

# ةنمآلا ةياهنلا ةطقنل ةصاخلا ةباحسلا جم د ينورتكلإلا ديربلا و نمآلا بيولا عم

## تايوتحملا

---

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[لمك تالا ةعباتم لبق ةحصلا نم ققوحتلا](#)

[عارجلا](#)

[ةنمآلا ةياهنلا ةطقنل ةصاخلا ةباحسلا نيوك](#)

[نمآلا بيو زاهج نيوك](#)

[Cisco نم نمآلا ينورتكلإلا ديربلا نيوك](#)

[ينورتكلإلا ديربلا و نمآلا بيولا نم AMP تالجس راضح او طخ](#)

[Secure Endpoint Private ةباحسو Secure Web Appliance نيول لمك تالا راب تخ](#)

[SWA ليلا لوصولا تالجس](#)

[SWA ل AMP تالجس](#)

---

## ةمدقملا

زاهج عم ةصاخلا ةنمآلا ةياهنلا ةطقن ةباحس جم دل ةبولطملا او طخلال دنن تسملا اذه فص ي  
(ESA) ةنمآلا ينورتكلإلا ديربلا ةباوبو (SWA) نمآلا بيولا

## ةيساسألا تابلطتملا

ةيلال عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- AMP ةنمآلا ةياهنلا ةطقنل ةيرهاظلا ةصاخلا ةباحسلا
- (SWA) نمآلا بيولا زاهج
- ةنمآلا ينورتكلإلا ديربلا ةباوب

## ةمدختسملا تانوكملا

SWA (نمآلا بيولا زاهج) 15.0.0-322

AMP 4.1.0\_20231109226 ةيرهاظلا ةصاخلا ةباحسلا

14.2.0-620 ةنمآلا ينورتكلإلا ديربلا ةرابع

---

عيمي جلة فيضارت فال او في دام لال تاني اب تال نم لك لة حل اص قئ اول دعت :ة طحال مة  
ة في نعمل اتاجت نم لال

---

ة صاخة في لمعم ة ئي ب في ة دوجوم لال ة زهجال نم دنن سمل ال اذ في ة دراو لال تامول عمل ال عاشن ا م ت  
ت ناك اذ (في ضار ت فال) حوس مم نيوك ت ب دنن سمل ال اذ في ة مدخت سمل ال ة زهجال ال عي مج ت اد ب  
رم ا ل ال لمحت حم لال ري ثا ت ل ل كم ه ف نم دك ا ت ف ، لي غ ش ت ال دي ق ك ت ك ب ش

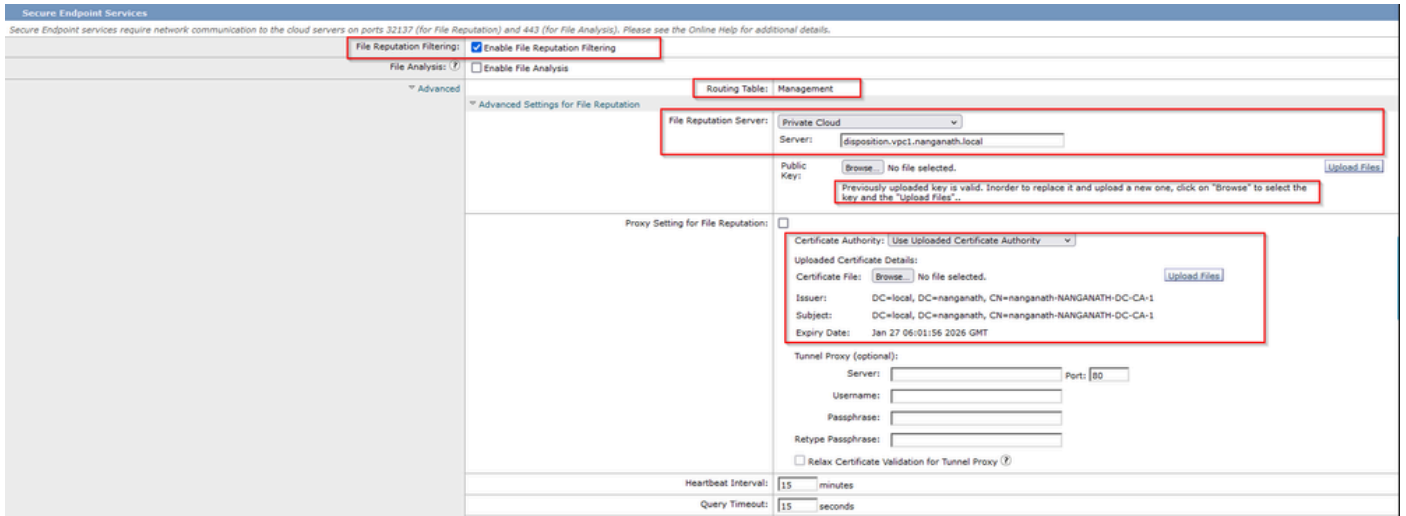
## لم ا ك ت ال ة ع ب ا ت م ل ب ق ة ح ص ل ال نم ق ق ح ت ال

