CXS1779BCN

### vmware<sup>®</sup> EXPLORE

## Demystifying Distributed Security

Tim Burkard (He/Him/His) Staff Technical Learning Engineer

#vmwareexplore #CXS1779BCN



#### **Required Disclaimer**

- This presentation may contain product features or functionality that are currently under development.
- This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

#### Presenter



#### Tim Burkard

#### Staff Technical Learning Engineer

Tim is a VMware employee and has been a technical instructor for 20+ years. He has trained IT professionals in the areas of operating systems, security and networking. Tim specializes in teaching VMware NSX and has previously taught courses covering the entire vSphere product line.





#### NSX-T Data Center Distributed Protection



## You Shall Not Pass!

#### NSX-T Data Center Distributed Protection



# Fly, you Fools!



## VMware NSX Distributed Protection









Distributed Firewall (DFW) Policy contains rules



The Rules in the MiddleEarthPolicy rejects specific VM to VM communication while allowing intra-segment traffic and oneway traffic from Shire to Moria.

The Policy Default rejects anything not allowed leading to Zero Trust

Distri	buted Firewall	hiles						
								ACTIONS V REVERT PUBLIS
Λ Ident	tity Firewall is disabled. Rules co	ntaining groups with identity e	entities (e.g. AD groups), will not be enfo	rced.				Enab
	ETHERNET (1)		INFRASTRUCTURE (5)	ENVIRONMENT (15)	APPLICA			
		CLONE SUN						Filter by Name, Path and more
	Name		Sources	Destinations	Services	Context Profiles	Applied To	Action
	MiddleEarthPolic	y (7) Applied T						
	Sackville-Nope	3055	🖧 0-ME-Sackville	🖧 0-ME-Sackville		None	DFW	🔴 _ Reject 🛛 🗸 🛞 🖗
	Khazad-Dum-Nope	e 3056	음음 1-ME-Balrog 응음 1-ME-Khazad	음을 1-ME-Khazad 음을 1-ME-Balrog			DFW	🔴 _ Reject 🛛 🗸 🍥 🖗
	SSH-MiddleEarth	1018	22 MiddleEarth	Ba MiddleEarth	♦ SSH	🐻 SSH	DFW	● <u>Allow ~</u> C @ @
	ShiretoMoria	1014	22 Shire	B-0 Moria		None	DFW	● <u>Allow ~</u> C @ @
	WithinMoria	1015	🖁 Moria	Ba Moria			DFW	● _Allow @ @
	WithinShire	1016	Shire	88 Shire			DFW	● <u>Allow ~</u> € @ @
	DefaultReject	1017					DFW	🔴 Reject 🗸 🌔 🖗 🛛

Tagging Virtual Machines as an attribute of the VM

	Virtu	ual N	Macl	nines						
Inventory Overview										
🗘 Services										EXPAND ALL
B Groups				Name	Source	Tags		Operating System		Power State
G Context Profiles				Log-insignt						Unning United States
🗿 Virtual Machines				ME-Balrog				Ubuntu Linux (64-	bit)	Running
<ul> <li>Containers</li> <li>Physical Servers</li> <li>Tags</li> </ul>				ME-Bilbo	192.168.0.99	Tag \$cope Max 30 allowed. Click (+) to add. No Items Found		Übuntu Linux (64-	bit)	
						MiddleEarth Shire X Total: 1				
				Computer Name	ME-Bilbo		Compute M	Manager	vcsa7.middle	
				Instance ID	50367f39-4dda-a2e8-479f-0be	53c173dac 🕦	External ID		50367f39-4d	da-a2e8-479f-0be53c173da
				Host Local ID			Managed (	Object ID	64 🕕	
				BIOS ID	423682c8-84d3-c7f8-d27c-3afe	3bc80dce ①	Location II		564df8dc-9f	a2-62d1-9a59-a24302212167
				ME-DeepDark	192.168.0.99			Ubuntu Linux (64-	bit)	Running
				ME-Frodo	192.168.0.99			Ubuntu Linux (64-	bit)	Running
								111	L-143	

Put a Group Together using the Tags

Home	Networking	Security	Inv	entory	Plan & Troubleshoot	System		
		C	Group	s				
Inventor	y Overview							
Services			ADD GR	OUP				
🔡 Groups					Name			Compute Members
🐻 Context	Profiles			88	Group-5 (AllTenants-6Aug			
📅 Virtual M	lachines			8.8	Group-6 (AllTenants-6Aug	3)		
🛄 Containe	ers				MiddleEarth			1 Criteria
🚦 Physical	Servers						<u> </u>	
📎 Tags					Description	Description		
					RAVE			
					SAVE			

Select Members   MiddleEarth		×
Add Compute Members either by creating or by Compute members to define effective membersh	directly adding them. You can also add Identity members sepa hip of the group.	rately. Identity members intersect with the
Membership Criteria (1) Members (0) IP	Addresses (0) MAC Addresses (0) AD Groups (0)	
+ ADD CRITERIA		Maximum: 5 Criteria
✓ Criteria 1		
Virtual Machine V Tag	<u>✓ Equals ∨</u> <u>MiddleEarth ⊗ ∨</u> Scope (	Moria           
		CANCEL

