

Cisco SWA-Umbrella Integration: Unified Policies and Common Reporting





Overview

The cyber-attack vectors can be present anywhere in an enterprise or individual's network making it really difficult for network security administrators to enforce the policies for their organisational users. In this modern era, the hybrid work has taken over the conventional campus working models. The users can now join the network physically or virtually from a remote location. Also the organisations are relying more and more on cloud-delivered applications allowing users to access them from any device of their choice, making it really difficult for administrators to manage the web policies or grant access to web applications in the same way they would do it for their campus networks.

The need for hybrid deployment is prevalent for the organisations that have global presence. The data sovereignty laws and in general, the law of land varies and sometimes changes significantly. These laws governing the user-confidential data such as their browsing patterns, any Personally Identifiable Information (PII), or exporting the web-browsing logs outside the state or region where the users are based in.



Introduction to Secure Web Appliance Integration with Cisco Umbrella: A Hybrid Approach

Hybrid deployment mode is essentially deploying Secure Web Appliance (SWA), alongside Cisco Umbrella – Secure Internet Gateway (SIG) for those specific scenarios where the administrators want to enforce the same web policies and application access to the users as they have defined it for their user-base in cloud delivered web gateway solution. SWA can now deeply integrate with the Umbrella SIG Web Policies and adapt the same granular policies that are defined in Rulesets and Rules for various for the Identity types. These SIG policies can now be translated and push down to On-Premise appliances. This allows network administrators to keep the web-policies synchronised between the Cloud proxy and On-Premise proxy solutions, simplifying the process to manage the policies from one-singe dashboard.



"Hybrid deployments lack feature parity and seamless integration between the two products. For example, the policies share common categories, but must be managed separately."

Gartner, Magic Quadrant for Secure Web Gateways, 2019

Product requirements

- Secure Web Appliance (support for all hardware and virtual platforms)
- Cisco Umbrella SIG Bundle (Essentials or Advantage)





Configuration

Step 1 - Log in to the Secure Web Appliance UI using the admin credential: <u>https://wsa_hostname:8443</u>.

Step 2 - Navigate to Network > Umbrella Settings , and click on the Edit Settings button:

| ٢ | 🕢 Cisco Seo | cure Web Applianc | е | | Secure Web Appliance is getting a new look | . Try |
|---|--------------|------------------------------|-------------------|---------|--|-------|
| Ļ | \$100v | | | | | |
| ٨ | Reporting | Web Security Manager | Security Services | Network | System Administration | |
| | | | | | | |
| | Umbrella Set | ttings | | | | |
| | | Hybrid Service Registration: | Not Registered | | | |
| | | Hybrid Policy: | Disabled | | | |
| | | Hybrid Reporting: | Disabled | | | |
| | | | | | Edit Settings | |

Step 3 – To register an appliance with Umbrella SIG, create an API key and secret pair on your Umbrella dashboard (and store it in file for future reference – optional).

| Our law | | | | |
|--|---|---|--------------|------------|
| Add New API Key | | | | |
| Deployments > To add this unique API key to Umbrella, select | its scope-what it can do-and set an expiry | date. The key and secret created here are unique. | | |
| Policies > | ay break or interrupt integrations that use t | mis key. For more information, see Ombrelia's help. | | |
| Reporting > API Key Name | | Description (Optional) | | |
| DMZ Hybrid Demo | | Registering SWA instance with org. | | |
| Admin V | | | | |
| Key Scope / Deployments | what this ADI key can do | 3 selected | | Remove All |
| Accounts Select the appropriate access scopes to define | what this API key can do. | Scope | | |
| User Roles Policies | | Auth / SWA | Read-Only | ~ X |
| Log Management | | Auth / API Auth | Read=Only | × × |
| Authentication Reaming Computers | | | nood only | |
| Bypass Users Sites | | Deployments / Registered Appliances | Read / Write | ~ X |
| Bypass Codes Tag Devices | | | | |
| API Keys | | | | |
| Licensing Expiry Date | | | | |
| Sahil Kukreja > Never expire | | | | |
| sakukrej lab O Expire on May 25 2024 | | | | |
| | | | | |
| Documentation | | | | |
| Learning Center | | | | CREATE KEY |

Step 4 – Register the appliance using the created Umbrella API Key and Secret pair, save and commit the change on SWA to successfully complete the process.