1. صي خا ر ت ال م ه ي د ل ن ا ك Secure Endpoint Private Cloud/SWA/Secure Email Gateway اذ ا م ق ق ح ت ال  
ص ي خ ر ت ال ن ي ك م ت د ن ع SWA/Secure Email ة ز ي م ل ال ح ا ت ف م نم ق ق ح ت ال ك ن ك م ي . ة ب و ل ط م ل  
ي ك ذ ل ل .
2. ت ن ا HTTPS رورم ة ك ر ح ص ح ف ل ط ا خ ت ت ن ك اذ SWA ل ع HTTPS ل ي ك و ن ي ك م ت ب ح ي .  
ق ي ق د ت ة م س ف ل م ي ا ت ز ج ن ا HTTPS in order to ة ك ر ح ر ي ف ش ت ك ف ي ن ا ج ا ت ح ت  
ة ص ا خ ل ال ة ب ا ح س ل ال ة ا د ا ل / ة م د ق ت م ل ال ة ي ا م ح ل ا ب ة ص ا خ ل ال ة ب ا ح س ل ال ة ا د ا ل ن ي و ك ت ب ح ي .
3. ق ق ح ت ل ل VPC ة د ا ه ش ل ي ل د ل ع و ج ر ل ال ة ا ج ر ل ال . ة م ز ا ل ل ال ت ا د ا ه ش ل ال ع ي م ج و ة ي ر ه ا ط ل ال



## نم آل بي و زا ه ني و كت

1. Secure Endpoint Services GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings
2. عمسة في فصت ني كمت "رايخ لة يور كن كمي" نم آل اة اهن لة طقن تامدخ" مسق تحت "مدق تم" اديج القح رايخ لة اذه ره ظي "ق قحت لة" و، "فلمل"
3. دح "Private Cloud" في File Reputation Server.
4. "Server" كة باحس لة لة اهن لة ري صم لة مداخل صاخ لة في ضم لة مسا ري فوت ب مق.
5. "تافلمل لة ليحت" قوف رقنا. اقباس ه ليزن ت ب تمق يذل ماع لة حات فمل لة ليحت ب مق.
6. نم "ه لة ليحت مة يذل ق دصم لة عجرم لة مادخت سا" رتخ. ق دصم لة عجرم لة ليحت لة رايخ لة كانه. اقباس ه لة ليحت ب تمق يذل ق دصم لة عجرم لة ادهش لة ليحت وة لدس نم لة عم لة لة.
7. ري غت لة لاس را.
8. ري غت لة اءارج.