Source, Destination and the Applied to Fields were populated by Groups built on Security Tags

All Rules Category Specific Ru	ıles							
	_							VERT PUBLI
A Identity Firewall is disabled. Rules con	taining groups with identity entitie:	s (e.g. AD groups), will not be enfo	prced.					<u>Ena</u>
			ENVIRONMENT (15)	APPLICA				
							Filter by Name, Path an	d more
Name		Sources	Destinations	Services	Context Profiles	Applied To	Action	
: V 🗌 MiddleEarthPolicy	(7) Applied To 1							
: Sackville-Nope	3055	8     0-ME-Sackville       8     0-ME-Bilbo	0-ME-Sackville	Any	None	DFW	eject	<u>~</u> C @
: C Khazad-Dum-Nope	3056	22 1-ME-Balrog	🖧 1-ME-Khazad	Any		DFW	e Reject	<u>~</u> C @
SSH-MiddleEarth	1018	器 MiddleEarth	🖁 MiddleEarth	♦ SSH	🐻 SSH	DFW	Allow	<u>~</u> 💽 @
: ShiretoMoria	1014	Shire	Ba Moria	Any	None	DFW	Allow	~ <b>(</b> ) @
	1015	문문 Moria	88 Moria	Any		DFW	Allow	~ <b>(</b> ) @
: WithinMoria								
: WithinMoria : WithinShire	1016	22 Shire	Shire	Any		DFW	Allow	<u>~ ()</u> @

#### NSX Distributed Protection Groups make life easier to populate DFW fields in each rule

#### Two options for Applied to: Policy and each rule. Policy has priority.

Distribu	uted Firewall			
All Rules	Category Specific Ru	les		
A Identity	Firewall is disabled. Rules cont	taining groups with identity	entities (e.g. AD groups), will not be e	nforced.
				ENVIRONMENT (15)
+ ADD POL				
	Name		Sources	Destinations
	MiddleEarthPolicy	(7) Applied 1	To 1 Groups	
	Sackville-Nope	3055	88 O-ME-Sackville	C-ME-Sackville
				0-0 - ME-BILDO
	Khazad-Dum-Nope	3056	88 1-ME-Khazad	Sa I-ME-Knazad
	SSH-MiddleEarth	1018	88 MiddleEarth	Sa MiddleEarth
			P9 china	PR Mada
	ShiretoMoria	1014	53 Shire	5.5 Moria
	WithinMoria	1015	B장 Moria	BB Moria
		1016	22 Shire	22 Shire
	vvitninsnire			

<u> </u>								
(1) P	olicy I Appli	evel ' ed To		d To' entities mentioned here, will take preceder	ice over rule level 'Applied To' en	lities of the same po	licy.	
Middle	Earth							
vildale	Earth							
ADD	GROU	P					Filter by Name, Path and more	
				Name	Compute Members		Status	
2				MiddleEarth			🥚 Success 😋	
			88				🥚 Success 🖱	
			0-0	A NLB.PoolLB.[dns][ShireLB]	View Members		🥥 Success C	
			80		View Members		😑 Success C	
			0-0 8-0	A NLB.VIP.[asdf]	View Members		🔵 Success 🖱	
1				A. NI R. VID (ShireVID)	View Members		Success (* 1 - 28 of 28 Gr	
							Show Only Selected	
							CANCEL	PLY

When using the Applied To field for the Policy, the Rule Applied To is prioritized over the Applied To for each rule.

Two options for Applied to: Policy and each rule. Policy has priority.

When using the Applied To field for the Policy, the Rule Applied To is prioritized over the Applied To for each rule. But if Policy is applied to DFW, Rule can be very granular.

								ACTIONS ~ REVERT	PUBL
LL RU	ILES CATEGORY SPECI	FIC RULES							
			INFRASTRUCTURE (0)		APPLICATION (3)				
+ AD	D POLICY + ADD RULE		DO 🔟 DELETE					Filter by Name, Path and more	
	Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action	
	MIDDLE-EARTH-PC	(7) Applied 1						Success (	
	Khazad-Dum-Nope	3049	88 Balrog 88 Khazad	88 Balrog 88 Khazad		None	22 Bairog 22 Khazad	🔴 _Reject 🗸 🥑	0
	Sackville-Nope	3050	22 Bilbo 22 Sackville	22 Bilbo 22 Sackville	Any	None	88 Bilbo 88 Sackville	e <u>Reject v</u>	0
	SSH-MiddleEarth	3051	22 MiddleEarth	28 MiddleEarth	O SSH	🗟 SSH	22 MiddleEarth	Allow ~ 🤇	) @
		3052	28 Moria	00 Moria		None	Sa Moria	Allow - 🤇	) @
	U Within-Moria			99 Shire		None	22 Shire	🔵 Allow 🗸 🧲	) @
	Within-Moria	3053	22 Shire	00 01110					
	Within-Moria	3053 3054	Sthire	88 Moria		None	Shire     88     Moria	o <u>Allow ~</u> 🤇	) @

