IP Network Assessment

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

This report is a summary of all the information collected during the IP Network Security Assessment Service during the reported timelapse.

Details in the **"Infrastructure and Generic information"** section describes the encountered scenario and its peculiarities.

The **"Security Related"** section shows all evidences (or the last 50 ones, with full details available in the database) of abnormal activities, policy violations, scans and possible risks inside your network infrastructure.

General considerations about observed traffic

Total Flows received: 99,251,400
Total Flows for timelapse: 21,230,000
Total Out of Matrix flows: 42,030,209
Total Out of Matrix flows for timelapse: 11,716,128
Ratio of OOM Flows against Total Flows: 42.34722029109917%
Ratio of OOM Flows against Total Flows for timelapse: 55.186660386245876%

The ratio between total flows and out of matrix flows (both globally and both for the report timelapse) is a good indicator of the network "safety" in terms of traffic variance.

A low percentage means a good regularity in the types of traffic inside the company network.

Infrastructure and generic information

Security related information

- BGP POLICY VIOLATIONS (TOP 50)
- SNMP POLICY VIOLATIONS (TOP 50)
- VPN POLICY VIOLATIONS (TOP 50)
- TUNNEL POLICY VIOLATIONS (TOP 50)
- SDN/CONTROLLER POLICY VIOLATIONS (TOP 50)
- SDN/VTEP POLICY VIOLATIONS
- BOGON NETWORKS (TOP 50)
- BAD IP ADDRESS/NETWORKS
- Possible CryptoCurrencies Connections
- High Risk Index to/from INTERNET (TOP 50)
- Possible Social Network Connections

Internal Networks usage by hits

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

This table summarizes the Fl0wer defined internal networks usage ordered by number of hits. They are defined in file /opt/fl0wer/etc/fl0wer_internal_networks.conf and their purpose is to identify and classify traffic.

	Name	Zone	Subnet	ipVersion	Description	Hits	Bytes
0	mgmt	IP6NET	10.1.30.0/24	4	Management	244325	511.4 MBytes
1	backend	IP6NET	10.1.20.0/24	4	Backend	61984	285.9 MBytes
2	ubiquiti	FWLAB	10.100.4.0/24	4	Ubiquiti testing	41627	123.1 MBytes
3	ospflab	FWLAB	10.100.5.0/24	4	OSPF Lab testing	11095	3.0 MBytes
4	opnsense	FWLAB	10.100.10.0/16	4	FWLAB	9286	63.6 MBytes
5	cisco	FWLAB	10.100.1.0/24	4	Router Internal	7901	219.0 MBytes
6	wifi	WIRELESS	10.1.60.0/24	4	Wifi	5306	35.0 MBytes
7	transport	IP6NET	10.1.50.0/24	4	Transport	2883	3.5 MBytes
8	frontend	IP6NET	10.1.10.0/24	4	Frontend	2035	22.9 MBytes
9	backupisp	DISMISSED	10.100.2.0/24	4	Backup Internet subnet	1657	169.1 KBytes
10	mainisp	FWLAB	10.100.3.0/24	4	Main Internet subnet	1654	168.9 KBytes
11	ciscoweb	FWLAB	10.100.6.0/24	4	CiscoWeb Lab testing	34	2.4 KBytes
12	wifiguest	WIRELESS	10.1.90.0/24	4	Wifi guest	7	3.8 KBytes
13	isp1-botnet2	ISP1	10.200.5.6/32	4	ISP1-BOTNET2	0	0 bytes
14	isp3-botnet1	ISP3	10.202.5.2/32	4	ISP3-BOTNET1	0	0 bytes
15	isp4-botnet2	ISP4	10.203.5.6/32	4	ISP4-BOTNET2	0	0 bytes
16	isp4-botnet1	ISP4	10.203.5.2/32	4	ISP4-BOTNET1	0	0 bytes
17	isp3-botnet2	ISP3	10.202.5.6/32	4	ISP3-BOTNET2	0	0 bytes
18	test	IP6NET	10.1.40.0/24	4	Testing Network	0	0 bytes
19	isp2-botnet2	ISP2	10.201.5.6/32	4	ISP2-BOTNET2	0	0 bytes
20	isp1-botnet1	ISP1	10.200.5.2/32	4	ISP1-BOTNET1	0	0 bytes
21	SXT2	WIRELESS	10.1.70.0/24	4	SXT2 Antenna	0	0 bytes
22	com09	TRUSTED	10.200.200.209/32	4	VPN to COM09	0	0 bytes
23	sonicnet	FWLAB	10.100.7.0/24	4	Sonicwall NSA-240 VPN Network	0	0 bytes
24	isp2-botnet1	ISP2	10.201.5.2/32	4	ISP2-BOTNET1	0	0 bytes
25	fortigate60int	FWLAB	10.100.108.0/24	4	Fortigate 60 Attack Network Internal	0	0 bytes
26	sonicwallint	FWLAB	10.100.107.0/24	4	Sonicwall VPN Network Internal	0	0 bytes

	Name	Zone	Subnet	ipVersion	Description	Hits	Bytes
27	fortigate60	FWLAB	10.100.8.0/24	4	Fortigate 60 Attack Network	0	0 bytes
28	hurricane	INTERNET	2001:470:8b5b:1b7::2/64	6	Tunnel Hurricane Electric	0	0 bytes
29	ip6test	INTERNET	2001:470:8b5b::/48	6	Internal IPv6 Testing	0	0 bytes
30	unused_network	DISMISSED	10.1.35.0/24	4	Lab testing unused network	0	0 bytes
31	public	INTERNET	195.94.163.182/30	4	OLD-PUBLICIP	0	0 bytes
32	vm1	FWLAB	10.1.24.0/24	4	VM1 Lab testing	0	0 bytes
33	vm2	FWLAB	10.1.23.0/24	4	VM2 Lab testing	0	0 bytes
34	vm3	FWLAB	192.168.254.0/24	4	Laptop VM testing	0	0 bytes
35	voip	VOIP	10.1.200.0/24	4	VoIP Lab testing	0	0 bytes
36	voip2	VOIP	10.1.201.0/24	4	VoIP Lab testing	0	0 bytes
37	voip3	VOIP	10.1.202.0/24	4	VoIP Lab testing	0	0 bytes
38	dismissed_network	DISMISSED	10.1.45.0/24	4	Lab testing dismissed network	0	0 bytes
39	oldgw	DISMISSED	10.1.246.0/24	4	Oldgw Lab testing	0	0 bytes
40	oldmonitor	DISMISSED	10.1.249.0/24	4	Oldmonitor Lab testing	0	0 bytes
41	oldboh	DISMISSED	10.1.84.0/24	4	Oldboh Lab testing	0	0 bytes
42	oldipsec	DISMISSED	10.1.4.0/24	4	Oldipsec Lab testing	0	0 bytes
43	wifiregione	WIRELESS	172.19.0.0/16	4	wifiregione Lab testing	0	0 bytes
44	private_lab_net	DISMISSED	10.10.10.0/24	4	Lab testing private net	0	0 bytes
45	mesh1	FWLAB	10.100.120.0/21	4	Mesh1 OSPF Lab testing	0	0 bytes
46	mesh2	FWLAB	10.100.128.0/21	4	Mesh2 OSPF Lab testing	0	0 bytes
47	audiolab	FWLAB	10.1.31.0/24	4	Audio Lab testing	0	0 bytes
48	multicast	INTERNAL	224.0.0.0/8	4	Multicast traffic	0	0 bytes

Flow Exporters usage by IPv4 Traffic

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

This table lists all the Netflow/sFlow/IPFix flow exporters that are currently providing data to Fl0wer. It is sorted by IPv4 Traffic seen by each exporter.

	Exporter	IPV4_Traffic	IPv6_Traffic	IPV4_Packets	IPV6_Packets	Netflow1_Packets	Netflow5_Packets	Netflow9_Packets	IPFIX_Packets	SFlowV5_Packets	AverageFPS	AveragePPS
0	10.1.30.99	368.5 MBytes	53796	760185	767	0	0	0	7841	0	40	2
1	10.100.0.20	143.6 MBytes	624	428179	6	0	0	6144	0	0	41	1
2	10.1.30.220	96.5 MBytes	0	141653	0	0	0	0	381	0	1	0
3	10.100.4.20	37.1 MBytes	0	197913	0	0	0	0	21221	0	44	6
4	10.100.1.1	18.8 MBytes	0	102297	0	0	0	0	16432	0	30	4
5	10.1.30.89	6.2 MBytes	336	11876	6	0	0	0	49	0	0	0
6	10.1.30.101	3.4 MBytes	376013	30644	2136	0	0	0	514	0	0	0
7	10.1.30.102	1.2 MBytes	605940	3689	3243	0	0	0	507	0	0	0
8	10.1.30.8	924.4 KBytes	0	1251	0	0	0	0	0	1567	0	0
9	10.1.30.16	439.8 KBytes	0	1178	0	0	0	0	0	2378	0	0
10	10.1.20.130	433.4 KBytes	0	569	0	0	0	0	0	2199	0	0
11	10.1.30.21	328.2 KBytes	1464	4158	21	0	0	24	0	0	0	0
12	10.1.20.100	145.9 KBytes	0	187	0	0	0	0	0	458	0	0
13	10.100.5.123	134.7 KBytes	0	1293	0	0	0	869	0	0	0	0
14	10.1.20.170	103.3 KBytes	0	126	0	0	0	0	0	408	0	0
15	10.1.30.9	100.3 KBytes	0	541	0	0	0	0	0	1793	0	0
16	10.1.20.171	88.5 KBytes	0	110	0	0	0	0	0	386	0	0
17	10.1.30.111	5.6 KBytes	2491	32	15	0	0	0	59	0	0	0
18	10.1.30.73	0 bytes	0	0	0	0	0	0	0	1644	0	0
19	10.1.10.30	0 bytes	0	0	0	0	0	0	0	91	0	0

Flow Exporters usage by Exporter

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

This table lists all the Netflow/sFlow/IPFix flow exporters that are currently providing data to Fl0wer. It is sorted by Exporter IP Address.

	Exporter	IPV4_Traffic	IPv6_Traffic	IPV4_Packets	IPV6_Packets	Netflow1_Packets	Netflow5_Packets	Netflow9_Packets	IPFIX_Packets	SFlowV5_Packets	AverageFPS	AveragePPS
0	10.1.10.30	0 bytes	0	0	0	0	0	0	0	91	0	0
1	10.1.20.100	145.9 KBytes	0	187	0	0	0	0	0	458	0	0
2	10.1.20.130	433.4 KBytes	0	569	0	0	0	0	0	2200	0	0
3	10.1.20.170	103.3 KBytes	0	126	0	0	0	0	0	408	0	0
4	10.1.20.171	88.5 KBytes	0	110	0	0	0	0	0	386	0	0
5	10.1.30.101	3.4 MBytes	376013	30644	2136	0	0	0	514	0	0	0
6	10.1.30.102	1.2 MBytes	605940	3689	3243	0	0	0	507	0	0	0
7	10.1.30.111	5.6 KBytes	2491	32	15	0	0	0	59	0	0	0
8	10.1.30.16	439.8 KBytes	0	1178	0	0	0	0	0	2378	0	0
9	10.1.30.21	328.2 KBytes	1464	4158	21	0	0	24	0	0	0	0
10	10.1.30.220	96.5 MBytes	0	141653	0	0	0	0	381	0	1	0
11	10.1.30.73	0 bytes	0	0	0	0	0	0	0	1644	0	0
12	10.1.30.8	924.4 KBytes	0	1251	0	0	0	0	0	1567	0	0
13	10.1.30.89	6.2 MBytes	336	11876	6	0	0	0	49	0	0	0
14	10.1.30.9	100.3 KBytes	0	541	0	0	0	0	0	1793	0	0
15	10.1.30.99	368.5 MBytes	53796	760185	767	0	0	0	7841	0	40	2
16	10.100.0.20	143.6 MBytes	624	428179	6	0	0	6144	0	0	41	1
17	10.100.1.1	18.8 MBytes	0	102297	0	0	0	0	16432	0	30	4
18	10.100.4.20	37.1 MBytes	0	197913	0	0	0	0	21221	0	44	6
19	10.100.5.123	134.7 KBytes	0	1293	0	0	0	869	0	0	0	0

Network Flow Matrix (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

This is the flow matrix for the timelapse period. It reports most used services between all security zones in terms of networks, hits, bytes and protocols.

