RELEASE NOTES

TELCO MANAGER

ESTATÍSTICAS DE TRÁFEGO DA SUBREDE

UM ALIADO NA CONFIGURAÇÃO DE PERFIL DE AMEAÇA

A configuração de perfis de ameaça pode ser uma tarefa muito difícil se você não tem informações sobre o tráfego dentro de uma subrede. Embora o gráfico lhe dê algumas informações, ele lhe fornece o tráfego agregado dentro do bloco.

É muito importante ter alguma noção do tráfego por endereço IP para escolher valores que caracterizem um comportamento anormal.

O TRAFwatcher passa a fornecer estas estatísticas para as subredes configuradas com perfil de ameaça. Não perca tempo tentando descobrir seus thresholds, deixe o TRAFWatcher trabalhar para você!

Top values	Source bytes		Source packets		Source flows		Source Ip Flood		Destination bytes		Destination packets		Destination flows		Destination Ip Flood	
	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum
25/10/2016 16:15:00 - 24/11/2016 16:15:00	46595.57	712347.14	24748.31	402479.29	9.58	570.00	23.82	29.16	46595.57	712347.14	24748.31	402479.29	9.58	570.00	2.12	2.88

Time	Source bytes		Source packets		Source flows		Source Ip Flood		Destination bytes		Destination packets		Destination flows		Destination Ip Flood	
	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum	Average	Maximum
24/11/2016 16:15:00	42.92	361.25	0.22	3.77	0.01	0.05	7.14	12.73	928.91	5842.56	1.53	47.75	0.11	2.43	0.15	0.16
24/11/2016 16:10:00	29.20	146.41	0.15	1.98	0.02	0.03	11.79	12.97	1182.55	6072.04	1.55	30.67	0.09	1.94	0.16	0.18
24/11/2016 16:05:00	20.94	94.93	0.09	1.01	0.01	0.03	10.53	12.56	742.06	4252.06	1.11	29.71	0.05	0.56	0.16	0.18
24/11/2016 16:00:00	45.91	915.77	0.17	3.31	0.01	0.04	4.48	4.82	597.84	4479.73	1.08	36.71	0.05	0.77	0.16	0.17
24/11/2016 15:55:00	68.26	1913.57	0.18	2.73	0.02	0.04	5.45	5.70	708.96	4427.62	1.14	36.46	0.06	0.61	0.17	0.17
24/11/2016 15:50:00	66.82	1709.42	0.17	1.82	0.02	0.03	6.13	6.58	804.22	3975.87	1.09	27.45	0.04	0.49	0.17	0.17

Figura 1: Estatísticas de tráfego

NOVOS ALARMES DE AMEAÇA

CARACTERIZE OS TIPOS DE ATAQUE

Atualmente existem várias técnicas de ataque DdoS sendo aplicadas. É interessante saber diferenciar um tráfego de um determinado tipo e poder alarmar esta situação específica (acionar um filtro de blackhole, por exemplo).

O perfil de ameaça ganhou novos parâmetros para identificação de ataques de aplicação e de SYN e ICMP flood.