Let's examine Distributed Intrusion Detection and Prevention

Intrusion Detection and Prevention are enabled in the Settings – Shared Tabs by Individual Cluster or All Standalone Hosts

IDS/	/IPS	& Malware Prevention				
Distril	buted	Rules Gateway Rules Profiles Settings				
Share	di	IDS/IPS Malware Prevention				
	Inter	net Connectivity				
	Go T	o Internet Proxy Server				
	Defin	e Scope for Malware Prevention & IDS/IPS Deployment				
	~ A	tivate Hosts & Clusters for East-West Traffic				
	Host			IDS/IPS		
	All S	tandalone Hosts		•	Off	
	#IDS/	IPS Enabled Clusters				
	() E	efore starting the service deployment, ensure that all the prerequisit istructions. After completing the prerequisites, click the link in below	es for deploying the NSX Distributed Malware Prevention service are or table to deploy the service.	ompleted.	Click 'View Prerequisites' fo	r detailed View Prerequisites
	TURN	TURN OFF			Filter t	ny Name, Path and more 🔤
		Cluster Name	Compute Manager	IDS/IPS		Malware Prevention (Defined in Service VM deployment)
		Compute-Cluster	sa-vcsa-01.vclass.local	0	Off	0 Deployment(s)
	D	Management-Cluster	sa-vcsa-01.vclass.local		Off	0 Deployment(s)

Distributed Intrusion Detection and Prevention Signatures



We then look at the Signature Database.

#### **Distributed Intrusion Detection and Prevention Signatures**

	Distributed R	ules Gateway Rules Profiles Setting	<u>is</u>	Globally	I Intrusic	on Signatı	Ire Management ctions or exclude specific sigr						
	Shareu					EXCLUDE GLOB	IALLY				Filter by	Signature ID, Details	i, Product
	Intrusion Dete	ction and Prevention Signatures			Signature ID	IDS Severity	Details	Affected	Attack Target	Attack Type	cvss	:VE(S) Action ()	State
	Version	Aug 2, 2022, 8:59:03 AM Osuccess C	View and change ver		1060759				Client_Endpoi nt	trojan-activity		Reject	- 5
		Auto Update new versions (recommende	d)				NSX - Detect Zeus activity		Client_Endpoi nt	trojan-activity		Alert	<u>~</u>
	Manage	8494 Intrusion Signatures View and manage	global signature set>>	0 1	106110801		NSX - Detect NetwiredRC		Client_Endpoi nt	trojan-activity		Reject	
		Globally excluded 0 Signatures globally change	ged by user O	0					Client_Endpoi	trojan-activity		Alert	
							NSX - Detect Locky		Client_Endpoi	trojan-activity		Reject	~ 🔍
						High	NSX - Detect Angler EK		Client_Endpoi	attempted-		Reject	
							NSX - Detect Admedia Angler EK		Client_Endpoi	attempted- user		Reject	
						High	- NSX - Detect Angler EK		Client_Endpoi nt	attempted- user		Alert	- •
					106122801	High	NSX - Detect Angler EK	NONE	Client_Endpoi nt	attempted- user		Reject	
Ne then look at t	he Signa	ture Database.			1061234	High	NSV - Detect Malicious	NONE	Client Endooi	attemptede			
					RESH						، ۲ <u>۲</u>	1 / 170 > >	1 - 50 of
The default action	h for the i	maiority of the		🅥 si									
		5 5											

This fact becomes important in Intrusion Prevention.

#### Distributed Intrusion Detection and Prevention Profiles

Name		Description	Taga	EXPAN	ID ALL Filter by N	status
Custom-IDS-Profile		Description	0 _ Max 30	Tag allowed. Click (+) to add.	Scope	
IDS Signatures Included: Intrusion Severities Critical (4857) V Hit Additional Options	1467 Total: 8494 gh (3214) 🔲 Medium (25) 🗌 Low	(2) 🔽 Suspicious (396)				
IDS Signatures Included: Intrusion Severities Critical (4857) Intervention Additional Options Filter Intrusion signatures	3467 Total: 8494 gh (3214) Medium (25) Low to include in this profile by attack type,	(2) Suspicious (396) CVSS and more.	0/6		]	
IDS Signatures Included: Intrusion Severities Critical (4857) IIII Additional Options Filter Intrusion signatures Attack Types Attack Targets	3467 Total: 8494 gh (3214) Medium (25) Low to include in this profile by attack type, Select Select	(2) Suspicious (396) CVSS and more.	CVSS Products Affected		]	
IDS Signatures Included: Intrusion Severities Critical (4857) IIII Additional Options Filter Intrusion signatures Attack Types Attack Types Attack Targets Manage (optional) - chan	s467 Total: 8494 gh (3214) Medium (25) Low to include in this profile by attack type, Select Select ge actions and/or exclude signatures sp	<ul> <li>(2) Suspicious (396)</li> <li>CVSS and more.</li> <li>pecific to this profile. Manage signatures for this profile.</li> </ul>	CVSS Products Affected			

Profiles are the description of the IDS Signatures to be examined, by severity and inclusion based on Types, Targets, CVSS or Products.