| [| | cure Web Appliance | 9 | | | Secure Web Appliance is getting a ne | w look. Try it ! |
|---|-------------------|------------------------------|--------------|-------------|------------------|--------------------------------------|------------------|
| ٨ | Reporting | Web Security Manager | Security | Services | Network | System Administration | |
| | Edit Umbrell | a Settings | | | | | |
| | Umbrella Settings | | | | | | |
| | Hy | brid Service Registration: ? | Umbrella Reg | istration | | | |
| | | | API Key: | 1346597 | 24a)05/60 | 4a 0 49 | |
| | | | API Secret: | e4bJJ1ebJJ3 | a4uleb3uli55uuja | 2 culic | |
| | | | | Register | | | |
| | | Hybrid Policy: | Enable | | | | |
| | | Hybrid Reporting: | Enable | | | | |
| | | Source Interface: | Managemen | t 🕶 | | | |
| | Cancel | | | | | | Submit |

Step 5 - Click on the Submit button complete the process.

| 51000 | | | | |
|-------------------|-------------------------------|-----------------------|---------|-----------------------|
| Reporting | Web Security Manager | Security Services | Network | System Administration |
| dit Umbrel | la Settings | | | |
| Success — Hybr | id Registration completed suc | cessfully | | |
| Jmbrella Settings | | | | |
| н | ybrid Service Registration: ? | Umbrella Registration | | |
| | | API Key: | | |
| | | API Secret: | | |
| | | Deregister | | |
| | Hybrid Policy: | Enable | | |
| | Hybrid Reporting: | Enable | | |
| | Source Interface: | Management 🗙 | | |
| | | | | |



Step 6 – Hybrid configuration allows admins to selectively enable the Hybrid Policies sync and Reporting on SWA UI.

| | Cisco Sec s100v | cure Web Appliance | | | | S | Secure Web Appliance is getting a new look. Try it ! | | | | | | |
|----|------------------------|------------------------------|----------------------------|------------|---|-----------|--|----|--|--|--|--|--|
| Ĥ. | Reporting | Web Security Manager | Security Security Security | ervices | Netwo | rk | System Administration | | | | | | |
| | | | | | | | | | | | | | |
| E | Edit Umbrella Settings | | | | | | | | | | | | |
| | Success — Hybrid | d Registration completed su | | | | | | | | | | | |
| | Umbrella Settings | | | | | | | | | | | | |
| | Hyl | brid Service Registration: ? | Umbrella Regist | ration | | | | | | | | | |
| | | | API Key: | | | | | | | | | | |
| | | | API Secret: | | | | | | | | | | |
| | | | | Deregister | | | | | | | | | |
| | | Hybrid Policy: | Enable | | Enable Hybri | d Repo | orting | × | | | | | |
| | | Hybrid Reporting: | 🗹 Enable | E | Enabling Hybrid Reporting will send only Umbrella configured policy's Secure We | | | | | | | | |
| | | Source Interface: | Management 🗸 |) (| Appliance rep | ording us | ata to the ombrena Reporting dashboard. | | | | | | |
| | Cancel | | | | | | | Ok | | | | | |
| | | | | _ | | | | | | | | | |

Step 7 – Once the appliance is successfully registered with the Umbrella Org., the status will be displayed under Network > Umbrella Settings main page on SWA UI with hybrid services status, registered OrgID, Source Interface used to sync policies and exporting reporting data with Umbrella, and Serial number of SWA to uniquely identify the registered appliance.