This type of data is very useful because it helps you to track down all most used flows and can help you to build both Firewall rules (if you filter by IP Flow Direction using INTERNAL_TO_INTERNET and INTERNET_TO_INTERNAL) and both ACL filters (INTERNAL_TO_INTERNAL) that you can apply on your internal switches.

If you see INTERNET_TO_INTERNET traffic, it means that both the source and destination networks are not known to Fl0wer.

	srcZone	dstZone	srcSubnet	dstSubnet	srcDescription	dstDescription	FlowDirection	Protocol	NPAR	RULE	hits	bytes	packets	firstSeen	lastSeen	trafficCategory
0	FWLAB	IP6NET	10.100.4.0/24	10.1.30.0/24	Ubiquiti testing	Management	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	flowtraffic	26840	71.6 MBytes	156687	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
1	IP6NET	IP6NET	10.1.20.0/24	10.1.30.0/24	Backend	Management	INTERNAL_TO_INTERNAL	ip/0	L2 Ether Protocol: 0 (0x0)		7806	13.0 MBytes	28288	09/03/2022 11:07:00	09/03/2022 11:59:49	UNCLASSIFIED
2	INTERNET	IP6NET	0.0.0.0/0	10.1.30.0/24	INTERNET	Management	INTERNET_TO_INTERNAL	udp/53	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		7366	2.1 MBytes	25572	09/03/2022 11:07:00	09/03/2022 11:59:49	UNWANTED
3	IP6NET	IP6NET	10.1.30.0/24	10.1.20.0/24	Management	Backend	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	hypervisor	5538	47.8 MBytes	53430	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
4	FWLAB	IP6NET	10.100.4.0/24	10.1.20.0/24	Ubiquiti testing	Backend	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	flowtraffic	5339	40.1 MBytes	88125	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
5	FWLAB	IP6NET	10.100.1.0/24	10.1.20.0/24	Router Internal	Backend	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	flowtraffic	5112	100.2 MBytes	79075	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
6	IP6NET	IP6NET	10.1.30.0/24	10.1.20.0/24	Management	Backend	INTERNAL_TO_INTERNAL	udp/6343	UDP 6343 InMon sFlow Protocol	flowtraffic	4560	8.0 MBytes	16962	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
7	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	ip/0	L2 Ether Protocol: 0 (0x0)		4479	6.6 MBytes	16109	09/03/2022 11:07:00	09/03/2022 11:59:49	UNCLASSIFIED
8	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	udp/ 51413	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		4114	165.0 KBytes	5554	09/03/2022 11:07:00	09/03/2022 11:59:49	UNWANTED
9	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	udp/53	UDP 53 DNS Protocol	hypervisor	4069	848.1 KBytes	8085	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
10	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	hypervisor	3981	18.4 MBytes	29535	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
11	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6881	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3801	231.0 KBytes	5376	09/03/2022 11:08:34	09/03/2022 11:59:48	UNWANTED

	srcZone	dstZone	srcSubnet	dstSubnet	srcDescription	dstDescription	FlowDirection	Protocol	NPAR	RULE	hits	bytes	packets	firstSeen	lastSeen	trafficCategory
12	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6889	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3724	226.7 KBytes	5275	09/03/2022 11:07:02	09/03/2022 11:59:48	UNWANTED
13	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/4662	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3679	225.3 KBytes	5242	09/03/2022 11:08:36	09/03/2022 11:59:49	UNWANTED
14	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6888	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3673	233.5 KBytes	5434	09/03/2022 11:08:35	09/03/2022 11:59:48	UNWANTED
15	IP6NET	FWLAB	10.1.20.0/24	10.100.5.0/24	Backend	OSPF Lab testing	INTERNAL_TO_INTERNAL	icmp/0	ICMP Protocol Code: Not available		3614	742.1 KBytes	4446	09/03/2022 11:08:33	09/03/2022 11:56:40	NETWORK OPERATION
16	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6885	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3545	219.2 KBytes	5102	09/03/2022 11:07:02	09/03/2022 11:59:48	UNWANTED
17	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6883	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3536	226.3 KBytes	5267	09/03/2022 11:08:35	09/03/2022 11:59:49	UNWANTED
18	IP6NET	FWLAB	10.1.20.0/24	10.100.4.0/24	Backend	Ubiquiti testing	INTERNAL_TO_INTERNAL	icmp/0	ICMP Protocol Code: Not available		3506	4.3 MBytes	8490	09/03/2022 11:08:33	09/03/2022 11:56:40	NETWORK OPERATION
19	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6886	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3470	231.9 KBytes	5396	09/03/2022 11:07:02	09/03/2022 11:59:48	UNWANTED
20	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6884	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3445	210.9 KBytes	4909	09/03/2022 11:08:35	09/03/2022 11:59:48	UNWANTED
21	INTERNET	IP6NET	0.0.0.0/0	10.1.30.0/24	INTERNET	Management	INTERNET_TO_INTERNAL	udp/ 25826	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	flowtraffic	3381	32.6 MBytes	25324	09/03/2022 11:07:00	09/03/2022 11:59:49	UNWANTED
22	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6887	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3367	208.9 KBytes	4861	09/03/2022 11:08:35	09/03/2022 11:59:48	UNWANTED
23	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/6882	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		3355	207.2 KBytes	4822	09/03/2022 11:08:35	09/03/2022 11:59:48	UNWANTED
24	FWLAB	IP6NET	10.100.10.0/16	10.1.20.0/24	FWLAB	Backend	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	flowtraffic	2659	37.7 MBytes	27873	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
25	IP6NET	IP6NET	10.1.20.0/24	10.1.20.0/24	Backend	Backend	INTERNAL_TO_INTERNAL	ip/0	L2 Ether Protocol: 0 (0x0)		2617	2.0 MBytes	5391	09/03/2022 11:07:00	09/03/2022 11:59:49	UNCLASSIFIED
26	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	udp/161	UDP 161 SNMP Protocol		2612	444.3 KBytes	5698	09/03/2022 11:08:36	09/03/2022 11:58:39	NETWORK OPERATION
27	IP6NET	IP6NET	10.1.20.0/24	10.1.20.0/24	Backend	Backend	INTERNAL_TO_INTERNAL	udp/6343	UDP 6343 InMon sFlow Protocol	flowtraffic	2522	3.2 MBytes	8144	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
28	IP6NET	INTERNET	10.1.30.0/24	0.0.0.0/0	Management	INTERNET	INTERNAL_TO_INTERNET	udp/53	BOGON: Warning: Dst IP: 10.101.22.100 is a BOGON IPv4 address.		2263	863.4 KBytes	11789	09/03/2022 11:07:00	09/03/2022 11:59:49	UNWANTED
29	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	tcp/111	TCP 111 RPC Portmapper Protocol	hypervisor	2199	1.1 MBytes	18248	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
30	IP6NET	FWLAB	10.1.30.0/24	10.100.10.0/16	Management	FWLAB	INTERNAL_TO_INTERNAL	icmp/0	ICMP Protocol Code: Not available		2172	229.9 KBytes	2802	09/03/2022 11:08:34	09/03/2022 11:56:40	NETWORK OPERATION
31	IP6NET	INTERNET	10.1.30.0/24	0.0.0.0/0	Management	INTERNET	INTERNAL_TO_INTERNET	icmp/0	BOGON: Warning: Dst IP: 10.101.16.100 is a BOGON IPv4 address.		1870	178.8 KBytes	2222	09/03/2022 11:08:35	09/03/2022 11:56:39	UNWANTED
32	FWLAB	IP6NET	10.100.10.0/16	10.1.30.0/24	FWLAB	Management	INTERNAL_TO_INTERNAL	udp/ 25826	UDP 25826 collectd	flowtraffic	1869	5.9 MBytes	4543	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
33	FWLAB	IP6NET	10.100.5.0/24	10.1.30.0/24	OSPF Lab testing	Management	INTERNAL_TO_INTERNAL	udp/2056	UDP 2056 probably Cisco Netflow/IPFIX Protocol	flowtraffic	1831	567.2 KBytes	4045	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION

	srcZone	dstZone	srcSubnet	dstSubnet	srcDescription	dstDescription	FlowDirection	Protocol	NPAR	RULE	hits	bytes	packets	firstSeen	lastSeen	trafficCategory
34	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	tcp/892	TCP 892 probably NFS RPC mountd	hypervisor	1696	952.3 KBytes	13338	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
35	IP6NET	FWLAB	10.1.20.0/24	10.100.1.0/24	Backend	Router Internal	INTERNAL_TO_INTERNAL	ip/0	L2 Ether Protocol: 0 (0x0)		1690	3.9 MBytes	7155	09/03/2022 11:07:00	09/03/2022 11:59:49	UNCLASSIFIED
36	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/9050	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.		1577	98.4 KBytes	2291	09/03/2022 11:07:00	09/03/2022 11:59:49	UNWANTED
37	WIRELESS	DISMISSED	10.1.60.0/24	10.100.2.0/24	Wifi	Backup Internet subnet	INTERNAL_TO_INTERNAL	icmp/0	ICMP Protocol Code: Not available		1538	161.4 KBytes	2951	09/03/2022 11:08:33	09/03/2022 11:56:40	NETWORK OPERATION
38	WIRELESS	FWLAB	10.1.60.0/24	10.100.3.0/24	Wifi	Main Internet subnet	INTERNAL_TO_INTERNAL	icmp/0	ICMP Protocol Code: Not available		1532	161.1 KBytes	2945	09/03/2022 11:08:33	09/03/2022 11:56:40	NETWORK OPERATION
39	IP6NET	FWLAB	10.1.20.0/24	10.100.4.0/24	Backend	Ubiquiti testing	INTERNAL_TO_INTERNAL	ip/0	L2 Ether Protocol: 0 (0x0)		1466	3.4 MBytes	6721	09/03/2022 11:07:00	09/03/2022 11:59:49	UNCLASSIFIED
40	IP6NET	FWLAB	10.1.20.0/24	10.100.10.0/16	Backend	FWLAB	INTERNAL_TO_INTERNAL	ip/0	L2 Ether Protocol: 0 (0x0)		1432	3.1 MBytes	5726	09/03/2022 11:07:00	09/03/2022 11:59:49	UNCLASSIFIED
41	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	udp/ 25826	UDP 25826 collectd	hypervisor	1282	18.6 MBytes	14472	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
42	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/ 50002	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.		1098	52.0 KBytes	1209	09/03/2022 11:07:01	09/03/2022 11:59:49	UNWANTED
43	IP6NET	IP6NET	10.1.20.0/24	10.1.30.0/24	Backend	Management	INTERNAL_TO_INTERNAL	udp/ 25826	UDP 25826 collectd	flowtraffic	1082	7.4 MBytes	6414	09/03/2022 11:07:00	09/03/2022 11:59:49	NETWORK OPERATION
44	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/8333	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.		1067	50.6 KBytes	1178	09/03/2022 11:07:01	09/03/2022 11:59:49	UNWANTED
45	IP6NET	IP6NET	10.1.30.0/24	10.1.30.0/24	Management	Management	INTERNAL_TO_INTERNAL	udp/8089	UDP 8089 possibly Splunk Daemon or InfluxDB	hypervisor	1057	14.9 MBytes	12799	09/03/2022 11:07:00	09/03/2022 11:59:49	SYSTEMS OPERATION
46	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/443	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.		980	68.9 KBytes	1658	09/03/2022 11:07:00	09/03/2022 11:59:49	UNWANTED
47	IP6NET	IP6NET	10.1.30.0/24	10.1.20.0/24	Management	Backend	INTERNAL_TO_INTERNAL	udp/161	UDP 161 SNMP Protocol		980	152.4 KBytes	2156	09/03/2022 11:09:19	09/03/2022 11:58:39	NETWORK OPERATION
48	INTERNET	INTERNET	0.0.0.0/0	0.0.0.0/0	INTERNET	INTERNET	INTERNET_TO_INTERNET	tcp/21	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	FTP	957	59.5 KBytes	1410	09/03/2022 11:08:36	09/03/2022 11:59:47	UNWANTED
49	IP6NET	FWLAB	10.1.50.0/24	10.100.4.0/24	Transport	Ubiquiti testing	INTERNAL_TO_INTERNAL	icmp/0	ICMP Protocol Code: Not available		941	1.2 MBytes	2367	09/03/2022 11:08:33	09/03/2022 11:56:40	NETWORK OPERATION

Out of Matrix Flows (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

The traffic reported here is all traffic that didn't make into the Flow Matrix for some reason and is grouped by NPAR, IP Version, Protocol, Source and Destination.

