Installation service Snort



Connecter vous au PfSense, cliquez sur système puis Package Manager.

System / Package Manager / Installed Packages	
Installed Packages Available Packages	
Installed Packages	
Please wait while the list of packages is retrieved and formatted.	

Cliquez sur Available Packages.

	System 👻 In	iterfaces 👻 Fir	ewall - Services	• VPN •	Status 🕶	Diagnostics 👻	Help 🕶	# 2
WARNING: The 'ad	Imin' account pass	sword is set to the c	lefault value. Change th	ne password in the	User Manager.			
System / Pa	ackage Mar	nager / Avai	able Packages					
Installed Package	s Available I	Packages						
Search								(
Search term	sno	rt r a search string or '	nix regular expression	to search package	Both names and des	h v	Q Search Clear	
Packages								
Name Version	Description							
snort 4.1.6_17	Snort is an open s based inspection. Package Depende	source network intra encies:	usion prevention and de	etection system (ID	IS/IPS). Combini	ing the benefits of s	signature, protocol, and and	omaly- + Ins

Dans la barre de recherche tapez « snort » puis sur recherché et enfin cliquez sur installer.

Installed Packages Available Packages Package Installer	
Package Installation	
au packages to be INSTALLED.	·
dag: 2.2.2 3 [nfsense]	
libdnet: 1.13 4 [pfSense]	
libpcap: 1.10.4 [pfSense]	
libpfctl: 0.8 [pfSense]	
pfSense-pkg-snort: 4.1.6_17 [pfSense]	
snort: 2.9.20_8 [pfSense]	
umber of packages to be installed: 6	
he process will require 10 MiB more space.	
MiB to be downloaded.	
<pre>1/6] Fetching libdnet-1.13_4.pkg: done</pre>	
2/6] Fetching short-2 9 20 8 nkg·	•

Le téléchargement va débuter et installer tous les packages nécessaire

In	stalled Pa	ackages			
	Name	Category	Version	Description	Action
~	snort	security	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies:	亩仁 i
~	zabbix- agent64	net- mgmt	1.0.6	Zabbix agent is deployed on a monitoring target to actively monitor local resources and applications (hard drives, memory, processor statistics etc). The agent gathers operational information locally and reports data to Zabbix server for further processing. In case of failures (such as a hard disk running full or a crashed service process), Zabbix server can actively alert the administrators of the particular machine that reported the failure. Zabbix is an enterprise-class open source distributed monitoring solution. Package Dependencies: visit with the failure cameurolice.com Package Dependencies:	亩 t i

Dans l'onglet Installed Packages, l'add-on « Snort » est bien installé.

WARNING: The 'admin' accourt	int password is set to the default valu	Auto Config Backup Captive Portal	he User Manager.	
System / Package	Manager / Installed Pa	DHCP Relay DHCP Server		0
Installed Packages Ava	ailable Packages	DHCPv6 Server DHCPv6 Server DNS Forwarder DNS Resolver		
Name Category Ver	ersion Description	Dynamic DNS		Action
✓ snort security 4.	 1.6_17 Snort is an open source net and anomaly-based inspect Package Dependencies: Ø snort-2.9.20_8 	IGMP Proxy NTP PPPoE Server Router Advertisement	d detection system (IDS/IPS). Combining the benefits of signature, protocol,	面で i
✓ zabbix- net- 1. agent64 mgmt	.0.6 Zabbix agent is deployed or statistics etc). The agent ga failures (such as a hard disl particular machine that rep	SNMP Snort UPnP & NAT-PMP Wake-on-LAN	ely monitor local resources and applications (hard drives, memory, processor n locally and reports data to Zabbix server for further processing. In case of rvice process), Zabbix server can actively alert the administrators of the reterprise-class open source distributed monitoring solution.	面 た i

Dans la catégorie services, un onglet snort est disponible, cliqué dessus

nort Interfaces Glo	bal Settings	Updates Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
nstalled Rule Set MI	D5 Signature									
ule Set Name/Publisher			M	D5 Signature Ha	ih		MD5 Signature	e Date		
Snort Subscriber Ruleset			N	ot Enabled			Not Enabled			
Snort GPLv2 Community Rules				ot Enabled			Not Enabled			
Emerging Threats Open Ru	ules		N	ot Enabled			Not Enabled			
Snort OpenAppID Detector	rs		N	ot Enabled			Not Enabled			
Snort AppID Open Text Ru	les		N	ot Enabled			Not Enabled			
eodo Tracker Botnet C2 I	P Rules		N	ot Enabled			Not Enabled			
pdate Your Rule Se	t									
Last Update	Unknown	Result: Unkno	wn							
S 1 5					A Sec	e Lindate.				