| <u>ж</u> | 👌 Cisco Se | cure Web Appliance | | | Secure Web Appliance is getting a | new look. Try it | | | | | |
|----------|--|---|--|--------------------|-----------------------------------|------------------|--|--|--|--|--|
| 1 | > s100v | | | | | | | | | | |
| | Reporting Web Security Manager Security Services Network System Administration | | | | | | | | | | |
| U | mbrella Se | ttings | | | | | | | | | |
| W | /arning — Enab | ling Hybrid Reporting might i | mpact the Secure Web An | nliance reporting | orformanco | | | | | | |
| | - | | | phance reporting (| Jerrormance. | | | | | | |
| U | mbrella Settings | | | phance reporting (| Seriormance. | | | | | | |
| U | mbrella Settings | Hybrid Service Registration: | Registered | plance reporting | enomance. | | | | | | |
| U | mbrella Settings | Hybrid Service Registration: 1 Hybrid Policy: | Registered Enabled | plance reporting (| errormance. | | | | | | |
| U | mbrella Settings | Hybrid Service Registration: 1 Hybrid Policy: 1 Hybrid Reporting: 1 | Registered Enabled Enabled | phance reporting (| errormance. | | | | | | |
| | mbrella Settings | Hybrid Service Registration: 1 Hybrid Policy: 1 Hybrid Reporting: 1 Org ID: | Registered Enabled Enabled 7997125 | | enumante. | | | | | | |
| | mbrella Settings | Hybrid Service Registration: Hybrid Policy: Hybrid Reporting: Org ID: Source Interface: | Registered Enabled Enabled 7997125 Management | | enumante. | | | | | | |
| | mbrella Settings | Hybrid Service Registration: Hybrid Policy: Hybrid Reporting: Org ID: Source Interface: Serial Number: | Registered Enabled 2997125 Management 564DA1205954BB50B753-3 | 34233976BA7 | enumance. | | | | | | |

(Note : Source Interface needs to access to Internet or exception to reach out to Umbrella SIG FQDN or Umbrella anycast IPs)

Step 8 – Login to Umbrella dashboard, navigate to Deployments > Registered Appliance to check the status. It shows the hostname individual hybrid services status, last Policy sync with the registered appliance, installed AsyncOS version and Serial Number of appliance to uniquely identify the SWA. The Policy Push can be selectively enabled or disabled for each appliance using the toggle switch.

| Cisco Umbrella | ahaha | Deployments / Core | Identities | | | | | | | |
|---------------------|--------------|--|---------------------|------------------|-----------------------|---------------------------|------------------|---|------------------|--|
| | cisco. | Registere | u Appilan | ces o | | | | | | |
| | Cisco Secu | re Web Appliance is a | network security d | evice that can b | e integrated with Cis | co Umbrella. To integrati | e vour device, r | egister it on Cisco Umbrella. The device appear | s as an identity | |
| | on the Cisc | the Cisco Umbrelia interface. You can now directly create and manage policies for this identity without any physical device. recister the Cisco Secure Web Appliance on Cisco Imbrelia, use the API Keys and the Key Secrets. To generate the API Key, payingte to Admin > API Keys in the Cisco Imbrelia navination. | | | | | | | | |
| | bar. To lear | n more about how to i | ntegrate your devic | es with Cisco U | mbrella, read here. | r nay occord. To genere | no 010 Pe 1 Noy, | havgate to Plannin > Per Kaya in the Olaco onto | iono nongocorr | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| 🕦 Sahil Kukreja 🛛 🚿 | Q, Searc | h by SWA name or seri | al number. | | | | | | | |
| | Secure | Web Appliances | | | | | | | | |
| | | | | | | | | | | |
| | Name | | Hybrid Reporting | Hybrid Policy | Policy Sync Status | Policy Sync Time | Version | Serial Number | Policy Push | |
| | wsa004 | 4.ciscodmz.com | Offline | Offline | Success | 08:58 Feb 4, 2023 | 14.6.0-077 | 564DFDC5EFDE4EA04D22-4CD34E703EBC | | |
| | | del ciscodara com | Activo | Active | Success | 05-50 Dec 15 2022 | 15 1 0-297 | E64D4120E0E4DDE0D7E2-22422207ED47 | | |
| | wsauu | +.dc1.ciscodm2.com | ACTIVE | ACOVE | Success | 05:59 Dec 15, 2023 | 15.1.0=267 | 504DA1205954BB50B753-334233976BA7 | | |
| | | | | | | | | 1-2 | of 2 < 🔀 | |

Step 9 – Confirm the Web Policies once pushed down to SWA from Umbrella. A default Identification Profile should be added to SWA. Also, each rule should be translated to Access Policies with either a subnet or User-group.



Use cases for hybrid configuration

The following section walks through a few common use cases adopted by organizations.

Rules based on Internal Networks or Subnets

The above configuration will translate all web policies on Umbrella and push them down to SWA. This section will walk administrators through the testing step by step and show the translated policies on SWA to ensure the same access privileges for On-Premise users.