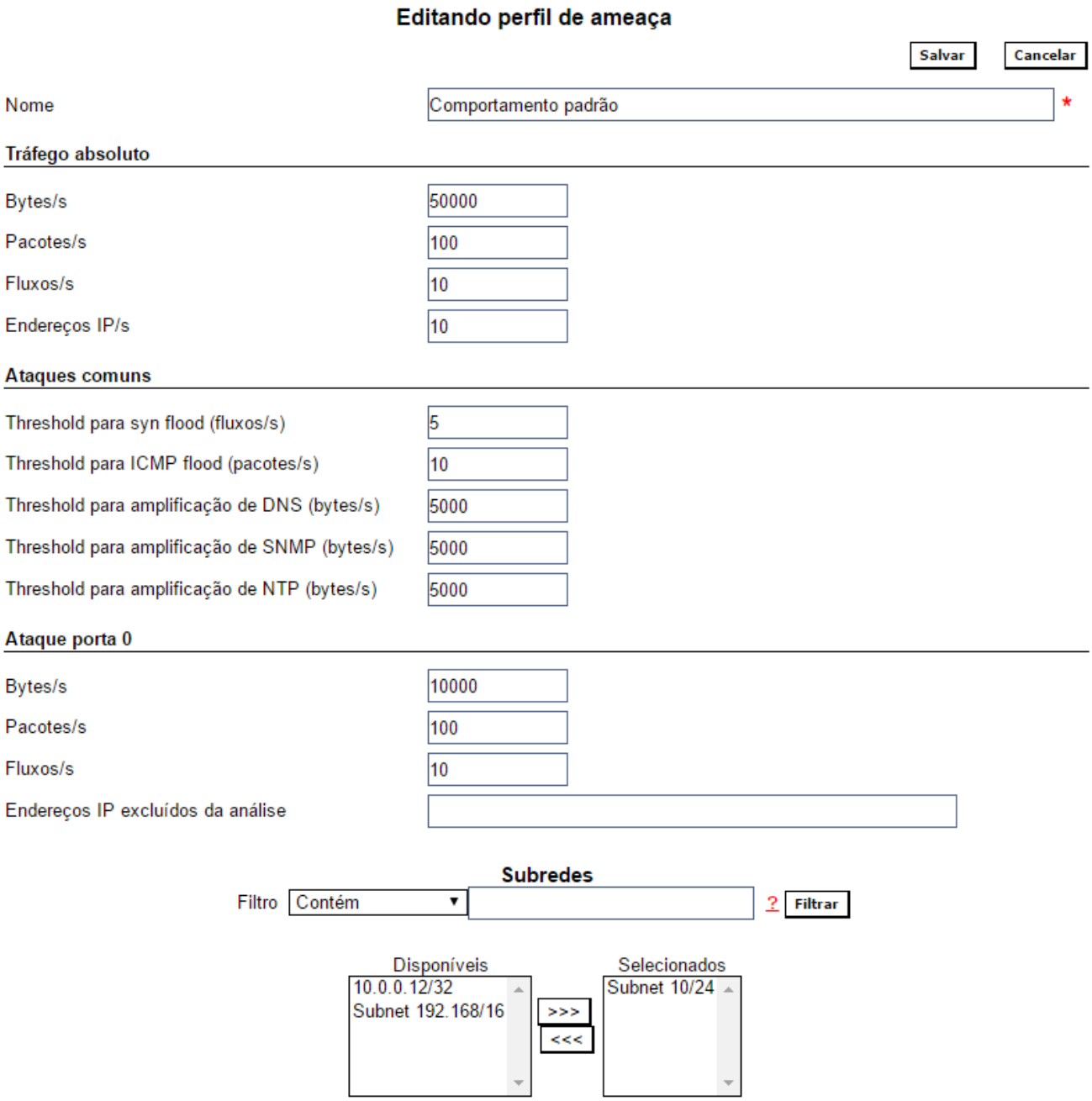

Figura 2: Novos tipos de ataque

ANUNCIAR IP NO BLACKHOLE

PROTEJA SUA REDE FILTRANDO ENDEREÇOS IP

A técnica de blackhole é bastante usada para filtrar endereços IPs atacados na sua rede. Através de configurações num roteador é possível marcar um endereço com uma comunidade específica para filtrar os acessos àquele endereço específico.

Este anúncio pode ser feito automaticamente ou manualmente no TRAfwatcher. Para isto basta criar um script para aplicar a configuração no seu dispositivo de preferência.

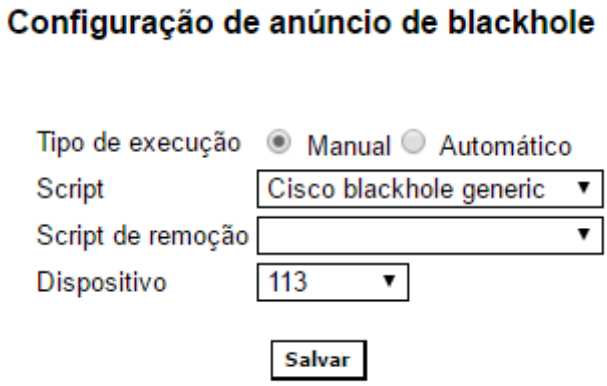

Figura 3: Configuração de anúncio de blackhole

RESUMO DE AMEAÇAS

CONFIRA QUAIS ENDEREÇOS IP SÃO SUSPEITOS

O TRAFwatcher fornece um resumo dos IPs que estão alarmados no último minuto. Este resumo é super últil para ter uma ideia de número de ameaças identificadas pelo sistema.

