NOTA TECNICA

IIT B4-06/2021

STRATEGIE PER LA PROTEZIONE PERIMETRALE DEI DISPOSITIVI DI STAMPA CONNESSI AD UNA CAMPUS AREA NETWORK

F. Lauria

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

Strategie per la protezione perimetrale dei dispositivi di stampa connessi ad una campus area network

Filippo Maria Lauria
filippo.lauria@iit.cnr.it

Computer and Communication Networks
Istituto di Informatica e Telematica - Consiglio Nazionale delle Ricerche
via G. Moruzzi, 1 - 56124 Pisa, Italy

Abstract
Per la protezione perimetrale dei dispositivi di stampa connessi ad una campus area network (CAN) possono essere utilizzate diverse strategie. Una di queste è il blacklisting, ovvero una politica di firewalling che prevede l'applicazione di filtraggi basati su una blacklist. In questo contesto, la blacklist contiene gli indirizzi delle stampanti interne da proteggere affinché sia impedito loro di ricevere eventuali contatti dall'esterno, ovvero da Internet. Le attività legate alla gestione della blacklist delle stampanti sono afflitte però da criticità specifiche per il contesto presentato. Questo documento analizza la relazione tra l'effettiva distribuzione delle stampanti in rete e la blacklist, proponendo alcuni rimedi per risolvere, o almeno mitigare, tali criticità.

Keywords: CAN, *firewall, NGFW, stampanti, blacklist, whitelist*

1. Introduzione
Il presente documento è stato redatto con lo scopo di analizzare una particolare politica di firewalling per la protezione in rete dei dispositivi di stampa. La rete, a cui il documento fa riferimento, è una rete di tipo *campus area network* (*CAN),* ovvero adibita all'interconnessione tra gli edifici facenti parte dello stesso *campus* (ad es. un campus universitario).

Tutti i concetti esposti all'interno del presente documento sono generici e riferibili idealmente all'intera classe delle reti CAN ma, al fine di dare al documento un taglio teorico-pratico, si farà riferimento alla **CAN di riferimento** descritta nel sottoparagrafo successivo.

1.1 Il contesto
Il contesto a cui il presente documento fa riferimento è una CAN costituita da 8 sottoreti. Ciascuna sottorete appartiene ad una diversa *organizzazione*[1] e ovviamente, tutte le organizzazioni sono ubicate all'interno dello stesso campus.

In questo contesto è installata *on premise* una soluzione di sicurezza di rete, adibita alla protezione perimetrale delle diverse sottoreti costituenti la CAN di riferimento, basata su apparati NGFW posti fisicamente *a confine* tra la CAN stessa e Internet, distinguendo, come esemplificato in Figura 1, due zone di sicurezza[2]: la *zona esterna* (che rappresenta l'intera Internet), e la *zona interna* (che rappresenta la CAN di riferimento). Chiaramente, le sessioni originate[3] dalla zona interna verso la zona esterna (direzione interno ⇨ esterno) e viceversa (direzione esterno ⇨ interno) transitano attraverso il firewall. In tal senso, si noti che il traffico interno ⇨ esterno non è soggetto a particolari restrizioni. Invece, il traffico esterno ⇨ interno è soggetto ad una politica di firewalling, applicata mediante gli apparati NGFW, basata sul *blacklisting*[4].

---

[1] o anche più genericamente dipartimento, reparto, istituto, ecc.
[2] nell'ambito del firewalling, una zona di sicurezza è una porzione logica di rete i cui nodi, agli occhi del firewall, si trovano tutti allo stesso livello di fiducia
[3] in fase di inizializzazione di una sessione, il firewall decide, sulla base delle security policies, se la sessione può essere instaurata o non instaurata. Dal momento in cui la sessione viene instaurata, il traffico di ritorno è consentito, ferma restando l'eventuale applicazione di filtri anti-virus, anti-spyware, ecc.
[4] il blacklisting è definito nel paragrafo *"Politiche di firewalling in breve: blacklisting vs. whitelisting"*

Infine, si tenga presente che, in questo contesto, l'utenza della CAN è costituita principalmente dal personale afferente alle organizzazioni ospitate all'interno del campus. Per quanto riguarda l'amministrazione della CAN, invece, sono individuabili *almeno* le seguenti figure professionali gestionali:

- i referenti di rete di ciascuna sottorete;
- i gestori dell'indirizzamento (assegnazione indirizzi[5], registrazione nomi a dominio, ecc.) di ciascuna sottorete[6];
- i gestori del firewall nonché i gestori degli apparati e dei cablaggi di rete costituenti l'infrastruttura di rete.