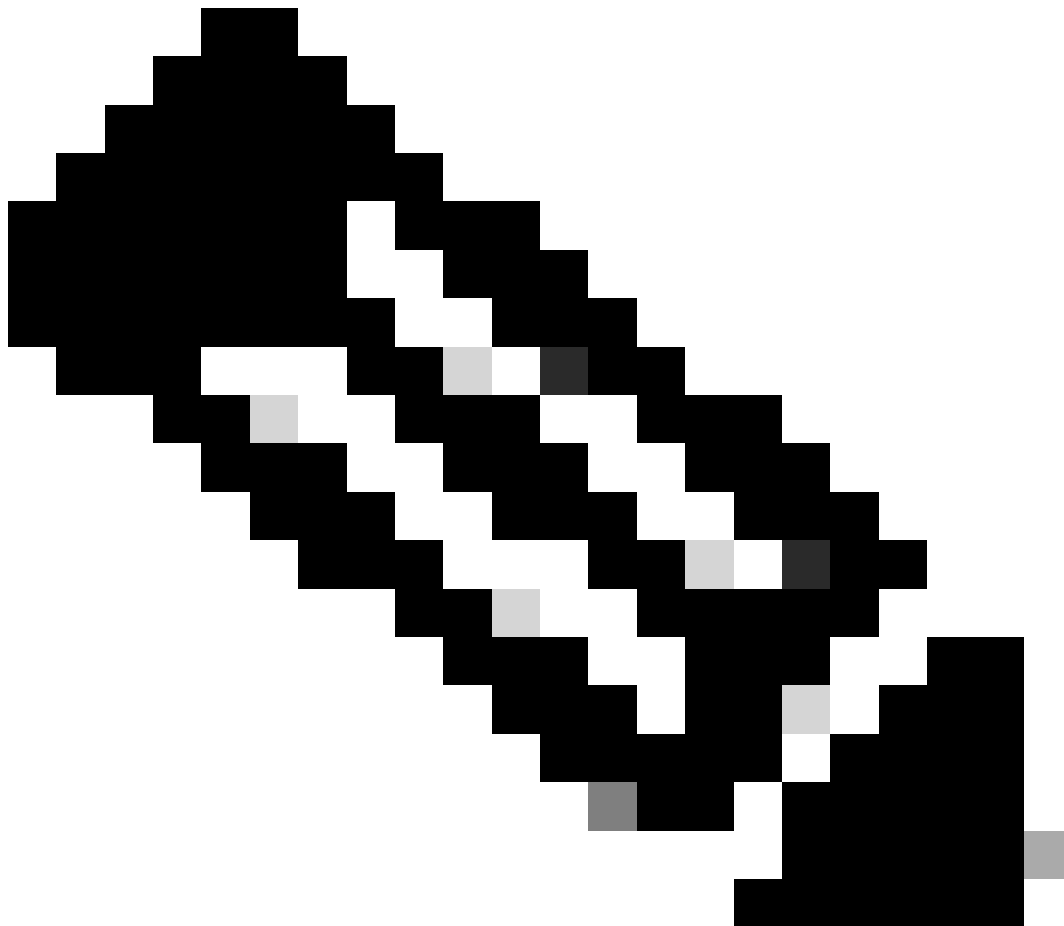


## Cisco نم نم آل بي و نور ت ك لة لة ادي ر ب لة ني و كت

1. Secure Email GUI > Security Services" > "File Reputation and Analysis" > Edit Global Settings > "Enable" or "Edit Global Settings"
2. "فلمل عمسة مداخ" في "ة صاخ لة باحس لة" دح
3. "Server" كة باحس لة لة اهن لة ري صم لة مداخل صاخ لة في ضم لة مسا ري فوت ب مق.
4. "تافلمل لة ليحت" قوف رقنا. اقباس ه ليزن ت ب انمق يذل ماع لة حات فمل لة ليحت.
5. عم لة لة نم "ه لة ليحت مة يذل ق دصم لة عجرم لة مادخت سا" رتخ. ت ادهش لة اة يه لة ليحت. اقباس ه لة ليحت ب تمق يذل ق دصم لة عجرم لة ادهش لة ليحت وة لدس نم لة.
6. ري غت لة لاس را.
7. ري غت لة اب مق.