Step 1 – Login to Umbrella dashboard and add Deployment > Network and subnets under Deployment > Internal Network.

| Cisco Umbrella | | altalta cisco | Deployments / Configuration | | | | ٢ |
|--------------------------------|---|------------------|---|---|--|---|---------------|
| | - | | Internal Networks | | | | Add |
| | | The internal | Networks identity defines a subset that's non-mutable for | BEC1918 compliant) to which you can then apply a policy | To meate an internal Networks identity, riefine a subnet that's non- | mutable or BFC 1918 compliant | |
| Core Identities | | | | | | | |
| Networks | | | | | | | |
| | | Q, Search | h Internal Networks (minimum 4 characters) | | | | |
| | | | | | | | |
| | | 2 Total | | | | | |
| Registered Appliances | | Name A | | Association With | P | Policy | |
| | | client new | augu 1 | - DM7 Lab | 100 140 100 0/04 | Darbert Baller | |
| | | Colemana | NUMBER 1 | 111 OWE COD | 12.100.02.024 | Contact Policy | |
| | | client ne | itwork 2 | n DMZ Lab | 192.168.104.0/24 | Default Policy | |
| Configuration | | | | | | Page: 1 ∨ Results per page: 10 ∨ 1-2 of 2 | \rightarrow |
| Domain Management | | | | | | | |
| Sites and Active Directory | | | | | | | |
| | | | | | | | |
| Root Certificate | | | | | | | |
| SAML Configuration | | | | | | | |
| Service Account Exceptions | | | | | | | |
| | | | | | | | 8 |
| | | | | | | | et Sta |
| | | | | | | | inted |
| | | | | | | | |
| Sahi Kukreja > sakukrej lab | | | | | | | |

Step 2 – Register the appliance with Umbrella, navigate to Policies > Web Policy on Umbrella to create ruleset selecting the added Internal Networks as Ruleset Identities. And add Rules to either Block, Warn or Allow URL Categories.

| Cisco Umbrella | • | abab | Policies / | Management | | | | | | | | | 0 | ٢ | | |
|-----------------------------|---|------------|-------------------------------|-------------------------------------|--|--|--------------------------|---------------------|---|--|---|---------------------|----------------|------------------|--------------|----------|
| | - | chico | vvec | Policy | • | | | | | | | | Add 0 | iobal Settings P | olicy Tester | |
| | | A Web or | sicula mada | up of palaeets a | od pulasats are may | de un of miles. A mile determin | ne brow i imbenila's une | ious securities or | fect your consciousling's | s identifies. This ca | curlu protection includes configurations | that control acces | us to internet | destinations A | nde cao the | in he |
| | | applied to | a subset of are met. Clici | those ruleset id k Add to add ar | entities. A ruleset c d configure a new r | an include all or a subset of all pulset to your organization's V | of your organization's | identities. Rules a | are evaluated in descent Web policies, rulesets, a | iding order and app and rules, see Limb | ply their action when the identity and des | stination match, an | d when any r | ule conditions, | such as time | e of day |
| Management | - | | | | | | , | | | | | | | | | |
| | | 1.0 | | | | | | | | | Assolution To | | and Meedland | | | |
| | | | Internal N | letwork Rules | et | | | 2 Identifies 2 Rv | | | | | Feb 27, 2024 | | ^ | |
| | | | | | | | | | | | | | | | | |
| Data Loss Prevention Policy | | | ADD BULL | es | | | | | | | | | | | | |
| Policy Components | | | | | | | | | | | | | | | | |
| IPS Signature Lists | | | Priority | Rule Name | | Rule Action | Identiti | ** | Destinations | | Rule Configuration | | | | | |
| Destination Lists | | | | | | | | | | Any Day, Any Time | | | | | | |
| Content Categories | | | 11 | Client network | 2 | Block | 1 Inter | nal Network | 3 Categories | | No additional configuration applied Protected File Bypass Disabled | | | | | |
| Application Settings | | | | | | | | | | | Umbrella Block and Warn Page (Inheri | ited) 🕤 | | | | |
| | | | | | | NO.011 1 | | | | | Any Day, Any Time No additional configuration applied | | | | | |
| Schedule Settings | | | H 2 | Client network | 1 | Block | 1 Inter | nal Network | 4 Categories | | Protected File Bypass Disabled | ited) | | | | |
| Security Settings | | | | | | | | | | | | | | | | |
| Block Page Appearance | | | A Ruleset Se | tions affect the | nder within the rule | district balance too are bee tee | theoughout user Web | noliny Marinus set | tinos listed must be con | found through the | air menantika componente hafore haino e | at here | | | | |
| Integrations Settings | | | Therefore and | congo anece one | | ant and are not approve growing | integrate you mad | porcy. He coust an | anga nano moat de con | ingenes encognised | er respective components before being a | es nere. | | | | - |
| Selective Decryption Lists | | | Ruleset M | Name | | | Internal Net | work Ruleset | | | | Edit | | | | 8 |
| Data Classification | | | Ruleset I | dentities | | | 2 Identities | | | | | Edit | | | | Get S |
| porting > | | | Block an | d Warn Pages | | | Umbrella B | lock Page Applied | | | | Edit | | | | tartec |
| ventione > | | | Tenned C | nataola | | | Giobal Tea | et Controls | | | | E-0 | | | | |
| tmin > | | | remain o | | | | Crocker Herri | in comos | | | | | | | | |
| | | | File Analy | ysis | | | 1 Setting E | hadweid | | | | EOI | | | | |
| p Sahi Kukreja > | | | File Type | Control | | | Disabled | | | | | Edit | | | | |
| | | | | | | | | | | | | | | | | |