Distributed Intrusion Detection and Prevention Setup for Prevention (Drop or Reject)



#### If the rule is modified to **Detect** and **Prevent**...

Distributed Intrusion Detection and Prevention Setup for Prevention (Drop or Reject)

If the rule is modified to Detect and Prevent...



Distributed Intrusion Detection and Prevention Setup for Prevention (Drop or Reject)

bally customize recommended act	e Management tions or exclude specific signa	stures to tailor fit	your environmen	L						
Signature ID IDS Severity	Details	Product Affected	Attack Target	Attack Type	cvss	CVE(S) Action ()	State	Standalone hosts: Off Clusters: V	Gateways: 0/2 Last 24 Hour	s v Timeline
_ 4101536 High	SLR Alert - Apache CouchDB Remote Privilege Escalation (CVE-2017- 12635)	Apache_Couc hdb	NONE	web- application- attack	9.8	2017- 2635 Reject	✓ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	✓ • SUSPICIOUS 0	Filter by Attack Type or r	nore =
	s	uspicious Aug 2	09:49 0	9:50 09:51	¢	e52 085	First Occurrence Au	such BB Remote Privilege Esculation Ig 2, 2022, 9:53:30 AM 08:55 08:59	(CVE-2017-12635) High 08.57 08.5	3 08-5
e rule is modifie	ed	Aug 2	09:49 0	9:50 09:51		9.52 09.5	9 13 00:54	09:55 09:58	09:57 09:54	09.5
etect and vent the		impact Score (	Severity 20.10.101 Port:35731	Last Detected		Details	Use	rs Affected Workloads	CVE Details CVSS	
nature must hav action of Drop o	r	Attack Direction established.to Service	on Attack Target _server NONE Signature ID	Attack Type web-application Signature Revis	n-attack sion	Product Affected Apache_Couchd Mitre Technique	d Total Eveni Ib 1 Mitre Tactio	ts Intrusion Activity * Detecte	d Only = Prevented • Workloa	Last 14 Days ds affected
ect to effectively ent this flow	/	TCP	4101536	3			2	Jul 19 Jul 21 Jul 23	Jul 25 Jul 27 Jul 29 Jul 31	Aug 03

Distributed Intrusion Detection and Prevention Results



IPS results show in the same interface with a green bar added to the chart indicating Prevented.



## NSX Native Tools

Tools used for troubleshooting the NSX-T Data Center Distributed Firewall (DFW):

Traffic Analysis

- Traceflow
- Live Traffic Analysis

#### Traceflow



#### Traceflow

			_		
Traceflow Select the source and destination to capture observat	ons regarding when the packet is forwarded and received b	etween workloads (VMs or conta	ainers). If you have the Antrea plugi	n installed, you can choose to run a trace between the pods/service	Image: signal state of the state o
		Packet Information	reset c Type Protocol Ty	ne	
		<u>IPv4 → Unica</u> ICMP ID <u>0</u>	<u>ICMP</u> ICMP		
Source Reser	-		Destination R	IESET	
Type VM Name	Virtual Machine ME-Bibo		Type VM Name	Virtual Machine ME-Barog sector(203-a7c1-4031-b888-2a580ab/18a8	
identify a virtual inte Virtual Interface	rface for packet injection Network adapter 1	<u> « ×</u>	s; Virtual Interface	Network adapter 1	
IP Address* MAC Address*	Segment Port.default:43e82694-1219-482b-8479-b93912880 172.16.100.11 00.50-56-94:5f:f6	c38a (8) 14	IP Address <sup>®</sup> MAC Address <sup>®</sup>	Segment Port.default.747b4492-182a-4d1c-b461-d935ea8047d6 17216-200.11 00:50:56:94:0d-4e	
		ADVAN	ACED SETTINGS		
			TRACE		

#### Traceflow

					o V N
Observations All 1	Delivered 0 Dropped	Transport Node	Component	Timestamo P Address	Actions
	(Interted)		Abharde adarter 1 (0)	12/20/09 056 338	
	Received	[] sa-esai-Ot velass local	EII Distributed Firewall	1210:09.056.000	
	Forwarded			12:10:09.056.206	
•	Forwarded	🛛 sa-esxi-01 vclass Jocal	shire	12:10:09.056.225	
	Received				
	Forwarded				
•	(Received)	📋 sa-esai-01.vclass.local	හ Moria	12:10:09:057:385	
0	Received				
•	Forwarded			12:10:09:057.424	
	Delivered	🛛 sa-esxi-01.vclass.local	📾 ME-Balrog.vmx@Oc064897-ae2d-4271-8189-Ob97b4c641ca	1210:09.057.429	

© 2023 VMware, Inc.