Subnet 10/24				
IPs origem e destino	Tipo de Ataque	Tipo do limite	Valor do limite	Valor observado
10.0.0.1 - 10.0.0.17	Tráfego absoluto	Bytes/s	3000	3174
10.0.0.1 - 10.0.0.188	Tráfego absoluto	Bytes/s	3000	3184
10.0.0.17 - 10.0.0.1	Tráfego absoluto	Bytes/s	3000	3174
10.0.0.188 - 10.0.0.1	Tráfego absoluto	Bytes/s	3000	3184
10.0.0.225	Threshold para amplificação de DNS	Bytes/s	100	100
10.0.0.231	Threshold para amplificação de DNS	Bytes/s	100	102

Figura 4: Resumo de ameaças

NOVAS OPÇÕES NO RELATÓRIO TOPN

EXTRAIA MAIS INFORMAÇÕES NUM MESMO RELATÓRIO

O relatório topn do TRAFip ganhou a opção de escolher ambas as direções dos dados. Esta funcionalidade exibe a entrada e a saída no mesmo relatório e ainda lhe dá a opção de agrupar as direções no relatório, para que elas não apareçam espalhadas pelo mesmo.

Uma simples mudança que pode lhe oferecer visões importantes sobre o seu tráfego.

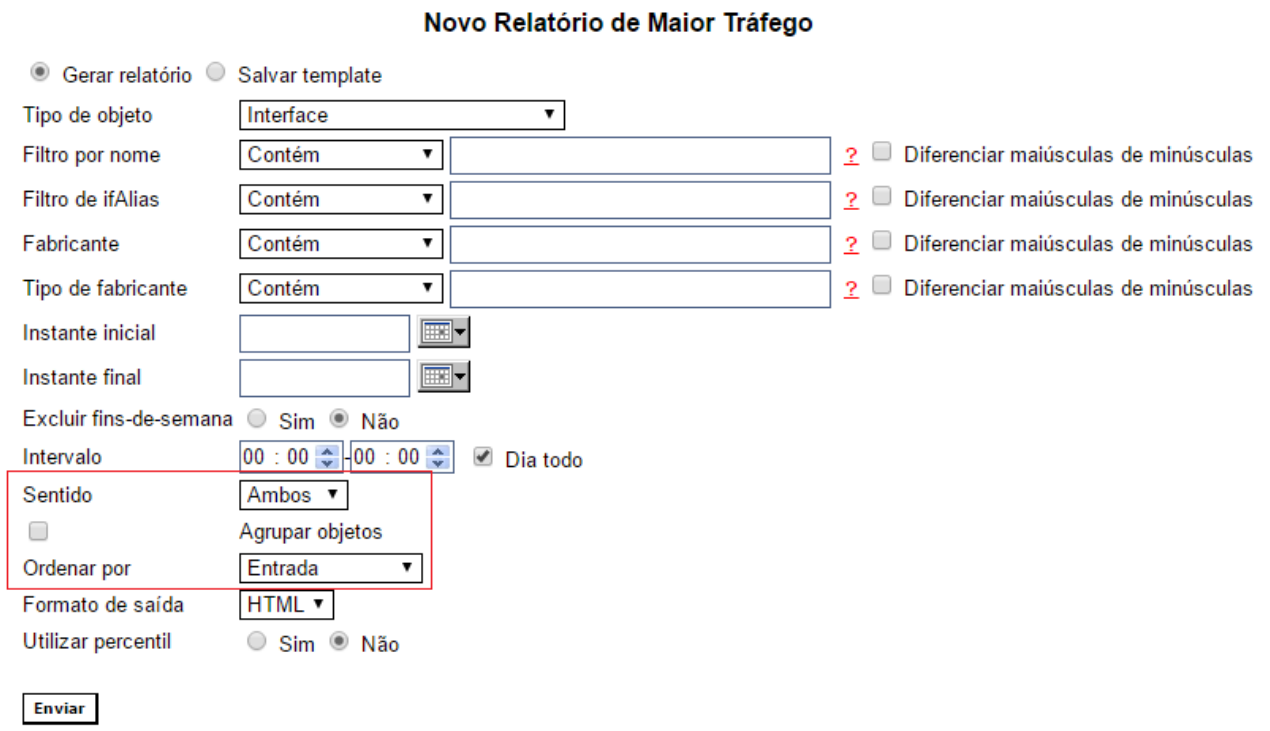

Figura 5: Ambas as direções no relatório topn do TRAFip

NOVO FORMATO DE FÓRMULAS DO SLAVIEW