Dans l'onglet Updates, cliquez sur Update Rules.



Dans l'onglet Global Settings, créer un compte gratuit snort, enfin prenez le code Oinkmaster. Enfin ajoutez les différentes options cochées ci-dessous.

ervices / Snort	/ Global S	ettings								0
nort Interfaces Glo	bal Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
nort Subscriber Rul	es									
Enable Snort VRT	Click to er	nable downloa	ed of Snort fr	ee Registered	User or paid Sub	scriber rules				
	Sign Up for a Sign Up for p	free Registere aid Snort Sub	ed User Rule scriber Rule	s Account Set (by Talos)						
nort GPLv2 Commu	nity Rules									
Enable Snort GPLv2	Click to er	nable downloa	d of Snort G	PLv2 Commu	nity rules					
	The Snort Co ruleset is upd	mmunity Rule lated daily and	set is a GPL d is a <mark>sub</mark> set	/2 Talos certifi of the subscri	ed ruleset that is ber ruleset.	distributed free	of charge wit	hout any Snort S	ubscriber License	e restrictions. This
merging Threats (E	T) Rules									
Enable ET Open	Click to er	nable downloa	d of Emergi	ng Threats Op	en rules					
	ETOpen is an	open source	set of Snort	rules whose c	overage is more l	imited than ETP	ro.			
Enable ET Pro	Click to er	nable downloa	id of Emergi	ng Threats Pro	rules					
	Sign Up for an ETPro for Sno	n ETPro Acco ort offers daily	unt / updates an	d extensive co	werage of current	malware threat	15.			
ourcefire OpenAppl	D Detectors									
		nahla downlos	d of Source	ire OpenAppII	Detectors					
Enable OpenAppID	Click to er	nable obminor								
Enable OpenAppID	Click to er	DD Detectors	package cor	tains the appl	ication signature	s required by the	AppID prepro	cessor and the (OpenAppID text n	ules.
Enable OpenAppID OpenAppID Version	Click to er	DD Detectors	package cor	tains the appl	ication signature	s required by the	e AppID prepro	cessor and the (OpenAppID text n	ules.

Botnet C2 IP Rules	Click to enable download of FEODO Track	er Botnet C2 IP rules
	Feodo Tracker tracks certain families that are to commit ebanking fraud. Since 2010, variou	related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals is malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.
Rules Update Setting	S	
Update Interval	1 DAY	×
	Please select the interval for rule updates. Ch	oosing NEVER disables auto-updates.
Update Start Time	00:46	
	Enter the rule update start time in 24-hour for chosen above starting at the time specified h at 00:08 and 12:08 each day. The randomized simultaneous requests.	mat (HH.MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval ere. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update I minutes value should be retained to minimize the impact to the rules update site from large numbers of
Hide Deprecated Rules Categories	Click to hide deprecated rules categories i	in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	Click to disable verification of SSL peers d	uring rules updates. This is commonly needed only for self-signed certificates. Default is not checked.
General Settings		
Remove Blocked Hosts	30 MINS	
Interval	Please select the amount of time you would li	ike hosts to be blocked. In most cases, one hour is a good choice.
Remove Blocked Hosts After Deinstall	Click to clear all blocked hosts added by S	inort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	Click to retain Snort settings after package	e removal.
25572 2259785	Click to output detailed messages to the s	system log when Snort is starting and stopping. Default is not checked.

Puis cliquez sur Save

Serv	/ices / Sr	ort / Interfa	ces								0
Snort	Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Inter	face Settin	gs Overview									
	Interface	Snor	t Status	Patt	ern Match	Blo	cking Mode		Description	Action	ıs
	WAN (igc0)	8	0	AC-	AC-BNFA LEGA		ACY MODE WAN		WAN	Ø [7
										Ę	Add 🔟 Delet

Sur l'onglet Snort Interfaces, cliquez sur Add et ajouté l'option Wan.

Cochez les différentes options dans l'onglet Wan Settings.

inort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
VAN Settings V	VAN Categories	WAN Rules	WAN V	ariables	WAN Preprocs	WAN IP Rep	WAN	Logs		
eneral Settings										
Enal	ole 🛛 🗹 Enable i	nterface								
Interfa	ce WAN (igc0))				~				
	Choose the	interface where	this Snort in	istance will i	nspect traffic,					
Descripti	on WAN									
	Enter a mea	aningful descript	tion here for	your reference	ce.					
Snap Leng	th 1518				10					
112122-01220	1.2717.									