#### Traceflow

Traceflow	P Type: IPv4 Traffic Type: Unicast Protocol Type: ICMP	Source: ME-Bilbo IP: 172.16.100.11 MAC: 00:50:56:9d:5f:16	Destination: ME-Sack IP: 172.16.100.13 MAC: 00:50:56:9d:8c	kville Aug 2, 2022, 1 c2d	214:50 PM				
	•••••	ME-Bibbo Virtual Machine 172.16.100.1	Shire Segmen	172.16.100	ME-Sackville Virtual Machine D.13	Packet Dropped Component Port Reason	Distributed Fi ME-Bibo vma 414- bdf-75 Dropped by I	× rewall #2742ceafa-8ba2- a7bb27c48 Firewall Rule	
Observations All O	Delivered 1 Dropper								-
Physical Hop Count	Observation Type	Transport Nod	le	Component		Timestamp	IP Address	Actions	
	injected			Network adapter		12:14:52:034:216			
	Received								
	Dropped by Firewall Rule	ID: 3050				12:14:52.034.372			

Discover & Plan S Discover & Take Action	Select a source for Note: Live Traffic A	<ul> <li>All ICLY SIS</li> <li>your session and enable</li> <li>nalysis is only supported</li> </ul>	one or more options to captu on overlay-backed NSX-T Da	re live traffic generated from the ta Center environments and it is	he source: Trace, Packet C is persisted only for one h	apture. You can also select one destination to cap pur.	oture bidirectional traffi	ic data.	V
C Recommendations	Session Optio	Test-Bilbo-Ping		Trace & Packet Capture	e FirstNSampling 💿	Trace Sampling value	* <u>50</u>	Packet Capture Sampling value" 500	
② IPFIX	Trace	💽 Yes 🛈		Packet Capture	🦲 Yes 🛈		value between 1101	po value versen i i	0.900
Traffic Analysis									
Consolidated Capacity		Source Reset	Matural Manhara				Destination	RESET	
		VM Name	ME-Bilbo Host/3cfc203-a7c1-4931-b88	9-24580ebf18a8			VM Name	Virtual Machine         ∨           ME-Frodo         ⑧ ∨           Nost:228375d5-0e12-4a0a-8c99-100cd33d6006         ●	
						-			
		Virtual Interface Segment Port	ME-Bilbo.vmx@742ceaf 8ba2-414c-b4df- 75a71b827c48 IP: 172:16:100:11	ar⊹.			Virtual Interface Segment Port	Network adapter 1 © ~ ME-Frodo www98c24431- 3567-49bcch77- 1/2324fa5269 #772.6 90612	
								CANCEL	RT SESSION

	Live Traffic Analysis					0
	NEW SESSION				Filter by Name, Path and more	
	Session ID	Source	Destination	Status	Created On	
_	: Test-Bilbo-Ping	ME-Bilbo Segment Port: ME-Bilbo.vmx@742ceafa-Bba2-414c-b4df- 75a71b827c48	ME-Frodo Segment Port: ME-Frodo.vmx@19c34a31-3567-49bc-b7f7- 112233fa53c9	● In Progress C	Aug 2, 2022, 12:33:16 PM	
)						
	Live Traffic Analysis					0
	NEW SESSION				Filter by Name, Path and more	
	Session ID	Source	Destination	Status	Created On	
	: Test-Bilbo-Ping	ME-Bilbo Segment Port: ME-Bilbo.vmx@742ceafa-8ba2-414c- b4df-75a71b827c48	ME-Frodo Segment Port: ME-Frodo.vmx@19c34a31-3567-49bc- b7f7-112233fa53c9	Finished	Aug 2, 2022, 12:33:16 PM	
_ /						
	Live Traffic Analysis for Test-Bill	oo-Ping		[		EW TRACE
	Live Traffic Analysis for Test-Bill	oo-Ping			RERUN DUPLICATE SESSION NE	EW TRACE
	Live Traffic Analysis for Test-Bill Observations Source ME-Bilbo Source IP 172.16.100.11	DO-Ping Destination ME-Frodo Destination IP -	Packet ID 1 @ ADVANCED SETTINGS	V Sampling Type FirstNSampling Trace Sampling value 50	RERUN DUPLICATE SESSION NE	EW TRACE
	Live Traffic Analysis for Test-Bill Observations Source ME-Bilbo Source IP 172.16.100.11 Observations All 0 Delivered 0 Dropp	Destination ME-Frodo Destination IP -	Packet ID 1 @ ADVANCED SETTINGS	V Sampling Type FirstNSampling Trace Sampling value 50	RERUN DUPLICATE SESSION NE	EW TRACE
	Live Traffic Analysis for Test-Bill Observations Source ME-Bilbo Source IP 172.16.100.11 Observations AI 0 Delivered 0 Dropp Physical Hop Count Observation Type	Destination ME-Frodo Destination IP -	Packet ID 1 @ ADVANCED SETTINGS Component	Sampling Type FirstNSampling     Trace Sampling value 50     Timestamp	RERUN DUPLICATE SESSION NE DOWNLOAD	EW TRACE
	Live Traffic Analysis for Test-Bill Observations Source ME-Bilbo Source IP 172.16.100.11 Observations AI 0 Delivered 0 Dropp Physical Hop Count Observation Type 0 Injected	Destination ME-Frodo Destination IP - red Transport Node	Packet ID 1 @ ADVANCED SETTINGS Component	Sampling Type FirstNSampling     Trace Sampling value 50     Timestamp     12:45:08.879.395	RERUN DUPLICATE SESSION NE	EW TRACE