At a certain point, the flow matrix freezes after reaching the set limit of entries or after a defined period, so it is possible that some usual flows are not reported in the flow matrix.

The Out of matrix traffic is grouped here for further analysis since can reveal traffic patterns that could be unnoticed.

Ideally, in this report you should see only sparse and unrelated traffic, but if you see recurring patterns, a deeper analysis should be performed to understand its causes.

Risks and Indicator of Compromise (IOC)

The related risks are that some recurring network activities could be not allowed nor enforced by policies and go unnoticed.

Suggested actions

The suggested action is to carefully check recurring patterns to identify unallowed behaviours.

	Type	Exporter	Protocol	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix	Bytes	Packets
0	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	675957
1	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	707486
2	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	699996
3	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	691363
4	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	715362
5	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	759925
6	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	694823
7	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	718102
8	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	741045
9	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	656999
10	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	737611
11	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	718757
12	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	743347
13	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	694643
14	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 2049 NAS Sun Microsystems NFS Protocol	DATA_STORAGE	10.1.30.251	10.1.30.220	10.1.30.0/24	10.1.30.0/24	4.0 GBytes	690807
15	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.50.100	10.1.30.74	10.1.50.0/24	10.1.30.0/24	428.5 MBytes	710624
16	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.20.201	10.1.30.74	10.1.20.0/24	10.1.30.0/24	287.6 MBytes	671947

	Type	Exporter	Protocol	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix	Bytes	Packets
17	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.20.218	10.1.30.74	10.1.20.0/24	10.1.30.0/24	143.3 MBytes	333998
18	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.20.216	10.1.30.74	10.1.20.0/24	10.1.30.0/24	137.6 MBytes	252096
19	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.20.217	10.1.30.74	10.1.20.0/24	10.1.30.0/24	137.6 MBytes	207480
20	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL	TCP 22 SSH/SFTP Protocol	MANAGEMENT	10.1.60.131	10.1.30.220	10.1.60.0/24	10.1.30.0/24	66.5 MBytes	45987
21	IPv4	10.1.30.99	tcp	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	10.1.30.220		10.1.30.0/24	65.6 MBytes	1562864
22	IPv4	10.1.30.99	tcp	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	192.168.179.1			59.7 MBytes	1423432
23	IPv4	10.100.0.20	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2055 Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.220	10.100.1.0/24	10.1.30.0/24	55.5 MBytes	43778
24	IPv4	10.100.0.20	tcp	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	192.168.179.1			53.8 MBytes	1282234
25	IPv4	10.100.0.20	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2055 Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.220	10.100.1.0/24	10.1.30.0/24	34.8 MBytes	27401
26	IPv4	10.100.0.20	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2055 Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.220	10.100.1.0/24	10.1.30.0/24	33.4 MBytes	26313
27	IPv4	10.100.4.20	tcp	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	10.1.30.220		10.1.30.0/24	32.1 MBytes	764621
28	IPv4	10.100.0.20	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2055 Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.220	10.100.1.0/24	10.1.30.0/24	30.3 MBytes	23848
29	IPv4	10.100.4.20	tcp	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	192.168.179.1			28.0 MBytes	667698
30	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.30.74	10.1.50.100	10.1.30.0/24	10.1.50.0/24	26.4 MBytes	212815
31	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.30.74	10.1.20.201	10.1.30.0/24	10.1.20.0/24	23.8 MBytes	205071
32	IPv4	10.100.1.1	tcp	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	192.168.179.1			22.2 MBytes	529978
33	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	19.2 MBytes	15127
34	IPv4	10.100.4.20	icmp	FLOW_INTERNAL_TO_INTERNAL	ICMP Protocol Code: Not available	NETWORK OPERATION	10.1.50.100	10.100.4.20	10.1.50.0/24	10.100.4.0/24	18.3 MBytes	35862
35	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	15.7 MBytes	12367
36	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	15.7 MBytes	12356
37	IPv4	10.100.1.1	tcp	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	10.1.30.220		10.1.30.0/24	15.3 MBytes	363455
38	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	14.9 MBytes	11750
39	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	14.3 MBytes	11315
40	IPv4	10.1.30.220	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.60.10	10.1.30.220	10.1.60.0/24	10.1.30.0/24	14.3 MBytes	5075
41	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	13.6 MBytes	10695
42	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	12.4 MBytes	9744
43	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	12.3 MBytes	9724
44	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.30.74	10.1.30.220	10.1.30.0/24	10.1.30.0/24	12.3 MBytes	141176
45	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	12.3 MBytes	9679
46	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	12.3 MBytes	9676
47	IPv4	10.1.30.220	udp	FLOW_INTERNAL_TO_INTERNAL	UDP 2057 probably Cisco Netflow/IPFIX Protocol	NETWORK OPERATION	10.100.1.1	10.1.30.210	10.100.1.0/24	10.1.30.0/24	12.0 MBytes	9443
48	IPv4	10.100.0.20	tcp	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100	10.1.30.220		10.1.30.0/24	11.8 MBytes	281685
49	IPv4	10.1.30.99	tcp	FLOW_INTERNAL_TO_INTERNAL		UNCLASSIFIED	10.1.30.74	10.1.20.218	10.1.30.0/24	10.1.20.0/24	11.8 MBytes	98212

Possible TOR Connections (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

The TOR (The Onion Router) network was conceived to protect the privacy and anonimity of its users, by means of hiding the original source of communication and targets between a series of software routers managed in an independent way.

While this can help users to protect their privacy, it's also true that this network is often used by Cybercrime to sell illegal things, to hide illegal services, and to hide Command & Control centers for botnets or malwares.

Risks and Indicator of Compromise (IOC)

The related risks of seeing traffic using the TOR network are several like the above said. Further, if these connection happen from several systems or internal servers, it is possible that your internal network is already compromised.

Suggested actions

The suggested action is to review carefully the evidence of traffic, review your company policies for I/T asset usage and enforce users to avoid this kind of traffic unless strictly necessary to your business.

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
0	2022-03-09 11:58:37	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50393	10.1.30.220/9001		10.1.30.0/24
1	2022-03-09 11:58:37	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50392	10.1.30.220/9001		10.1.30.0/24
2	2022-03-09 11:58:37	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50394	10.1.30.220/9001		10.1.30.0/24
3	2022-03-09 11:58:25	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/45142	220.244.111.183/9050		
4	2022-03-09 11:58:22	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48095	10.1.30.220/9050		10.1.30.0/24
5	2022-03-09 11:58:22	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48094	10.1.30.220/9050		10.1.30.0/24
6	2022-03-09 11:58:22	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48093	10.1.30.220/9050		10.1.30.0/24
7	2022-03-09 11:58:21	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/62751	220.134.225.18/9050		
8	2022-03-09 11:58:21	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/62750	220.134.225.18/9050		
9	2022-03-09 11:58:13	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/62751	220.134.225.18/9050		
10	2022-03-09 11:58:13	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/62750	220.134.225.18/9050		
11	2022-03-09 11:58:07	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/64606	219.91.20.79/9050		

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
12	2022-03-09 11:58:01	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/53113	192.168.179.10/9050		
13	2022-03-09 11:58:01	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/53113	192.168.179.10/9050		
14	2022-03-09 11:58:01	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/53112	192.168.179.10/9050		
15	2022-03-09 11:57:58	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/53112	192.168.179.10/9050		
16	2022-03-09 11:57:52	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/58665	220.244.111.183/9050		
17	2022-03-09 11:57:52	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/58665	220.244.111.183/9050		
18	2022-03-09 11:57:49	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/35358	220.233.73.236/9050		
19	2022-03-09 11:57:46	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48095	10.1.30.220/9001		10.1.30.0/24
20	2022-03-09 11:57:46	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48093	10.1.30.220/9001		10.1.30.0/24
21	2022-03-09 11:57:43	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/55056	220.233.73.236/9050		
22	2022-03-09 11:57:43	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/55056	220.233.73.236/9050		
23	2022-03-09 11:57:28	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/49046	220.233.178.199/9050		
24	2022-03-09 11:57:28	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/49045	220.233.178.199/9050		
25	2022-03-09 11:57:27	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/47216	220.135.161.136/9050		
26	2022-03-09 11:57:27	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/47216	220.135.161.136/9050		
27	2022-03-09 11:57:25	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/35525	220.135.161.136/9050		
28	2022-03-09 11:57:25	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/35524	220.135.161.136/9050		
29	2022-03-09 11:57:13	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/35358	220.233.73.236/9050		
30	2022-03-09 11:57:07	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42215	219.91.20.79/9050		
31	2022-03-09 11:57:07	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42215	219.91.20.79/9050		
32	2022-03-09 11:57:07	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42214	219.91.20.79/9050		
33	2022-03-09 11:57:07	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42214	219.91.20.79/9050		
34	2022-03-09 11:57:01	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/53420	219.91.20.79/9050		
35	2022-03-09 11:56:58	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/58095	192.168.179.10/9050		
36	2022-03-09 11:56:58	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48094	10.1.30.220/9001		10.1.30.0/24
37	2022-03-09 11:56:58	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNAL	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/48093	10.1.30.220/9001		10.1.30.0/24
38	2022-03-09 11:56:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42314	220.244.111.183/9050		

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
39	2022-03-09 11:56:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/50660	192.168.179.1/9001		
40	2022-03-09 11:56:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/50661	192.168.179.1/9001		
41	2022-03-09 11:56:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/50658	192.168.179.1/9001		
42	2022-03-09 11:56:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/50659	192.168.179.1/9001		
43	2022-03-09 11:56:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/50657	192.168.179.1/9001		
44	2022-03-09 11:56:46	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/55743	192.168.179.1/9001		
45	2022-03-09 11:56:46	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/55742	192.168.179.1/9001		
46	2022-03-09 11:56:46	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (4397 flows)	UNWANTED	10.101.16.100/55741	192.168.179.1/9001		
47	2022-03-09 11:56:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/37668	220.233.73.236/9050		
48	2022-03-09 11:56:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/37668	220.233.73.236/9050		
49	2022-03-09 11:56:37	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/64952	192.168.179.10/9050		

Possible P2P Connections

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

Peer-to-peer (P2P) networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application.

TWhile P2P systems had previously been used in many application domains, the architecture was popularized by the file sharing system Napster, eMule, BitTorrent,etc.

Risks and Indicator of Compromise (IOC)

There are several risks in allowing internal connections to a P2P network. Most P2P networks nowadays are used for illegal file-sharing, which often contains malwares, illegal softwares and hog bandwidth.

Suggested actions

The suggested action is to review carefully the evidence of traffic, review your company policies for I/T asset usage and enforce users to avoid this kind of traffic unless strictly necessary to your business.

***** NO DATA AVAILABLE FOR THE SELECTED TIMELAPSE**

Possible Covert Channels (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

In network security, a covert channel is a type of attack that creates a capability to transfer information objects between systems that are not supposed to be allowed to communicate by the network security policy.