Alert Settings

_	
Send Alerts to System Log	Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures	Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	128 Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_igc09545 is rotated and a new file opened.
Enable Unified2 Logging	 Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
Legacy Mode V
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Checking this option will kill firewall established states for the blocked IP. Default is checked.
BOTH Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performan	ce Settings		
Search Method	AC-BNFA		
	Choose a fast pattern matcher algor	vrithm. Default is AC-BNFA.	
Split ANY-ANY	Enable splitting of ANY-ANY port	rt group. Default is Not Checked.	
Search Optimize	Enable search optimization. Defa	/ault is Not Checked.	
Stream Inserts	Do not evaluate stream inserted	packets against the detection engine. Default is Not Checked.	
Checksum Check Disable	Disable checksum checking with	hin Snort to improve performance. Default is Not Checked.	

Choose the Networks	s Snort Should Inspect and Whitelist
Home Net	pfSenseInterfaces
	Choose the Home Net you want this interface to use.
	Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.
	Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.
External Net	default View List
	Choose the External Net you want this interface to use.
	External Net is networks that are not Home Net. Most users should leave this setting at default.
Pass List	pfSenseInterfaces
	Choose the Pass List you want this interface to use.
	The default Pass List adds local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to customize. This option will only be used when block offenders is on and IPS Mode is set to Legacy Mode.
Choose a Suppressio	n or Filtering List (Ontional)
Alert Suppression and	Wansuppress_6/da856/5d3cb
Custom Configuration	n Options
Advanced Configuration	
Pass-Through	
	6
	Enter any additional configuration parameters to add to the Snort configuration here, separated by a newline
	Save

Sauvegarder la configuration.

Dans l'onglet Wan Categories, cochez les différentes

Automatic Flowbit R	esolution	
Resolve Flowbits	If checked, Snort will auto-enable rules required for checked flowbits. De Snort will examine the enabled rules in your chosen rule categories for chec automatically enabled and added to the list of files in the interface rules dire	fault is Checked. :ked flowbits. Any rules that set these dependent flowbits will be ectory.
Select the rulesets (Categories) Snort will load at startup	
 Category is auto-enable Category is auto-disal 	led by SID Mgmt conf files bled by SID Mgmt conf files	
		Select All Unselect All Save
Enable	Ruleset: Snort GPLv2 Community Rules	
	Snort GPLv2 Community Rules (Talos certified)	
rules are not enabled.	Snort Subscriber rules are not enabled.	Snort OPENAPPID rules are not enabled.
	B Save	

Dans la catégorie WAN Preprocs cochez les options suivantes

ervices / Sn	ort / Interfac	ce Setting	s/ WAI	N - Prepr	ocessors an	d Flow					0
nort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
AN Settings	WAN Categories	WAN Rules	WAN V	ariables	WAN Preprocs	WAN IP Rep	WAN L	ogs			
nportant Prepr les may be depende o not disable any def eprocessors, trying r	ocessor Inform ent on enbled preproc sult-enabled preproce resetting all preproces	nation ressors! Disabling essors on this pa ssor configuration	preprocessi ge unless yo ns to their de	ors may result u are very skill faults, and the	in Snort startup faili led with using Snort. en attempt to start S	ire unless all of the If you experience s nort.	correspondi Snort start-up	ng preprocessor c errors or failures	dependent rules ar after making chan	e also disabl ges to	ed.
eprocessors B	asic Configura	tion Settings	1								e
Enable Performan St	ats Snort will an Statistics m	Performance Sta utomatically ger hay be viewed or	atistics for the nerate perforn the LOGS 1	his interface. rmance stati: tab for this in	Default is Not Che stics for this interfa terface. Performan	cked. ce. Enabling this ce Statistics are o	option may I lisabled by d	nave a slight neg lefault.	ative performanc	e impact.	
Protect Customia Preprocessor Ru	ted Enable to Les Enable this updates. Th option unch	his only if you m only if you use only only if you use only if you use only if you use only only only only only only only only	aintain cust customized ibled when t	tomized prep preprocessor Snort Subscri	rocessor text rules r text rules files and iber Rules downloa	files for this inter I you do not want d is not enabled o	face. Default them overw in the Global	t is Not Checked ritten by automa Settings tab. M	tic Snort Subscril ost users should	per Rules leave this	
Auto Rule Disa	ble 🗹 Auto-dis	able text rules d	lependent o	n disabled pr	eprocessors for thi	s interface. Defau	ilt is Not Che	ecked.			
	Enabling thi preprocessi compromis	is option allows ors you have not e the level of pro	Snort to aut t enabled, Ti stection by a	omatically di his may facili automatically	sable any text rules tate starting Snort disabling detection	s containing rule o without errors rel n rules. Enabling t	options or co ated to disat his feature v	intent modifiers bled preprocesso vill result in decr	that are depende ors, but can subst eased protection	nt upon the antially from Snort.	
able RPC Decode a Back Orifice Detec	and 🔽 Normali. stor	ze/Decode RPC	traffic and o	detects Back	Orifice traffic on th	e network. Defau	t is Checked	E.			
Enable DCE/RP Detect	C2 The DCE	RPC preproces	ssor detects	and decodes	s SMB and DCE/RP	C traffic, Default	s Checked.				
Enable SIP Detect	ion 🛛 🔽 The SIP	preprocessor de	ecodes SIP	traffic and de	tects vulnerabilitie:	. Default is Chec	ked.				

