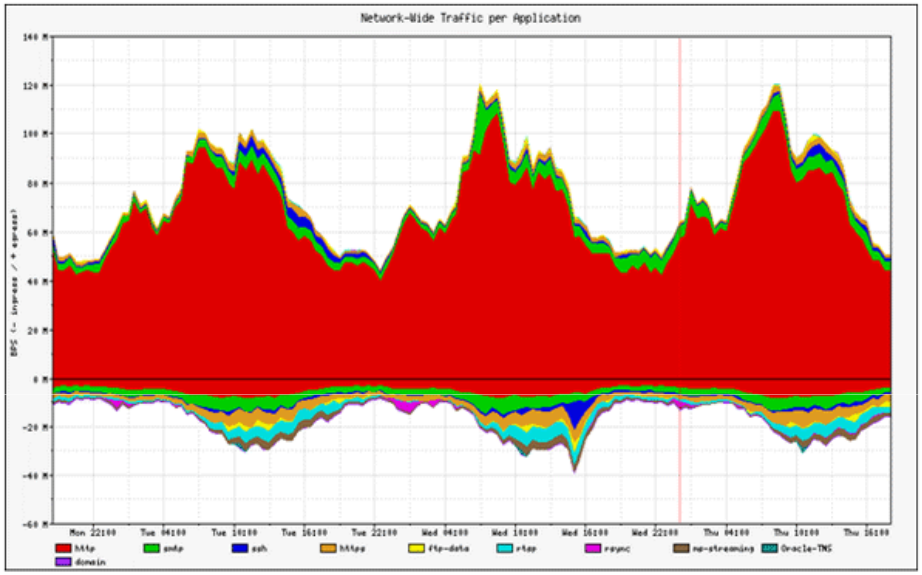
Scenariji korištenja : **lokacija uređaja**

- Detekcija istovremenog spajanja istog korisnika na dvije udaljene lokacije – alarm nedozvojenog dijeljenja accounta
- Korelacija sa autentikacijom fizičkog pristupa u sistem salu
- Istovremeno spajanje korisnika VPN-om i on-site



Scenariji korištenja : **profiliranje po SGT**

- Korelacija security group taga (SGT) i identiteta sa netflow (i ostalim) profilima
- Detekcija odstupanja pojedinog korisnika od profila SGT kojem pripada
- Profiliranje tokova prometa uređaja i korisnika za koje je posture status *failed*



Scenariji korištenja

- Izmjene u profilu uređaja (npr. printer -> notebook) – mogućnost MAC address spoofinga)
- Određivanje izvorišnog identiteta korisnika kod evenata (kaskadirano spajanje VPN, višestruki remote desktop, ssh port tunneling…)
- …

References

- Cisco TrustSec™ 2.0: Design and Implementation Guide
- Cisco Identity Services Engine User Guide, Release 1.0.4
- Cisco Identity Services Engine User Guide, Release 1.1
- Worldwide Sales Enablement : Global Online Lab Delivery – ISE labs
- Cisco TrustSec Security Group Access Solution Configuration Guide Version 1.5
- Cisco Identity Services Engine Overview

Zašto S&T?

- Jedinstvena kombinacija dugogodišnjeg iskustva sa naprednim Cisco sigurnosnim tehnologijama i vodećim Enterprise Threat and Risk Management (ETRM) rješenjima (ArcSight)
- Implementacije za široki spektar industrija, tipova namjena i razina složenosti
- Mogućnost integracije sa najvećim brojem tipova, proizvođača i modela opreme, uključujući i opremu koja nije na službenom popisu podržanih uređaja
- Realizacija najsloženijih zahtjeva i izvan standardnih mogućnosti ETRM rješenja (realizacija naprednih add-on funkcionalnosti)