## Edit File Reputation and Analysis Settings

Advanced Malware Protection	
Advanced Malware Protection services require network communication to the cloud servers on ports 443 (for File Reputation and File Analysis). Please see the Online Help for additional details.	
File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: (?)	<input type="checkbox"/> Enable File Analysis
Advanced Settings for File Reputation	
File Reputation Server:	Private reputation cloud
Server:	disposition.vpc1.nanganath.local
Public Key:	<input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload File"/>
A valid public key has already been uploaded. To upload a new one, click on "Browse" to select the key and then the "Upload File".	
SSL Communication for File Reputation:	Use SSL (Port 443)
Tunnel Proxy (Optional):	
Server:	<input type="text"/>
Port:	<input type="text"/>
Username:	<input type="text"/>
Passphrase:	<input type="text"/>
Retype Passphrase:	<input type="text"/>
<input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy (?)	
Heartbeat Interval:	15 minutes
Query Timeout:	20 seconds
Processing Timeout:	120 seconds
File Reputation Client ID:	cb1b31fc-9277-4008-a396-6cd486ecc621
File Retrospective:	<input type="checkbox"/> Suppress the verdict update alerts (?)
<a href="#">Cache Settings</a>	Advanced settings for Cache
<a href="#">Threshold Settings</a>	Advanced Settings for File Analysis Threshold Score



Cisco نم ةنمآلآ ينورتك لآل دي ربل ةب اوبو Cisco نم نمآلآ بي و زاه دن تسي : ةظحالم فللمل ةعمس ةئيهت دنع ابيرقت تالچسلا سفن في نكراشي و AsyncOS لآل دي ربل ةرابع" وأ "نمآلآ بي و زاهج" ب ةصاخلا AMP تالچس في AMP لچس ةظحالم نكمي ةئيهت لآل طقف اذه ريشي . (ني زاهجلا الك في ةلثامم تالچس) "ةنمآلآ ينورتك لآل لاصتالآ حاجن لآل ريشي مل . SWA و ةنمآلآ ينورتك لآل دي ربل ةب اوب لآل ةمدخللا ءاطخالآ ةدهاشم كنكمي ، ةدهاشللا وأ لاصتالآ في لكاشم يآ دوجو ةلاچ في . لمالكلاب لوصوللا رذعتي" أظخ لآل ريشي ام ابلاغ . "فللمل ةعمس" ةئيهت مت "ةلاس رلا دعب" ةححص ريشي ةدهاش "أظخ وأ "هيلي

## ينورتك لآل دي ربل او نمآلآ بي و لآل نم AMP تالچس راضح اوطخ

1. ةنمآلآ ينورتك لآل دي ربل ةب اوب ةصاخلا (CLI) رم اوآل رطس ةهجاو لآل لوخدلا لچس .  
رمآلآ بتك او "grep"

2. ددح "amp" or "amp\_logs"

3. راهظال تالچسلا ليذت ب مق . تالچسلا ليذتل "Y" بتك او يه امك ىرخالآ لوقحلا ةفاك كرتأ .  
"يداع ريبعت" في خيراتلا ةباتك كنكمي في ، ةميدق ثادحأ نع ثحبت تنك اذا . ةرشابملا ثادحالآ

```
Tue Feb 20 18:17:53 2024 Info: connecting to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info: connected to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info: File reputation service initialized successfully
Tue Feb 20 18:17:53 2024 Info: The following file type(s) can be sent for file analysis: Executables, Document, Microsoft Documents, Database, Miscellaneous, Encoded and Encrypted, Configuration, Email, Archived and compressed. To allow analysis of new file type(s), go to Security Services > File Reputation and Analysis.
```

## إچراخ Secure Web Appliance ةب اوب و Secure Endpoint Private ني ب لمالك تال رابتخ

ققحتلل تاهي بننتللا وأ تالچسلا صحف بچي . SWA نم لاصتالآ رابتخال رشابم رايخ دجوي ال لكاشم يآ دوجو نم .

چاتحت كنأ ةظحالم ءاچرلا . HTTPS نم ال دب HTTP URL ناو نع رابتخاب موقن ، ةطاس ب لآل نم فللمل ةعمس نم ققحت تاي لمع يآل HTTPS رورم ةكرح ريفشت ك في لآل .

AMP صحف صرف متي و SWA لآل لوصوللا جهن في ني وكتللا متي .