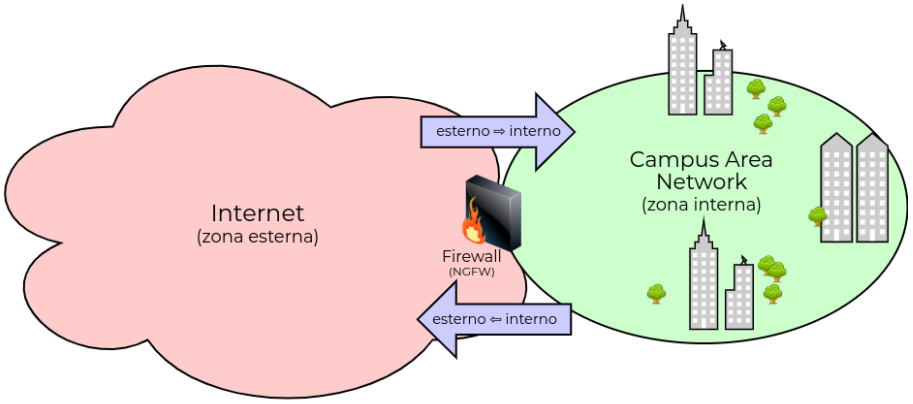


Figura 1: suddivisione logica in zone di sicurezza che esemplifica, dal punto di vista del firewall, la relazione tra Internet e la CAN di riferimento

1.2 Politiche di firewalling in breve: blacklisting vs. whitelisting

1.2.1 Premesse. In questo contesto, dal punto di vista del firewall possono essere impiegate diverse **entità di rete** (come, ad esempio, nomi utente, indirizzi IPv4, indirizzi IPv6, porte TCP, porte UDP, applicazioni, ecc.) per la definizione di regole di sicurezza. Inoltre, con T si intende il traffico di rete in transito attraverso il firewall. Gli apparati di tipo NGFW sono in grado di classificare questo traffico sulla base di diversi parametri tra cui le entità di rete definite precedentemente. Tenendo conto di questo, ad esempio, il traffico di rete classificato dal firewall come traffico di rete generato dall'applicazione app_i è indicato con T_{app_i}, ecc. Infine, si suppone che il firewall può compiere semplicemente due azioni sul traffico di rete:

- $allow(T, D)$: permette il transito del traffico di rete T nella direzione D;
- $deny(T, D)$: non permette il transito del traffico di rete nella direzione D.

1.2.2 Blacklisting. Il *blacklisting* è una politica di firewalling che, mediante il firewall perimetrale, prevede l'applicazione di *filtraggi basati su una blacklist,* dove il termine blacklist indica un insieme di *entità di rete non fidate*.

Esempio 1.2.2.1 - blacklisting per il filtraggio di applicazioni indesiderate. Data la blacklist $A_{BL} = \{app_1, ..., app_n\}$, contenente n *applicazioni* indesiderate, una politica di blacklisting per il loro filtraggio potrebbe essere così definita:

IF: $app_i \in A_{BL} \Rightarrow deny(T_{app_i}, esterno \rightarrow interno)$

ELSE: $allow(T_{app_i}, esterno \rightarrow interno)$.

In altre parole, tale politica impedirebbe il transito in direzione esterno ⇨ interno del traffico relativo alle applicazioni contenute nella blacklist A_{BL}, consentendo allo stesso tempo il transito del traffico relativo a tutte le altre applicazioni.

---

[5] si tenga presente che in questo contesto l'indirizzamento è di tipo pubblico: tutti gli indirizzi IP usati nelle sottoreti sono indirizzi pubblici

[6] si noti che per alcuni istituti i referenti di rete ed i gestori dell'indirizzamento coincidono

Esempio 1.2.2.2 - blacklisting per impedire contatti dall'esterno a nodi interni. Data la blacklist $N_{BL} = \{addr_1, ..., addr_n\}$, contenente gli indirizzi di n *nodi di rete* interni, una politica di blacklisting per la loro "protezione dall'esterno" potrebbe essere così definita:

IF: $addr_i \in N_{BL} \Rightarrow deny(T_{addr_i}, esterno \rightarrow interno)$
ELSE: $allow(T_{addr_i}, esterno \rightarrow interno)$.

In altre parole, attraverso tale politica, il firewall consentirebbe il transito in direzione esterno ⇨ interno al traffico destinato a tutti i nodi, ad eccezione di quello destinato ai nodi i cui indirizzi sono contenuti nella blacklist N_{BL}.

1.2.3 Whitelisting. Il *whitelisting* è una politica di firewalling contrapposta al blacklisting che, mediante il firewall perimetrale, prevede l'applicazione di *filtraggi basati su una whitelist,* ovvero un elenco di *entità di rete fidate*.