A covert channel is so called because it is hidden from the access control mechanisms of secure networks since it does not use the normal data protocols conceived for data transfers, and therefore cannot be detected or controlled by the security mechanisms that underlie secure networks.

Risks and Indicator of Compromise (IOC)

The related risks are data exfiltration and remote Command & Control if the internal network is already compromised.

Suggested actions

The suggested action is to review carefully the evidence of traffic, indagate on systems using a passive network analyzer grabbing full packets and review that type of communication.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:51:33	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 299 Byte/Packet Ratio (28448 bytes - 95 packets in 109 seconds)
1	2022-03-09 11:43:40	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 420 Byte/Packet Ratio (29000 bytes - 69 packets in 155 seconds)
2	2022-03-09 11:41:04	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 312 Byte/Packet Ratio (32816 bytes - 105 packets in 131 seconds)
3	2022-03-09 11:24:08	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 435 Byte/Packet Ratio (26560 bytes - 61 packets in 63 seconds)
4	2022-03-09 11:11:43	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 260 Byte/Packet Ratio (18480 bytes - 71 packets in 78 seconds)
5	2022-03-09 02:41:31	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 271 Byte/Packet Ratio (30928 bytes - 114 packets in 135 seconds)
6	2022-03-09 02:35:33	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 390 Byte/Packet Ratio (26532 bytes - 68 packets in 51 seconds)
7	2022-03-09 02:30:03	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 249 Byte/Packet Ratio (16456 bytes - 66 packets in 58 seconds)
8	2022-03-09 02:07:26	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 416 Byte/Packet Ratio (21636 bytes - 52 packets in 82 seconds)
9	2022-03-09 01:55:33	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 378 Byte/Packet Ratio (24228 bytes - 64 packets in 53 seconds)
10	2022-03-09 01:41:56	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 368 Byte/Packet Ratio (38344 bytes - 104 packets in 56 seconds)
11	2022-03-09 01:39:58	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 440 Byte/Packet Ratio (42301 bytes - 96 packets in 117 seconds)
12	2022-03-09 01:13:00	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 373 Byte/Packet Ratio (75048 bytes - 201 packets in 282 seconds)
13	2022-03-09 01:03:47	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 420 Byte/Packet Ratio (26472 bytes - 63 packets in 102 seconds)
14	2022-03-09 00:55:01	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 342 Byte/Packet Ratio (18468 bytes - 54 packets in 57 seconds)
15	2022-03-09 00:51:54	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 321 Byte/Packet Ratio (33128 bytes - 103 packets in 83 seconds)
16	2022-03-09 00:36:13	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 416 Byte/Packet Ratio (64508 bytes - 155 packets in 148 seconds)
17	2022-03-09 00:30:33	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 309 Byte/Packet Ratio (25096 bytes - 81 packets in 58 seconds)
18	2022-03-09 00:20:47	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 192 Byte/Packet Ratio (14264 bytes - 74 packets in 73 seconds)

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
19	2022-03-08 23:55:44	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 306 Byte/Packet Ratio (22344 bytes - 73 packets in 85 seconds)
20	2022-03-08 23:28:23	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 376 Byte/Packet Ratio (50484 bytes - 134 packets in 186 seconds)
21	2022-03-08 23:16:23	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 457 Byte/Packet Ratio (126139 bytes - 276 packets in 277 seconds)
22	2022-03-08 23:11:47	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 377 Byte/Packet Ratio (76160 bytes - 202 packets in 243 seconds)
23	2022-03-08 23:05:55	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 332 Byte/Packet Ratio (26300 bytes - 79 packets in 88 seconds)
24	2022-03-08 22:51:53	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 274 Byte/Packet Ratio (24712 bytes - 90 packets in 91 seconds)
25	2022-03-08 22:27:47	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 448 Byte/Packet Ratio (24648 bytes - 55 packets in 52 seconds)
26	2022-03-08 22:25:11	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 368 Byte/Packet Ratio (22500 bytes - 61 packets in 51 seconds)
27	2022-03-08 22:16:34	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 344 Byte/Packet Ratio (36860 bytes - 107 packets in 146 seconds)
28	2022-03-08 22:13:15	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 519 Byte/Packet Ratio (30664 bytes - 59 packets in 84 seconds)
29	2022-03-08 22:07:17	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 420 Byte/Packet Ratio (56700 bytes - 135 packets in 126 seconds)
30	2022-03-08 22:04:20	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 462 Byte/Packet Ratio (32360 bytes - 70 packets in 105 seconds)
31	2022-03-08 22:02:32	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 354 Byte/Packet Ratio (43648 bytes - 123 packets in 114 seconds)
32	2022-03-08 21:56:28	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 296 Byte/Packet Ratio (16296 bytes - 55 packets in 53 seconds)
33	2022-03-08 21:53:25	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 413 Byte/Packet Ratio (100056 bytes - 242 packets in 249 seconds)
34	2022-03-08 21:28:24	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 424 Byte/Packet Ratio (22516 bytes - 53 packets in 59 seconds)
35	2022-03-08 21:13:02	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 497 Byte/Packet Ratio (30352 bytes - 61 packets in 82 seconds)
36	2022-03-08 21:11:37	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 360 Byte/Packet Ratio (57608 bytes - 160 packets in 145 seconds)
37	2022-03-08 21:05:03	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 461 Byte/Packet Ratio (47088 bytes - 102 packets in 108 seconds)
38	2022-03-08 20:59:53	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 397 Byte/Packet Ratio (21072 bytes - 53 packets in 50 seconds)
39	2022-03-08 20:56:05	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 379 Byte/Packet Ratio (48148 bytes - 127 packets in 137 seconds)
40	2022-03-08 20:40:42	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 321 Byte/Packet Ratio (27636 bytes - 86 packets in 57 seconds)
41	2022-03-08 20:35:08	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 436 Byte/Packet Ratio (22708 bytes - 52 packets in 42 seconds)
42	2022-03-08 20:35:08	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 458 Byte/Packet Ratio (44932 bytes - 98 packets in 108 seconds)
43	2022-03-08 20:19:54	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 335 Byte/Packet Ratio (47016 bytes - 140 packets in 176 seconds)
44	2022-03-08 20:00:57	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 329 Byte/Packet Ratio (51704 bytes - 157 packets in 220 seconds)
45	2022-03-08 19:55:36	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 319 Byte/Packet Ratio (34176 bytes - 107 packets in 136 seconds)
46	2022-03-08 19:46:59	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 391 Byte/Packet Ratio (72460 bytes - 185 packets in 292 seconds)
47	2022-03-08 19:20:26	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 333 Byte/Packet Ratio (29704 bytes - 89 packets in 59 seconds)
48	2022-03-08 19:04:50	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 480 Byte/Packet Ratio (27840 bytes - 58 packets in 63 seconds)
49	2022-03-08 18:55:16	WARNING	UNWANTED	10.1.30.220	ICMP: ANOMALY (possible Covert Channel) - Flow between 10.1.30.220 and 10.1.30.220 has a 476 Byte/Packet Ratio (26688 bytes - 56 packets in 55 seconds)

VERTICAL SCANS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

A portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself.

A vertical portscan is a typical scan towards a single IP address and can be originated by a software trying to figure out which network services are active on a single system.

Risks and Indicator of Compromise (IOC)

While this can be performed by system administrators or other softwares to gain some knowledge about a system, it is commonly used to find out vulnerabilities on the systems and is often the prelude to a direct attack to a system.

Suggested actions

The suggested action is to **quickly** review carefully the source address of the scanning system to understand the reasons for the scanning and to deny this type of traffic if possibile.

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
0	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.60 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.60/51413		
1	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.60 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.60/51413		
2	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.59 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.59/51413		
3	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.59 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.59/51413		
4	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.59 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.59/51413		
5	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.58 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.58/51413		
6	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.58 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.58/51413		
7	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.58 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.58/51413		
8	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.57 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.57/51413		
9	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.57 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.57/51413		
10	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.56 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.56/51413		
11	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.56 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.56/51413		
12	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.56 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.56/51413		

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
13	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.55 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.55/51413		
14	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.55 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.55/51413		
15	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.55 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.55/51413		
16	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.54 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.54/51413		
17	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.53 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.53/51413		
18	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.53 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.53/51413		
19	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.53 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.53/51413		
20	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.52 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.52/51413		
21	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.52 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.52/51413		
22	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.52 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.52/51413		
23	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.51 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.51/51413		
24	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.51 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.51/51413		
25	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.51 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.51/51413		
26	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.50 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.50/51413		
27	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.49 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.49/51413		
28	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.48 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.48/51413		
29	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.47 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.47/51413		
30	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.46 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.46/51413		
31	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.45 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.45/51413		
32	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.44 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.44/51413		
33	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.43 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.43/51413		
34	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.42 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.42/51413		
35	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.41 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.41/51413		
36	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.40 (294 flows)	UNWANTED	10.101.16.100/38173	192.168.179.40/51413		
37	2022-03-09 11:58:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.40 (294 flows)	UNWANTED	10.101.16.100/38172	192.168.179.40/51413		
38	2022-03-09 11:57:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.54 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.54/51413		
39	2022-03-09 11:57:31	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.54 (294 flows)	UNWANTED	10.101.16.100/60903	192.168.179.54/51413		

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
40	2022-03-09 11:57:28	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.54 (294 flows)	UNWANTED	10.101.16.100/60903	192.168.179.54/51413		
41	2022-03-09 11:57:28	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.53 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.53/51413		
42	2022-03-09 11:57:28	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.52 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.52/51413		
43	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.50 (294 flows)	UNWANTED	10.101.16.100/60903	192.168.179.50/51413		
44	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.50 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.50/51413		
45	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.49 (294 flows)	UNWANTED	10.101.16.100/60903	192.168.179.49/51413		
46	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.49 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.49/51413		
47	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.48 (294 flows)	UNWANTED	10.101.16.100/60903	192.168.179.48/51413		
48	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.48 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.48/51413		
49	2022-03-09 11:57:27	IPv4	10.100.0.20	udp	28 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making an UDP scan to host: 192.168.179.47 (294 flows)	UNWANTED	10.101.16.100/60904	192.168.179.47/51413		

HORIZONTAL SCANS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

A portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself.

An horizontal scan is a typical scan looking for a certain port open on all systems in a network. An example would be "I want to know all systems providing 23/tcp (telnet) port service that I can reach"

Risks and Indicator of Compromise (IOC)

The related risks are quite high, since a portscan of this type could be the evidence of a worm (malware or ransomware) trying to propagate himself inside the network or the sign of someone already in that looks for a well known vulnerability on other systems of your internal network.