بي و لآل زاهج لآل تاسايسلا ني وكت ةيفي ك مهفل SWA [مدختسم لي لآل](#) ةعجارم يچري : ةظحالم Cisco نم نمآلآ .

### Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP.Users Identification Profile: ID.Users All identified users	(global policy)	(global policy)	Monitor: 342	(global policy)	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Disabled	(global policy)		



## SWA AMP تالچس

ت. او طخال هذه مادختساب AMP تالچس راضح| نكمي

1. "grep" رمأل بتكاو SWA ىل لوخذل لچس.

2. ددح "amp\_logs"

3. راهظال تالچس لى لىذت ب مق. تالچس لى لىذت ل "Y" بتكاو يه امك ىرخأل لوقحل افة فاك كرتأ. "يداع ريبعت" ي فخيراتل ابةاتك كنكمي ف، ةمي دق ثادحأ نع ثحبت تنك اذا. ةرشابم لثادحأل

طلخت ال. ةماعل ابةاحس لى او ةصاخال ابةاحس لى لىش لى س فن و دى اذه "ةباحس لى لى cverdict\_from: ةماعل ابةاحس لى نم مكحل لى ب و ه نى ب

```
{'category': 'amp', 'spyname': 'win.ransomware.protected::Trojan.agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status': '18', 'verdict_num': 3, 'analysis_score': 0, 'upload': false, 'file_name': 'bomberbermania.exe.zip', 'decision_source': 'ال', 'extract_file_decision_list': '', 'decision_decision': 'نم', 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_reason': 'نوكم ريغ فللمل اءون', 'sandboxing', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8', 'decision_stmalicious': '', 'malicious_child': none}
```

ةنمأل اةي اهنل اةطقنل ةصاخال ابةاحس لى لىثادحأ تالچس

/data/cloud/log تحت لىثادحأل تالچس رفوتت

"فللمل اةممس لىممع فرعم" مادختساب و SHA256 مادختساب ام لىثادحأل نع لىثحبال كنكمي SWA ب ةصاخال AMP نى وكت ةحفص ي ف "فللمل اةممس لىممع فرعم" دجوى. SWA ب صاخال