Esempio 1.2.3.1 - whitelisting per consentire soltanto le applicazioni ammesse. - Data la whitelist $A_{WL} = \{app_1, ..., app_n\}$, contenente le n *applicazioni ammesse*, una politica di whitelisting potrebbe essere così definita:

IF: $app_i \in A_{WL} \Rightarrow allow(T_{app_i}, esterno \rightarrow interno)$
ELSE: $deny(T_{app_i}, esterno \rightarrow interno)$.

In altre parole, tale politica consentirebbe il transito in direzione esterno ⇨ interno del traffico relativo alle applicazioni contenute nella whitelist A_{WL}, impedendo allo stesso tempo il transito del traffico relativo a tutte le altre applicazioni.

Esempio 1.2.3.2 - whitelisting per consentire contatti dall'esterno soltanto ad alcuni nodi interni.
Data la whitelist $N_{WL} = \{addr_1, ..., addr_n\}$ contenente gli indirizzi di n nodi di rete interni (ad esempio alcuni servers) a cui dev'essere consentito di ricevere connessioni *"iniziate"* dall'esterno, una politica di whitelisting potrebbe essere così definita:

IF: $addr_i \in N_{WL} \Rightarrow allow(T_{addr_i}, esterno \rightarrow interno)$
ELSE: $deny(T_{addr_i}, esterno \rightarrow interno)$.

In altre parole, attraverso tale politica, il firewall non consentirebbe il transito in direzione esterno ⇨ interno al traffico destinato a tutti i nodi, ad eccezione di quello destinato ai nodi i cui indirizzi sono contenuti nella whitelist N_{WL}.

1.2.4 Altre considerazioni. In generale, il blacklisting prevede l'identificazione delle entità da negare e la permissione di tutte le altre, mentre il whitelisting prevede l'identificazione delle entità da permettere e la negazione di tutte le altre.

Entrambi gli approcci sono validi e presentano aspetti sia positivi che negativi. Per sua natura, il blacklisting consente agli utenti di avere una maggiore libertà di rete rispetto al whitelisting che costituisce una politica di firewalling più stringente. Si noti però che l'attività di aggiornamento della blacklist (ingresso/uscita delle entità di rete) dev'essere intensa e tempestiva, al fine di mantenere la blacklist il più possibile coerente con la realtà e quindi la relativa politica di blacklisting efficace. Di conseguenza, per via dell'elevata frequenza di aggiornamento richiesta, la gestione di una blacklist può risultare più complicata rispetto a quella di una whitelist.

2. Politica di protezione delle stampanti

Come già menzionato precedentemente, nello scenario descritto gli indirizzi IP assegnati ai nodi di rete interni alla CAN sono tutti pubblici. Per questo motivo, è necessaria l'applicazione di una strategia di protezione perimetrale dei dispositivi interni.

Inoltre, laddove possibile, ciascun dispositivo deve avere anche strumenti di protezione locale (endpoint protection) come ad esempio firewall personali, antivirus, antispyware, ecc. Questo vale, ovviamente, anche per le stampanti che, come tutti gli altri dispositivi interni, nel caso di un'assente o inadeguata protezione, risulterebbero raggiungibili ed utilizzabili dall'esterno da chiunque.[7]

In generale, una strategia di protezione basata sul blacklisting offre la possibilità di applicare *in parallelo* politiche di blacklisting distinte. Ad esse possono essere "*associate*" blacklists che coinvolgono entità eterogenee tra loro, come ad es. indirizzi di nodi esterni conosciuti come nodi malevoli, nomi di applicazioni considerate obsolete o intrinsecamente insicure, indirizzi di nodi interni che non devono essere raggiungibili dall'esterno, ecc.

In particolare, per la protezione dall'esterno delle stampanti di rete installate all'interno della CAN di riferimento, sono applicate *in parallelo* le politiche:

2.1. **IF:** $proto_i \in P_{BL} \Rightarrow deny(T_{proto_i},\ esterno \rightarrow interno)$
ELSE: $allow(T_{proto_i},\ esterno \rightarrow interno)$

dove $P_{BL} = \{proto_1, \ldots, proto_n\}$ è una blacklist contenente gli n *protocolli di stampa più diffusi;*

2.2. **IF:** $addr_i \in S_{BL} \Rightarrow deny(T_{addr_i},\ esterno \rightarrow interno)$
ELSE: $allow(T_{addr_i},\ esterno \rightarrow interno)$

dove $S_{BL} = \{addr_1, \ldots, addr_n\}$ è una blacklist contenente gli n *indirizzi delle stampanti di rete* installate nelle sottoreti costituenti la CAN.

La politica di blacklisting 2.1 impedisce gli eventuali tentativi di stampa (mediante i protocolli contenuti in P_{BL}) dall'esterno verso *tutti* i dispositivi collegati alla CAN di riferimento. Contemporaneamente, la politica 2.2 impedisce *completamente*[8] l'accesso dall'esterno alle stampanti interne *"censite"*, ovvero contenute in S_{BL}.