CONSTRUA GRÁFICOS BASEADOS NAS SUAS REGRAS DE NEGÓCIO

O SLAview vem ganhando inúmeras mudanças no sentido de facilitar o seu uso. Uma das dificuldades que ele tinha era a manipulação das fórmulas do perfil que deviam ser preenchidas no formato RPN.

Este problema está felizmente resolvido e as fórmulas já podem ser feitas num formato amigável e natural.

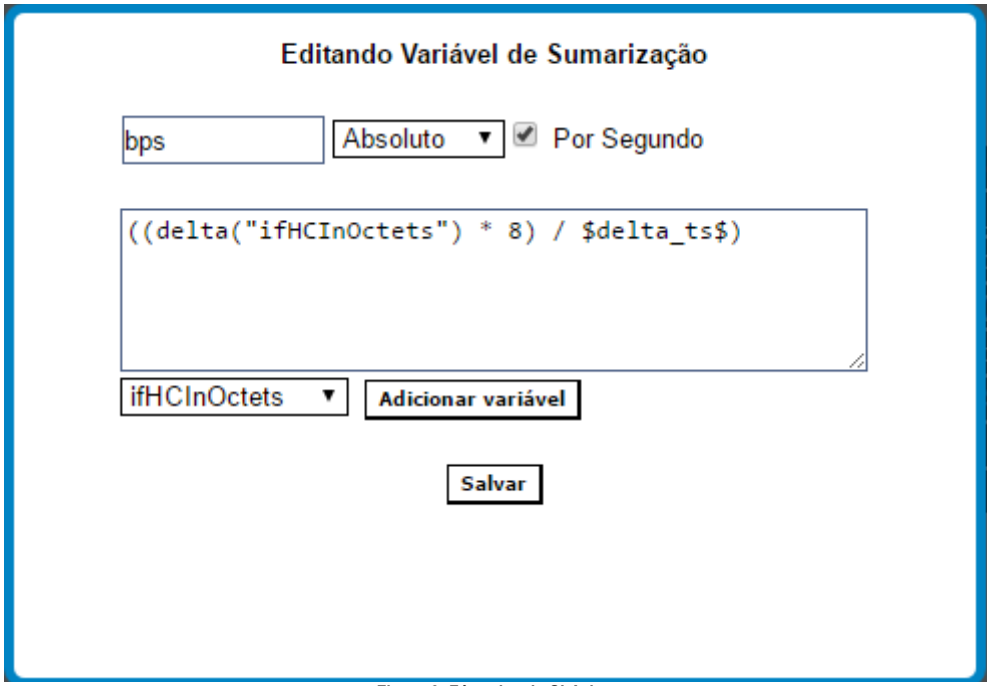

Figura 6: Fórmulas do SLAview

ALARMES POR SYSLOG

MAIS UMA FERRAMENTA PARA CUIDAR DA SUA INFRAESTRUTURA

Syslog é uma ferramenta de log bastante utilizada e que exporta inúmeras informações a respeito do equipamento em que está sendo usada.

Esses logs podem conter informações extremamente úteis que não são exportadas via SNMP, por exemplo.

Para aproveitar o poder do syslog um novo tipo de alarme foi criado no SLAview. A partir de regras de ativação e desativação em cima dos syslogs recebidos, dispositivos podem ser gerenciados com alarmes seguindo regras definidas por você.

Deixe o SLAview trabalhar por você!