Suggested actions

The suggested action is to **quickly** review carefully the source address of the scanning system to understand the reasons for the scanning and to deny this type of traffic if possibile.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:59:49	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (32 flows on 21 different tuples dstip/dstport)
1	2022-03-09 11:58:40	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (126 flows on 21 different tuples dstip/dstport)
2	2022-03-09 11:57:00	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (65 flows on 21 different tuples dstip/dstport)
3	2022-03-09 11:55:28	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (42 flows on 21 different tuples dstip/dstport)
4	2022-03-09 11:54:06	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (73 flows on 21 different tuples dstip/dstport)
5	2022-03-09 11:52:45	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (86 flows on 21 different tuples dstip/dstport)
6	2022-03-09 11:51:33	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (64 flows on 21 different tuples dstip/dstport)
7	2022-03-09 11:50:05	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (44 flows on 21 different tuples dstip/dstport)
8	2022-03-09 11:49:15	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (105 flows on 21 different tuples dstip/dstport)
9	2022-03-09 11:48:55	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (81 flows on 21 different tuples dstip/dstport)
10	2022-03-09 11:47:56	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (111 flows on 21 different tuples dstip/dstport)
11	2022-03-09 11:45:37	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (68 flows on 21 different tuples dstip/dstport)
12	2022-03-09 11:43:40	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (83 flows on 21 different tuples dstip/dstport)
13	2022-03-09 11:42:16	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (98 flows on 21 different tuples dstip/dstport)
14	2022-03-09 11:41:04	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (117 flows on 21 different tuples dstip/dstport)
15	2022-03-09 11:39:46	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (97 flows on 21 different tuples dstip/dstport)
16	2022-03-09 11:38:14	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (133 flows on 21 different tuples dstip/dstport)
17	2022-03-09 11:36:46	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (27 flows on 21 different tuples dstip/dstport)
18	2022-03-09 11:35:19	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (57 flows on 21 different tuples dstip/dstport)

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
19	2022-03-09 11:34:31	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (142 flows on 21 different tuples dstip/dstport)
20	2022-03-09 11:33:31	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (60 flows on 21 different tuples dstip/dstport)
21	2022-03-09 11:32:00	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (104 flows on 21 different tuples dstip/dstport)
22	2022-03-09 11:30:28	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (105 flows on 21 different tuples dstip/dstport)
23	2022-03-09 11:28:57	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (69 flows on 21 different tuples dstip/dstport)
24	2022-03-09 11:27:03	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (69 flows on 21 different tuples dstip/dstport)
25	2022-03-09 11:26:09	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (100 flows on 21 different tuples dstip/dstport)
26	2022-03-09 11:25:36	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (161 flows on 21 different tuples dstip/dstport)
27	2022-03-09 11:24:08	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (85 flows on 21 different tuples dstip/dstport)
28	2022-03-09 11:22:36	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (167 flows on 21 different tuples dstip/dstport)
29	2022-03-09 11:22:36	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (128 flows on 21 different tuples dstip/dstport)
30	2022-03-09 11:20:53	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (66 flows on 21 different tuples dstip/dstport)
31	2022-03-09 11:19:16	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (110 flows on 21 different tuples dstip/dstport)
32	2022-03-09 11:18:50	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (113 flows on 21 different tuples dstip/dstport)
33	2022-03-09 11:17:26	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (100 flows on 21 different tuples dstip/dstport)
34	2022-03-09 11:14:22	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (45 flows on 21 different tuples dstip/dstport)
35	2022-03-09 11:13:07	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (145 flows on 21 different tuples dstip/dstport)
36	2022-03-09 11:11:43	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (78 flows on 21 different tuples dstip/dstport)
37	2022-03-09 11:09:21	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (60 flows on 21 different tuples dstip/dstport)
38	2022-03-09 11:08:37	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (140 flows on 21 different tuples dstip/dstport)
39	2022-03-09 02:50:35	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (72 flows on 21 different tuples dstip/dstport)
40	2022-03-09 02:49:23	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (110 flows on 21 different tuples dstip/dstport)
41	2022-03-09 02:46:33	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (69 flows on 21 different tuples dstip/dstport)
42	2022-03-09 02:45:16	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (82 flows on 21 different tuples dstip/dstport)
43	2022-03-09 02:43:32	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (94 flows on 21 different tuples dstip/dstport)
44	2022-03-09 02:42:31	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (53 flows on 21 different tuples dstip/dstport)
45	2022-03-09 02:40:05	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (42 flows on 21 different tuples dstip/dstport)
46	2022-03-09 02:38:56	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (56 flows on 21 different tuples dstip/dstport)
47	2022-03-09 02:36:55	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (116 flows on 21 different tuples dstip/dstport)
48	2022-03-09 02:35:33	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (89 flows on 21 different tuples dstip/dstport)
49	2022-03-09 02:33:39	ALERT	UNWANTED	10.101.16.100	HORIZONTAL_SCAN: IP: 10.101.16.100 is probably making a UDP horizontal scan on port 51413 (90 flows on 21 different tuples dstip/dstport)

DNS POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

In Fl0wer you can define the IP addresses for DNS servers used in your network infrastructure. These files must be customized and are in:

- /opt/fl0wer/iplist/dns4.txt for IPv4 DNS servers
- /opt/fl0wer/iplist/dns6.txt for IPv6 DNS servers

All the DNS traffic that is on port UDP/53 and TCP/53 that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

There are several related risks that are possible in your internal infrastructure, ranging from wrongly unresolved hosts for users to redirecting internal servers (and users) to criminal managed systems with unknown consequences.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:59:57	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
1	2022-03-09 11:59:57	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
2	2022-03-09 11:59:57	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
3	2022-03-09 11:59:57	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
4	2022-03-09 11:59:57	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
5	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
6	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 10.1.30.220 is an unallowed IPv4 DNS server replying to 10.101.16.100
7	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server replying to 10.1.30.54
8	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server queried by 10.1.30.54
9	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server replying to 10.1.30.54
10	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server queried by 10.1.30.54
11	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
12	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
13	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
14	2022-03-09 11:59:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
15	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
16	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 10.1.30.220 is an unallowed IPv4 DNS server replying to 10.101.16.100

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
17	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server replying to 10.1.30.54
18	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server queried by 10.1.30.54
19	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
20	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
21	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
22	2022-03-09 11:59:49	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
23	2022-03-09 11:59:49	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
24	2022-03-09 11:58:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server replying to 10.1.30.54
25	2022-03-09 11:58:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server queried by 10.1.30.54
26	2022-03-09 11:58:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
27	2022-03-09 11:58:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
28	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.100.0.20	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
29	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server replying to 10.1.30.54
30	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.143.19 is an unallowed IPv4 DNS server queried by 10.1.30.54
31	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.220	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
32	2022-03-09 11:58:49	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.60.132
33	2022-03-09 11:58:49	POLICY	NETWORK OPERATION	10.1.30.220	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
34	2022-03-09 11:58:49	POLICY	NETWORK OPERATION	10.1.30.220	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
35	2022-03-09 11:58:46	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 192.168.179.1 is an unallowed IPv4 DNS server replying to 10.101.16.100
36	2022-03-09 11:58:46	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 192.168.179.1 is an unallowed IPv4 DNS server queried by 10.101.16.100
37	2022-03-09 11:58:46	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 192.168.179.1 is an unallowed IPv4 DNS server replying to 10.101.16.100
38	2022-03-09 11:58:46	POLICY	NETWORK OPERATION	10.100.4.20	DNS: 192.168.179.1 is an unallowed IPv4 DNS server queried by 10.101.16.100
39	2022-03-09 11:58:46	POLICY	NETWORK OPERATION	10.100.0.20	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
40	2022-03-09 11:58:43	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 192.168.179.1 is an unallowed IPv4 DNS server replying to 10.101.16.100
41	2022-03-09 11:58:43	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 192.168.179.1 is an unallowed IPv4 DNS server queried by 10.101.16.100
42	2022-03-09 11:57:58	POLICY	NETWORK OPERATION	10.100.1.1	DNS: 10.1.30.220 is an unallowed IPv4 DNS server queried by 10.101.16.100
43	2022-03-09 11:57:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.182.3 is an unallowed IPv4 DNS server replying to 10.1.30.54
44	2022-03-09 11:57:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.182.3 is an unallowed IPv4 DNS server queried by 10.1.30.54
45	2022-03-09 11:57:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20
46	2022-03-09 11:57:58	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
47	2022-03-09 11:57:55	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server queried by 10.1.30.20
48	2022-03-09 11:57:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 195.94.182.3 is an unallowed IPv4 DNS server queried by 10.1.30.54
49	2022-03-09 11:57:52	POLICY	NETWORK OPERATION	10.1.30.99	DNS: 10.1.30.154 is an unallowed IPv4 DNS server replying to 10.1.30.20

NTP POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

In Fl0wer you can define the IP addresses used in your infrastructure to keep system time aligned on the whole network. These files must be customized and are in:

- /opt/fl0wer/iplist/ntp4.txt for IPv4 NTP servers
- /opt/fl0wer/iplist/ntp6.txt for IPv6 NTP servers

All the NTP traffic on ports UDP/123 and TCP/123 that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

The related risks are that systems can be unaligned on current time, you could have Kerberos (thus Active Directory) authentication issues and also making unallowed traffic inside your internal network.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:59:52	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
1	2022-03-09 11:59:49	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
2	2022-03-09 11:57:16	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 93.94.88.51 is an unallowed IPv4 NTP server replying to 10.1.60.170
3	2022-03-09 11:57:16	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 93.94.88.51 is an unallowed IPv4 NTP server queried by 10.1.60.170
4	2022-03-09 11:54:07	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.22.100 is UNKNOWN, destination 10.1.30.151 is known.
5	2022-03-09 11:54:07	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.151 is known, destination 10.101.22.100 is UNKNOWN.
6	2022-03-09 11:53:26	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
7	2022-03-09 11:53:26	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
8	2022-03-09 11:53:07	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
9	2022-03-09 11:53:07	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.150 is known, destination 10.101.16.100 is UNKNOWN.
10	2022-03-09 11:53:06	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.150 is known, destination 10.101.16.100 is UNKNOWN.
11	2022-03-09 11:53:06	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
12	2022-03-09 11:53:06	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.150 is known, destination 10.101.16.100 is UNKNOWN.
13	2022-03-09 11:51:36	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 188.213.165.209 is an unallowed IPv4 NTP server replying to 10.1.60.170
14	2022-03-09 11:51:36	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 188.213.165.209 is an unallowed IPv4 NTP server queried by 10.1.60.170
15	2022-03-09 11:49:21	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.152 is UNKNOWN, destination 10.1.30.21 is UNKNOWN.
16	2022-03-09 11:49:21	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.21 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
17	2022-03-09 11:44:56	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
18	2022-03-09 11:44:56	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
19	2022-03-09 11:44:47	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 212.237.55.238 is an unallowed IPv4 NTP server replying to 10.1.60.170
20	2022-03-09 11:44:47	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 212.237.55.238 is an unallowed IPv4 NTP server queried by 10.1.60.170
21	2022-03-09 11:44:44	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
22	2022-03-09 11:44:44	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.150 is known, destination 10.101.16.100 is UNKNOWN.
23	2022-03-09 11:44:44	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.100.10.22 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
24	2022-03-09 11:44:44	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.100.10.22 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
25	2022-03-09 11:44:41	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.150 is known.
26	2022-03-09 11:44:41	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.150 is known, destination 10.101.16.100 is UNKNOWN.
27	2022-03-09 11:44:29	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
28	2022-03-09 11:44:26	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.100.10.22 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
29	2022-03-09 11:44:26	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.152 is UNKNOWN, destination 10.100.10.22 is UNKNOWN.
30	2022-03-09 11:44:26	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.100.10.22 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
31	2022-03-09 11:44:26	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.152 is UNKNOWN, destination 10.100.10.22 is UNKNOWN.
32	2022-03-09 11:44:17	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
33	2022-03-09 11:44:17	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.152 is UNKNOWN, destination 10.101.16.100 is UNKNOWN.
34	2022-03-09 11:44:17	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
35	2022-03-09 11:44:17	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.152 is UNKNOWN, destination 10.101.16.100 is UNKNOWN.
36	2022-03-09 11:44:14	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
37	2022-03-09 11:44:14	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.152 is UNKNOWN, destination 10.101.16.100 is UNKNOWN.
38	2022-03-09 11:40:55	POLICY	NETWORK OPERATION	10.100.1.1	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
39	2022-03-09 11:40:46	POLICY	NETWORK OPERATION	10.100.0.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
40	2022-03-09 11:40:37	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.152 is UNKNOWN, destination 10.1.30.21 is UNKNOWN.
41	2022-03-09 11:40:37	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.21 is UNKNOWN, destination 10.1.30.152 is UNKNOWN.
42	2022-03-09 11:40:31	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
43	2022-03-09 11:40:31	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.151 is known, destination 10.101.16.100 is UNKNOWN.
44	2022-03-09 11:40:31	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
45	2022-03-09 11:40:31	POLICY	NETWORK OPERATION	10.100.4.20	NTP: source 10.1.30.151 is known, destination 10.101.16.100 is UNKNOWN.
46	2022-03-09 11:40:31	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.101.16.100 is UNKNOWN, destination 10.1.30.151 is known.
47	2022-03-09 11:40:31	POLICY	NETWORK OPERATION	10.1.30.99	NTP: source 10.1.30.151 is known, destination 10.101.16.100 is UNKNOWN.
48	2022-03-09 11:40:13	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 10.1.30.152 is an unallowed supposed IPv4 NTP server queried by 10.1.30.220
49	2022-03-09 11:40:13	POLICY	NETWORK OPERATION	10.1.30.99	NTP: 10.1.30.152 is an unallowed supposed IPv4 NTP server replying to 10.1.30.220