La scelta di applicare due politiche, ovvero due blacklist distinte, in parallelo garantisce una maggiore sicurezza perimetrale dei dispositivi. Se fosse applicata solamente la politica di blacklisting basata su S_{BL}, nel momento in cui questa blacklist si venisse a trovare in uno stato inconsistente, alcune stampanti risulterebbero accessibili da Internet, non solo per quanto riguarda l'accesso alle interfacce web di gestione dei dispositivi stessi, ma anche per quanto riguarda la stampa dei documenti. Con l'applicazione in parallelo anche della politica basata su P_{BL}, quest'ultima eventuale problematica viene mitigata.

---

[7] ad esempio, un attaccante esterno potrebbe utilizzare una stampante interna non protetta al fine di stampare volantini contenenti spam, slogan, ecc.

[8] oltre a fornire le funzionalità di stampa *"classiche"*, una stampante può esporre altri servizi, come ad es. un'interfaccia di management web oppure servizi per il monitoraggio del dispositivo stesso basati sul protocollo SNMP, ecc.

3. Gestione della blacklist degli indirizzi delle stampanti $\left(S_{BL}\right)$

La protezione di rete perimetrale dei dispositivi di stampa si basa sulla politica descritta nel paragrafo *"Politica di protezione delle stampanti"*. Politiche di protezione di questo tipo offrono, ai referenti di rete di ciascuna delle sottoreti costituenti la CAN di riferimento, la piena libertà di configurazione delle stampanti ma, allo stesso tempo, richiedono una complicata *attività di aggiornamento*[9] della blacklist S_{BL} da parte dei gestori del firewall. Il presente paragrafo, insieme al paragrafo *"Relazione tra distribuzione delle stampanti e blacklists* $\left(S_{BL}^{(subnet_i)}\right)$*"*, ha lo scopo di mettere in evidenza questo aspetto. Per questo motivo, d'ora in avanti il documento si concentrerà esclusivamente sulla blacklist S_{BL}, tralasciando la blacklist P_{BL}.

In Figura 2 è mostrato il procedimento che, ad oggi, dovrebbe essere utilizzato per la corretta installazione di una nuova stampante in una delle sottoreti costituenti la CAN di riferimento. Dal punto di vista dell'implementazione della politica di blacklisting, tale procedimento produce l'ingresso di un nuovo indirizzo nella blacklist S_{BL}. Inoltre, sebbene sia suddiviso in passi successivi molto semplici da mettere in atto, il procedimento richiede, da parte delle figure gestionali coinvolte, un alto grado di coordinamento. Se tale coordinamento dovesse essere scarso o assente, potrebbe verificarsi la non esecuzione o l'esecuzione parziale di uno o più passi che causerebbe un'errata esecuzione del procedimento.

Figura 2: procedimento per la corretta installazione di una nuova stampante, ovvero l'aggiunta di un nuovo indirizzo alla blacklist S_{BL}

Ad esempio, si noti che l'aggiornamento della blacklist S_{BL} deve avvenire prima dell'installazione e l'uso della stampante. A volte però può capitare che i passi 3 e 4 vengano fusi in unico passo che comincia da *installazione ed uso* della stampante e termina con la comunicazione dell'indirizzo per l'effettivo *aggiornamento della blacklist* S_{BL}. In questo modo, nel lasso di tempo che precede la comunicazione dell'indirizzo, la S_{BL} viene a trovarsi in uno stato inconsistente. Altre volte questa comunicazione non avviene e S_{BL} resta in uno stato inconsistente per un tempo indefinito.

Inoltre, si noti che, oltre al processo descritto in Figura 2 che comporta *l'ingresso di un indirizzo nella blacklist* S_{BL}, occorre tener conto anche del processo duale di *uscita di un indirizzo dalla blacklist* S_{BL}, qui non discusso al fine di non appesantire troppo la trattazione.

[9] ovvero l'ingresso/uscita degli indirizzi delle stampanti nella/dalla blacklist

Infine, si osservi che, in realtà, ciascuna sottorete costituente la CAN di riferimento è dotata di una sua relativa blacklist delle stampanti $\left(S_{BL}^{(subnet_i)}\right)$ e che la blacklist S_{BL}, menzionata e descritta finora come un insieme *monolitico* di indirizzi, è costituita dalla loro unione:
$S_{BL} = \bigcup_{i=1}^{k} S_{BL}^{(subnet_i)} \Rightarrow S_{BL}^{(subnet_i)} \subset S_{BL}$, dove $S_{BL}^{(subnet_i)}$ rappresenta la blacklist delle stampanti relativa alla sottorete i-esima e k il numero totale di sottoreti costituenti la CAN.