	4	ME-I	3ilbo.vmx@742ceafa-8b	a2-414c-b	o4df-75a71b827c	48 Test-Bilbo-Pir	a Source Tue Aua 02	2 2022.pcap	<b>– –</b> X
nar-01.	File Edit View	Go Canture Analyz	Statistics Telephony	Nireless To	ools Help	-			
er 📘				~~~	2.0				
	Apply a display fi	iter <ctrl-></ctrl->							+
	No. Time	Source	Destination	Pr	rotocol Length Info				
Inn & Te		172.16.100.	172.16.100.12		CMP 98 Ech	o (ping) request	id=0x0001, seq=486	/58881, ttl=64 (no r	es
	2 1.001	140 172.16.100.	1/2.10.100.12		422224-52-0 T	b (ping) request	10=0x0001, Seq=407	/ 5915/, tt1=04 (10 1	
4		ME-Frodo.v	mx@19c34a31-3567-49	I-\T\d-Dd	12233Ta53C9_1es	t-Bilbo-Ping_Des	tination_Tue Aug 02 a	2022.pcap	
File E	Edit View Go (	Capture Analyze Statis	tics Telephony Wireless	Tools He	elp				
<b>/  </b>	1 💿 🌗 🛅	🗙 🖸 🍳 🗢 🔿 🕾	🗿 👲 📃 📃 🍳 🍳 🤅	<b>N</b> 🔛					
Appl	y a display filter <ct< td=""><td>trl-/&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td>+</td></ct<>	trl-/>							+
No.	Time	Source	Destination	Protocol	Length Info				
	1 0.000000	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seq=486/58881,	ttl=64	
	2 1.000967	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seq=487/59137,	ttl=64	
	3 2.002757	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seq=488/59393,	tt1=64	
	4 3.003324	1/2.16.100.12	172.16.100.11	TCMP	98 Echo (ping	) reply 1d=0x	0001, seq=489/59649,	tt1=64	
	6 5.006396	172.16.100.12	172.16.100.11	TCMP	98 Echo (ping	) reply id=0x	0001, seq=490/59905, 0001. seq=491/60161.	ttl=64	
	7 6.007455	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seg=492/60417,	ttl=64	
	8 7.008448	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seq=493/60673,	ttl=64	
	9 8.009950	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seq=494/60929,	ttl=64	1
	10 9.011199	172.16.100.12	172.16.100.11	ICMP	98 Echo (ping	) reply id=0x	0001, seq=495/61185,	ttl=64	
▷ Pac	ket comments								
Fra	me 3: 98 bytes o	on wire (784 bits),	98 bytes captured (784	bits) on :	interface unknow	n, id 0			
D Eth	ernet II, Src: \	/Mware_9d:dc:d5 (00:	50:56:9d:dc:d5), Dst: \	Mware_9d:	5f:f6 (00:50:56:	9d:5f:f6)			
P Int	ernet Protocol N	version 4, Src: 1/2.: assage Protocol	16.100.12, Dst: 1/2.16.	100.11					
v inc	ernet control ne	essage Protocor							P
									1
0000	00 50 56 9d 5f	f6 00 50 56 9d dc d	5 08 00 45 00 ·PV·_·	• P V•••• E	E+				
0010	00 54 15 ba 00 64 0b 00 00 7c	00 40 01 44 b7 ac 1 e5 00 01 01 e8 ff 7	be9 62 00 00 dl	@ Dd.					
0030	00 00 cf 7f 0a	00 00 00 00 00 10 1	1 12 13 14 15						
0040	16 17 18 19 1a	1b 1c 1d 1e 1f 20 2	1 22 23 24 25	····!"#\$	\$%				
0050	26 27 28 29 2a	2b 2c 2d 2e 2f 30 3	1 32 33 34 35 &'()*+	,/01234	45				
0000	30 37		07						

## Using the CLI to Validate Distributed Security Results

© 2023 VMware, Inc.

Is the DFW doing its job?



[root@esxcomp-2a:~] vsipioctl -h Usage: help <cmd> <options> below is a list of available cmd: getfilters : get list of filters getfwconfig : get rules, addrsets and containers of a filter : get rules of a filter getrules getaddrsets : get addrsets of a filter getcontainers : get containers of a filter getspoofguard : get spoofguard setting of a filter : get flows of a filter getflows getconncount : get active connection count getconnections : get active connections getsisvmstats : get service insertion service VM stats getsisvctable : dump service insertion service table getsinshtable : display service insertion nsh table getsiproxytable : display service insertion proxy table getsifailedspis : get service insertion failed spi table getsiflowprogtable : get service insertion flow programming table getsislotid : get service insertion slot id getsilbenablestatus: get service insertion load balance enable status

getmeminfo : get meminfo data initvsiplogging : init vsip logger getfqdnentries : get fqdn entries getdnsconfigprofile : get dns config profile for a filter getfilterstat : get statistics of a filter gettimeout : get connection timeout setting of a filter getfloodstat : get flood protection status getsidcache : get sid cache of a filter help : this help message run `vsipioctl <cmd> -h' to find out available options of a cmd.

