cisco live!

Let's go



Secure Firewall – Threat Defense Data–Path Troubleshooting A practical hands on lab

John Groetzinger, Technical Leader, CX Foster Lipkey, Principal Engineer, CX





Agenda

- Introduction
- Architecture Overview
- Troubleshooting Framework Overview
- Self-Paced Lab Scenarios
- Conclusion



Introduction



Your Presenters

John Groetzinger

- Technical Leader for Firepower TAC
- 12+ Years experience in Network Security
- Original Sourcefire employee
- Open Source, devops and Linux enthusiast





Your Presenters

Foster Lipkey

- TAC Security Principal Engineer
- 12+ Years of Security Experience
- Snort Expert
- Sourcefire Veteran
- Automation Enthusiast
- Malware Detection Patent Holder





Snorty Collectables





cisco live!

Key Learning Objectives





Framework to Isolate Problematic Component



Individual Component Troubleshooting Skills



Architecture Overview



ASA/virtual FTD





SSP (4100/9300)





LTRSEC-3880 © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 13

SSP (2100)



Virtual/Software diagram





Virtual/Software diagram



Troubleshooting Framework Overview





Troubleshooting Methodology





Methodology

Tools show iCapture Hardware bypass Layer 1 w/Trace Conn Events nterface Capture w/Trace Layer 2 Conn Events Capture w/Trace Laver 3 Packet Tracer Conn Events Capture w/Trace Layer 4 Packet Tracer Conn Events Layers 5-7

Trace Phases CAPTURE SNORT ACCESS-LIST **EXTERNAL-INSPECT** ADJACENCY-LOOKUP SNORT **EXTERNAL-INSPECT** ACCESS-LIST ACCESS-LIST SNORT ROUTE-LOOKUP NAT FLOW-LOOKUP **IP-OPTIONS** CONN-SETTINGS NAT EXTERNAL-INSPECT FLOW-CREATION ACCESS-LIST **EXTERNAL-INSPECT** CONN-SETTINGS **FLOW-CREATION** FLOW-LOOKUP SNORT NAT SNORT

Firepower Data-Path Troubleshooting Framework flow diagram



cisco ile

Introduction to Problem Component Identification



Tool Introduction

- Capture w/Trace
- Prefilter policy



cisco live!

DAQ (Data Acquisition)





- Capture W/ Trace
- Debug Packet



Remediations

- Prefilter Policy
 - Policies > Access Control > Prefilter
 - Create or edit Prefilter policy
 - Add a fastpath rule for the traffic
 - Make sure to use the Prefilter policy in the AC policy



Capture w/Trace:





Capture w/Trace:



cisco live!

Capture w/Trace:

Advanced Troubleshooting

NGFW1	
File Download Threat Defense CL	I Packet Tracer Capture w/Trace
C Auto Refresh Interval (seconds): 10	C Enable Auto Refresh
Name Interface	Type Trace Buf Buffer Packet Buffer Proto Source Destination Status
	Add Capture ? ×
	Name*: Interface*: Select an interface Y
	Match Criteria:
	Protocol*: IP
	Source Host*: any Source Network:
	Destination Host*: any Destination Network:
	SGT number: 0 (0-65533)
¢	Buffer:
	Packet Size: 1518 14-1522 bytes O Continuous Capture I Trace
	Buffer Size: 524288 1534-33554432 bytes Image: Stop when full Trace Count: 50
	Save Cancel

Add Capture				? ×	Protocol: Bad CIDR
Name*: Match Criteria:	Test	Interface*:	Inside	•	172.31.100.0 255.255.0.0 Destination Host: Destination Netmask:
Protocol*: Source Host*: Destination Host*: SGT number: Buffer:	TCP 192.168.1.200 any 0	Source Network: Destination Network: (0-65535)	255.255.255		SGT number: Error 0 Unable to execute the command properly. Please see logs for more details. Buffer: Packet Size: Buffer Size: OK Continuous Capture
Packet Size: Buffer Size:	1518 14-1522 524288 1534-335 bytes	bytes Continuous Ca 554432 Stop when ful	apture I Trace	0 Cancel	Clicking Add Capture button will display this popup window
Advanced Troubleshoo 10.83.181.27 File Download Threat Defens C Auto Refresh Interval (seconds): 11	ting e CLI Packet Tracer Capture w/Trace				Add Capture
Name Test		Interface Type Trace Buffer E Inside raw-deta * # 5	Buffer Packet Buffer Protocol Source 24288 1518 Cepturing TCP 192.168.1.200	Destination	Status Running 🥔 🛱 🤊 II 🗟
					View of all current captures
cisco 🗸	ive			I TRSEC-	C-2880 @ 2024 Cisco and/or its affiliates All rights reserved. Cisco Public. 35



Advanced Troubleshooting

10.83.181.27

File Download Threat Defense CLI Packet Tracer Captur	re w/Trace		
C Packets Shown: 577 / Packets Captured: 577 / Traces: 298	▼ Forr	mat: Raw	
Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MC Access list		0	
Phase: Type: ACCESS-LIST Subtype: Result: ALGOW Config: Implicitude Implicitude Additional Information: MC Access list			shows the
Phase: 3 Type: FLOW-LOCKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id 2672128, using existing flow			blocked by
Phase: 4 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT Inspect'			Snort
Phases 5 Type: SNORT Subtype: Result: DROP Config: Additional Information:		drop this	naakat
Result: input-inface: Inside input-status: up		arop this	ρασκει
Last login on Thursday, 2017-05-11 at 14:54:07 PM from 10.151.32.47		, i i i i cisco	

cisco live!