BGP POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

In Fl0wer you can define the IP addresses for BGP endpoints used in your SDN to distribute routes internally and allow intra-vpc communcation. These files must be customized and are in:

- /opt/fl0wer/iplist/bgp4.txt for IPv4 BGP servers
- /opt/fl0wer/iplist/bgp6.txt for IPv6 BGP servers

All the BGP traffic that is on port TCP/179 that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

The related risks are that your VPC systems can be unreachable or wrong routes could be injected inside your SDN.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:59:49	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
1	2022-03-09 11:58:55	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer replying to 10.100.5.1
2	2022-03-09 11:58:55	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
3	2022-03-09 11:58:55	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
4	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer replying to 10.100.5.1
5	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
6	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
7	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
8	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
9	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
10	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
11	2022-03-09 11:58:52	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
12	2022-03-09 11:57:58	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
13	2022-03-09 11:57:40	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
14	2022-03-09 11:57:34	POLICY	NETWORK OPERATION	10.100.1.1	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
15	2022-03-09 11:57:34	POLICY	NETWORK OPERATION	10.100.1.1	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
16	2022-03-09 11:57:27	POLICY	NETWORK OPERATION	10.100.5.123	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
17	2022-03-09 11:57:07	POLICY	NETWORK OPERATION	10.1.30.9	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
18	2022-03-09 11:55:58	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
19	2022-03-09 11:55:58	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
20	2022-03-09 11:55:55	POLICY	NETWORK OPERATION	10.100.1.1	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
21	2022-03-09 11:55:49	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
22	2022-03-09 11:55:49	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer replying to 10.100.5.1
23	2022-03-09 11:55:40	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
24	2022-03-09 11:55:40	POLICY	NETWORK OPERATION	10.1.30.99	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
25	2022-03-09 11:55:37	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
26	2022-03-09 11:55:37	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer replying to 10.100.5.1
27	2022-03-09 11:55:34	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
28	2022-03-09 11:55:34	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.101 is an unallowed IPv4 BGP peer queried by 10.100.5.1
29	2022-03-09 11:55:34	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.20 is an unallowed IPv4 BGP peer queried by 10.100.5.1
30	2022-03-09 11:55:28	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
31	2022-03-09 11:55:28	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
32	2022-03-09 11:55:28	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
33	2022-03-09 11:55:28	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
34	2022-03-09 11:55:27	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
35	2022-03-09 11:55:27	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
36	2022-03-09 11:55:27	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
37	2022-03-09 11:54:58	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
38	2022-03-09 11:54:58	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
39	2022-03-09 11:54:58	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer replying to 10.100.5.1
40	2022-03-09 11:54:46	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1
41	2022-03-09 11:54:46	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
42	2022-03-09 11:54:43	POLICY	NETWORK OPERATION	10.100.4.20	BGP: 192.168.179.1 is an unallowed IPv4 BGP peer queried by 10.101.16.100
43	2022-03-09 11:54:15	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
44	2022-03-09 11:54:15	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
45	2022-03-09 11:54:15	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
46	2022-03-09 11:54:13	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
47	2022-03-09 11:54:13	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
48	2022-03-09 11:54:13	POLICY	NETWORK OPERATION	10.100.0.20	BGP: 10.1.30.220 is an unallowed IPv4 BGP peer queried by 10.101.16.100
49	2022-03-09 11:53:57	POLICY	NETWORK OPERATION	10.100.5.123	BGP: 10.100.5.123 is an unallowed IPv4 BGP peer queried by 10.100.5.1

SNMP POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.

Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

In Fl0wer you can define the IP addresses for SNMP monitoring systems used in your network infrastructure. These files must be customized and are in:

- /opt/fl0wer/iplist/snmp4list.txt for IPv4 SNMP monitors
- /opt/fl0wer/iplist/snmp6list.txt for IPv6 SNMP monitors

All the SNMP traffic that is on port UDP/161 that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

Most versions of SNMP currently deployed still use unauthenticated public communities, thus allowing attackers to gain a lot of information about their target systems.

There are risks in exposing critical system information to unallowed people could be very dangerous, as well as trying to mask unallowed traffic in a monitoring protocol.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:58:39	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.15 is a BOGON IPv4 address.) from 10.1.30.81/60077 to 10.1.80.15/161 (71 bytes in 1 packets)
1	2022-03-09 11:58:39	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.15 is a BOGON IPv4 address.) from 10.1.30.81/60077 to 10.1.80.15/161 (71 bytes in 1 packets)
2	2022-03-09 11:58:39	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.15 is a BOGON IPv4 address.) from 10.1.30.81/60077 to 10.1.80.15/161 (142 bytes in 2 packets)
3	2022-03-09 11:58:39	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.14 is a BOGON IPv4 address.) from 10.1.30.81/35114 to 10.1.80.14/161 (142 bytes in 2 packets)
4	2022-03-09 11:58:39	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.11 is a BOGON IPv4 address.) from 10.1.30.81/42744 to 10.1.80.11/161 (284 bytes in 4 packets)
5	2022-03-09 11:57:00	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55744 to 192.168.179.1/161 (176 bytes in 4 packets)
6	2022-03-09 11:57:00	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55743 to 192.168.179.1/161 (176 bytes in 4 packets)
7	2022-03-09 11:57:00	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55742 to 192.168.179.1/161 (176 bytes in 4 packets)
8	2022-03-09 11:57:00	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55741 to 192.168.179.1/161 (176 bytes in 4 packets)
9	2022-03-09 11:55:27	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38841 to 192.168.179.1/161 (44 bytes in 1 packets)
10	2022-03-09 11:55:27	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38840 to 192.168.179.1/161 (44 bytes in 1 packets)
11	2022-03-09 11:55:27	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38839 to 192.168.179.1/161 (44 bytes in 1 packets)

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
12	2022-03-09 11:55:27	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55743 to 192.168.179.1/161 (44 bytes in 1 packets)
13	2022-03-09 11:55:27	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55744 to 192.168.179.1/161 (44 bytes in 1 packets)
14	2022-03-09 11:55:27	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55744 to 192.168.179.1/161 (44 bytes in 1 packets)
15	2022-03-09 11:45:37	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52009 to 10.1.30.220/161 (176 bytes in 4 packets)
16	2022-03-09 11:45:37	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52008 to 10.1.30.220/161 (176 bytes in 4 packets)
17	2022-03-09 11:43:40	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56755 to 192.168.179.1/161 (44 bytes in 1 packets)
18	2022-03-09 11:43:40	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56751 to 192.168.179.1/161 (44 bytes in 1 packets)
19	2022-03-09 11:43:40	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56753 to 192.168.179.1/161 (44 bytes in 1 packets)
20	2022-03-09 11:43:40	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56752 to 192.168.179.1/161 (44 bytes in 1 packets)
21	2022-03-09 11:43:40	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56754 to 192.168.179.1/161 (44 bytes in 1 packets)
22	2022-03-09 11:38:13	POLICY	MANAGEMENT	10.100.4.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48728 to 192.168.179.1/161 (44 bytes in 1 packets)
23	2022-03-09 11:38:13	POLICY	MANAGEMENT	10.100.4.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48728 to 192.168.179.1/161 (44 bytes in 1 packets)
24	2022-03-09 11:36:45	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48728 to 192.168.179.1/161 (44 bytes in 1 packets)
25	2022-03-09 11:36:45	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48727 to 192.168.179.1/161 (44 bytes in 1 packets)
26	2022-03-09 11:36:45	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48726 to 192.168.179.1/161 (44 bytes in 1 packets)
27	2022-03-09 11:36:45	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48727 to 192.168.179.1/161 (44 bytes in 1 packets)
28	2022-03-09 11:36:45	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48726 to 192.168.179.1/161 (44 bytes in 1 packets)
29	2022-03-09 11:35:18	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/44581 to 192.168.179.1/161 (44 bytes in 1 packets)
30	2022-03-09 11:35:18	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56408 to 192.168.179.1/161 (44 bytes in 1 packets)
31	2022-03-09 11:35:18	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56407 to 192.168.179.1/161 (44 bytes in 1 packets)
32	2022-03-09 11:35:18	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56406 to 192.168.179.1/161 (44 bytes in 1 packets)
33	2022-03-09 11:34:30	POLICY	MANAGEMENT	10.100.4.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/57657 to 10.1.30.220/161 (44 bytes in 1 packets)
34	2022-03-09 11:34:30	POLICY	MANAGEMENT	10.100.4.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/57655 to 10.1.30.220/161 (44 bytes in 1 packets)
35	2022-03-09 11:34:30	POLICY	MANAGEMENT	10.100.4.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/57656 to 10.1.30.220/161 (44 bytes in 1 packets)
36	2022-03-09 11:33:31	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.16 is a BOGON IPv4 address.) from 10.1.30.81/56455 to 10.1.80.16/161 (142 bytes in 2 packets)
37	2022-03-09 11:33:30	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/62668 to 192.168.179.1/161 (44 bytes in 1 packets)
38	2022-03-09 11:33:30	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/44585 to 192.168.179.1/161 (44 bytes in 1 packets)
39	2022-03-09 11:33:30	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/44585 to 192.168.179.1/161 (44 bytes in 1 packets)
40	2022-03-09 11:33:30	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Dst IP: 10.1.80.16 is a BOGON IPv4 address.) from 10.1.30.81/56455 to 10.1.80.16/161 (142 bytes in 2 packets)
41	2022-03-09 11:31:59	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/39909 to 192.168.179.1/161 (44 bytes in 1 packets)
42	2022-03-09 11:31:59	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/39908 to 192.168.179.1/161 (44 bytes in 1 packets)
43	2022-03-09 11:31:59	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/39907 to 192.168.179.1/161 (44 bytes in 1 packets)
44	2022-03-09 11:31:59	POLICY	MANAGEMENT	10.100.1.1	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/39906 to 192.168.179.1/161 (44 bytes in 1 packets)
45	2022-03-09 11:28:57	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40921 to 10.1.30.220/161 (176 bytes in 4 packets)
46	2022-03-09 11:28:57	POLICY	MANAGEMENT	10.1.30.99	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40920 to 10.1.30.220/161 (176 bytes in 4 packets)
47	2022-03-09 11:28:56	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37789 to 192.168.179.1/161 (44 bytes in 1 packets)
48	2022-03-09 11:28:56	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37788 to 192.168.179.1/161 (44 bytes in 1 packets)
49	2022-03-09 11:28:56	POLICY	MANAGEMENT	10.100.0.20	SNMP: Unallowed SNMP Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37791 to 192.168.179.1/161 (44 bytes in 1 packets)

VPN POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

The benefits of a VPN include increases in functionality, security, and management of the private network. It provides access to resources inaccessible on the public network and is typically used for telecommuting workers.

Encryption is common, although not an inherent part of a VPN connection.