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]# less eventlog | grep -E "46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
[cpu:3] ip: "10.186.39.144", "si":0, "ti":3, "tv":6, "qt":42, "pr":1, "ets":1788326235, "ts":1788326232, "tsn":707403179, "lu": "9a7a27a1-46aa-452f-a070-ed78e215b717", "ai":1, "aptus":1344, "ptus":975590, "spero":{"h":00, "fa":0, "fs":0, "ft":0, "hd":1}, "sha256":{"h": "46EE42FB79A161BF3763E8E34A047018BD16D8572F8D31C2CDECAE3D2E7A57A8", "fa":0, "fs":0, "ft":0, "hd":3}, "nord":{"a":1, "dn": "win.Ransomware.Protected::Trojan.Agent.Talos", "url": "http://static1.1.sgsqcdn.com/static/17830757/21908425/1350888016307/Bombermania.exe.zip?token=g5FK10FLU0mnyjXw%2Bpg31jK9wQ%3D", "rd":3, "ra":2, "n":0}
```

TCP ىل لىرشى 3، لوكوتورب لى رادص | PV

ىل لىف لى IP ناو نع ىل لىل لىل اذه هى ف رىشى نامض دجوى ال لىل لىل لىل اذه لهات اءجرل - ip ةممس لى مالعتساب ماق لىل لىمعلل

WSA/ESA ي ف فللمل اةممس لىممع فرعم - UU

SHA256 - فللمل نم SHA256

فشك لى مس ا - DN

ك. لىذ فالى 0، AMP لىل بق نم فللمل اةئجت صحف م لىل اذا 1 - n

rd - DISP\_MALICIOUS ينعى 3 انه. ةباحتس لى ال هى جوت -

1 DISP\_UNKNOWN دعوى فللمل لىتت دى



2. ديمح فلم وه DISP\_CLEAN فلملا نأ دقتعي .

3. راض فلملا نأ دقتعي DISP\_MALICIOUS .

7. فلملا اهيف ىرن يتلا لىلوالا ةرمللا يهو فورعم ريغ فلملا بيترت دعي DISP\_UNSEE .

13. DISP\_BLOCK فلملا ذيفنت مدع بجي .

14. disp\_ignore xxx

15. موقى ةراض تافلم يأ عم لماعتلا بجي و، ديمح فلملا نأ DISP\_CLEAN\_PARENT ربتعي .  
ةفورعم ريغ اهانأ لىل ع اهئاشناب .

16. رورم ةكرح ةبقارم ليمعلا لىل ع بجي نكل و، ديمح فلملا نأ DISP\_CLEAN\_NFM دقتعي .  
هب ةصاخلا ةكبشلا .

ةصاخلا AMP ةباحسو نمآلا ينورتكللالا ديربلا نيبلماكتلا رابتخا

صحف بجي . نمآلا ينورتكللالا ديربلا ةباوب نم لاصتالا رابتخال رشابم راىخ دجوي ال  
لكاشم يأ دوجو نم ققحتلل تاهيبنننلا وأ تالجسلا .

AMP ةطساوب صحفلا ضرفل نمآلا دراوالا ينورتكللالا ديربلا جهن في نيوكتلا ءارجا متي .

### Incoming Mail Policies

Find Policies									
Email Address:				<input checked="" type="radio"/> Recipient <input type="radio"/> Sender		<a href="#">Find Policies</a>			
Policies									
<a href="#">Add Policy...</a>									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	amp-testing-policy	Disabled	Disabled	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ... ...	(use default)	(use default)	(use default)	(use default)	

## Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
<b>Policy:</b>	amp-testing-policy
<b>Enable Advanced Malware Protection for This Policy:</b>	<input checked="" type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> Use Default Settings (AMP and File Analysis Enabled) <input type="radio"/> No
<b>Message Scanning</b>	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
<b>Unscannable Actions on Message Errors</b>	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
<b>Unscannable Actions on Rate Limit</b>	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
<b>Unscannable Actions on AMP Service Not Available</b>	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
<b>Messages with Malware Attachments:</b>	
Action Applied to Message:	Drop Message
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: MALWARE DETECTED]
Advanced	Optional settings.
<b>Messages with File Analysis Pending:</b>	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Message Attachments with File Analysis Verdict Pending : (?)	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: ATTACHMENT(S) MAY CONTAIN
Advanced	Optional settings.

ESA فلم اذه .راض ريغ فلم مادختساب ربتخمل ال

تالچس الـينورتكلال دي ربل ني مات

```

Tue Feb 20 11:55:58 2024 Info: New SMTP ICID 43855 interface Management (10.106.39.193) address 10.110.172.122 reverse dns host unknown verified no
Tue Feb 20 11:55:58 2024 Info: ICID 43855 ACCEPT 5g UNKNOWNLIST match sbrs[none] SBRS rfc1918 country not applicable
Tue Feb 20 11:55:58 2024 Info: Start MID 660 ICID 43855
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 From: <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSC0-W-PF253NKG, env-from: gmail.com, header-from: Not Present, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 RID 0 To: <ajayra@cisisco.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 Subject: testing amp private cloud
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSC0-W-PF253NKG, env-from: gmail.com, header-from: gmail.com, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Tracker Header : 65d445f6_TdY46k/XzoIL66+HhA4cFJo0192j3QSDhLDnEkX9DPC LxVhx3o3lC136to+TzXqIaVfPh6X+cND+5IQ=
Tue Feb 20 11:55:58 2024 Info: MID 660 ready 5467 bytes from <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 attachment: Training Details.csv
Tue Feb 20 11:55:58 2024 Info: MID 660 matches all recipients for per-recipient policy amp-testing-policy in the inbound table
Tue Feb 20 11:56:59 2024 Warning: graymail [RPC CLIENT] MID 660 Graymail scan timed out
Tue Feb 20 11:57:01 2024 Info: MID 660 AMP file reputation verdict : UNKNOWN (File analysis pending)
Tue Feb 20 11:57:01 2024 Info: MID 660 SHA-90381C261f0be3e9330710ab96647358c461f6834c0ca001408e40decdf19d8e filename Training Details.csv queued for possible file analysis upload
Tue Feb 20 11:57:01 2024 Info: MID 660 Outbreak Filters: verdict: negative
Tue Feb 20 11:57:01 2024 Info: MID 660 Message-ID : <99221a1xwesi.nanganath.local>
Tue Feb 20 11:57:01 2024 Info: MID 660 queued for delivery
Tue Feb 20 11:57:01 2024 Info: New SMTP ICID 542 interface (10.106.39.193) address 173.37.147.230 port 25
Tue Feb 20 11:57:02 2024 Info: Delivery start DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: Message done DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: MID 660 RID [0] Response: ok: Message 142767851 accepted
Tue Feb 20 11:57:04 2024 Info: Message finished MID 660 done
Tue Feb 20 11:57:09 2024 Info: DCID 542 close
Tue Feb 20 11:57:23 2024 Info: ICID 43855 lost
Tue Feb 20 11:57:23 2024 Info: ICID 43855 close
    