ı

information

	ice Result: 🔮 ALLOW	
 i usdqvfmd) i usdqvfmd (triange) i usdq	Packet Details: 22:54:32.14 -	
 Second Product Product Product France Equation for the control of the co	inside(vrfid:0)	
 PB-LOCKUP [pakkp-rod8 PAR-LOCKUP [pakkp-rod8 PACUTE-LOCKUP [Reakbe Egness Entertacs PAT [rep-reaks PAT [rep-reaks PAT [rep-reaks PACUTE-LOCKUP [Reakbe Egness Entertacs PAT [rep-reaks PACUTE-LOCKUP [Reakbe Egness Entertacs PAT [rep-reaks PAT [rep-reaks PAT [rep-reaks PAT [rep-reaks PAT [rep-reaks PACUTE-LOCKUP [Reakbe Egness Entertacs PACUTE-LOCKUP [Reakbe Egness Entertacs	SUBOPTIMAL-LOOKUP suboptimal next-hop	
 NetT-ROUTE-LOOKLP Resulte Egress Interface ORECT, gROUP, SEARCH ACCSSS-LIST tog CORN-SETTINGS P-OPTIONS OG NaT rgh-check NaT rgh-check NaT rgh-check NaT rgh-check NaT rgh-check NaT rgh-check NaT 	PBR-LOOKUP policy-route	
 BARCT_GROUP_SEARCH ACGENTS Ing CONV-SETTINGS P-OPTIONS MAT pri-tension Int pri-tension P-OPTIONS MAT pri-tension MAT pri-tension	INPUT-ROUTE-LOOKUP Resolve Egress Interface	
 ACCESS-LIST fog Conservations NAT per-destion P-OPTIONS O OS NAT per-destion P-OPTIONS P-OPTIONS P-OPTIONS P-OPTIONS PLOW-CREATION Subjuit Subjuit ALLOW Subjuit Subjuit ALLOW Subjuit Subjuit	OBJECT_GROUP_SEARCH	
 CONV-SETINGS NAT NAT PP-OPTIONS QOG NAT (per-testion) PP-OPTIONS QOG NAT (per-testion) P-OPTIONS PLOPTIONS PLOPTIONS<td>ACCESS-LIST log</td><td></td>	ACCESS-LIST log	
 NAT NAT per-session O OS NAT per-session Procentions Procentions	CONN-SETTINGS	
 NAT per-session O OS NAT per-session IP-ortons AT per-session IP-ortons Row CREATION External-Nestort Shofty spoid Best: Subpre: Config Type: Shofty spoid Subpre: Config Shofty spoid Shofty spoid Subpre: Config Shofty spoid Shofty spoid<	NAT	
 P-Prince Province Province<	NAT per-session	
 a cos A AT rpt-theck a cos MAT rpt-theck a cos A LLOW a cos a c	IP-OPTIONS	
 NAT rpf-check OGS NAT rpf-check OGS NAT rpf-check IP-OPTIONS IP-OPTIONS FLOW-CREATION SUBTIONS SUBTIONS ALLOW Busity Urgen SUBTIONS ALLOW Busity Subtions SUBTIONS ALLOW Busity Subtions SUBTIONS ALLOW Busity Subtions SUBTIONS SUBTIONS ALLOW Busity Subtions SUBTIONS <li< td=""><td>QOS</td><td>Dacket Trace and Canture M// Trace now</td></li<>	QOS	Dacket Trace and Canture M// Trace now
 ors NAT I per-session IP-OPTIONS FLOW-CREATION KTERNA-INSPECT SNORT appid Config: Type: SNORT ALLOW subject (0), client: (0), payload: (0), miss: (0) 	NAT rpf-check	
 NAT per-session IP-oPTONS FLOW-CREATION ExtERNAL-INSPECT SNORT appid Result: Subtype: Confg: Type: SNORT Additional Information service: (0), client: (0), psyload: (0), mist: (0) 	QOS	
IP-OPTIONS FUNC-SEATION EXTERNAL-INSPECT SNORT SNORT SNORT Additional Information service: (0), client: (0), psyload: (0), mise: (0)	NAT per-session	have Firewall Fngine Debug output
 FLOW-CREATION EXTERNAL-INSPECT SNORT SNORT Additional Information service: (0), client: (0), psyload: (0), misc: (0) 	IP-OPTIONS	have hierran Engine Debag eatpat
EXTERNAL-INSPECT IIICIUUUUU SNORT ALLOW Subppe: appid Config: Type: Type: SNORT	FLOW-CREATION	included
SNORT jæpid Result: • ALLOW Subtype: subtype: apid Confe:	EXTERNAL-INSPECT	
Result: • ALLOW Subtype: apold Config: Type: SNORT • Additional Information service: (0), elient: (0), psyload: (0), misc: (0)	SNORT appld	
Config: Type: SNORT Additional Information service: (0), client: (0), payload: (0), misc: (0)	Result: O ALLOW Subtype: apoid	
rype: Dorwrti ✓ Additional Information service: (0), client: (0), payload: (0), misc: (0)	Config:	
✓ Additional Information service: (0), client: (0), payload: (0), misc: (0)	Type: SNORT	
	Additional Information service: (0), client: (0), payload: (0), misc: (0)	
Network () Inspection (), Detection 2, Rule ID 268434433	Config: Network 0, Inspection 0, Detection 2, Rule ID 268434433	
Subtype: firewall		

cisco Live!

SHELL

> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

1:01:17:38.498906	192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss 0,nop,wscale="" 1045829951="" 1460,sackok,timestamp="" 7="">,</mss>
2:01:17:38.510898	10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackok,timestamp="" 513898266<="" td=""></mss>
1045829951,nop,wscale	7>
3: 01:17:38.511402	192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956="" 513898266=""></nop,nop,timestamp>
4:01:17:38.511982	192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp 1045829957<="" td=""></nop,nop,timestamp>
513898266>	
5:01:17:38.513294	10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp 1045829957="" 513898268=""></nop,nop,timestamp>
6:01:17:38.528125	10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win 140 <nop,nop,timestamp 513898282<="" td=""></nop,nop,timestamp>
1045829957>	
7:01:17:38.528613	192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop.nop.timestamp 1045829961="" 513898282=""></nop.nop.timestamp>

cisco ive!

SHELL	
> show capture ssh_traffic packet-number 4 trace	Phase: 3 Type: FLOW-LOOKUP
7 packets captured	Subtype: Result: ALLOW
4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp< td=""><td>Config: Additional Information:</td></nop,nop,timestamp<>	Config: Additional Information:
1045829957 513898266> Phase: 1	Found flow with id 626406, using existing flow
Type: CAPTURE Subtype:	Phase: 4 Type: EXTERNAL-INSPECT
Config:	Result: ALLOW
MAC Access list	Additional Information:
Phase: 2 Type: ACCESS-LIST	
Subtype: Result: ALLOW	
Config: Implicit Rule	
Additional Information: MAC Access list	

cisco live!

SHELL

Phase: 5 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: TCP, ACK, seq 4250994242, ack 903999423 AppID: service SSH (846), application unknown (0) Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0 Firewall: trust/fastpath rule, id 268435458, allow NAP id 1, IPS id 0, Verdict WHITELIST Snort Verdict: (fast-forward) fast forward this flow

Result: input-interface: inside input-status: up input-line-status: up Action: allow

cisco live!

Add Prefilt	er Rule										? ×	1		
Prefilter	rules perform early handli	ng of traffic	based on simp	le network cha	racteristics. Fastp	athed traffic byp	asses access	control and QoS.						
Name	fastpath 192.168.62.60			🗹 En	abled	Insert	below rule		▼ 1					
Action	⇒ Fastpath		*											
		_												
Interfa	ce Objects Network	s VLAN	Tags Ports	; 	- Networks (4)			Destination No.	Co	mment Lo	gging			
Available Ne	etworks C			Sourc	e Networks (1)		9	Destination Ne	tworks (U)					
					2.100.02.00			uny						
IPv4-Priv	ate-All-RFC1918													
10_83_1	81_1												Click	king Add
🚔 62_netw	ork		Add Sour	to te									Drof	ltor Dulo
📄 any-ipv4			Add	:0									Pret	liter Rule
any-ipv6			Destina	tion									butte	
IPv4-Ber	ichmark-Tests												Dulle	
IPV4-Lini	ticast												dicol	av this
IPv4-Priv	ate-10.0.0.0-8												uispi	ay uns
				Enter	an IP address		bbA	Enter an IP add	ress		Add		noni	in window
											, inde		ρορι	
									Add	Ca	ncel			
												-		
factna	th test											Save Sancel		
Enter Descri	intion													
Rules														
							🗿 Add	Tunnel Rule	Add Prefilter	Rule Search	Rules	×		
#	Name F	tule Type	Source Interface	Destination Interface	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel	I Zo		View of all
1	fastpath 192.168.62.60 P	refilter	any	any	👳 192.168.62.6	o any	any	any	any	👄 Fastpat	h na	📄 o 🥒 🗒		rules in the
Non-tunne	led traffic is													
														tastpath test
														Prefliter policy

cisco live!



View of connection events matching

	✓ <u>First Packet</u> ×	Last Packet ×	Action ×	<u>Reason</u> ×	Initiator IP ×	Responder × IP	Source Port / X ICMP Type	Destination Port / × ICMP Code	Prefilter × Policy	<u>Tunnel/Prefilter</u> × <u>Rule</u>
↓ □	2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	<u>48480 / tcp</u>	<u>22 (ssh) / tcp</u>	fastpath test	fastpath 192.168.62.60

cisco ile

Security Intelligence

cisco live!