4. Relazione tra distribuzione delle stampanti e blacklists $\left(S_{BL}^{(subnet_i)}\right)$

Il presente paragrafo ha l'obiettivo di fornire un'analisi della relazione che intercorre tra ciascun insieme degli indirizzi delle stampanti *detected* $S_{DE}^{(subnet_i)}$, ovvero l'insieme costituito dagli indirizzi delle stampanti rilevate attraverso scansioni *ad hoc* della sottorete i-esima, e il relativo insieme degli indirizzi delle stampanti *blacklisted* $S_{BL}^{(subnet_i)}$, ovvero la blacklist delle stampanti relativa alla sottorete i-esima.

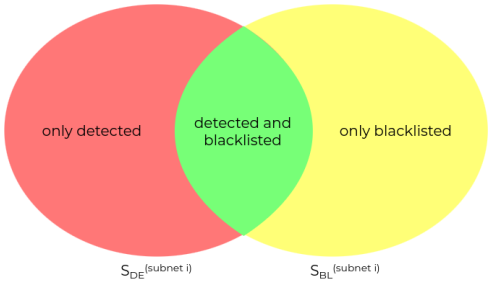


Figura 3: relazione tra l'effettiva distribuzione delle stampanti e la blacklist

Il diagramma di Venn, rappresentato in Figura 3, descrive graficamente la relazione tra questi due insiemi e mette in risalto la distinzione tra tre classi di indirizzi:

- il colore rosso indica indirizzi *solo detected, ma non blacklisted*. In altre parole si tratta di stampanti *sconosciute* agli occhi del firewall, ma rilevate mediante le scansioni;
- il colore giallo indica indirizzi *solo blacklisted, ma non detected*. In altre parole si tratta di stampanti non rilevate mediante le scansioni, ma presenti all'interno della blacklist. Questo può essere dovuto a cause diverse: come ad esempio la presenza di stampanti non attive al momento delle scansioni oppure un'inconsistenza nella blacklist stessa, ecc.;
- il colore verde indica indirizzi *sia detected che blacklisted*.

Si tenga presente che, affinché la politica di protezione sia considerata efficace, in una gestione ideale S_{DE} e S_{BL} sono insiemi coincidenti $\left(S_{DE}^{(subnet_i)} = S_{BL}^{(subnet_i)}\right)$ mentre, in una situazione reale, può essere sufficiente che $S_{DE}^{(subnet_i)} \subseteq S_{BL}^{(subnet_i)}$.

Al fine di approfondire questo aspetto per quanto riguarda la CAN di riferimento, a ciascuna organizzazione afferente al campus d'esempio è stato dedicato un sottoparagrafo che mostra più nel dettaglio, servendosi di alcuni **schemi di distribuzione**, la relazione tra gli elementi di $S_{DE}^{(subnet_i)}$ e quelli di $S_{BL}^{(subnet_i)}$.

Si noti che negli schemi di distribuzione i colori usati sono gli stessi ed hanno lo stesso significato di quelli descritti precedentemente e mostrati in Figura 3. Inoltre, per ciascuno schema di distribuzione valgono le seguenti considerazioni:

- per non appesantire troppo la rappresentazione grafica, le varie sottoreti $subnet_i$ costituenti la CAN sono state suddivise in *porzioni* $slice_{i,j}$ contenenti 256 indirizzi ciascuna;
- reti o porzioni di rete per cui le scansioni non hanno individuato alcuna stampante sono state omesse.

4.1 Organizzazione 1 - $subnet_1/21$

$subnet_1/21$ - $slice_{1,2}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

$subnet_1/21$ - $slice_{1,4}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

$subnet_1/21$ - $slice_{1,5}$

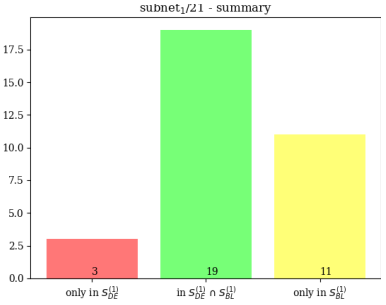
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

$subnet_1/21$ - $slice_{1,6}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

$subnet_1/21$ - $slice_{1,8}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Come si evince dai relativi schemi di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 22 stampanti attive. Gli indirizzi di 3 tra queste non erano contenuti all'interno della blacklist che invece già conteneva gli indirizzi di altre 11 stampanti non rilevate attraverso le scansioni.