In Fl0wer you can define the IP addresses for VPN endpoints used in your network infrastructure. These files must be customized and are in:

- /opt/fl0wer/iplist/vpn4list.txt for IPv4 VPN endpoints
- /opt/fl0wer/iplist/vpn6list.txt for IPv6 VPN endpoints

All the VPN traffic known to Fl0wer (OpenVPN, IPSec, Wireguard, PPTP, SKIP, L2TP) that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

There are risks in allowing out of policy VPN traffic, from loss of control on your internal infrastructure to trying to mask unallowed traffic in a vpn protocol.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 02:10:57	POLICY	VPN	10.1.30.220	VPN: possibly VPN Traffic (TCP 1194 VPN OpenVPN Protocol) from 10.1.30.220/9618 to 10.1.30.220/1194
1	2022-03-07 19:32:39	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
2	2022-03-07 19:31:41	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
3	2022-03-07 19:31:41	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
4	2022-03-07 19:29:31	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
5	2022-03-07 19:29:31	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
6	2022-03-07 19:26:58	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
7	2022-03-07 19:26:58	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
8	2022-03-07 19:26:58	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
9	2022-03-07 19:17:56	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
10	2022-03-07 19:11:47	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
11	2022-03-07 19:11:47	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
12	2022-03-07 19:09:30	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
13	2022-03-07 19:08:58	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
14	2022-03-07 19:08:58	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
15	2022-03-07 18:55:48	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
16	2022-03-07 18:33:59	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
17	2022-03-07 18:30:59	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
18	2022-03-07 18:29:39	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
19	2022-03-07 18:29:39	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
20	2022-03-07 18:23:33	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
21	2022-03-07 18:21:32	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
22	2022-03-07 17:58:55	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
23	2022-03-07 17:55:37	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
24	2022-03-07 17:54:46	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
25	2022-03-07 17:54:46	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
26	2022-03-07 17:49:49	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
27	2022-03-07 17:49:49	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
28	2022-03-07 17:49:49	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
29	2022-03-07 17:49:49	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
30	2022-03-07 17:43:57	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
31	2022-03-07 17:42:59	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
32	2022-03-07 17:42:59	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
33	2022-03-07 17:35:47	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
34	2022-03-07 17:35:47	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
35	2022-03-07 17:06:51	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
36	2022-03-07 17:06:51	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
37	2022-03-07 17:03:26	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
38	2022-03-07 17:03:26	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
39	2022-03-07 16:58:59	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
40	2022-03-07 16:58:59	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
41	2022-03-07 16:52:46	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
42	2022-03-07 16:46:35	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
43	2022-03-07 16:41:23	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
44	2022-03-07 16:41:23	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
45	2022-03-07 16:38:41	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
46	2022-03-07 16:38:41	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
47	2022-03-07 16:31:50	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
48	2022-03-07 16:29:30	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500
49	2022-03-07 16:29:30	POLICY	VPN	10.100.4.20	VPN: possibly VPN Traffic (UDP 500 IPSec ISAKMP/IKE Protocol) from 10.100.7.20/500 to 10.100.5.165/500

TUNNEL POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

In computer networks, a tunneling protocol is a communications protocol that allows for the movement of data from one network to another.

Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, it can hide the nature of the traffic that is run through a tunnel.

A tunneling protocol may, for example, allow a foreign protocol to run over a network that does not support that particular protocol, such as running IPv6 over IPv4.

In Fl0wer you can define the IP addresses for Tunnel endpoints used in your network infrastructure. These files must be customized and are in:

- /opt/fl0wer/iplist/tun4list.txt for IPv4 Tunnel endpoints
- /opt/fl0wer/iplist/tun6list.txt for IPv6 Tunnel endpoints

All the Tunnel traffic known to Fl0wer (HTTP Proxy, TOR Network, Socks Proxy, VXLAN, L2TP, GRE, IP-inIP, EtherIP, ENCAP,) that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

There are risks in allowing out of policy Tunnel traffic, from loss of control on your internal infrastructure to trying to mask unallowed traffic in a tunnel protocol.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-07 23:17:47	POLICY	NETWORK TUNNEL	10.1.30.9	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33396 (1500 bytes in 1 packets)
1	2022-03-07 23:17:47	POLICY	NETWORK TUNNEL	10.1.30.9	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33670 to 10.1.10.30/3128 (52 bytes in 1 packets)
2	2022-03-07 23:17:47	POLICY	NETWORK TUNNEL	10.1.30.9	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33578 to 10.1.10.30/3128 (52 bytes in 1 packets)
3	2022-03-07 23:17:47	POLICY	NETWORK TUNNEL	10.1.30.9	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33576 (824 bytes in 1 packets)
4	2022-03-07 23:17:47	POLICY	NETWORK TUNNEL	10.1.30.9	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33430 to 10.1.10.30/3128 (52 bytes in 1 packets)
5	2022-03-07 19:37:05	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33874 to 10.1.10.30/3128 (1042 bytes in 16 packets)
6	2022-03-07 19:33:45	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33838 to 10.1.10.30/3128 (52 bytes in 1 packets)
7	2022-03-07 19:33:45	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33838 to 10.1.10.30/3128 (52 bytes in 1 packets)
8	2022-03-07 19:33:44	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33840 to 10.1.10.30/3128 (1134 bytes in 18 packets)
9	2022-03-07 19:33:44	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33840 (15804 bytes in 16 packets)
10	2022-03-07 19:32:39	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33824 to 10.1.10.30/3128 (52 bytes in 1 packets)
11	2022-03-07 19:32:39	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33824 to 10.1.10.30/3128 (52 bytes in 1 packets)
12	2022-03-07 19:31:42	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33814 to 10.1.10.30/3128 (1030 bytes in 16 packets)

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
13	2022-03-07 19:29:31	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33786 to 10.1.10.30/3128 (1082 bytes in 17 packets)
14	2022-03-07 19:29:31	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33786 (15706 bytes in 15 packets)
15	2022-03-07 19:29:31	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33786 to 10.1.10.30/3128 (1082 bytes in 17 packets)
16	2022-03-07 19:29:31	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33786 (15706 bytes in 15 packets)
17	2022-03-07 19:29:31	POLICY	NETWORK TUNNEL	10.100.0.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33786 to 10.1.10.30/3128 (1030 bytes in 16 packets)
18	2022-03-07 19:28:40	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33776 to 10.1.10.30/3128 (1134 bytes in 18 packets)
19	2022-03-07 19:28:40	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33776 (15701 bytes in 16 packets)
20	2022-03-07 19:28:40	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33776 to 10.1.10.30/3128 (1134 bytes in 18 packets)
21	2022-03-07 19:28:40	POLICY	NETWORK TUNNEL	10.100.4.20	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.1.10.30/3128 to 10.100.10.14/33776 (15701 bytes in 16 packets)
22	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
23	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
24	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
25	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
26	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
27	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
28	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
29	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
30	2022-03-07 19:28:39	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33764 to 10.1.10.30/3128 (52 bytes in 1 packets)
31	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
32	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
33	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
34	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
35	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
36	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
37	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
38	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
39	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
40	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
41	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
42	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
43	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
44	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
45	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
46	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
47	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (242 bytes in 1 packets)
48	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (52 bytes in 1 packets)
49	2022-03-07 19:27:41	POLICY	NETWORK TUNNEL	10.100.1.1	TUNNEL: possibly TUNNEL Traffic (TCP 3128 PROXY SQUID Protocol) from 10.100.10.14/33756 to 10.1.10.30/3128 (60 bytes in 1 packets)

SDN/CONTROLLER POLICY VIOLATIONS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

Software-defined networking (SDN) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management.

SDN is meant to address the fact that the static architecture of traditional networks is decentralized and complex while current networks require more flexibility and easy troubleshooting.

SDN attempts to centralize network intelligence in one network component by disassociating the forwarding process of network packets (data plane) from the routing process (control plane).

The control plane consists of one or more **controllers**, which are considered the brain of the SDN network where the whole intelligence is incorporated.

In Fl0wer you can define the IP addresses for SDN controllers used in your SDN infrastructure. These files must be customized and are in:

- /opt/fl0wer/iplist/sdncontroller4list.txt for IPv4 SDN controllers
- /opt/fl0wer/iplist/sdncontroller6list.txt for IPv6 SDN controllers

All the SDN traffic known to Fl0wer (Netconf and OpenFlow) that is not going to this servers could be a security and management risk.

Risks and Indicator of Compromise (IOC)

There are risks in allowing out of policy SDN Controller traffic, from loss of control on your internal SDN to trying to mask unallowed traffic in an SDN Controller protocol.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems violating the policies.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:58:39	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48095 to 10.1.30.220/6646
1	2022-03-09 11:58:39	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48094 to 10.1.30.220/6646
2	2022-03-09 11:58:39	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/48093 to 10.1.30.220/6646
3	2022-03-09 11:56:59	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/55742 to 192.168.179.1/6646
4	2022-03-09 11:55:27	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/35768 to 10.1.30.220/6646
5	2022-03-09 11:54:06	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/41863 to 192.168.179.1/6646
6	2022-03-09 11:54:06	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/41862 to 192.168.179.1/6646
7	2022-03-09 11:52:45	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37648 to 10.1.30.220/6646
8	2022-03-09 11:52:45	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37647 to 10.1.30.220/6646
9	2022-03-09 11:52:45	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37646 to 10.1.30.220/6646
10	2022-03-09 11:52:44	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37648 to 10.1.30.220/6646

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
11	2022-03-09 11:51:32	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37647 to 10.1.30.220/6646
12	2022-03-09 11:51:32	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37646 to 10.1.30.220/6646
13	2022-03-09 11:51:32	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/37648 to 10.1.30.220/6646
14	2022-03-09 11:50:05	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/44051 to 10.1.30.220/6646
15	2022-03-09 11:50:05	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/44050 to 10.1.30.220/6646
16	2022-03-09 11:50:05	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/44052 to 10.1.30.220/6646
17	2022-03-09 11:47:55	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/45835 to 10.1.30.220/6646
18	2022-03-09 11:47:55	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/45834 to 10.1.30.220/6646
19	2022-03-09 11:47:55	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/45833 to 10.1.30.220/6646
20	2022-03-09 11:45:37	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52010 to 10.1.30.220/6646
21	2022-03-09 11:45:37	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52009 to 10.1.30.220/6646
22	2022-03-09 11:42:16	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52293 to 10.1.30.220/6646
23	2022-03-09 11:41:04	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/53772 to 10.1.30.220/6646
24	2022-03-09 11:38:13	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38638 to 10.1.30.220/6646
25	2022-03-09 11:38:13	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38637 to 10.1.30.220/6646
26	2022-03-09 11:38:13	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38638 to 10.1.30.220/6646
27	2022-03-09 11:38:13	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38636 to 10.1.30.220/6646
28	2022-03-09 11:38:13	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38637 to 10.1.30.220/6646
29	2022-03-09 11:38:13	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/38636 to 10.1.30.220/6646
30	2022-03-09 11:35:18	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56405 to 192.168.179.1/6646
31	2022-03-09 11:35:18	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56405 to 192.168.179.1/6646
32	2022-03-09 11:32:00	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/62665 to 192.168.179.1/6646
33	2022-03-09 11:32:00	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/62665 to 192.168.179.1/6646
34	2022-03-09 11:31:59	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/62665 to 192.168.179.1/6646
35	2022-03-09 11:30:28	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/39906 to 192.168.179.1/6646
36	2022-03-09 11:28:56	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40922 to 10.1.30.220/6646
37	2022-03-09 11:28:56	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40921 to 10.1.30.220/6646
38	2022-03-09 11:28:56	POLICY	VPN	10.1.30.99	SDN: 10.1.30.99 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40920 to 10.1.30.220/6646
39	2022-03-09 11:27:02	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40922 to 10.1.30.220/6646
40	2022-03-09 11:27:02	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40921 to 10.1.30.220/6646
41	2022-03-09 11:27:02	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/40920 to 10.1.30.220/6646
42	2022-03-09 11:22:34	POLICY	VPN	10.100.4.20	SDN: 10.100.4.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/41934 to 10.1.30.220/6646
43	2022-03-09 11:17:25	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/35750 to 10.1.30.220/6646
44	2022-03-09 11:14:22	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52172 to 192.168.179.1/6646
45	2022-03-09 11:14:22	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52171 to 192.168.179.1/6646
46	2022-03-09 11:14:22	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/52170 to 192.168.179.1/6646
47	2022-03-09 11:10:24	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/61781 to 192.168.179.1/6646
48	2022-03-09 11:10:24	POLICY	VPN	10.100.0.20	SDN: 10.100.0.20 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/61781 to 192.168.179.1/6646
49	2022-03-09 11:09:20	POLICY	VPN	10.100.1.1	SDN: 10.100.1.1 detected out of policy SDN Controller Traffic (BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.) from 10.101.16.100/56496 to 192.168.179.1/6646

SDN/VTEP POLICY VIOLATIONS

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

SDN/VTEP traffic is commonly used if you have in-house SDN or on-premises Cloud solutions (eg. Apache Openstack, etc.). VTEP (VXLAN Tunnel End Point) are network entities encapsulating network traffic into VXLAN (Virtual Extensible LAN) Tunnels for easy transportation and IP Layering over different addresses.