Step 3 - Ensure that the Web Policies are being translated to Access Policies: Login to SWA UI and navigate to Web Security Manager > Access Policies.

| Appetie Note Search Name Name Name Search Manualization Appetie Appetie </th <th>Secure Web Appliance is getting a new look. Try it i My Revorker . Options : Support an</th> <th></th> <th>a new look. Try it I</th> <th>ecure Web Appliance is getting :</th> <th>S</th> <th></th> <th></th> <th></th> <th colspan="10">lisco Secure Web Appliance 1100v</th> | Secure Web Appliance is getting a new look. Try it i My Revorker . Options : Support an | | a new look. Try it I | ecure Web Appliance is getting : | S | | | | lisco Secure Web Appliance 1100v | | | | | | | | | |
|--|--|----------------------|----------------------|---|------------------|----------------|--------------|------------------------------|---------------------------------------|---|--|--|--|--|--|--|--|--|
| View distribution Section S | 96 | | | | R. | m Administrati | Syste | Network | Security Services | rg Web Security Manager | Reporting | | | | | | | |
| Second Se | | | | | | | | | | | | | | | | | | |
| Note:::::::::::::::::::::::::::::::::::: | | | | | | | | | | Policies | ess Pe | | | | | | | |
| Cal | | | | | | | | | | | ties | | | | | | | |
| Impact And Antimation Control (Control (Contro) (Contro) (Control (Control (Control (Contro) (Control (Contro) (| | | | | | | | | | | d Policy | | | | | | | |
| Build and status 3 and a spectra from a spectra f | Objects Anti-Halware and Reputation HTTP ReWrite Profile Clane Policy Delete | le Clone Policy Dele | HTTP ReWrite Profile | Anti-Malware and Reputation | Objects | Applications | URL Pibering | Protocols and User Agents | | , | er Group | | | | | | | |
| public flored reflection 2 : 2 and | (ghidan parliqe) (ghidan parliqe) (ghidan parliqe) 🅵 🔹 | e = | (global policy) | (global policy) | (global policy) | Manitor: 342 | Block: 3 | (global poicy) | ty udio, Streaming Video | rella Client network 2 1 stication Profile: umbrella global identity entified users ets: 152.168.104.0/24 Categories: Personal VPN, Streaming Au | Lidentif All iden Subnet URL Ca | | | | | | | |
| Bit Market Registrari Bit Market Registrari Description Description <thdescription< th=""> Description Descriptio</thdescription<> | (global policy) (global policy) (global policy) 🕵 😫 | 6 D | (global policy) | (global policy) | (glebai policy) | Hanitori 242 | Block: 4 | (global policy) | ty Sucation, Terrorism and | rella Client network 1 2 dication Profile: umbrella global identity antified users ets: 152.168.103.0/24 Categories: Adult, Pernography, Sex Edu | umbre Identif All iden Sabret URL G | | | | | | | |
| Bernstein Mit Bernstein Mit Ber | (gholai policy) (global policy) (global policy) 🌊 😫 | 6 9 | (global policy) | (global policy) | (global policy) | Nonitors 342 | Monitor: 107 | (global poicy) | ty 1/24 ohol, Animals and Pets, | rella Internal Network Ruleset 3 bication Profile: umbrella global identity antified usero ets: 192.168.103.0/24, 192.168.104.0/ Categories: Adult, Advertisements, Alcol | Umbre Identif All iden Subnet URL Ca | | | | | | | |
| citable Palicy No blocked items Montor: 107 Mainter: 544 No blocked items None | (phias palip) (plaal palip) (plaal palip) 🌄 🔹 | <i>6</i> 3 | (global policy) | (global policy) | (global policy) | Nanitor: 242 | Monitor: 107 | (global policy) | ty)/24 ohol, Animals and Pets, | rella Default Web Policy 4 stication Profile: umbrella global identity antified users ets: 152.158.103.0/24, 192.158.104.0/ Categories: Adult, Advertisements, Alcol | Umbre Identif All iden Sabret URL Ca | | | | | | | |
| Anti-Maware Scarong: Erablid | No blocket items Secure Enabled None None | | None | Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled | No blocked items | Nonitor: 342 | Monitor: 107 | No blocked items | | al Policy ification Profile: All | Global Identif | | | | | | | |
| dt reley créen. | | | | | | | | | | | | | | | | | | |