Tool Introduction

- Connection / Security
 Intelligence Events
- Unified Event Viewer





Security Intelligence





- Capture W/ Trace
- Check SI events for Blocks
 - Analysis > Connections > Security
 Intelligence Events
 - Unified Event Viewer



Remediations

- Add to do-not-block IP/URL/DNS
- Remove IP/URL/DNS from Block List
 if custom list
- If reputation is wrong open Talos
 reputation ticket

cisco / ille
Talos Reputation Center

https://www.talosintelligence.com/reputation_center

← → C ■ talosintelligence.com/reputation_center/lookup?search=snort.org	🕲 🗅	🖈 👦 🖈 🖬 🔲 🔮 (Error :
😍 CDETS 🖹 Cylon / Fireonsole 🗎 SXO/AO 📄 Cisco Links 📄 APIs 📄 BDB 🗎 TechZone 🗎 My Lab 📄 etherpads	🗎 Articles 🛛 🗭 EasyBems Test SR 📓 ICAA 🗮 Cisco AWS Login 🗎 sharepoint 💧 Error	E Other Bookmarks
		CISCO LOGIN
CISCO CISCO Software Vulnerability Information Reputation Center Su	oport Incident Response Careers Blog Podcasts About	
Lookup data results for Domain	146))114((0))11	
snort.org	Q	REPUTATION DETAILS
Search by IP, domain, or net	work owner for real-time threat data.	
IP & Domain Reputation Overview	File Reputation Lookup Email & Sparn Data	
state to the state of the state		
OWNER DETAILS	REPUTATION DETAILS	
DOMAIN shortlorg	⑦ WEB REPUTATION ✓ Trusted	
MAIL SERVERS 🔞		
alt1.aspmx1.google.com		—
alt2.aspmx1.google.com	TALOS SECURITY INTELLIGENCE BLOCK LIST	—
aspmx.l.google.com	STATUS EXPIRED	
aita.aspirrx.tgoogle.com		
CONTENT DETAILS		
O CONTENT CATEGORY Computer Security		
Think these category details are incorrect?		
Submit Content Categorization Ticket		

cisco ile

Unified Event Viewer

	Firewall Managen Analysis / Unified Events	nent Center	Overview Analysis	Policies Devices (Objects Integration			Deploy Q	. 🗳 🌣 🕜 adm	nin ▼	
QS	elect									× Refre	
Øs	nowing all 2,195 events (\$	2,031 🗋 82 🌞 82) 🚊	<u>+</u>				Po 2023	3-04-26 00:52:08 EDT -	• 2023-04-27 12:52:09 EE	OT 1d 12h OG L	
m	Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Cont	
>	2023-04-26 08:10:45	S Connection	Allow		192.168.147.50	172.18.108.43	57843 / udp	53 (domain) / udp		omni_inspe	
~	2023-04-26 08:10:45	S Connection	e Block	File Block	192.168.147.50	10.83.79.20	37860 / tcp	80 (http) / tcp		omni_inspe	
	Eve	ent Type: 😫 Connection		Client Appli	ication Tag: file sharing/transfer,	User-Agent Exclusion, e		Ingress Interface: insi	de		
		Time: 2023-04-26 0	8:10:45	Applic	cation Risk: Medium			Egress Interface: out	side		
	Las	t Packet: 2023-04-26 0	8:10:45	Business	Relevance: Medium		Ingress Virtual Router: Global				
		Action: 😑 Block			URL: http://stubbedtoe.de	vit.ciscolabs.com/archive	Eg	ress Virtual Router: Glo	bal		
		Reason: File Block		URI	L Category: Computers and Inter	net		Initiator Packets: 81			
	S	ource IP: 192.168.147.5	0	URLI	Reputation: Trusted		R	esponder Packets: 96			
	Destir	nation IP: 10.83.79.20		HTTP Resp	onse Code: 200		QoS-Droppe	d Initiator Packets: 0			
	Ingress Secur	rity Zone: inside_routed		Refere	enced Host: stubbedtoe.devit.cis	colabs.com	QoS-Dropped Responder Packets: 0				
	Egress Secur	rity Zone: outside_routed		ι	User Agent: Wget/1.21.2			Initiator Bytes: 5,5	39		
	Source Port / ICI	MP Type: 37860 / tcp		Intrus	sion Events: 0			Responder Bytes: 134	,136		
	Destination Port / ICM	MP Code: 80 (http) / tcp			Files: 1		QoS-Drop	ped Initiator Bytes: 0			
	Application	Protocol: HTTP		Access Cor	ntrol Policy: JG AC		QoS-Dropped	d Responder Bytes: 0			
	Application Protocol C	ategory: network protoco	ols/services	Access Co	ontrol Rule: omni_inspect			Detection Type: App	ND		
>	2023-04-26 08:10:45	D File	Malware Block		10.83.79.20	192.168.147.50	80 (http) / tcp	37860 / tcp			
>	2023-04-26 08:10:45	👬 Malware	Malware Block		10.83.79.20	192.168.147.50	80 (http) / tcp	37860 / tcp			
>	2023-04-26 08:10:42	S Connection	S Allow		192.168.147.50	91.189.94.4	41325 / udp	123 (ntp) / udp		omni_inspec	
>	2023-04-26 08:10:42	S Connection	Allow		192.168.147.50	172.18.108.43	53533 / udp	53 (domain) / udp		omni_inspec	

cisco live!

Security Intelligence - Logging

					Inheritance Settings Policy Assignments (
Rules Security Intelligence HTTP Responses	Logging Advanced			Prefilter Policy: Demo Prefilter Policy	SSL Policy: None Identity Policy: None
DNS Protection					
DNS Protection blocks traffic from known threats by the do	omain name. Intelligence for these threats is derived from	both TALOS and Cisco Umbrella.			
DNS Policy 💉 📋			Umbrella DNS Policy 💉 🏷		
Default DNS Policy_1		▼ →	None		•
Network and URL Block List					
Available Objects (33) C	+				
Q Search for a URL					
Networks URLs	Available Zones 🗠		Do-Not-Block List(2)	Block List (C)	
Global-Block-List-for-URL_1	Any	Add to Do-No	t- Networks	Networks	
Global-Do-Not-Block-List-for-URL_1	InZone	Block List	Global-Do-Not-Block-List_1 (Any Zone)	cirobal-Block-List_1 (Any Zone)	• T
URL Attackers	OutZone	Add to Block I	URLs	Attackers (Any Zone)	• 🗑
URL Banking_fraud		Add to block E	Global-Do-Not-Block-List-for-URL_1 (Any Zone)	Banking_fraud (Any Zone)	• ¥
URL Bogon				URL 🗒	
URL Bots				Global-Block-List-for-URL_1 (Any	/ Zone) 🗢 🗑
URL CnC				URL Attackers (Any Zone)	• 🖬
URL Cryptomining				LIDL Danking fraud (Any Zono)	• = [•]

Ensure logging is enabled

cisco live!