Services / Snort /	Updates		(
Snort Interfaces Glob	al Settings Updates	Alerts Blocked Pass Lists Sup	opress IP Lists SID Mgmt Log Mgmt Sync
Installed Rule Set MD	5 Signature		
Rule Set Name/Publisher		MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset		Not Enabled	Not Enabled
Snort GPLv2 Community Ru	ules	b0c300c5610bb3793c46cdd7655916b5	Tuesday, 18-Mar-25 10:02:16 UTC
Emerging Threats Open Ru	les	Not Enabled	Not Enabled
Snort OpenAppID Detectors	s	Not Enabled	Not Enabled
Snort AppID Open Text Rule	es	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP	' Rules	Not Enabled	Not Enabled
Update Your Rule Set			
Last Update	Mar-18 2025 10:08	Result: Success	
Update Rules	Vpdate Rules		🛃 Force Update
	Click UP the MD5 Check for a	nd install only new updates of the latest version	dates for selected rules packages. Clicking FORCE UPDATE will zero ou s of the enabled rules packages.
Manage Rule Set Log			
	View Log		T Clear Log
	The log file is limited to	1024K in size and is automatically cleared when that I	limit is exceeded.

Créer une Pass list (Revenir sur Wan Setting pour valider

Configured Pass Lists	
Tables Astron	
List Name Assigned Description Ac pfSenseInterfaces No	ions

Services / Snort /	Pass Lis	t / Edit									6
Snort Interfaces Glob	al Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
General Information											
Name	pfSenseInte	rfaces									
	The list name	e may only cor	sist of the c	haracters 'a-z,	A-Z, 0-9 and _'.						
Description											
	You may ente	er a descriptio	n here for yo	ur reference.							
Auto-Generated IP Ad	ldresses										
Local Networks	Add firew	all Locally-Att	ached Netwo	orks to the list	(excluding WAN)	. Default is Chec	cked.				
WAN Gateways	Add WAN	Gateways to	the list. Defa	ult is Checked	Le la						
WAN DNS Servers	🛃 Add WAN	DNS servers	to the list. De	efault is Check	ed.						
Virtual IP Addresses	🗹 Add Virtu	al IP Addresse	s to the <mark>lis</mark> t.	Default is Che	ecked.						
VPN Addresses	Add VPN	Addresses to	the list. Defa	ault is Checked	i.						
ustom IP Addresses	and Config	ured Firew	all Aliase	S							
Hint	Enter as man name) direct and updated	ly IP addresse ly! To use a FC by the firewall	s or <mark>alias na</mark> IDN, first cre . You can al:	mes as desire ate the neces so provide an l	d. Enter ONLY an sary firewall alias P subnet with a p	IP address, IP si , and then provid roper netmask	ubnet or alias de the alias na of the form ne	name! Do NOT e me here. FQDN a twork/mask suc	nter a FQDN (full) aliases are period h as 1.2.3.0/24.	y qualified o ically re-res	don
IP or Alias	Address					Dele	ste				
	D Save	Add IP									

Services / Snort	/ WAN - Interface Settings	0
Snort Interfaces Glob	ibal Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt	Sync
WAN Settings WAN	Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs	
General Settings		
Enable	Z Enable interface	
Interface	WAN (igc0) ~	
	Choose the interface where this Short instance will inspect traffic.	
Description	WAN	
	Enter a meaningful description here for your reference.	
Snap Length	1518	
	Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.	
Alert Settings		
Send Alerts to System Log	Short will send Alerts to the firewall's system log. Default is Not Checked.	
Enable Packet Captures	Checking this option will automatically capture packets that generate a Snort alert into a topdump compatible file	
Packet Capture File Size	128	
	Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet directory /var/log/snort/snort_igc09545 is rotated and a new file opened.	capture file in
Enable Unified2 Logging	Checking this option will cause Short to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for th Default is Not Checked.	iis interface.
	Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.	
Block Settings		
Block Offenders	Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.	