Figura 7: Filtro de syslog

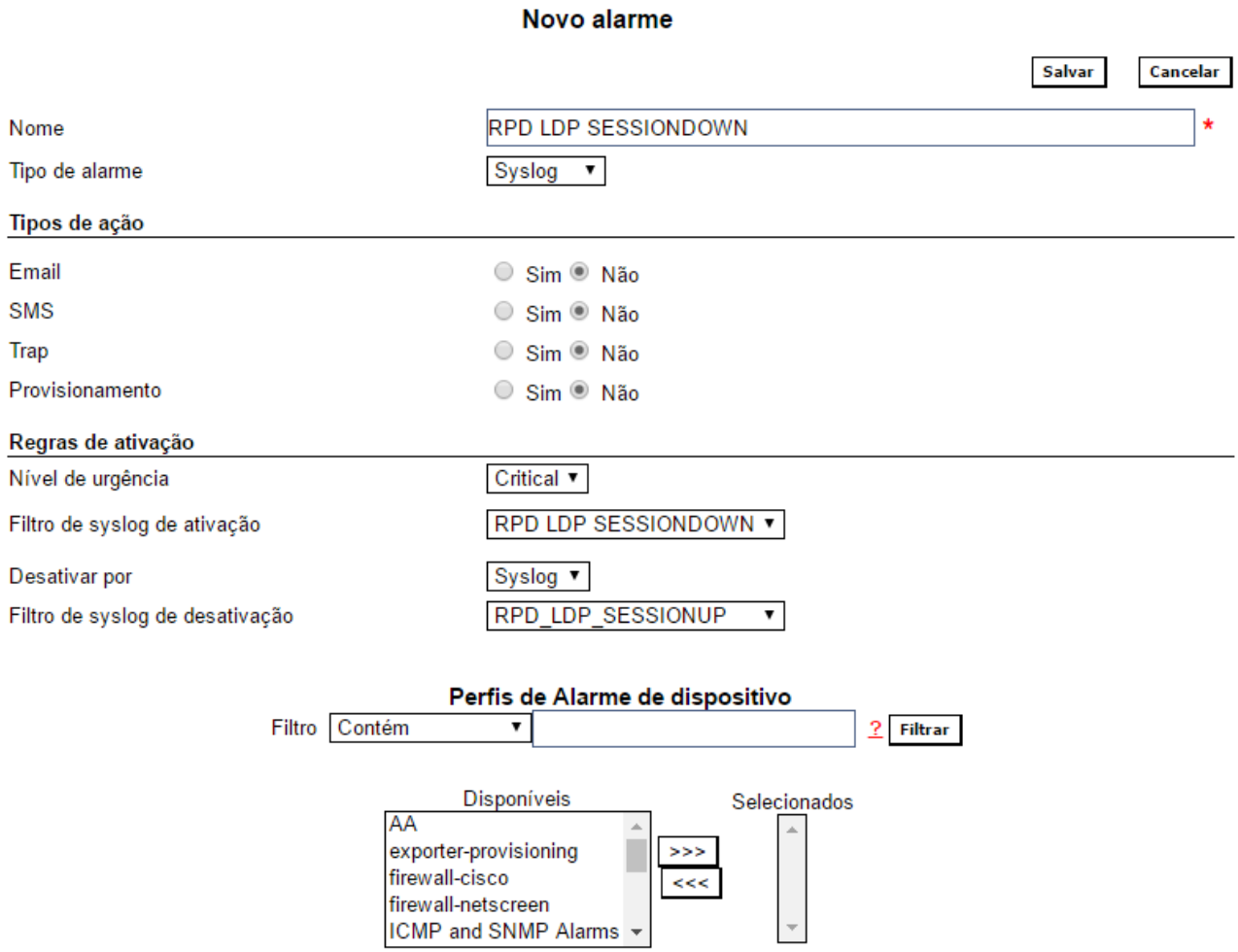

Figura 8: Alarme de syslog

SISTEMA DE INTEGRIDADE DE ARQUIVOS

AUMENTE A SEGURANÇA DA SUA INFRAESTRUTURA

Garantir a segurança dentro de uma infraestrutura é uma tarefa muito importante e que pode ser bastante trabalhosa sem as ferramentas corretas.

O CFGtool é uma ferramenta que irá lhe ajudar bastante, oferencendo um módulo de integridade de arquivos. Este módulo irá armazenar hashes de arquivos presentes nos equipamentos do seu interesse. Arquivos importantes podem ser monitorados e qualquer alteração ou remoção de um arquivo será detectada e alarmada no CFGtool.