Configure Destination Lists, Microsoft 365 feeds for Proxy Bypass and Selective HTTPS Inspection for AD Users or Internal Networks

Step 1 – Go to Policies > Web Policy on Umbrella to create ruleset selecting the added Internal Networks as Identity.

Step 2 – Create Selective Decryption Lists and add that to HTTPS Inspection.

Step 3 – Add a Rule with policy action set to WARN for a URL Category.



Common Reporting dashboard for Secure Web Gateway – Exporting SWA Logs to Umbrella and Filtering in Activity Search

Step 1 – Login to SWA and navigate to Network > Umbrella Settings to enable Hybrid Reporting for the registered appliance.

| ٢ | Cisco Secure Web Appliance | | | | | | | | | | | | |
|----------|----------------------------|------------------------------|------------------------|--------------|-----------------------|---------------|--|--|--|--|--|--|--|
| <u>د</u> | ♥> \$100V | | | | | | | | | | | | |
| A | Reporting | Web Security Manager | Security Services | Network | System Administration | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | Umbrella Settings | | | | | | | | | | | | |
| | Umbrella Settings | | | | | | | | | | | | |
| | H | lybrid Service Registration: | Registered | | | | | | | | | | |
| | | Hybrid Policy: | Enabled | | | | | | | | | | |
| | | Hybrid Reporting: | Enabled | | | | | | | | | | |
| | | Org ID: | 7997125 | | | | | | | | | | |
| | | Source Interface: | Management | | | | | | | | | | |
| | | Serial Number: | 564DA1205954BB50B753-3 | 334233976BA7 | | | | | | | | | |
| | | | | | | Edit Settings | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

Step 2 – Check the status of Hybrid Reporting service on Umbrella Dashboard > Deployments > Registered Appliances.

| Cisco Umbrella | alaha | Deployments / Core Identities | | | | | | | | | | |
|-------------------|-----------------------------|------------------------------------|--|-----------------------|-------------------------------|---------------------------------|-----------------------|--|------------------------------------|--|--|--|
| | | Registered App | liances o | | | | | | | | | |
| | Cisco Seci | ure Web Appliance is a network set | curity device that can be in | tegrated with Cisco L | Jmbrella. To integrate your d | evice, register it on Cisco Umb | rella. The device app | ears as an identity on the Cisco Umbrella interface. You can now d | irectly create and manage policies | | | |
| Core Identities | for this ide To register | sentra whoch any shysical device. | | | | | | | | | | |
| | here. | | unco device neo regularite un disco universi, ser ser vez ser ser vez rengene se ver ser negene se ven ser | | | | | | | | | |
| Network Devices | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| Mobile Devices | 4, 5680 | on by Swin name or senal number. | | | | | | | | | | |
| | Secure | Web Appliances | | | | | | | | | | |
| | | | | | | | | | | | | |
| Network Tunnels | Name | | Hybrid Reporting | Hybrid Policy | Policy Sync Status | Policy Sync Time | Version | Serial Number | Policy Push | | | |
| | wsa00 | 4.ciscodmz.com | @ Offline | @ Offline | Success | 08:58 Feb 4, 2023 | 14.6.0-077 | 564DFDC5EFDE4EA04D22-4CD34E703EBC | 0 | | | |
| Configuration | wsa004.dc1.ciscodmz.com | | Active | Active | Success | an hour ago | 15.1.0-287 | 564DA120595488508753-334233976BA7 | | | | |
| Domain Management | | | | | | | | | 1-2012 | | | |
| | | | | | | | | | | | | |



Step 3 – Navigate to Reporting > Activity Search to see all the transactions that match the policies created on Umbrella web policies and synchronised with registered SWAs.