Serv	rices / Sn	ort / Interfac	es									Ø
Snort	Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Inter	face Setting	gs Overview										
	Interface	Snort	Status	Patte	ern Match	Blo	cking Mode		Description	Actio	าร	

- North	Interface	5	Global Setti	ngs Upo	Jates Alerts	Blocked Pas	is Lists Suppress		Ngini Cog Mgi	пі зупс
WAN	Settings	۷	VAN Categor	ies WA	N Rules WAN Va	riables WAN	Preprocs WAN IP Rep	WAN Logs		
Avail	lable Ru	ıle Ca	tegories							
c	Category S	Selectio	SIN: GPL	v2_communit	y.rules		~			
			Selec	t the rule cate	gory to view and man	age.				
Rule	Signate	ure ID	(SID) Ena	ble/Disab	le Overrides					
	SI	D Actio	ns 🖬 🖌	eely	C' Result	All	C Reset Current	🛞 Disable All	0	Enable All
			When	finished, clic	k APPLY to save and s	end any SID enable.	/disable changes made on 1	his tab to Snort.		
Contraction of the	THE REAL PROPERTY OF	1015	3							
Rule: Selec Legend	s View cted Ca d: Ø Defi	Filter tegor ault Enal	y's Rules	oled by user	Auto-enabled by SID Mg	mt 🙁 Action/conten	t modified by SID Mgmt 🛕 R	le action is alert.		
Rules Selec Legend	s View cted Ca d: Ø Def 8 Def Action	Filter tegor ault Enal ault Disa GID	y's Rules bled 🔮 Enab bled 😵 Disa SID	oled by user 🔇 bled by user 🧔 Proto	Auto-enabled by SID Mg Auto-disabled by SID Mg Source	mt 😳 Action/conten mt SPort	t modified by SID Mgmt 🛕 R	le action is alert DPort	Messag	
Rules Selec Legend State	s View cted Ca d: Opfi S Defi Action	Filter tegor ault Enal ault Disa GID 1	y's Rules bled C Enab bled Disa SID 105	oled by user & bled by user & Proto tcp	Auto-enabled by SID Mg Auto-disabled by SID Mg Source \$HOME_NET	mt O Action/conten mt SPort 2589	t modified by SID Mgmt A R Destination \$EXTERNAL_NE	de action is alert DPort F any	Message MALWA Dagger,	RE-BACKDOOR - 1.4.0
Rules Selec Legend State (8) (8)	s View cted Ca d: ② Def. (※ Def. Action (Action) (A	Filter tegor ault Enal ault Disa GID 1	y's Rules bled © Enab bbled © Disa SID 105 108	bled by user Control of the proto of the pro	Auto-enabled by SID Mg Auto-disabled by SID Mg Source \$HOME_NET \$EXTERNAL_NET	mt O Action/conten mt SPort 2589 any	t modified by SID Mgmt A R. Destination SEXTERNAL_NE SHOME_NET	de action is alert DPort T any 7597	Messag MALWA Dagger MALWA Worm C	RE-BACKDOOR - 1.4.0 RE-BACKDOOR QAZ dient Login access
Rules Selec Legend State (®) (®) (®)	s View 1 cted Ca d: ② Def Action Action	Filter tegor ault Enal ault Disa GID 1 1	y's Rules bled C Enab SID 105 108 110	eled by user Contract of the point of the po	Auto-enabled by SID Mg Auto-disabled by SID Mg Source SHOME_NET SEXTERNAL_NET SEXTERNAL_NET	mt Action/conten pmt SPort 2589 any any	t modified by SID Mgmt A R Destination SEXTERNAL_NE SHOME_NET SHOME_NET	de action is alert DPort T any 7597 12345:12	Messag MALWA Dagger. MALWA Worm C 346 MALWA getinfo	RE-BACKDOOR - .1.4.0 .RE-BACKDOOR QAZ ilient Login access .RE-BACKDOOR nett
Rules Selec Legend State (&) (&) (&) (&) (&) (&) (&) (&) (&) (&)	s View cted Ca d: ② Def. Action Action	tegor ault Enal ault Disa GID 1 1	y's Rules bled © Enab bled © Disa SID 105 108 110 115	Ned by user Colored by User Co	Auto-enabled by SID Mg Auto-disabled by SID Mg Source SHOME_NET SEXTERNAL_NET SEXTERNAL_NET SHOME_NET	mt Action/conten mt SPort 2589 any any 20034	t modified by SID Mgmt A R Destination SEXTERNAL_NE SHOME_NET SHOME_NET SEXTERNAL_NE	de action is alert DPort r any 7597 12345:12 r any	Message MALWA Dagger, MALWA 346 MALWA getinfo MALWA NetBus establis	RE-BACKDOOR - 1.4.0 RE-BACKDOOR QAZ lilent Login access RE-BACKDOOR nett RE-BACKDOOR Pro 2.0 connection hed
Rules Selec Legend State (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	s View cted Ca d: ② Def. Action A A A A	tegor ault Enala ault Disa GID 1 1 1 1	y's Rules bled © Enab bled © Disa SID 105 108 110 115 115	Ned by user Colored by User Co	Auto-enabled by SID Mg Auto-disabled by SID Mg Source SHOME_NET SEXTERNAL_NET SEXTERNAL_NET SHOME_NET SHOME_NET	Action/conten sPort 2589 any any 20034 any	t modified by SID Mgmt A R Destination SEXTERNAL_NE SHOME_NET SHOME_NET SEXTERNAL_NE SEXTERNAL_NE	de action is alert DPort r any 7597 12345:12 r any r any	Message MALWA Dagger, MALWA Worm C 346 MALWA getinfo MALWA NetBus establis MALWA Infector	RE-BACKDOOR - 1.4.0 RE-BACKDOOR QAZ dilent Login access RE-BACKDOOR nett RE-BACKDOOR Pro 2.0 connection hed RE-BACKDOOR 1.x