4.2 Organizzazione 2 - $subnet_2/22$

subnet$_2$/22 - slice$_{2,1}$

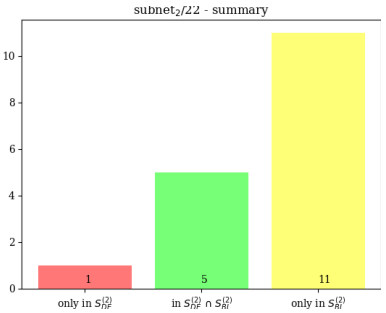
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

subnet$_2$/22 - slice$_{2,3}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

subnet$_2$/22 - slice$_{2,4}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Come si evince dai relativi schemi di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 6 stampanti attive. Soltanto l'indirizzo di una tra queste non era contenuto all'interno della blacklist che invece già conteneva gli indirizzi di altre 11 stampanti non rilevate attraverso le scansioni.

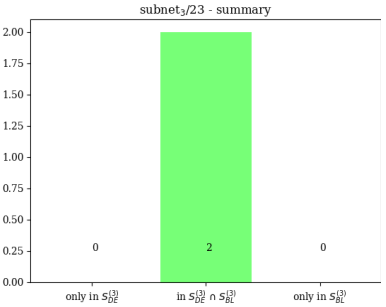
4.3 Organizzazione 3 - $subnet_3/23$

subnet$_3$/23 - slice$_{3,1}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

subnet$_3$/23 - slice$_{3,2}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Come si evince dai relativi schemi di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 2 stampanti attive. Tutti gli indirizzi delle stampanti rilevate facevano già parte della blacklist che non conteneva indirizzi di altre stampanti.

4.4 Organizzazione 4 - $subnet_4/22$

subnet$_4$/22 - slice$_{4,1}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

subnet$_4$/22 - slice$_{4,2}$

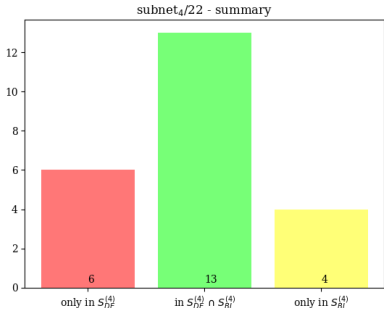
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

subnet$_4$/22 - slice$_{4,3}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

subnet$_4$/22 - slice$_{4,4}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

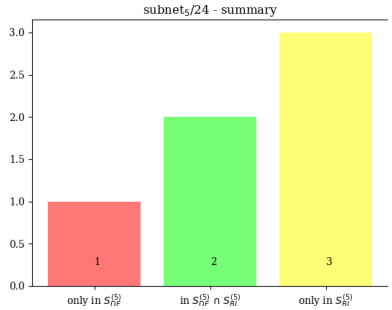


Come si evince dai relativi schemi di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 19 stampanti attive. Gli indirizzi di 6 tra queste non erano contenuti all'interno della blacklist che invece già conteneva gli indirizzi di altre 4 stampanti non rilevate attraverso le scansioni.

4.5 Organizzazione 5 - $subnet_5/24$

subnet$_5$/24 - slice$_{5,1}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Come si evince dal relativo schema di distribuzione e di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 3 stampanti attive. Soltanto l'indirizzo di una tra queste non era contenuto all'interno della blacklist che invece già conteneva gli indirizzi di altre 3 stampanti non rilevate attraverso le scansioni.

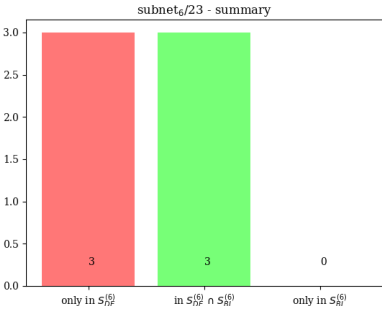
4.6 Organizzazione 6 - $subnet_6/23$

$\text{subnet}_6/23$ - $\text{slice}_{6,1}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

$\text{subnet}_6/23$ - $\text{slice}_{6,2}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

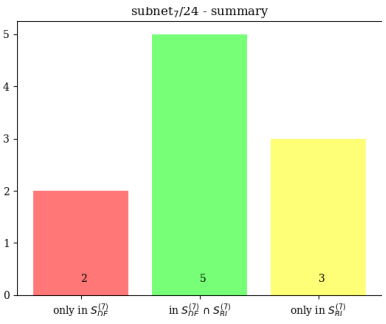


Come si evince dai relativi schemi di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 6 stampanti attive. Gli indirizzi di 3 tra queste non erano contenuti all'interno della blacklist che non conteneva indirizzi di altre stampanti.

4.7 Organizzazione 7 - $subnet_7/24$

$\text{subnet}_7/24$ - $\text{slice}_{7,1}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Come si evince dal relativo schema di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 7 stampanti attive. Gli indirizzi di 2 tra queste non erano contenuti all'interno della blacklist che invece già conteneva gli indirizzi di altre 3 stampanti non rilevate attraverso le scansioni.

