NetFlow

PK di partenza 8.1.2.5

Su switch 1 configurare la community SNMP

- R1(config)#int se0/0/0
- R1(config-if)#ip flow ingress
- R1(config-if)#ip flow egress
- R1(config-if)#exit
- R1(config)#ip flow-export destination 10.0.1.4 9996
- R1(config)#ip flow-export version 9

Su PC1 attivare l'applicazione NetFlow Collector

• PC1 – Tab "Desktop" – MIB Browser



Materiale didattico prodotto da eForHum e rilasciato alle Cisco Academy, partner del progetto IT Excellence. Tutti i diritti riservati.

PC1				
Physical 🏾	Config	Desktop	Software/Services	
Netf	low Col	lector		X
Service				🖲 On 🔘 Off
				t
				1

Su R1 è possibile verificare lo stato della cache del flusso NetFlow tramite il seguente comando:

show ip cache flow

Rl#show ip cache flow IP packet size distribution (0 total packets): 1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480 000. 000. 000. 000. 000. 000. 000. 000. 000. 000. 000. 000. 000. 000. 512 544 576 1024 1536 2048 2560 3072 3584 4096 4608 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 IP Flow Switching Cache, 278544 bytes 0 active, 4096 inactive, 0 added 2 ager polls, 0 flow alloc failures Active flows timeout in 30 minutes Inactive flows timeout in 15 seconds IP Sub Flow Cache, 34056 bytes O active, 1024 inactive, O added, O added to flow O alloc failures, O force free 1 chunk, 1 chunk added last clearing of statistics never Total Flows Packets Bytes Packets Active(Sec) Idle(Sec) Protocol _____ Flows /Sec /Flow /Pkt /Sec /Flow /Flow 0 0.0 0 0 0.0 0.0 0.0 Total: SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts R1# Сору Paste

Materiale didattico prodotto da eForHum e rilasciato alle Cisco Academy, partner del progetto IT Excellence. Tutti i diritti riservati. Generando del traffico HTTP da PC2 verso 64.103.224.2 od un semplice ping è possibile vedere come il flusso NetFlow catturi le informazioni:

PC1			
hysical Config Desktop Software/Servic	es		
			1
Netflow Collector		×	a.
Service		🖲 On 🔿 Of	f 7
IPV4 SOU IPV4 SOU	Traffic Contribution: 8.33333% Flow information: IPV4 SOURCE ADDRESS: IPV4 DESTINATION ADDRESS: INTERFACE INPUT: TRNS SOURCE PORT: TRNS DESTINATION PORT: IP TOS: IP PROTOCOL: FLOW SAMPLER ID:	(1/12) 10.0.2.3 64.103.224.2 Gig0/2 1028 80 0×00 6 0 0	tor
other	FLOW DIRECTION: ipv4 source mask: ipv4 destination mask: counter bytes: ipv4 next hop address: top flags:	Output /24 /0 205 0.0.0.0 0x02 	
۲	timestamp first:	5 00:24:21.485	11 1

R1								_ 🗆 ×		
Physical 🖡 Conf	ig CLI									
						_				
IOS Command Line Interface										
Total:	Z	0.0	4	41	0.1	0.0	15.0			
		• -								
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts										
RI#SNOW 1p ca	ache Ilow	769.8	otel neck	ret.cl.						
1-32 64	96 128 1	60 192	224 256	288 Z	320 3.	52 384 416	448 480			
.000 .884	.000 .116 .0	00 .000	.000 .000	.000	.000 .00	000.000.000	.000 .000			
512 544	576 1024 15	36 2048	2560 3072	3584	4096 460	08				
.000 .000	.000 .000 .0	00 .000	.000 .000	000. 0	.000 .00	00				
TD D1 (
IP Flow Swite	ching Cache,	278544 b	ytes lod							
9 accive, 4	s O flow el	, 14 add loc fail	ures							
Active flow	s, o 1100 af s timeout in	30 minu	tes							
Inactive fl	ows timeout	in 15 se	conds							
IP Sub Flow C	ache, 34056	bytes								
O active, 1	.024 inactive	, O adde	d, O adde	ed to :	low					
O alloc fai	lures, 0 for	ce free								
l chunk, l	chunk added									
last cleari	ng of statis	tics nev	rer							
Protocol	Total	Flows	Packets	Bytes	Packet:	s Active(Sec)	Idle(Sec)			
TOWD	Flows	/Sec	/Flow	/Pkt	/Sec	c /Flow	/Flow			
TCHP TCD_UTTD	2	0.0	4	128	0.0	u 3.U	15.0			
TCP-other	6	0.0	5	41	0.0	n 0.0	15.0			
Total:	14	0.0	4	51	0.0	0 0.4	15.0			
	11	0.0	-		0.1		20.0			
SrcIf	SrcIPaddres	s Dst	If	Dst]	Paddres:	s Pr SrcP	DstP Pkts			
R1#								_		
-							1			
							Сору	Paste		

Materiale didattico prodotto da eForHum e rilasciato alle Cisco Academy, partner del progetto IT Excellence. Tutti i diritti riservati.