#### Common Commands to validate DFW on a vSphere transport node:

- summarize-dvfilter to find the filter name
- vsipioctl getrules -f <filter name>
- vsipioctl getaddrset -f <filter name>
- vsipioctl getflows -f <filter name>

© 2023 VMware, Inc.

```
[root@sa-esxi-01:~] summarize-dvfilter | grep -A 4 ME-Bil
world 808359 vmm0:ME-Bilbo vcUuid:'50 1d a4 8c cb f5 ce c7-b3 a6 85 25 20 ab ee d8'
port 67108914 ME-Bilbo.eth0
vNic slot 2
name: nic-808359-eth0-vmware-sfw.2
agentName: vmware-sfw
state: IOChain Attached
[root@sa-esxi-01:~]
```

```
[root@sa-esxi-01:~] summarize-dvfilter | grep -A 4 ME-Bil
world 808359 vmm0:ME-Bilbo vcUuid:'50 1d a4 8c cb f5 ce c7-b3 a6 85 25 20 ab ee d8"
 port 67108914 ME-Bilbo.eth0
   vNic slot 2
    name: nic-808359-eth0-vmware-sfw.2
    agentName: vmware-sfw
    state: IOChain Attached
[root@sa-esxi-01:~]
[root@sa-esxi-01:~] vsipioctl getrules -f nic-808359-eth0-vmware-sfw.2
ruleset mainrs {
 # generation number: 0
 # realization time : 2022-08-02T18:56:55
 # PRE FILTER rules
 rule 3050 at 1 inout protocol any from addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 to addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 reject;
 rule 3052 at 2 inout protocol tcp strict from not addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 to addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 port
22 with attribute profile 8caa3b4d-444a-4031-b057-4b3f51a05954 accept;
 rule 3053 at 3 inout protocol any from addrset 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 8081bb70-88e6-433c-8985-cfb05632f126 accept;
 rule 3055 at 4 inout protocol any from addrset 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 5b71c129-072a-4856-b34f-db649c6d4195 accept;
 rule 3056 at 5 inout protocol any from any to any reject;
 # FILTER (APP Category) rules
 rule 3 at 1 inout inet6 protocol ipv6-icmp icmptype 135 from any to any accept;
 rule 3 at 2 inout inet6 protocol ipv6-icmp icmptype 136 from any to any accept;
 rule 4 at 3 inout protocol udp from any to any port {67, 68} accept;
 rule 2 at 4 inout protocol any from any to any accept;
 # IDP rules
 rule 3061 at 1 inout protocol any from any to any with ids profile 8a7465b3-363c-46ad-8117-7e702fce4d62 idp protect;
```

```
[root@sa-esxi-01:~] summarize-dvfilter | grep -A 4 ME-Bil
world 808359 vmm0:ME-Bilbo vcUuid: 50 1d a4 8c cb f5 ce c7-b3 a6 85 25 20 ab ee d8'
 port 67108914 ME-Bilbo.eth0
   vNic slot 2
    name: nic-808359-eth0-vmware-sfw.2
    agentName: vmware-sfw
    state: IOChain Attached
 [root@sa-esxi-01:~]
[root@sa-esxi-01:~] vsipioctl getaddrsets -f nic-808359-eth0-vmware-sfw.2
addrset is shared for this filter
global addrset
addrset 0236f0d8-1735-4850-a3a0-ed1273dcdcc2 {
ip 172.16.200.11,
ip 172.16.200.13,
mac 00:50:56:9d:03:97,
mac 00:50:56:9d:0d:4e,
3
addrset 2ebcfe60-e797-4628-bdc0-5be214f57c91 {
ip 172.16.100.11,
ip 172.16.100.13,
mac 00:50:56:9d:5f:f6,
mac 00:50:56:9d:8c:2d,
addrset 5b71c129-072a-4856-b34f-db649c6d4195 {
ip 172.16.100.11,
ip 172.16.100.12,
ip 172.16.100.13,
mac 00:50:56:9d:5f:f6,
mac 00:50:56:9d:8c:2d,
mac 00:50:56:9d:dc:d5,
```

© 2023 VMware, Inc.