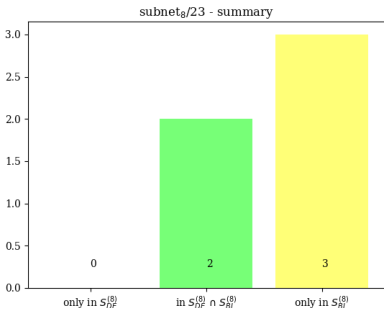
4.8 Organizzazione 8 - $subnet_8/23$

$subnet_8/23$ - $slice_{8,1}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

$subnet_8/23$ - $slice_{8,2}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255



Come si evince dai relativi schemi di distribuzione e dal grafico di riepilogo mostrato a sinistra, per questa organizzazione è stato possibile rilevare 2 stampanti attive. Tutti gli indirizzi delle stampanti rilevate facevano già parte della blacklist che conteneva anche gli indirizzi di altre 3 stampanti non rilevate attraverso le scansioni.

4.9 Considerazioni finali sugli schemi di distribuzione

Gli schemi di distribuzione, condensati nei relativi grafici di riepilogo, mettono in risalto diverse criticità specifiche per il contesto della CAN di riferimento:

- con il trascorrere del tempo il processo di scelta degli indirizzi da assegnare alle stampanti ha portato ad una loro distribuzione frammentata all'interno delle varie sottoreti e di conseguenza ad un'eccessiva frammentazione delle relative blacklists;
- come già descritto nel paragrafo *"Gestione della blacklist degli indirizzi delle stampanti* $\left(S_{BL}\right)$*"*, la corretta gestione della blacklist è fondamentale. Se ci dovesse essere uno squilibrio tra le attività di ingresso e le attività di uscita degli indirizzi dalla blacklist, l'approccio risulterebbe essere poco scalabile poiché, con il trascorrere del tempo, la blacklist tenderebbe sempre più a crescere;
- infine, l'approccio richiede un grado di coordinamento elevato tra le diverse figure professionali menzionate nell'introduzione.

5. Rimedi proposti

Al fine di risolvere le problematiche individuate nel paragrafo precedente, è possibile ricorrere all'uso di diverse strategie. In questo paragrafo ne andremo a descrivere qualcuna, presentandone anche vantaggi e svantaggi.

Figura 4: semplificazione del processo di installazione di una nuova stampante

L'obiettivo comune a tutte le strategie descritte è quello di semplificare il processo attualmente in uso per la corretta installazione di una nuova stampante (mostrato in Figura 2) con uno più snello, mostrato in Figura 4, che scorrela l'installazione fisica di un nuovo dispositivo dalla gestione della blacklist.

5.1 Usare il whitelisting

Una possibile strategia potrebbe incentrarsi sull'abbandono dell'approccio basato sulle blacklists e passare ad un approccio basato sulle whitelists. Alcuni vantaggi e svantaggi di questa strategia sono descritti nel sottoparagrafo *"Politiche di firewalling in breve: blacklisting vs. whitelisting"*. Inoltre, nel contesto presentato, tra gli altri svantaggi, si può segnalare che:

- i tempi di conversione delle blacklists in whitelists potrebbero essere molto lunghi;
- sebbene minimizzabili, nella fase di transizione dal blacklisting al whitelisting i disservizi sono inevitabili.

5.2 Automatizzare la gestione della blacklist

Un'altra possibile strategia potrebbe essere quella di continuare ad utilizzare il blacklisting, affidando il task di gestione delle blacklists ad un software. Quest'ultimo, scansionando periodicamente le sottoreti costituenti la CAN, andrebbe a rilevare la presenza delle stampanti e di conseguenza si occuperebbe dell'ingresso/uscita dei loro indirizzi nelle/dalle diverse blacklists.

Il vantaggio principale di questa strategia è la semplificazione della gestione delle blacklists. Gli svantaggi, invece, derivano dal fatto che le scansioni periodiche possono essere suscettibili a falsi positivi/negativi che porterebbero le varie blacklists ad essere inconsistenti nel tempo. Inoltre, questa strategia non risolverebbe il problema dell'eccessiva frammentazione delle blacklists.

5.3 Riservare alle stampanti un pool di indirizzi contigui

Un'altra strategia potrebbe essere quella di riservare, per ciascuna sottorete, un pool di indirizzi contigui all'installazione delle stampanti. In questo modo, anziché considerare le blacklists nella loro forma più elementare, ovvero liste di indirizzi appartenenti a dispositivi "sparpagliati" all'interno di un'intera sottorete, sarebbe possibile considerarle come liste di indirizzi contigui. Applicando questo concetto, si ottengono questi vantaggi:

- la frammentazione delle blacklists si elimina o si riduce drasticamente;
- la blacklist è costituita "solamente" da due informazioni: l'inizio e la fine del pool.