Analysis > Connections > Security Intelligence Events

→ <u>First Packet</u> ×	Last Packet ×	Action ×	<u>Reason</u> ×	Initiator IP ×	Responder IP ×	Security Intelligence × Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	old state in the state of the s	i	DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95	0	Malware

With logging enabled for all SI types you should be able to easily see what is being blocked by SI.

cisco ile

Security Intelligence – Domain and Global Lists



LTRSEC-3880

Access Control



Tool Introduction

• firewall-engine-debug





Identification - Access Control Policy





- Capture W/ Trace
- Check Connection Events
- Firewall Engine Debug > system support firewall-engine-debug



Remediations

- Update Access Control Rule to comply with intent of the policy
- Create a trust rule for traffic above rule that is blocking
- Disable block rules



system support firewall-engine-debug



system support firewall-engine-debug



cisco ile

Check logging for block rules

#	Name		Sou Zon	Dest Zon	Sou Net	Dest Net	VLA	Use	Арр	Sou	Des	URLs	ISE Attr	Acti	V 🗈 🤉 🕹	_	
🔻 Man	datory - My AC Policy (1-	-2)															
1	block with logging		any	any	any	any	any	any	🔤 You	IT <i>any</i>	any	any	any	💢 Bloc	10 6 2 4	0	0
2	block no logging		any	any	any	any	any	any	any	any	any	Je Gan	nl <i>any</i>	💢 Bloc	10 D 2 C	D o	0
Add trust rule																	
1	Trust traffic		any	any	i92.	any	any	any	any	any	any	any	any	🔿 Trus) h <u>2 h </u>	0	a 🖉
2	block with logging		any	any	any	any	any	any	🗖 You 🗖 You	T _{any}	any	any	any	💢 Bloc	0 6 2 4 [0	a 🖉
3	block no logging		any	any	any	any	any	any	any	any	any	📑 Gam	any	💢 Bloc	00,261	0	a 🖉
_								↓	Cre	ate	blan	k AC	; pol	icy			
#	Name	Sour Zones	Dest Zones	Sour Netw	Dest Netw	VLA	.N Us	ers A	ppli S	Sour	Dest	URLs	ISE/ Attri	Action	V 🗈 🕫 🕁		
🔻 Man	datory - Test - No rules (-))															
There ar	re no rules in this section. Add	d Rule or	Add Cate	gory													
🔻 Defa	✓ Default - Test - No rules (-)																
There ar	re no rules in this section. Add	d Rule or	Add Cate	gory		_		_	_								
Default	Action									Intru	sion Preve	ntion: Bala	anced Secu	urity and C	Connectivity	*	Ş 📕

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S Attrib	Acti
-	Mandatory - JG AC	(all) (1-6)											
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	🥭 SSH	Any	Any	\Rightarrow Trust 🛈 โก
2	inspect	Any	Any	👳 10.0.0.0/8 🗜	Any Origi	nal Clier	nt IP»(HT	TP)	Any	Any	Any	Any	🛹 Allow 🤍 📭
3	trust server backup	Any	Any	2192.168.62.3	👼 10.123.175.22	Any	Any	Any	Any	Any	Any	Any	\Rightarrow Trust 🕡 顺

SSH Connection from 192.168.62.3 to 10.123.175.22

SYN 192.168.62.3 → 10.123.175.22
 SYN,ACK 10.123.175.22 → 192.168.62.3
 ACK 192.168.62.3 → 10.123.175.22
 SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule

Pending AppID

Service identified as SSH No match 'inspect' rule (non-http) Match 'trust server backup' rule and Trust flow



SSH Connection from 192.168.62.3 to 10.123.175.22





First SSH Packet (client to server)

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 New session 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 **Starting with minimum 4, 'inspect',** and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: (), **svc 0**, payload 0, client 0, misc 0, user 9999997, icmpType 0, ismpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, p ayload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: (**, svc 846**, **p** yload -1, client 200000846, misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', **XFF non-http** 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust

SYN

ACK

SYN, ACK

How to Map service ID (svc) to name

firewall-enginedebug



SHELL

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[...omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, **svc 846**, payload -1, client 200000846, misc 0, user 9999997, icmpType 0, icmpCode 0 192.168.62.3-46594 > 10.133.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http 192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust

[! How to map service/application ID to name]
> expert
\$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh

cisco ile

Intrusion Prevention System (IPS)

cisco live!

Tool Introduction

• system support trace



cisco live!

Identification - Intrusion Policy





- Capture W/ Trace
- Check Connection Events
- Review Snort Configurations
- Check Intrusion Events
- System Support Trace



Remediations

- Disable rule(s) impacting traffic
- Targeted intrusion policies
- Open SR for False Positive/Coverage
- Use No Rules Active policy
- Disable Drop when Inline

cisco ile

system support trace

SHI SHI	ELL
> system support trace	
Please specify an IP protocol: tcp Please specify a client IP address: 192.168.62.69 Please specify a client port: Please specify a server IP address:	Specify Filter
Please specify a server port: Enable firewall-engine-debug too? [n]: y Monitoring packet tracer debug messages	See Verdict Info per packet
[output omitted for brevity]	
173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, a 173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application 192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 0 URL SI: ShmDBLookupURL("	nck 3856774965 on Cisco (2655) http://www.cisco.com/ php") returned 0</th
 192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect 192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action	it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', a	llow
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111	, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session 192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKUS	т
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS	
Verdict reason is sent to DAQ's PDTS	

cisco live!

Rules Security Intelligence HTTP Responses Advanced									Te Inhe	eritance Setting	s 🖳 Policy Ass	ignments (0)
General Settings				Ø	Transport/Network Layer P	reprocesso	or Settings					0
Maximum URL characters to store in connection events				1024	Ignore the VLAN header when tracking connections No							
Allow an Interactive Block to bypass blocking for (seconds)				600	Detection Enhancement Se	ttings						a
Retry URL cache miss lookup				Yes	Network Analysis and Intr	usion Polic	ies			2 X		Enabled
Enable Threat Intelligence Director				Yes		usion i one						Disabled
Inspect traffic during policy apply				Yes	rule is determined	s Control	No Rules Active			<u> </u>		a
Identity Policy Settings				ø	Intrusion Policy Variable Set		Default-Set			✓		5
Identity Policy				None	Network Analysis Rules	<u>P</u>	No Custom Rules	1	Network Analysis Policy	List		300
SSL Policy Settings				Ø	Default Network Analysis Policy		Balanced Security and Connectivi	у		×	Def	ault Value
SSL Policy to use for inspecting encrypted connections				None	Revert to Defaults				ок са	ncel	Def	ault Value
Prefilter Policy Settings				Ø	Intrusion Event Logging Limits -	Max Events	Stored Per Packet					8
Prefilter Policy used before access control			Default Prefilt	ter Policy	Latency-Based Performance Settings							
Network Analysis and Intrusion Policies					Applied from Installed Rule Upd	ate						true
Intrusion Policy used before Access Control rule is determined			No Ru	le Active	Packet Handling							Enabled
Intrusion Policy Variable Set			De	fault-Set	Packet Handling - Threshold (mi	croseconds)						256
Default Network Analysis Policy		8	Balanced Security and Con	nectivity	Rule Handling							Enabled
Files and Malware Settings				(J)	Rule Handling - Threshold (micr	oseconds)						512
Prefilter Policy: Default Prefilter Policy S	SL Policy: None			Iden	tity Policy: None							
Rules Security Intelligence HTTP Responses Advanced										Ta	Inheritance Set	tings 🖳 Policy A
Filter by Device							Rule Conflic	Detection 🥹	Add Category	Add Rule	e Search Rul	es
# Name Source Dest Zones Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Por	rts Dest Ports	URLs	ISE/SGT Attributes	Acti	on	U 🗅 🔒 🗇 I
✓ Mandatory - test_rest (-)												
There are no rules in this section. Add Rule or Add Category												
✓ Default - test_rest (-)												
There are no rules in this section. Add Rule or Add Category				_		_						
Default Action									Network Disco	very Only		

cisco Live!