Step 4 – Apply filter Identity type as Secure Web Appliance. Click on View full details to see the search results.

| Cisco Umbrella | Activity Search | | Schedule Export CSV |
|--------------------------------|---|---|--|
| nting \checkmark | | | |
| ora Reports | | | |
| Security Activity | PLTIRS Q, Search by domain, id | tentity, or URL Advanced * CLEAR | Customize Columns All - |
| Activity Search | | | |
| App Discovery | WARN PAGE BEHAVIOR Warne | d X IDENTITY TYPE Secure Web Appliances X | |
| Top Threats | Q. Search filters | 2 Total 💍 Viewing activity trom Feb 26, 2024 6:49 PM to Feb 27, 2024 6:49 PM Page: 1 × Results per page: 50 × 1 - 2 of 2 < > | Event Details × |
| iditional Reports | Response Select A | Request Identity Policy or Ruleset Identity 🕼 Destination Destination IP Internal IP Externs 🖒 | Action |
| Total Requests | Allowed Q Advanced | www. 5 www.04.dc1.ciscodmz.com 5 www.04.dc1.ciscodmz.com http://www.chat.com/ 192.168.103.11 192.168 | Time |
| Activity Volume | Blocked Selectively Provied | Image: Second and the second | Feb 27, 2024 6:48 PM |
| Top Destinations | | | Ruleset or Rule Bypass Authenticated traffic |
| Top Categories | Warn Page Behavior Select A | | Ly Rule Neme |
| Top Identities | 2 0 Warned | | Issue Warning Social networking |
| Cloud Mahware | Accessed Aster Warn | | Manaha |
| Data Loss Prevention | Isolate | | 15 wsa004.dc1.ciscodmz.com |
| enagement | solated | | Policy or Ruleset Identity |
| Exported Reports | IDS Simplers | | To wsa004.dc1.ciscodmz.com |
| Scheduled Reports | O Log Only | | User Identity Source Secure Web Appliance - Hybrid |
| Admin Audit Loa | Would Block | | Internal IP Address |
| | C Blocked | | 192.168.103.11 |
| , | Protocol Select A | | 192.168.101.14 |
| n > | I w HTTP | | Destination 97 |
| Sohi Kukreja > sakukrej lab | □ | | http://snapchat.com/ |
| | Event Type Select A | | Hostname snapchat.com |
| Documentation | Public Application Destination List Any Security Category According Coherence | | Categories Social Networking, Social Networking Dispute Categorization |

Conclusion

SWA hybrid mode will offer a deeper integration with Cisco Umbrella, allowing network administrators to manage the secure web gateway (both the cloud and on-premise appliance) and observe user activity from one single place. This enhances the overall experience while ensuring the security posture for all type of users irrespective of their location, devices or authentication mechanism.

- Gives an opportunity to Secure Web Appliance customers to start planning the migration to Cisco Umbrella.
- Common Reporting Dashboard to see all activity on Umbrella dashboard makes the whole experience seamless and smooth.

- Head-end approach to achieve hybrid web gateway solution for existing Umbrella customers.
- Selective Policy push and Hybrid Reporting functionality on-demand give finer control over the appliance allowing administrators to manage the policies for On-Premise users.
- Organisations can choose the logs storage location from Umbrella dashboard, even for Secure Web Appliance.



Package information

Hybrid mode will be supported for all the Umbrella Orgs that either have the SIG Essentials or Advantage packages. There's no separate Hybrid SKUs for SWA to synchronising on-premise appliance with Umbrella Web Policies or allow reporting logs to be exported and viewed on Umbrella Activity Search for the policies created on Umbrella dashboard and pushed down to registered appliances.

For more information

For detailed information on Cisco Secure Web Appliance, go to www.cisco.com/go/wsa.

A Cisco sales representative, consulting system engineer, or channel partner can help to evaluate how Cisco Secure Web Appliance will enhance your security.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) C22-4328099-00 04/24