Last integrity check: Fri Nov 25 17:45:00 2016

Arquivo	Data de modificação do MD5	MD5	Data de modificação do SHA	SHA	Ação
/etc/ssh/ssh_host_dsa_key.pub	-	326a97593635b2ef4b4b64a2186ddbd6	-	00a9351288af183539beb38bbc6d7cf2fbc8f30d	
/etc/ssh/ssh_host_ecdsa_key	-	a6d131911530c8458be342300933fb59	-	00173c31e989dee5330b31bc0072772ec001766a	
/etc/ssh/ssh_host_ecdsa_key.pub	-	5f293c774f6f704cb53857b5c8e79731	-	00f0b3e4d11ae81a527ef25abf11e536a26b7a2e	
/etc/ssh/ssh_host_ed25519_key	-	104b11c7d92097599ecaf8d13d1fa30d	-	005582221ff4b2b2df74186b5aefe11e0b946ff1	
/etc/ssh/ssh_host_ed25519_key.pub	-	a6c778ad44d74f5804792bd2be6350b9	-	00239a7c493321533f36525a3c7423092eb57fe1	
/etc/ssh/ssh_host_rsa_key	-	518dfda0063d1ebef681b26a2e0b1068	-	00af5c420560dbed737595b4c541e88418b219d0	
/etc/ssh/ssh_host_rsa_key.pub	-	94cf1f2566d195f2fd970ede959b693c	-	00cf065101ef48526f739596d263eb103ab0563d	
/etc/ssh/sshd_config	25/10/2016 17:42	11dadda2b0c2b1bfccf3c01f2855ee04 -> 80d9cb5208317d4667b2374be9e808de	25/10/2016 17:42	002d3484723b247daec438c0e62f6fad1c4623f3 -> 00f50b6abd12a41d452d9d777a2c67cee6b60882	
/etc/ssl/certs/README.RootCerts	-	ef30e85fa0d395c733218bb0afe590fb	-	0053e7e43d1d207292c8ca88662e9b4f2fecadab	
/etc/ssl/certs/demo/3f77a2b5.0	-	e4160fea763261c38df744cb9b9fa10b	-	00fd7d69dc1f4c1cbb308cbd32a1e01f068bfd7c	
/etc/ssl/certs/demo/ca-cert.pem	-	e4160fea763261c38df744cb9b9fa10b	-	00fd7d69dc1f4c1cbb308cbd32a1e01f068bfd7c	
/etc/ssl/certs/demo/cbdbd8bc.0	-	96ce4a8d7545ccb56c30c746997e2b25	-	00cc95492027ba98afe0c7f0abcd69280c342340	
/etc/ssl/certs/demo/de4fa23b.0	-	d038ef2b4ce2084ef25ef743d0107dbd	-	00450c733de8367c68579ee71d7fa411d4c5e64c	
/etc/ssl/certs/demo/dsa-ca.pem	-	96ce4a8d7545ccb56c30c746997e2b25	-	00cc95492027ba98afe0c7f0abcd69280c342340	
/etc/ssl/certs/demo/dsa-pca.pem	-	d038ef2b4ce2084ef25ef743d0107dbd	-	00450c733de8367c68579ee71d7fa411d4c5e64c	
/etc/ssl/certs/demo/e83ef475.0	-	1eb08eee36c6142b60d3e38836ded59c	-	005ee3954e7ae9c5cb06bf6624f488bd51f7ceed	
/etc/ssl/certs/demo/pca-cert.pem	-	1eb08eee36c6142b60d3e38836ded59c	-	005ee3954e7ae9c5cb06bf6624f488bd51f7ceed	
/etc/ssl/certs/expired/ICE.crl	-	109e4e5364e7cb5c92cf86e506a4313d	-	009a2d0b551ef3dc83135b78bafc96b35b81c621	
/etc/ssl/misc/CA.pl	-	9909f53baab25b7347952323468 23d2f	-	00f1fb57b69ad653eab0644221263929 8a00a988	
/etc/ssl/misc/CA.sh	-	948439fd3f17dc7d9511305aa1f1355a	-	0049c358473a0ed23a335360befc29d1b03492ea	
/etc/ssl/misc/c_hash	-	11612e0bac6e19e1bb35d038e691b72c	-	00bb1d58b936be53e4de00fcca51453964a2e7cb	
/etc/ssl/misc/c_info	-	45bbf2e1f1a5a2ff772ac81ecab10729	-	00667fc7a808530f5c71fb69171ec2443ff29125	