Create a new Intrusion policy

Create Intrusion Policy		7 X
Policy Information Name * Description	Targeted disabled rules	
Drop when Inline Base Policy * Required	My Intrusion Policy	Use your custom policy as base policy
		Filter: SID:"23111"
	Create and edit policy and set rule state(s)	Rule State Event Filtering Dynamic State Alerting Comments Generate Events Drop and Generate Events Disable Generate Events Disable

cisco ile

Add AC rule to use intrusion policy on targeted hosts



			Editing F	Rule - Targete	ed IPS inspec	tion						? ×		
Terret			Name T Action	argeted IPS inspe	<u>Move</u>									
source	Us tar	e geted	Intrusion F Targeted	Intrusion Policy Targeted disabled rules Variable Set Default Set										
hosts	pol	icy	File Policy jg file									v <i>Ø</i>		
											Save	Cancel		
						_								
4 Targeted IPS inspection	Any Any	🚍 62_netw Ar	ny Any	Any	Any Ar	ny Any	Any	Any	🖌 🚺 🗸 🗸 🖌	2 🖆 🗾 0	a			
➡ Default - JG AC (all) (5-	-5)													
5 inspect it all	Any Any	Any Ar	iy Any	Any	Any Ar	ny Any	Any	Any	🖌 Mlow 🤟 🥼	R 📩 📘 0	I			
Default Action						Intrusi	on Prevention: I	My Intrusion Po	licy	× 🦉	ş 📕			

Snort Performance



Low IPS performance? ... rule it out by FTD rule profiling!

Edit /ngfw/var/sf/detection_engines/<uuid>/ advanced/perf_monitor.conf

config profile_rules: print all, sort avg_ticks, filename /ngfw/var/log/profiling-rules.log config profile_preprocs: print all, sort avg_ticks, filename /ngfw/var/log/profiling-preprocs.log

Performance Settings					? ×
Pattern Matching Limits	Performance	e Statistics	Regular Expression Limits	Intrusion Event Logging Limits	
Sample time (seconds)		300			
Minimum number of packets		0			
Troubleshooting Options					*
Log Session/Protocol Distribu	ition				
Summary	(v			
Revert to Defaults				OK Cancel	

Restart Snort pmtool restartbytype snort Start rule profiling > system support run-rule-profiling

Low IPS performance? ... rule it out by FTD rule profiling!

Jan	30	10:34:07	ciscoasa	SF-IMS[29795]:	Prepr	ocessor Profile Statist	ics (wo	orst 100)							
Jan		10:34:07	ciscoasa	SF-IMS[29795]:											
Jan		10:34:07	ciscoasa	SF-IMS[29795]:	Num	Preprocessor	Layer	Checks	Exits	Microsecs	Avg/Check	Pct of Caller	Pct of Total		
Jan		10:34:07	ciscoasa	SF-IMS[29795]:	===			======							
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		fwApp		388	388	13759	35.46	24.22	24.22		
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		fwAppTP		363	363	5530	15.23	40.19			
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		fwLibAppTP		52	52	4621	88.87	83.57	8.14		
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		fwServicePat		123	123	4692	38.15	34.10	8.26		
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		luaDetectors		72	72	3601	50.02	26.18	6.34		
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		cisco		72	72	3596		99.87	6.33		
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		<pre>1cisco_7e11c2fa-d3dd-42d</pre>	<mark>a9</mark> -b71a	-8db3e71d9571		71 71		3410	48.03	94.81	6.00
Jan		10:34:07	ciscoasa	SF-IMS[29795]:		2cisco_90d30535-1aec-459	98 <mark>-</mark> 835a	-e20c321b562e				175 1	175.25	4.87	0.31
Jan	30	10:34:07	ciscoasa	SF-IMS[29795]:	4	fwClientPat	1	83	83	624	7.53	4.54	1.10		

Jan	30	10:34:07	ciscoasa	SF-IMS[29795]:	Rule H	Profile St	atis	tics	(all rules)							
Jan	30	10:34:07	ciscoasa	SF-IMS[29795]:								==				
Jan	30	10:34:07	ciscoasa	SF-IMS[29795]:	Nur	n SII) GID	Rev	Checks	Matches	Alerts	Microsecs	Avg/Check	Avg/Match	Avg/Nonmatch	Disabled
Jan		10:34:07	ciscoasa	SF-IMS[29795]:	===		====	===								
	30	10:34:07	ciscoasa	SF-IMS[29795]:		42892						24	12.2	0.0	12.2	
	30	10:34:07	ciscoasa	SF-IMS[29795]:												

cisco ile

Performance graphs from the WebUI

hboards • Reporting	Summary > Intrusion Event Performance							
	Intrusion							
	Intrusion Event Statistics	Select Device	Select Graph(s)	Select Time Range				
			Avg Bytes/Packet	Last Hour				
	Intrusion Event Performance		ECN Flags Normalized in TCP Traffic/Packet	Last Day				
	Intrusion Event Graphs		ECN Flags Normalized in TCP Traffic/Packet * ECN Flags Normalized in TCP Traffic/Session	Last Week				
	Discovery		ECN Flags Normalized in TCP Traffic/Session *					
	Discovery Statistics		ICMPv4 Echo Normalizations					
	Discovery Performance		ICMPv4 Echo Normalizations *					
	biscovery renormance							
	Connection Summary		*Occurred when Inline Mode was disabled	Graph				

Average Bytes Per Packet (Last Day (24 hours)) - (2018-01-29 05:00:00 - 2018-01-30 04:09:24)



Why does Bytes/Packet matter?





Reassembly...

Posted throughput ratings for the Firepower appliances are usually rated at 1518 bytes packets. Smaller packets results in more processing.

- 1MB of traffic with 1518 bytes/packets = ~ 658 packets
- 1MB of traffic with 400 bytes/packet = ~ 2500 packets

Every packet header must be evaluated and the packet has to be placed into the buffer for re-assembly. The larger number of packets to process requires more CPU time.

Let's talk about the elephant in the room...



- Large flows are generally related backup, database replication, etc. which usually does not require inspection
- Sort Analysis > Connections for connection size to find top talkers
- Once we determine the top talkers, and confirm they can be safely ignored, we create trust rule for the IP conversations.
- Mitigations IAB / Pre-Filter fast-path

State	On 💙
Performance Sample Interval (seconds)	0
Bypassable Applications and Filters	O Applications/Filters
	O All applications including unidentified applications
inspection Performance Thresholds	Hide
Drop Percentage	0
Processor Utilization Percentage	90
Packet Latency (microseconds)	5000
Flow Rate (flows/second)	0
low Bypass Thresholds	Configure

Overview	Analysis	Poli	cies			
Access Cont	rol 🕨 Prefi	lter	Netv			
Access Contr	^{ol} efilte	r Po	licv			
Intrusion	cy with	default	action t			
Malware & Fi	le					
DNS	⇒ Fastpa	ath				
Identity	🛷 Analy:	🌶 Analyze				
SSL	🗙 Block	🕻 Block				
Prefilter	⇒ Fastpa	Fastpath				

Lab Overview & Instructions

cisco live!

Lab Topology – Interfaces, IPs and Credentials



Make Copy of AC Policy in local domain

For labs 2-4 you will need to make a copy of the AC Policy in your local domain and assign it to the device and deploy in order to start the lab. Some example screenshots for doing this are below.



Make Copy of AC Policy in local domain (cont)





Goals / Best Practices / Hints

- 1. Fix the problem without degrading the security posture of the network
- 2. Avoid deploys as a troubleshooting step to save time
 - Leverage tools to identify the problem
 - Deploy when you have possible solution
- 3. Some labs may have more than 1 problem
- 4. Do NOT change your security zones
- 5. Ask for help if you are stuck

Note at the start of each lab you should not be able to reach the resource. If the resource is immediately available, something has gone wrong with lab setup. Please ask for help!



Goals / Best Practices / Hints

WKST Desktop background

Hostname : EC2AMAZ-KKBF7JP Instance ID : i-0903b575521578f9a Private IP Address : 172.31.250.35 Public IP Address : 52.28.167.54 Instance Size : t2.small Availability Zone : eu-central-1a Architecture : AMD64 Total Memory : 2048 Network : Low to Moderate This is <u>NOT</u> the inside IP, it is the
RDP private IP. do not filter on this on the FTD, you will not see it there.