This can allow a company to keep its physical IP addressing different from virtual IP addressing used in different VPCs (Virtual Private Clouds) and allows IP address overlapping for different layers.

Risks and Indicator of Compromise (IOC)

Normally, VTEPs are well identified in a Cloud solution, so if something is reported here, it is probably trying to act or impersonate a VTEP trying to make its way into the Software Defined Network.

It's good to remember that a VXLAN is normally not encrypted nor compressed, so it is also subject to sniffing.

Suggested actions

The suggested action is to immediately check the reported flows against well known VTEPs in your infrastructure.

***** NO DATA AVAILABLE FOR THE SELECTED TIMELAPSE**

BOGON NETWORKS (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

A bogon is an illegitimate IP address that falls into a set of IP addresses that have not been officially assigned to an entity by an internet registration institute, such as the Internet Assigned Number Authority (IANA). Bogons arise as a result of a misconfiguration or intentional misuse that fools recipients about its source IP address. The term bogon is used as slang and is derived from the word bogus.

How does a bogon work?

IP addresses are used by the internet infrastructure to uniquely identify an entity, such as a website or server. IANA, or other regional internet registries, allocates each instance over a network and IP address. Once assigned, these addresses are then used to perform communication between two endpoints.

The range of registered IP addresses is known as the reserved space. A bogon occurs when its IP address does not fall into this registered range, or is part of the address space known as the bogon space.

Some IP addresses may only be considered a bogon temporarily, as the IANA registry is constantly updating and assigning new address spaces. Private IP addresses can fall under the bogon description as they cannot be found on the public internet.

Risks associated with bogons

Bogons are not normally visible over a network but are still a prime target for exploitation. For example, they are commonly used by hackers or spammers when initiating a distributed denial-of-service (DDoS) attack. This is because bogon packets cannot be traced back to an actual host or source.

Additionally, bogons can be used to launch Transmission Control Protocol (TCP) SYN scanning attacks and to secretly transfer malicious information. While bogons should never appear in the routing table, routers will not detect bogons as they only examine the destination IP address rather than the source IP address.

Prevention of bogons

Many internet service providers (ISP), firewalls and intrusion prevention systems block bogons. This can be accomplished through bogon filtering, or the practice of assigning access control lists (ACL) or Border Gateway Protocol (BGP) blacklists to a device. A list of bogons can be obtained from a variety of sources including HTTP, BGP peering, routing registries and the DNS.

If a bogon becomes legitimate, it can usually be found on the network operator mailing lists so that the address can be removed from filters.

Available data

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
0	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
1	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
2	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
3	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
4	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
5	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
6	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
7	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
8	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
9	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
10	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
11	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
12	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
13	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
14	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
15	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
16	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
17	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
18	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
19	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
20	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
21	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
22	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
23	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
24	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
25	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
26	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
27	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
28	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
29	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
30	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
31	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
32	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
33	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
34	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
35	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
36	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
37	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
38	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
39	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
40	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
41	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.22.100 is a BOGON IPv4 address.
42	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
43	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
44	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
45	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
46	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
47	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.

	TIMESTAMP	LEVEL	CATEGORY	SOURCE	MESSAGE
48	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.
49	2022-03-09 11:59:49	ALERT	UNWANTED	10.100.1.1	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.

BAD IP ADDRESS/NETWORKS

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

What does this mean ?

Blacklisted traffic is traffic to or from an IP Address that is present in the Fl0wer blacklist files. These files are built by collecting available data from OSINT Projects like Thalos Project, Malc0de, Ransomware IP Blocklist, etc.

The files containing the blacklisted IP definitions are in:

- /opt/fl0wer/iplist/reputation4.txt for IPv4 addresses provided by default in Fl0wer distribution
- /opt/fl0wer/iplist/reputation6.txt for IPv6 addresses provided by default in Fl0wer distribution
- /opt/fl0wer/iplist/blacklist4.txt for IPv4 addresses provided by customer
- /opt/fl0wer/iplist/blacklist6.txt for IPv6 addresses provided by customer

It should be taken under high consideration since traffic with one of these IP Address could be an Indicator of Compromise.

Risks and Indicator of Compromise (IOC)

Making traffic with a blacklisted address is highly risky, since it could be both a sign of compromise or (if your systems are already compromised) could reveal a data exfiltration in progress.

Suggested actions

The suggested action is to not ignore and underestimate this IOC and immediately check your internal systems dealing with the blacklisted IP.

Your firewall solution should already be dealing with this kind of problems, but if you see systems reported here, a double check is due.

***** NO DATA AVAILABLE FOR THE SELECTED TIMELAPSE**

Possible CryptoCurrencies Connections

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

Cryptocurrencies are a new reality you simply can't ignore. Often, company networks, which are rich of resources like cpu, network and storage, are the ideal place to hide cryptocurrencies transactions and mining.

Risks and Indicator of Compromise (IOC)

The related risks of doing cryptocurrencies transactions are the most heterogeneous. It is quite possible that the company network is already compromised if the core-business of the company is not related to cryptocurrencies usage.

Suggested actions

The suggested action is to review carefully the evidence of traffic, review your company policies for I/T asset usage and enforce users to avoid this kind of traffic unless strictly necessary to your business.

***** NO DATA AVAILABLE FOR THE SELECTED TIMELAPSE**

High Risk Index to/from INTERNET (TOP 50)

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

What does this mean ?

High risk traffic is .....

Risks and Indicator of Compromise (IOC)

The related risks are ....

Suggested actions

The suggested action is ....

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
0	2022-03-09 11:59:58	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/58664	220.244.111.183/9050		
1	2022-03-09 11:59:57	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (3756 flows)	UNWANTED	10.101.16.100/50661	192.168.179.1/161		
2	2022-03-09 11:59:57	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (3756 flows)	UNWANTED	10.101.16.100/50660	192.168.179.1/161		
3	2022-03-09 11:59:52	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (3756 flows)	UNWANTED	10.101.16.100/50659	192.168.179.1/161		
4	2022-03-09 11:59:52	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (3756 flows)	UNWANTED	10.101.16.100/50658	192.168.179.1/161		
5	2022-03-09 11:59:52	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (3756 flows)	UNWANTED	10.101.16.100/50657	192.168.179.1/161		
6	2022-03-09 11:59:52	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (3756 flows)	UNWANTED	10.101.16.100/50656	192.168.179.1/161		
7	2022-03-09 11:59:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/41857	220.233.73.236/9050		
8	2022-03-09 11:59:49	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/41856	220.233.73.236/9050		
9	2022-03-09 11:59:47	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/55056	220.233.73.236/9050		
10	2022-03-09 11:59:46	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/55055	220.233.73.236/9050		
11	2022-03-09 11:59:43	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/44745	220.233.178.199/9050		
12	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/44745	220.233.178.199/9050		
13	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/44744	220.233.178.199/9050		

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
14	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/44744	220.233.178.199/9050		
15	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52478	192.168.179.1/9001		
16	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52476	192.168.179.1/9001		
17	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52477	192.168.179.1/9001		
18	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52474	192.168.179.1/9001		
19	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52475	192.168.179.1/9001		
20	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52478	192.168.179.1/9001		
21	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52476	192.168.179.1/9001		
22	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52477	192.168.179.1/9001		
23	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52474	192.168.179.1/9001		
24	2022-03-09 11:59:40	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52475	192.168.179.1/9001		
25	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50871	220.135.161.136/9050		
26	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50871	220.135.161.136/9050		
27	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50870	220.135.161.136/9050		
28	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52478	192.168.179.1/9050		
29	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52476	192.168.179.1/9050		
30	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52477	192.168.179.1/9050		
31	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52474	192.168.179.1/9050		
32	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52475	192.168.179.1/9050		
33	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52478	192.168.179.1/9050		
34	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52476	192.168.179.1/9050		
35	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52477	192.168.179.1/9050		
36	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52474	192.168.179.1/9050		
37	2022-03-09 11:59:34	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	VERTICAL_SCAN: IP: 10.101.16.100 is probably making a TCP SYN scan to host: 192.168.179.1 (6800 flows)	UNWANTED	10.101.16.100/52475	192.168.179.1/9050		
38	2022-03-09 11:59:31	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/41111	220.233.178.199/9050		
39	2022-03-09 11:59:31	IPv4	10.100.1.1	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/41110	220.233.178.199/9050		
40	2022-03-09 11:59:31	IPv4	10.100.0.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50870	220.135.161.136/9050		

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
41	2022-03-09 11:59:28	IPv4	10.100.4.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/64605	219.91.20.79/9050		
42	2022-03-09 11:59:28	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42784	220.233.178.199/9050		
43	2022-03-09 11:59:28	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/42783	220.233.178.199/9050		
44	2022-03-09 11:59:28	IPv4	10.1.30.99	tcp	176 bytes	4	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/64605	219.91.20.79/9050		
45	2022-03-09 11:59:27	IPv4	10.100.4.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/64606	219.91.20.79/9050		
46	2022-03-09 11:59:27	IPv4	10.100.4.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/64605	219.91.20.79/9050		
47	2022-03-09 11:59:22	IPv4	10.100.4.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50661	192.168.179.1/161		
48	2022-03-09 11:59:22	IPv4	10.100.4.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50660	192.168.179.1/161		
49	2022-03-09 11:59:22	IPv4	10.100.4.20	tcp	44 bytes	1	FLOW_INTERNET_TO_INTERNET	BOGON: Warning: Src IP: 10.101.16.100 is a BOGON IPv4 address.	UNWANTED	10.101.16.100/50659	192.168.179.1/161		

Possible Social Network Connections

Timelapse for report: FROM: 04/03/2022 12:00:04 TO: 09/03/2022 12:00:04

Description

Social networks are a new reality you simply can't ignore. Often, company networks have appropriate policies regarding their usage.

Risks and Indicator of Compromise (IOC)

The related risks of allowing Social Networks are the most heterogeneous. It is quite possible that the company network is already compromised if the connections start from the company data center networks.

Suggested actions

The suggested action is to review carefully the evidence of traffic, review your company policies for I/T asset usage and enforce users to avoid this kind of traffic unless strictly necessary to your business.

	Timestamp	Type	Exporter	Protocol	Bytes	Packets	Direction	NPAR	CATEGORY	Source	Destination	srcPrefix	dstPrefix
0	2022-03-08 12:28:20	IPv6	10.1.30.101	tcp	72 bytes	1	FLOW_INTERNAL_TO_INTERNET	Instagram Social Network	SOCIAL	2001:470:8b5b:0:10:1:30:39/54850	2a03:2880:f06f:10:face:b00c:0:2/443	2001:470:8b5b::/48	
1	2022-03-08 12:28:18	IPv6	10.1.30.101	tcp	72 bytes	1	FLOW_INTERNAL_TO_INTERNET	Instagram Social Network	SOCIAL	2001:470:8b5b:0:10:1:30:39/63786	2a03:2880:f06f:11:face:b00c:0:2825/443	2001:470:8b5b::/48	
2	2022-03-08 12:28:18	IPv6	10.1.30.101	tcp	72 bytes	1	FLOW_INTERNAL_TO_INTERNET	Instagram Social Network	SOCIAL	2001:470:8b5b:0:10:1:30:39/54842	2a03:2880:f06f:10:face:b00c:0:2/443	2001:470:8b5b::/48	