HARA SE									
vailab	le Rule	Catego	ries						
Cate	gory Sele	ction:	GPLv2_commun	ity.rules		0			
			Select the rule cat	egory to view	v and manage.				
ule Si	gnature	ID (SID) Enable/Disat	ole Overrid	les		6		
	SID A	ctions	Apply	ADDIVA-	C Reset All	C Heart Current	Disable All	C Enable All	
ulee V	liow Fil	lot	when tinished, cli	CK APPLY 10	save and send any SID enable	/disable changes made on this	tab to Short.	Enable all rules in	the currently selected catego
electe	d Cate	lorv's R	ules					ĭ	
gend: (Default	Enabled	Enabled by user	Auto-enable	d by SID Mgmt 🙁 Action/conte	rt modified by SID Mgmt 🛕 Rule a	ction is alert		
(Default	Disabled	Disabled by user	Auto-disabk	ed by SID Mgmt				
te A	ction G	ID SID	Proto	Source	SPort JET 2589	Destination	DPort	Message	
-		103	i icp	SHOWE	VE1 2309	SEATERNAL MET	any	Dagger_1.4.0	
	1	108	tcp	\$EXTERN	IAL_NET any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access	
-	∆ 1	110	tcp	\$EXTERN	IAL_NET any	SHOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo	
	A 1	115	tcp	SHOME_1	NET 20034	\$EXTERNAL_NET	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established	
1	A 1	117	tcp	\$HOME_1	NET any	\$EXTERNAL_NET	any	MALWARE-BACKDOOR Infector.1.x	
1	A 1	118	tcp	\$HOME_N	NET 666	\$EXTERNAL_NET	any	MALWARE-BACKDOOR SatansBackdoor 2.0 Beta	
WAN :	Interfac Settings able R	es i V tule Ca	Global Settings VAN Categories	s Upo	jates Alerts	Blocked Pass Lists ables WAN Preproc	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
Snort WAN : Avail Ca	Interfac Settings able R ategory	es i I ule Ca Selectio	Global Settings VAN Categories ttegories on: <u>GPLv2</u> Select th	s Upo	Jates Alerts N Rules WAN Vari y.rules egory to view and manaç	Blocked Pass Lists ables WAN Preproc	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
Snort WAN : Avail C: Rule	Interfac Settings able R ategory Signa	es tule Ca Selectio	Global Settings VAN Categories Itegories Select th (SID) Enabl	s Upo WA .communit ne rule cate	Jates Alerts	Blocked Pass Lists ables WAN Preproc	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
Snort WAN : Avail Ca Rule	Interfac Settings able R ategory Signa	es ule Ca Selectio ture ID	Global Settings VAN Categories Integories Select th (SID) Enabl Ins PAPP	s Upo WA .communit ne rule cate e/Disab	Jates Alerts N Rules WAN Vari y.rules egory to view and manage le Overrides C Reset A	Blocked Pass Lists ables WAN Preproc je.	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
Snort WAN : Cu Rule	Interfac Settings able R ategory Signa	es tule Ca Selectio ture ID ID Actio	Global Settings VAN Categories tegories on: GPLv2. Select th (SID) Enabl ns PAPP When fir	s Upo WA .communit ne rule cate e/Disab	tates Alerts N Rules WAN Vari y.rules egory to view and manag le Overrides k APPLY to save and ser	Blocked Pass Lists ables WAN Preproc le.	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
WAN : Avail C: Rule	Interfac Settings able R ategory Signa S	es aule Ca Selectio ture ID ID Actio	Global Settings VAN Categories ntegories on: GPLv2, Select th (SID) Enabl ns App When fir	WAI WAI communit ne rule cate e/Disab	Sates Alerts N Rules WAN Vari y,rules egory to view and manag le Overrides Resert A k APPLY to save and ser	Blocked Pass Lists ables WAN Preproc	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