On your local desktop you will see a link to box that has all of the information for your personal lab. Use this to find the IPs you need to connect to and login information for the FMC, FTD, WKST.

Windows command tips

ctrl+r, type "cmd", press enter to get a terminal route print - prints routes, make sure only 1 default route going to FTD ipconfig - list interfaces and ip addresses ping <host> - simple icmp ping test



Lab 1

Introduction to Problem Component Identification



Lab 1 steps

- 1. Open an RDP session to WKST (IP address is on your sticky note)
- 2. Open a new window in chrome
- 3. Type "www.cisco.com" into the browser URL bar and hit enter
- 4. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue.



Problem Description

WKST is unable to reach www.cisco.com

Instructions

Using the tools introduced, determine why the connection is unsuccessful.

Hints

Prefilter policy fastpath
 Capture w/ Trace
 Ping next hop


- What is the first thing that a connection will do
- Domain Name Resolution
- What should be your Capture W/ Trace Filter

- Protocol IP
- Network 172.31.100.0 Netmask 255.255.252.0
 - Look for Port 53 traffic

Capture W/ Trace output structure

172.31.100.7.64579 > 8.8.8.8.53 UDP 28 Src IP.Port > Dst IP.Port Proto length





Root Cause

No route to host

Solution

Correct the default route by either specifying manually or by enabling DHCP route

Capture w/trace

Lab 1 - Troubleshooting	C Packets Shown: 26 / Packets Captured: 26 / Traces: 26 ✓ 1: 19:46:26.687159 172.31.100.12.58230 > 172.31.0.2.53: udp 34 > G Phase 1: Result=ALLOW Type=CAPTURE > G Phase 3: Result=ALLOW Type=ACCESS-LIST > G Phase 3: Result=ALLOW Type=INPUT-ROUTE-LOOKUP > G Phase 4: Result=ALLOW Type=undefined
SHELL	> C Phase 5: Result=ALLOW Type=ACCESS-LIST
	Phase 6: Result=ALLOW Type=CONN-SETTINGS
> ping 172.31.1.1	Phase 7: Result=ALLOW Type=NAT
Please use $ TR +C $ to cancel/abort	C Phase 8: Result=ALLOW Type=NAT
Sonding E 100 byte ICMD Echoc to 172 21 11 timoout is 2 coconds:	Phase 9: Result=ALLOW Type=IP-OPTIONS
sename 5, 100-byte ICINP ECHOS to 172.31.1.1, timeout is 2 seconds.	> 📁 Phase 10: Result=ALLOW Type=QOS
	> 📁 Phase 11: Result=ALLOW Type=INSPECT
Success rate is 0 percent (0/5)	> 📁 Phase 12: Result=ALLOW Type=NAT
>	> 📁 Phase 13: Result=ALLOW Type=QOS
	> 📁 Phase 14: Result=ALLOW Type=NAT
	> 📁 Phase 15: Result=ALLOW Type=IP-OPTIONS
	> 📁 Phase 16: Result=ALLOW Type=FLOW-CREATION
	> 📁 Phase 17: Result=ALLOW Type=EXTERNAL-INSPECT
	> 📁 Phase 18: Result=ALLOW Type=SNORT
	> 📁 Phase 19: Result=ALLOW Type=SNORT
SHELL	> 📁 Phase 20: Result=ALLOW Type=SNORT
	V 1 Phase 21: Result=ALLOW Type=INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
> show interface outside	Phase: 21
Interface TenGigabitEthernet0/1 "outside" is up line protocol is up	Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Hardware is not one BW 10000 Mbsc DIV 10 uses	Subtype: Resolve Preferred Egress interface
Hardware is het_ena, bw 10000 kings, Det to used	Result: ALLOW
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)	Elapsed time: 11253 ns
Input flow control is unsupported, output flow control is unsupported	Config:
MAC address 020b.7c28.ac87, MTU 1500	
IP address 172.31.200.170, subnet mask 255.255.255.0	Found next-hop 172.31.1.1 using egress ifc outside(vrfid:0)
	Result:
	input-interface: inside(vrfid:0)
	input-status: up
	input-line-status: up
	output-interface: outside(vrfid:0)
	output-status: up
Notice that 172 31 1 1 is not in subpet for out	output-line-status: up
	Action: allow
	Time Taken: 19067933 ns

cisco Live!

Lab 1 – Root Cause

Misconfigured routes - Only static route is for GW 172.31.1.1 which is incorrect for the outside subnet 172.31.200.0/24 the GW should be 172.31.200.1





Lab 1 – Solution

Step 1: Delete Static Route





Lab 1 – Solution – Continued



If you see this, you likely deleted the Static route, but didn't enable DHCP route





Lab 2 - Security Intelligence



Lab 2 steps

- 1. Make a copy of the "Lab 2 (SI)" AC Policy in your local domain and assign it to the FTD and deploy (see help slide)
- 2. Open an RDP session to WKST (see local note)
- 3. Open a new incognito window in chrome
- 4. Type "https://snort.org" into the browser URL bar and hit enter
- 5. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue.
- 6. Do NOT try to modify anything in the Global SI lists and do not delete them from the policy to fix this. Figure out how.....



Make a copy of the "Lab 2 (SI)" AC Policy in your local domain

								,
Access Control Policy	Domain	Status	Last Modified	Lock Status				
Base_Policy	Global	Targeting 0 devices	2024-01-22 15: Modified by "adm	28:15 nin"	r _e		٩	Ĩ
Branch Access Control Police	Global	Targeting 1 devices Up-to-date on all targe	2024-01-24 11: Modified by "jgro	53:49 betzi"	r _e	8	٩	Ì
Lab 2 (SI)	Global	Targeting 0 devices	2024-01-22 15: Modified by "adm	28:15 nin"	⁶ 8		٩	Ì
Lab 3 (AC)	Copy Access C	ontrol Policy		28:15 hin"	Fe		٩	Ì
Lab 4 (IPS)	Name:			28:15 1in"	F		٩	W
Lab 5 (Identity)	Local Lab 2 (51)			28:15 nin"	F <u>a</u>		٩	Ì
Minimal Access Control Po		Cance	ОК	28:15 nin"	F	8	٩	Ŵ

cisco live!

Assign Policy o. 💕 🌣 👩 admin 🗸 Deploy cisco SECURE Try New UI Layout Om Analyze Hit Counts Inheritance Settings Policy Assignments (SSL Policy: None dontity Dolin Default Prefilter Policy_3 \times Show Rule Conflicts 2 + Add Category Policy Assignments 0 Confirm **Targeted Devices** Select devices to which you want to apply this policy. Following devices already have assignments listed below. These devices will be Δ Available Devices Selected Devices Impacted Devices reassigned to current policy Q. Search by name or value device: NGFW1 - policy: Lab 2 (SI) Add to Policy Do you want to continue with above changes? No Cancel





Problem Description

WKST is unable to reach snort.org

Instructions

- Using the tools introduced, determine why you cannot reach snort.org.
- 2. BONUS Resolve the issue