/etc/ssl/misc/c_issuer	-	7a5ec6cc06ca0d45332feb59a9aaaf1a	-	00c791b7dc5957bf43b4cfcb5e689dea8d83b1ae	
/etc/ssl/misc/c_name	-	e6828944a8b442b7a040405fbe3f9a1f	-	00adfc186ff506274fa80660079daca8e52bb0bc	
/etc/ssl/misc/tsget	-	9ebe114de208f59f38826d70aeaa9122	-	0005155818b1827f3e7133ac67326d87cb7ddd2e	
/etc/ssl/openssl.cnf	-	ce31ab5015842bf7c2939514a634e0e4	-	00ecd3fa73384477469727c660e86e1be3aec859	
/etc/sysconfig/clock	-	dd4673783f7f032d024b675bffcca13e	-	005b1b45b4ad637ecb1f4bfe9a07448be0649a02	
/etc/sysconfig/console	-	9c5bc74a84e72566e4d5d4f89b380c6c	-	00dfeb8ed109d7f64c3c93f333de6f97f6014dc2	
/etc/sysconfig/createfiles	-	cd876a1accb3a5577b6eb1f1f9dd6858	-	008f695f88059d7d1fa0b9151b2e0917fe6f677a	
/etc/sysconfig/modules	-	929e585ff248299b79876366145ed6c5	-	0090ec262fe0694324dd4d7927204d7c4cd73ce1	
/etc/sysconfig/network	-	ab686638afbc94167fae17179495fe9d	-	0029bcf0bbc542ed9b8fca8767c936cbdd229f32	
/etc/sysconfig/network-devices/ifconfig.eth0/dhcpcd	-	0b8d3c761fbf1ceb533871f792900555	-	00ab0927c376c41abbca891695d9244eaf30c23f	
/etc/sysconfig/network-devices/ifdown	-	5a528ef8c7375f09768290055 4fb38fd	-	00efad616ce73cd3c8a4c30b416c40b938a04234	
/etc/sysconfig/network-devices/ifup	-	e9d583139b60f372ad249fb50c56ebe2	-	003c06a799d723232ff0177a5f3c050a55913ed6	
/etc/sysconfig/network-devices/services/ipv4-static	-	afa5d1684484f9c35f34aa1c10baac8a	-	005a0ab32613231ab229821f207df3e1de98ef08	
/etc/sysconfig/network-devices/services/ipv4-static-route	-	8c5eeaabd656b32a2ed3a0a78e85c4f8	-	00bf0d1b1ec91bd763e34aa1d0c0634184ff1dea	
/etc/sysconfig/rc	-	183153d02c4d8f8e05b877dafaedd85c	-	0036c861e89d19bebc6538df279d5ae6d16c6dda	
/etc/syslog.conf	-	9ec1fe94c50c5601671ea1f151b5af07	-	0027d9e7ef3ca77c0522bde523c29d603a193c68	
/etc/telco-config	-	654502bb0f57ec8737b4cf12117575b8	-	00f399069870cefdaaf87402e7687f0eb6d64583	Remover
/etc/telco-lfs-build.info	-	89b357e3c75f5525cd9b26c6b7b777ec	-	0021fe30905bf808c3ce750b0b300eaa1e0cab5b	
/etc/telco-web	25/10/2016 17:45	654502bb0f57ec8737b4cf12117575b8 -> c360ed8b7fa679378f5c80b4150645a8	25/10/2016 17:45	00f399069870cefdaaf87402e7687f0eb6d64583 -> 00605ee4d9af31441c0809b73a5e50f9f5abb5a5	
/etc/tmsecurity.conf	25/10/2016 17:42	301ab1728410845b3f2aa7eb0cf5299d -> 2c748f268cb1b7cf302e5760c59d1741	25/10/2016 17:42	007f20da66c05d9d637acd72635d9481fa53860f -> 00a2c1f45e6c001a3f5f511806e52a9dbe696e46	

Figura 9: Integridade de arquivos

CREDENCIAIS DE DISPOSITIVOS

CADASTRAR DISPOSITIVOS FICOU MAIS FÁCIL

É muito comum que exista uma credencial de acesso comum a inúmeros dispositivos num ambiente de rede. Digitar os dados em cada dispositivo no sistema pode ser uma tarefa trabalhosa.