Il principale svantaggio di questa strategia è legato al dimensionamento del pool[10]: se il pool viene scelto troppo piccolo, una blacklist basata su un pool di indirizzi contigui *degraderebbe* ad una blacklist "tradizionale", ovvero quella presentata nel sottoparagrafo *"Politiche di firewalling in breve: blacklisting vs. whitelisting"*. Viceversa, se il pool viene scelto troppo grande, potrebbe verificarsi uno *"spreco di indirizzi",* ovvero tanti indirizzi verrebbero riservati alle stampanti, ma una parte consistente di loro rimarrebbe inutilizzata.

Ad ogni modo, con un pool dimensionato adeguatamente, la frequenza di aggiornamento della blacklist si ridurrebbe drasticamente poiché essa rimarrebbe "statica" all'interno del firewall. Chiaramente il meccanismo funziona fintantoché i referenti di rete e i gestori dell'indirizzamento menzionati nell'introduzione siano a conoscenza del pool di indirizzi riservato alle stampanti e che al momento di installare una nuova stampante scelgano un indirizzo tra quelli riservati.

[10] il corretto dimensionamento del pool dipende da diversi fattori come ad es. l'effettiva utilizzazione di una sottorete, il numero di stampanti già presenti in una determinata sottorete, ecc.

5.4 Usare il firewall embedded nella stampante

I dispositivi di stampa più moderni dispongono di firewall *embedded* che consentono, mediante un'interfaccia di management avanzato, la possibilità di definire delle regole per il filtraggio del traffico in ingresso/uscita alla/dalla stampante. Se, idealmente, tutti i dispositivi di stampa offrissero questa funzionalità, non ci sarebbe bisogno di attuare alcuna politica di protezione perimetrale specifica, purché le regole di firewalling locali siano definite correttamente su ciascuno di essi. Ovviamente, non è detto che stampanti più datate o anche stampanti moderne, ma di basso costo, dispongano di un firewall embedded.

6. Conclusioni

Il presente documento ha analizzato le strategie di blacklisting adottate, per la protezione di rete perimetrale delle stampanti nell'ambito della rete CAN di riferimento, descrivendo in particolare il lavoro necessario per mantenere aggiornata e coerente con la realtà la blacklist S_{BL}.

Riportando diverse criticità specifiche dell'ambito descritto, il documento ha anche voluto mettere in evidenza il fatto che la gestione della strategia di protezione delle stampanti attualmente in uso non è un'attività semplice. Esso ha inoltre presentato diversi rimedi utilizzabili per risolvere (o almeno mitigare) problematiche derivanti da tali criticità che contestualmente migliorerebbero la stessa attività di gestione della strategia di protezione delle stampanti.

Sebbene tutti i rimedi presentino sia vantaggi che svantaggi, quello che si prefigge di utilizzare una strategia che *riservi alle stampanti un pool di indirizzi contigui*, risulta essere il più vantaggioso, per la CAN di riferimento, in termini di *costi/benefici*. Chiaramente, nessuna strategia di protezione può essere efficace nel tempo se il coordinamento tra le figure professionali menzionate nell'introduzione è scarso o assente.

Infine, si noti che sia le rilevazioni sia i dati presentati all'interno del documento sono stati effettivamente impiegati, senza apportare nessuna modifica alla politica di sicurezza in uso, al fine di aggiornare la blacklist S_{BL} ed accrescere il livello di sicurezza delle sottoreti costituenti la CAN di riferimento.

7. Riferimenti

- Campus area network - Wikipedia
  https://en.wikipedia.org/wiki/Campus_network

- Firewall - Wikipedia
  https://it.wikipedia.org/wiki/Firewall

- Next-generation firewall - Wikipedia
  https://en.wikipedia.org/wiki/Next-generation_firewall

- Zone-based firewall - GeeksForGeeks
  https://www.geeksforgeeks.org/zone-based-firewall/

- Blacklisting vs. Whitelisting - Consolidated Technologies, inc.
  https://consoltech.com/blog/blacklisting-vs-whitelisting/

- Access-control List / Networking ACLs - Wikipedia
  https://en.wikipedia.org/wiki/Access-control_list

- Endpoint security - Wikipedia
  https://en.wikipedia.org/wiki/Endpoint_security

- 80,000 printers are exposing their IPP port online - ZDNet
  https://www.zdnet.com/article/80000-printers-are-exposing-their-ipp-port-online/

- Hackers are spamming printers with ‘antiwork’ slogans - Metro.co.uk
  https://metro.co.uk/2021/12/03/hackers-are-spamming-printers-with-antiwork-slogans-15709807/