Hints



Connection Events

Capture w/Trace

Capture w/trace

Lab 2 - Troubleshooting

Capture W/ Trace tells us its dropped by Security Intelligence.. Device: FTD Seat 1 **Clear All Packets** C Auto Refresh Interval (seconds): 10 Enable Auto Refresh v Ruffer Buffer Buffer Packet N Interface Trace Protocol Source Destination Status Туре Mode Size Length Status outside raw. 33554432 1518 Cap. IP anv any ...But which Security Intelligence list? Format: Tree (Full) C Packets Shown: 109 / Packets Captured: 109 / Traces: 75 $\overline{}$ 31.721047 172.31.100.10.53626 > 104.18.139.9.443: \$ 567434125:567434125(0) win 62727 <mss 8961,nop,wscale 8,nop,nop,sackOK> Drop-reason: (snort-blacklist) Packet is blacklisted by snort, Drop-location: frame 0x00005574dc341f61 flow (NA)/NA 1: Result=ALLOW Type=CAPTURE 2: Result=ALLOW Type=ACCESS-LIST > D Phase 3: Result=ALLOW Type=FLOW-LOOKUP > Description Phase 4: Result=DROP Type=SNORT V C Result :drop Result input-interface: inside(vrfid:0) input-status: up input-line-status: up Action: dron rop-reason: (snort-blacklist) Packet is blacklisted by snort, Drop-location: frame 0x00005574dc341f61 flow (NA)/NA on sackOK> > 📫 3: 19:54:31.955547 172.31.100.10.53628 > 104.18.139.9.443 S 3342407677;3342407677(0) win 62727 <mss 8961.nop.wscale 8.nop.nop.sackOK> 54:34.676097 172.31.100.10.50786 > 172.217.16.196.443: udp.1250



Lab 2 - Continued





ENABLED

Security Intelligence Events (switch workflow)

No Search Constraints (Edit Search)

_	Secu	rity	Intelligence with Applie	cation Detail	ls Ta	ble View o	f Security Intelligen	ce Events				_			
	Jump	to.													
	(↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder I	Р	Responder Country	S. Cate	gence	Ingress Security Zone	
	• (2024-01-26 10:43:24		Block	IP Block	- 172.31.100.10		6 104.18.	139.9	🔤 USA	Custom_List	t	InZone	
	• (2024-01-26 10:42:25		Block	IP Block	- 172.31.100.10		0 104.18.	138.9	🚾 USA	Custom_List	t	InZone	
	• (2024-01-26 10:42:04		Block	IP Block	- 172.31.100.10		0 104.18.	139.9	🚾 USA	Custom_List	t	InZone	
										Open in New Window					
										Exclude					
										Whois					
										View	Host Profile				
	I of 1 > > Displaying rows 1-3 of 3 rows							Add IP to Block List							
	View Delete														
	Onen in Context Explorer														

cisco lite

SI List

Lab 2 – Continued – Do-Not-Block-List

We added the IP to the Do-Not-Block List

...Why does it still not work?

Loc	al Lab 2 (SI) 2	
Rules	Security Intelligence	Prefilter Pol

Umbrella DNS Policy	1 ¢ >
None	

📕 Important Note

- Do-Not-Block lists are specific to FMC domain(tenant).
- A user in a sub-domain on FMC can only add to their domains Do-Not-Block list





Lab 2 – Solution



Add Domain-Do-Not-Block URL & Network List to Access Control Policy



Add the 2 Snort.org IP addresses to the Domain-Do-Not-Block-List



Enable Logging for URL Security Intelligence Events



Add snort.org to the URL Domain-Do-Not-Block-List



Lab 3- Access Control



Lab 3 steps

- 1. Make a copy of the "Lab 3 (AC)" AC Policy in your local domain and assign it to the FTD and deploy (see help slide)
- 2. Open an RDP session to your WKST (See local note for IP)
- 3. Open a new incognito window in chrome
- 4. Type "http://www.cnn.com" into the browser URL bar and hit enter
- 5. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue. You should only modify the configuration to allow cnn traffic but do not just fastpath at the top of the policy, that is too easy ;) find what is blocking and make the appropriate change(s). Once you have the site allowed, see if anything else on the page isn't loading properly (but don't worry about fixing everything for the lab, just main site loading is all that is required but feel free to do more to get the site working to learn more)

Lab 3 Scenario



Problem Description

WKST is unable to reach www.cnn.com

Instructions

Using the tools introduced, determine why the connection is unsuccessful.

Hints

Prefilter policy fastpath
 Enable AC rule logging
 firewall-engine-debug

Lab 3 Solution

inside

Root Cause

Multiple AC Rules blocking the connection

Solution

Correct the AC rules to allow the traffic



aws

146.75.119.5

146.75.119.5

USA

USA



443 (https) / tcp

80 (http) / tcp

HTTPS

HTTP

CNN.com

CNN.com

https://www.cnn.com

http://www.cnn.com/favicon.ico

cisco	1 isol
CISCO	Me:

= 172.31.100.10

- 172.31.100.10

Block with reset

Block with reset

Access

Local Lab 3 (AC)

Local Lab 3 (AC)

Control Rule

Block Fake News

Block Fake News

Block Fake News

×



cisco ile

Lab 3 Solution





firewall-enginedebug



SHEL

> system support firewall-engine-debug

Please specify an IP protocol: tcp Please specify a client IP address: 172.31.100.10 Please specify a client port: Please specify a server IP address: Please specify a server port: Monitoring firewall engine debug messages

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 New firewall session

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Starting with minimum 9, 'block multimedia', and VLan first with zones 3 -> 4, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, svc 0, payload 0, client 0, misc 0, user 9999997 172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 pending rule order 9, 'block multimedia', AppID 172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 app event with client changed, service changed, payload changed, referred no change, misc no change, url changed, tls host no change, bits 0x969C

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Starting with minimum 9, 'block multimedia', and VLan first with zones 3 -> 4, geo 0(xff 0) -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, svc 676, payload 1190, client 589, misc 0, user 9999997, url http://www.cnn.com/, host www.cnn.com, no xff

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 match rule order 9, 'block multimedia', action Block 172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Sending HTTP block response page (605 bytes) 172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Deleting Firewall session

Enable logging



Turner Broadcasting System's news website.

dulu Context Explorer	w Wikipedia	G Google	Yahoo!	Bing				
Tags	displays	displays ads, NSG, SSL protocol						
Categories	multimedia (tv/video), news							
Business Relevance	High							
Risk	Very Lov	N						
Туре	Web Ap	plication						





Lab 3 Solution

Add a rule above "block multimedia" (Rule 9) to allows certain apps and add CNN.com app



cisco live!

Lab 4 – Intrusion Prevention System (IPS)

cisco live!

Lab 4 steps

- 1. Make a copy of the "Lab 4 (IPS)" AC Policy in your local domain and assign it to the FTD and deploy (see deploy help slide)
- 2. Open an RDP session to WKST (see local note for IP)
- 3. Open a new incognito window in chrome
- 4. Navigate to http://172.31.200.8/evil.pdf (browser may try to force http://">http://")
- Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue and retain as much security efficacy as possible (Pro Mode: Changes made should only impact 172.31.200.8).
- 6. Note: for proper completion of lab make sure you have a File event for the PDF Use https://docs.snort.org/start/rules for snort3 rule documentation

Bonus: Multiple rules blocked this, can you make 1 rule which has the criteria of all rules that were blocking this and still match? If you do show the instructor for a prize. Hint: <u>https://docs.snort.org/rules/options/payload/http/req_resp_detection</u>

Lab 4 Scenario



Problem Description

WKST is unable to download the file at http://172.31.20.8/evil.pdf

Instructions

Using the tools introduced, determine why the connection is unsuccessful.

Hints

Intrusion Events system support trace



113

Lab 4 Verify Completion

If the file is allowed you should see a file event with sha256 2f55d0b4d7bfe0f78636a990c8dd152245a0e6bc2daf3eee445c0300ea746672

Sending IP \times	Sending × Country	Receiving IP \times	Receiving × Country	Sending × Port ×	Receiving × Port	SSL Status ×	User ×	File Name ×	SHA256 ×	,	Threat × Score	Туре ×	Category ×	Size (KB) ×	URI ×
- 172.31.200.8		🖵 172.31.100.88		80 (http) / tcp	49791 / tcp			evil.pdf	O 2f55d0b4	ea746672		PDF	PDF files	33.558	/evil.pdf

Please note: If you just fastpath traffic and the PDF loads but you still want to try the lab after you have downloaded the PDF be aware the browser local cache will prevent more downloads, clear browser cache/history before retrying.