Para agilizar esse cadastro o sistema agora conta com um registro de credenciais. Nele você diz o protocolo de acesso e as informações pertinentes ao protocolo escolhido e cria uma credencial que poderá ser usada por qualquer dispositivo.

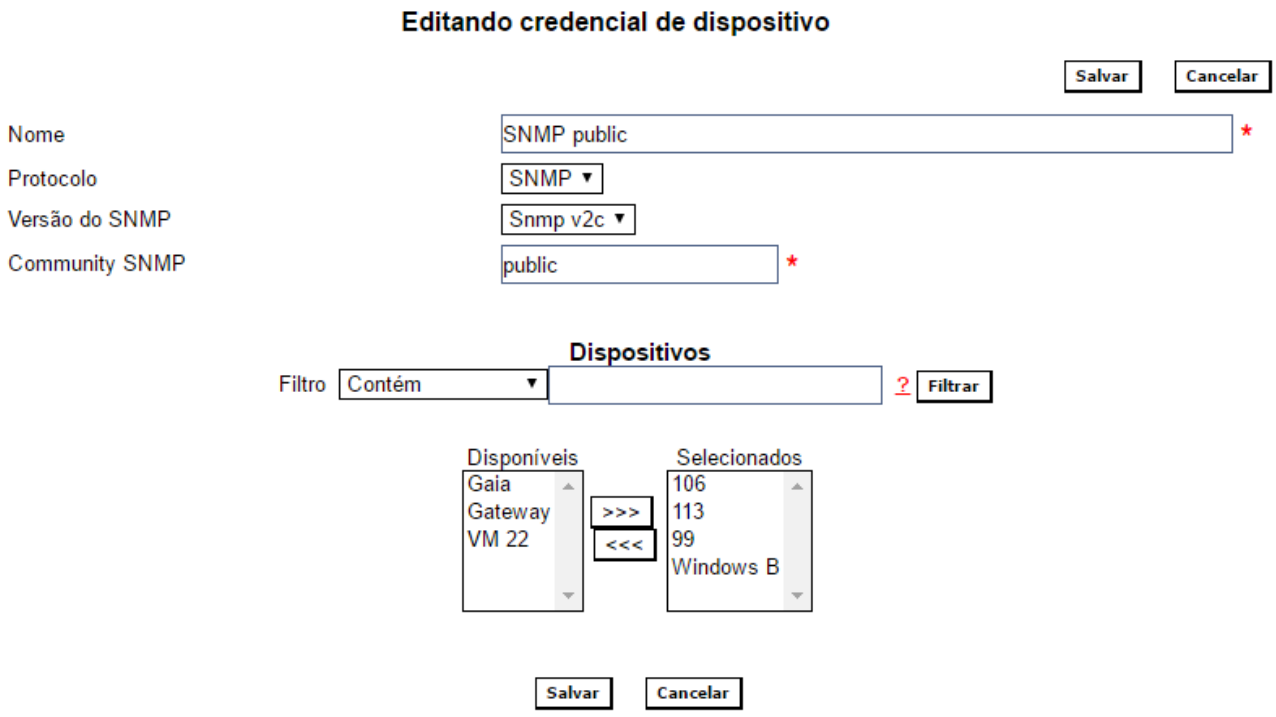

Figura 10: Credencial de dispositivo

NOTIFICAÇÃO VIA TELEGRAM

RECEBA NOTIFICAÇÕES NO SEU CELULAR

Receber notificações de alarmes no seu celular ajuda bastante para que você possa atuar o mais rapidamente possível em algum incidente na sua rede. Isso só era possível a partir da configuração de um gateway SMPP, para receber os alarmes via SMS.

O sistema agora oferece uma nova opção de recebimento dos alarmes a partir de uma integração com os serviços do Telegram. Basta instalar o Telegram em seu smartphone e seguir o passo a passo presente no manual de configuração da ferramenta que você passará a ser notificado dos alarmes.