WAN : Avail C: Rule	Interfac Settings able R ategory Signa S s View	es ule Ca Selectio ture ID ID Actio	Global Settings VAN Categories Itegories Select th (SID) Enabl When fir	s Upc WA communit ne rule cate e/Disab	Jates Alerts N Rules WAN Vari y,rules regory to view and manage le Overrides Remot A k APPLY to save and ser	Blocked Pass Lists ables WAN Preproc e. e.	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs © Disable All his tab to Snort.	Log Mgmt Sync
WAN : Avail C Rules Rules	Interface Settings able R ategory Signa S Signa S S View	es s I s Selection ture ID ID Action Filter ategor	Global Settings VAN Categories on: GPLv2. Select th (SID) Enabl ms App When fir y's Rules	s Upo WAI .communit ne rule cate e/Disab	Jates Alerts N Rules WAN Vari y,rules egory to view and manag le Overrides C Reset A k APPLY to save and ser	Blocked Pass Lists ables WAN Preproc le.	Suppress s WAN IP Rep	IP Lists SID Mgmt WAN Logs	Log Mgmt Sync
WAN : Avail C Rule Selec	Interface Settings able R ategory Signa S Signa S S View Sted C E : O Dr	es uule Cá Selectio ture ID ID Actio Filter fault Ena fault Ena	Global Settings VAN Categories ttegories on: GPLv2, Select th (SID) Enable ms App When fir Y'S Rules bled S Disable	s Upc	Sates Alerts N Rules WAN Vari y,rules egory to view and manaç le Overrides k APPLY to save and ser Auto-enabled by SID Mgm Auto-enabled by SID Mgm	Blocked Pass Lists ables WAN Preproc e. d any SID enable/disable t	Suppress s WAN IP Rep weet Current changes made on th d by SID Mgmt A Rul	IP Lists SID Mgmt WAN Logs © Disable All his tab to Snort.	Log Mgmt Sync
WAN : Avail C Rules Selec egend	Interfactors Setting: able R able R ategory Signal S Signal S Signal S Signal S Signal S Signal S Signal S Signal S Signal S Setting: Setting:	es uule Cá Selection ID Action Filter ategori fault Ena fault Diss GID	Global Settings VAN Categories ttegories on: GPLv2, Select th (SID) Enable (SID) Enable When fir y's Rules bled © Enabled bled © Disablet SID	s Upc	Sates Alerts N Rules WAN Vari y,rules egory to view and manage le Overrides k APPLY to save and ser Auto-enabled by SID Mgm Auto-disabled by SID Mgm Source	Blocked Pass Lists ables WAN Preproc e. e. d any SID enable/disable t SPort	Suppress s WAN IP Rep weet Current changes made on th d by SID Mgmt A Ru Destination	IP Lists SID Mgmt WAN Logs WAN Logs bis tab to Snort.	Log Mgmt Sync
WAN 1 Avail C Rules Rules Selec egend ate	Interfac Settings able R ategory Signa S S View Sted C E S View S View Action	es ule Ca Selection ID Action Filter fault Ena fault Disc GID 1	Global Settings VAN Categories Ategories on: GPLv2, Select th (SID) Enable (SID) Enable When fir y's Rules bled © isabled SID 105	s Upc WA communit er rule cate e/Disab	Sates Alerts Alerts N Rules WAN Vari y,rules regory to view and manage regory to view and manage Re Overrides Reference Al Auto-enabled by SID Mgm Auto-disabled by SID Mgm Source SHOME_NET	Blocked Pass Lists ables WAN Preproce e	Suppress S WAN IP Rep Seet Current Changes made on th d by SID Mgmt A Ru Destination SEXTERNAL_NET	IP Lists SID Mgmt WAN Logs WAN Logs Cisable All his tab to Snort.	Log Mgmt Sync