Lab 4 Troubleshooting (events)



Unified Event Viewer (UEV)



Lab 4 Solution (Variant: Disable IPS Rule from global rule settings)

Analysis > Intrusions > Events

)

			Plant C
Message ×	Classification ×	Generator ×	the glob
Evil pdf uri (2000:3000001:4)	Misc Activity	Standard Text Rule	
Evil pdf uri (2000:3000001:4)	Open in New Wi	ndow d Text Rule	
Evil pdf uri (2000:3000001:4)	Exclude	d Text Rule	
Evil pdf uri (2000:3000001:4)	Alert Rule	rd Text Rule	
Evil pdf uri (2000:3000001:4)	Block Rule	d Text Rule	
Evil pdf uri (2000:3000001:4)	Reject Rule	d Text Rule	
Evil pdf uri (2000:3000001:4)	Pass Rule	d Tex Rule	
	Drop Rule		
	Disable Rule		
	Threshold		
	Suppression		
	Edit Rule Action		Ø
	2000:300 Evil pd	furi	
	 O All Policies 	O Per Intrusion Policy	
	DISABLE		~
	Comments (optional)		
	Provide a reason to c	hange if applicable	[
	Comments can be tracked	d in rule comment history per Intrusion Policy	
			Cancel Save
isco ile			

Right click on the rule message > Disable Rule takes you to the global snort3 rules



If there are no IPS policies in your local domain you will see this view and you can not make changes from here since all polices are in global domain. You will need to create a new IPS policy in your domain

	All Rules										
	All rules assigned to current intrusion policy irrespective of rule group										
	Rule Actions V GID:2000 X SID:3000001 X										
→_ 1 ▼ 49,848 rules											
	GID:SID Info	Rule Action	Assigned Groups								
	> 2000:3000001 Evil pdf uri	Block V (Overridden)	ciscolive								

If there are IPS policies in your local domain you will see this view and you can disable per policy from here

Lab 4 Solution (make new IPS policy)

Navigate to Policies > Intrusion and create a new policy. Use "IPS Lab IPS Policy" as the base policy to keep same security posture.

Policies Devices Objects Integration	Deploy Q 🥥 🌣 🖉 Seat6 \ Seat6 V 📩	1 Create	e new Policy
olicy	All IPS Rules IPS Mapping Compare Policies Create Policy		
Base Policy Create Intrusion Policy Name* Local Lab IPS Policy Seat 6 Description	Usage Information Access Control Policies Device Snort 2 Version Snort 3 Version	2 Use "I as bas	PS Lab IPS Policy" se policy
Inspection Mode		Error	Ø
 Detection Prevention Intrusion rule actions are always applied. Connections that match a drop rule are blocked. Base Policy 		Error saving policy: Polic Policy names must be u different domain)	cy name "Local Lab IPS Policy" is in use. nique (Duplicate policy might exist in a
IPS Lab IPS Policy		If you get this e	error just add something
Cancel Sa			policy flattic, like seat h

Lab 4 Solution (edit new IPS policy)

Edit the newly created IPS Policy



Lab 4 Solution (edit AC policy)

Edit the AC Policy and use the new IPS Policy to target by IP





system support trace!


Lab 4 Troubleshooting

Trace



> system support trace

Please specify an IP protocol: tcp Please specify a client IP address: Please specify a client port: Please specify a server IP address: 172.31.200.8 Please specify a server port: 80 Enable firewall-engine-debug too? [n]: n Monitoring packet tracer debug messages [...Omitted for brevity...]

172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Packet 1297: TCP ***A****, 02/07-07:39:13.504353, seq 1778302888, ack 988312753, dsize 1380 172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 File: Type-PDF found 172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Event: 2000:3000002:4, Action block 172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Stream: pending block, drop 172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Policies: Network 0, Inspection 0, Detection 5 172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Verdict: blacklist 172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Verdict: blacklist

Snort configurations Lab 4 Solution (Find the suppression)



122

Go to Objects > Intrusion Rules [Snort3 All Rules] Then expand the local rules group and click "ciscolive"

> 2000:3000002 detect PDF options	Block (Default) (Overridden)	ciscolive Suppres	ision 💉 🗑
> 2000:3000005 this is a bad rule, do not even look	🖉 Disable (Default) 🗸	ciscolive None	X
> 2000:3000006 no bad-mouthing snort3!	Block (Default) V (Overridden)	ciscolive None	≠ îi
> 2000:3000003 block evil text	Block (Default) V (Overridden)	ciscolive None	1
> 2000:3000004 johns test rule	Alert (Default) V (Overridden)	ciscolive None	≠ îi
f trying to disable from this view you may get an error since this is trying to set the global setting and you don't have permission from this domain. Select "Per Intrusion Policy" instead Block (Overridden) Ciscolive Error while saving. Retry	Block Block Alert Rewrite Prop Pass C Disable (Default) C Propetoticular (C Propetoticular (C Propetoticular (C Propetoticular (C Propetoticular (C Propetoticular (C) Propetoticular (
cisco litter	Alternatively, you can go to	the intrusion policy to dis	sable it
	LTRSEC-	3880 © 2024 Cisco and/or its	affiliates. All rights reserved. Cisco Public

Lab 4 Solution



Disable for local IPS policy from Global rules view

Edit Rule Action		0
2000:300 detect PDF options		
O All Policies O Per Intrusion Policy		- 1
Policy	Rule Action	
Local Lab IP Policy Seat 6	BLOCK 🗸	
Add Another	BLOCK ALERT	
Provide a reason to change if applicable	REWRITE	
	PASS	
	DROP	Save
	REJECT	
	DISABLE	
	DEFAULT	



Lab 4 Solution



Root Cause

Multiple IPS Rules blocking the connection

Solution

Disable the IPS rules using a custom IPS policy and AC rule to only target the EC2 instance IP





Lab 4 Pro Mode Check and Extra Questions

- If you navigate to the external IP of the EC2 from WKST (http://18.196.106.219/evil.pdf), is the pdf blocked? If you targeted the internal IP of the EC2 correctly this should still be blocked (Assuming no local cache of the PDF)
- 2. Can you find the "hidden" text message in the PDF?
- 3. Go to /evil.txt uri on the EC2, is it blocked? It should block if you didn't break security posture during lab.
- 4. There is a rule for that text message, why didn't the IPS rule block the text in the PDF but it blocked the text in the .txt file?

Lab 4 Bonus

Bonus: Multiple rules blocked this pdf, can you make 1 rule which has the criteria of **all** of the rules that were successfully blocking this and still match? If you do show the instructor for a prize.

i.e. if 3 rules blocked this then can you combine all of the constraints (rule bodies) from those rules into 1 rule and have it block the pdf? If you do show the instructor for a prize.

Hint: <u>https://docs.snort.org/rules/options/payload/http/req_resp_detection</u>

Continuing Education

cisco live!

Cisco Secure Firewall YouTube

Knowledge from TAC / TMEs

- New Feature Walkthroughs
- Troubleshooting Tips
- Automation Guides









Cisco Secure



Cisco Security Beta Programs



Influence product design

Design research participants shape the look, feel, & functionality of new product features and offerings



Attention to Feedback

Beta customer bugs and enhancements receive high visibility & priority



Top notch communication Private conference calls with product team



E) Training

Customers receive early training & experience with new features

Customer Support

Feature experts will be on-hand & responsive to your issues

Sign-Up Now: https://cs.co/security-beta





Thank you





cisco live!

Let's go