Find information if the Host Credentials are not available – NSX Manager

<pre>sa-nsxmgr-01&gt; get nodes Tue Aug 02 2022 UTC 20:53:57.870 UUID ece51cee-4ac9-48c1-9735-ff065512440c f3cfc203-a7c1-4931-b889-2a580ebf18a8 22e375d5-0e12-4a0a-8c99-100cd33d6006 8cfe9d5e-29db-4008-8021-9833871fa8a0</pre>	Type Display Name edg sa-nsxedge-01 esx sa-esxi-01.vclass.local esx sa-esxi-02.vclass.local kvm sa-kvm-01
bdb81d42-7341-5abc-c3fc-4fa583fcdea8 sa-nsxmgr-01> on f3cfc203-a7c1-4931-b8	mgr sa-nsxmgr-01 89-2a580ebf18a8 exec get firewall vifs
f3cfc203-a7c1-4931-b889-2a580ebf18a8	esx sa-esxi-01.vclass.local
Firewall V.	IFs

VIF count: 7



#### Find information if the Host Credentials are not available – NSX Manager

3a-nsxmgr-01> on f3cfc203-a7c1-4931-b889-2a5	580ebf18a8 exec get firewall 742ceafa-8ba2-414c-b4df-75a71b827c48 ruleset rules
f3cfc203-a7c1-4931-b889-2a580ebf18a8 esx :	sa-esxi-01.vclass.local
Fue Aug 02 2022 UTC 20:53:17.162 Firewall Rules	
VIF UUID : 742ceafa-8ba2-414c-b4df-75a71b82'	7c48
Ruleset UUID : de6f9262-f6ca-4518-804a-5d2	25b2c639ca
rule 3061 inout protocol any from any to	o any with ids profile 8a7465b3-363c-46ad-8117-7e702fce4d62 idp protect:
Ruleset UUID : 02ed5703-a0e9-4d29-b152-3dc	d07d66c3ec
Rule count : 5	at $2abafafa_a707_4f29_bda0_fba214ff7a01 to addreat 2abafaf0_a707_4f29_bda0_fba214ff7a01 in nya filtay yaiaat.$
rule 3052 inout protocol top strict from	m not addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 to addrset 6aa5c80c-a8d8-4576-a8f6-dfedf87a93b1 port 22 with attribut
profile 8caa3b4d-444a-4031-b057-4b3f51a059	54 in pre_filter accept;
rule 3053 inout protocol any from addrse	et 5b71c129-072a-4856-b34f-db649c6d4195 to addrset 8081bb70-88e6-433c-8985-cfb05632f126 in pre_filter accept;
rule 3055 inout protocol any from addrse rule 3056 inout protocol any from any to	at SD/10129-072a-4856-D341-db64906d4195 to addrset SD/10129-072a-4856-D341-db64906d4195 in pre_filter accept; o any in pre filter reject:
	, and in her relation relation,
Ruleset UUID : ffffffff-8a04-4924-a5b4-540	130e81befe
Ruleset UUID : fffffff-8a04-4924-a5b4-54 Rule count : 4	d30e81befe
Ruleset UUID : fffffff-8a04-4924-a5b4-54 Rule count : 4 rule 3 inout inet6 protocol ipv6-icmp ic rule 3 inout inet6 protocol ipv6-icmp ic	d30e81befe cmptype 135 from any to any accept; cmptype 136 from any to any accept;
Ruleset UUID : ffffffff-8a04-4924-a5b4-54 Rule count : 4 rule 3 inout inet6 protocol ipv6-icmp ic rule 3 inout inet6 protocol ipv6-icmp ic rule 4 inout protocol udp from any to ar	d30e81befe cmptype 135 from any to any accept; cmptype 136 from any to any accept; ny port {67, 68} accept;
Ruleset UUID : ffffffff-8a04-4924-a5b4-54 Rule count : 4 rule 3 inout inet6 protocol ipv6-icmp i( rule 3 inout inet6 protocol ipv6-icmp i( rule 4 inout protocol udp from any to ar rule 2 inout protocol any from any to ar	d30e81befe cmptype 135 from any to any accept; cmptype 136 from any to any accept; ny port {67, 68} accept; ny accept;
Ruleset UUID : ffffffff-8a04-4924-a5b4-54 Rule count : 4 rule 3 inout inet6 protocol ipv6-icmp ic rule 3 inout inet6 protocol ipv6-icmp ic rule 4 inout protocol udp from any to ar rule 2 inout protocol any from any to ar Ruleset UUID : ffffffff-35f8-4611-a40f-545	d30e81befe cmptype 135 from any to any accept; cmptype 136 from any to any accept; ny port {67, 68} accept; ny accept; 5432e3119a
<pre>Ruleset UUID : ffffffff-8a04-4924-a5b4-54( Rule count : 4    rule 3 inout inet6 protocol ipv6-icmp i(    rule 3 inout inet6 protocol ipv6-icmp i(    rule 4 inout protocol udp from any to ar    rule 2 inout protocol any from any to ar    Ruleset UUID : ffffffff-35f8-4611-a40f-545 Rule count : 1</pre>	d30e81befe cmptype 135 from any to any accept; cmptype 136 from any to any accept; ny port {67, 68} accept; ny accept; 5432e3119a

## **vm**ware<sup>®</sup> **EXPLORE**

## Thank You