WAN : Avail C: Rule Selec egend ate	Interfac Settings able R ategory Signa S Signa S View Cted C C S view Action	es ule Cr Selection ID Action ID Action Filter GID 1 1	Global Settings VAN Categories Ategories on: GPLv2. Select th (SID) Enable (SID) Enabled When fir y's Rules bled © Enabled SID 105 108	s Upc WA communit er rule cate e/Disab y hished, clic by user (d by user (d b) user (d	Sates Alerts N Rules WAN Vari y,rules gory to view and manage gory to view and manage le Overrides CC Reset A Auto-enabled by SID Mgm Auto-disabled by SID Mgm Source SHOME_NET \$EXTERNAL_NET	Blocked Pass Lists ables WAN Preproc e	Suppress S WAN IP Rep Seet Comm Changes made on th Changes made on th SEXTERNAL_NET SHOME_NET	IP Lists SID Mgmt WAN Logs WAN Logs WAN Logs Uisable All his tab to Snort. ke action is alert DPort any 7597	Log Mgmt Sync
WAN : Avail C: Rules Seleccegend ate	Interfac Settings able R ategory Signa S Signa S View Cted C C E S D Action Action	es ule Ca Selection ID Action ID ID Action ID ID I	Global Settings VAN Categories Ategories on: GPLv2. Select th (GID) Enable (GID) Enabled When fir V's Rules SID 105 108 110	s Upc WA communit er rule cate e/Disab y hished, clic by user @ hished, clic by user @ Proto tcp tcp tcp	Sates Alerts Alerts Alerts N Rules WAN Variation of the second se	Blocked Pass Lists ables WAN Preproc e	Suppress Sup	IP Lists SID Mgmt WAN Logs WAN Lo	Log Mgmt Sync
WAN : Vail Ci Rule Selec egend ate	Interfac Settings able R ategory Signal S S View ted C E @ De Action Action A	es I ule Ca Selection ID Action Filter fault Ena fault Diss GID 1 1 1 1 1	Global Settings VAN Categories Ategories Carter Select th (SID) Enable (SID) Enab	s Upo wAl communit he rule cato e/Disab y hished, clic by user @ Proto top top top top	Sates Alerts Alerts N Rules WAN Variation of the second of	Blocked Pass Lists ables WAN Preproc e	Suppress s WAN IP Rep weet Current changes made on th d by SID Mgmt A Ru Destination SEXTERNAL_NET SHOME_NET SHOME_NET SEXTERNAL_NET	IP Lists SID Mgmt WAN Logs WAN	Log Mgmt Sync
WAN : Avail C: Rules Select egend ate	Interfac Settings able R ategory Signal S S View sted C Action Action A Action A	es I Iule Ca Selection ID Action Filter Ategory fault Ena fault Diss GID 1 1 1 1 1 1	Global Settings VAN Categories Ategories Select th (SID) Enable (SID) Enable (SID	s Upo wA .communit er rule cato e/Disab y hished, clic by user @ Proto top top top top top	Sates Alerts Alerts Alerts N Rules WAN Variation of the second of the se	Blocked Pass Lists ables WAN Preproce e	Suppress Sup	IP Lists SID Mgmt WAN Logs WAN Logs Cisable All his tab to Snort. Reaction is alert DPort any 12345:12346 any any any	Log Mgmt Sync
Snort WAN : Avail C: Rules Select .egend tate	Interfac Settings able R ategory Signa S S View Sted C C C C Action Action A A	es I ule Ca Selection ID Action ID ID Action ID ID Action ID ID Action ID ID Action ID ID I	Global Settings VAN Categories Ategories Select th (GPLv2, Select th (GID) Enable (GID) Enable	s Upc wA communit ne rule cate e/Disab y nished, clic d by user tcp tcp tcp tcp tcp tcp tcp	Sates Alerts Alerts Alerts Alerts N Rules WAN Variation of the second of	Blocked Pass Lists ables WAN Preproc e	Suppress Sup	IP Lists SID Mgmt WAN Logs WAN Logs Cisable All Cisable All Cisa	Log Mgmt Sync