```

ينورتكلال الـدي ربل AMP تالچس ني مات

عمس مالعتسال عم لتسمل ةباجتسال :تامولعم 2024 :57:01 2011 طابش/رياربف 20 خيرات  
ةباحسال نم فلمل = Training Details.csv، MID = 660، Disposition = FILE  
UNKNOWN، Malware = None، Analysis Score = 0، Sha256 =  
90381c261f8be3e933071dab96647358c461f6834c8ca014d8e40dec4f19dbe، ءارجإل  
وه ليلحتلل فلمل لاسرا وه، verdict\_source = amp، suspected\_category = none

ةمآلة ةياهنللة طقنللة ةصاخلة ةباحسال شادحأ تالحتس

```
{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":299  
97 4008-A396-  
6cd486ecc621,"ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fs":0,"ft":0,"hd":1},"sha256":{"h":"90381  
DAB96647358C461F6834C8CA0014D8E40DEC4F19DBE","fa":0,"fs":0,"ft":0,"hd":1},"hord":[32,4],"rd":1,"
```

فورعم ريغ فلمل ببيترت rd - 1 disp\_unknown.

## لشف لىل تدايتلاو تظحول يتلا ةعئاشل تالكشمل لماكلل

1. نوكة نأ بجة .نمآل ينورتكللال ديربلل وأ SWA في حيحصلا ريغ "هيجوتلا لودج" رايتخا |  
ETH1 ةصاخلا AMP ةكباش ةهجاوب لاصلتالا لىل ع ارداق لماكلتملا زاهجلا
2. امم نمآل ينورتكللال ديربلل وأ SWA في لجلل الباق DNS سيل VPC فيضم مسا .  
لاصلتالا عاشنل في لشف لىل يذوي
3. فيضم مسا VPC ل يئاهنللا ريصملا ةداهش في (عئاشللا مسالا) CN قباطت نأ بجة .  
ةنمآل ينورتكللال ديربلل ةباوب و SWA في روكذمللا مسالا لىل ةفاضللاب VPC
4. مدختست تنك اذا .اموعدم اميمصت ةباحس فلمل ليحت و ةصاخ ةباحس مادختسا دعيل  
يلحم مداخة عمسللاو فلمل ليحت نوكة نأ بجة في ،يلحم زاهج
5. ديرب ، SWA و ةصاخلا AMP ةباحس نيب تقولا ةنمازم في ةلكشم دوجو مدع نم دكأت  
نمآل ينورتكللال
6. تياباچيم 32 لىل SWA DVS كرحمب صاخلا نئاكلل يضارتفالا صحتفالا دح نييعت مت  
دادعإلا اذه نأ ةظحالما ءارجللا .ربكأ تافلحم حسم في بغيرت تنك اذا دادعإلا اذه طبضب مق  
كلذ لىل امو Sophos و Webroot لثم يئوضلا حسملا تاكلرحم ةفاك لىل ع رثوي ويمومع

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا