Cisco Umbrella: Secure Internet Gateway (SIG) Essentials Package

The new normal – decentralized networks

Enterprise security and networking are going through a significant transformation. Traditionally, all internet traffic from branch offices was routed back to a central location and security functions were performed there. Now, the wide-scale use of cloud applications has become fundamental to business operations at all locations. *32% of organizations report that the majority of their apps are SaaS based now and that number is expected to increase to 60% within two years.*[1] In branch offices, the centralized security approach has become impractical because of the high cost of backhauling traffic and the resulting performance issues. Many remote offices find ways to go direct to the internet because of the convenience and performance benefits. *85% of remote users reported that they sometimes go direct to the internet.* For these reasons, many organizations are adopting a more decentralized networking approach and implementing SD-WAN solutions to optimize performance at remote locations. This enables a more efficient direct-internet-access (DIA) path for these offices, but also highlights a set of new security challenges.

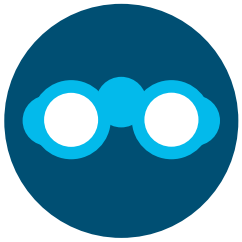
"85% of remote users reported that they sometimes go direct to the internet"

ESG Research, Market Dynamics Impacting Remote and Roaming User Security Requirements, Jan 2019

Security challenges

As networks become more decentralized, the centralized security policies are no longer enforced, so the risk of a successful attack or compliance violations increases. Security teams already struggle to keep up with cyber-security threats. Many of them have a large number of point solutions that are difficult to integrate and manage. *77% of organizations reported having over 25 separate security tools.*[1] These point products are generating thousands of alerts making it very difficult for analysts to keep up. Many alerts go untouched. *44% of daily alerts are not investigated* (Cisco 2018 Security Benchmark Study)

IT security pain points



Gaps in visibility and coverage

Volume and complexity of security tools

Limited budgets and security resources

The combination of the network decentralization trend and the security challenges is driving security leaders toward consolidated, cloud-delivered solutions that provide a broad set of protection for users and simplify their environment, while reducing both bandwidth costs and resource requirements.

© 2019 Cisco and/or its affiliates. All rights reserved.

Solution: Cisco Umbrella - SIG Essentials package

Cisco Umbrella unifies multiple security services in a single cloud platform to secure access to the internet and control cloud app usage. The Umbrella Secure Internet Gateway (SIG) Essentials package offers a broad set of security functions that until now required separate firewall, secure web gateway, DNS-layer security, threat intelligence, and cloud access security broker (CASB) solutions. By enabling all of this from a single platform and dashboard, Umbrella significantly reduces the time, money, and resources previously required for deployment, configuration, and integration tasks. It can be integrated with your SD-WAN implementation to provide a unique combination of performance, security, and flexibility that delights both your end users and security team.

Top 3 reasons organizations are looking for a SIG:

- Improved security coverage
- Centralized/consistent policies across remote locations
- Better performance and user satisfaction

Major components of Umbrella

The following components are integrated seamlessly in a single, cloud-delivered platform:

DNS-layer security

This is the first line of defense against threats because DNS resolution is the first step in internet access. Enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established — stopping threats over any port or protocol before they reach your network or endpoints. As a cloud-delivered service, it:

- Provides the visibility needed to protect internet access across all network devices, office locations, and roaming users.
- Logs and categorizes DNS activity by type of security threat or web content and the action taken — whether it was blocked or allowed.
- Retains logs of all activity as long as needed, ready to recall for deeper investigation.
- Can be implemented quickly to cover thousands of locations and users in minutes, to provide immediate return on investment.

This level of protection is enough for some locations and users, yet others need additional visibility and control to meet compliance regulations and further reduce risk.

Secure web gateway (full proxy)

Umbrella includes a cloud-based full proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. This includes:

- Real-time inspection of inbound files for malware and other threats using the Cisco AMP engine and third-party resources
- Advanced file sandboxing provided by Cisco Threat Grid, which uses static and dynamic threat intelligence to detect and report on malicious files
- Full or selective SSL decryption to further protect your organization from hidden attacks and time-consuming infections
- Detailed reporting with full URL addresses, user and network identity, allow or block actions, plus the external IP address
- Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations
- The ability to block specific user activities in select apps (e.g. file uploads to Box and Dropbox, attachments to GMail, and post/shares on Facebook and Twitter)

IPsec tunnels, PAC files and proxy chaining can be used to forward traffic to Umbrella for full visibility, URL and application level controls, and advanced threat protection.

© 2019 Cisco and/or its affiliates. All rights reserved.

Cloud access security broker (CASB) functionality

Umbrella exposes shadow IT by providing the ability to detect and report on the cloud applications that are in use across your environment. It automatically generates overview reports on the vendor, category, application name, and the volume of activity for each discovered app. The drill down reports include risk information such as the web reputation score, financial viability, and relevant compliance certifications.

App Discovery provides:

- Extended visibility into cloud apps in use
- App details and risk information
- Ability to block/allow specific apps

This insight enables better management of cloud adoption, risk reduction, and the ability to block the use of offensive or inappropriate cloud applications in the work environment.

Cloud-delivered firewall

With Umbrella's firewall, all activity is logged and unwanted traffic is blocked using IP, port, and protocol rules. To forward traffic, you simply configure an IPsec tunnel from any network device. Management is handled through the Umbrella dashboard, and as new tunnels are created, security policies can automatically be applied for easy setup and consistent enforcement throughout your environment.

Umbrella's cloud-delivered firewall provides:

- Visibility and control for internet traffic across all ports and protocols
- IPsec tunnel support for secure traffic routing to cloud infrastructure
- Automated reporting logs
- Customizable IP, port, and protocol policies in the Umbrella dashboard

Key benefits:

- Broad security coverage across all ports and protocols
- Security protection on and off network
- Rapid deployment and flexible enforcement levels
- Immediate value and low total cost of ownership
- Single dashboard for efficient management
- Unmatched speed and reliability with hybrid Anycast

"76% of respondents prefer a multi-function security platform to solve the remote security challenge"

ESG Research, Market Dynamics Impacting Remote and Roaming User Security Requirements, Jan 2019

Interactive threat intelligence for improved incident response

Umbrella analyzes over 180 billion DNS requests daily. We ingest all of that internet activity data from our global network into a massive graph database, and then continuously run statistical and machine learning models against it. This information is also constantly analyzed by the Umbrella security researchers and supplemented with intelligence from Cisco Talos to efficiently discover and block an extensive range of threats. Not only is Umbrella powered by this threat intelligence, but we give you access to the data to strengthen your ability to respond to incidents faster. One of the top reasons organizations deploy a SIG is to accelerate their threat response and detection.[1]

Analysts can leverage Umbrella Investigate for rich intelligence about domains, IPs, and malware across the internet. Investigate provides real-time access to all of Umbrella's threat intelligence and enables analysts to:

- Gain deeper visibility into threats with the most complete view of the internet
- Better prioritize incident investigations
- Speed up incident investigations and response
- Predict future attack origins by pinpointing and mapping out attackers' infrastructures
- Easily integrate Investigate data other security orchestration tools

Our unique view of the internet enables us to uncover malicious domains, IPs, and URLs before they're used in attacks, and helps analysts to accelerate investigations.

© 2019 Cisco and/or its affiliates. All rights reserved.

Cisco SD-WAN integration

Backhauling internet bound traffic is expensive, and adds latency. Many branch offices are upgrading their network infrastructure by adopting SD-WAN and enabling direct internet access (DIA). Based on a recent survey with ESG, 76% of organizations use SD-WAN extensively or selectively.[1] With the Umbrella and Cisco SD-WAN integration, you can deploy Umbrella across your network and gain powerful cloud-delivered security to protect against threats on the internet and when accessing the cloud. Umbrella offers flexibility to create security policies based on the level of protection and visibility you need — all in the Umbrella dashboard.

For DNS-layer security, Umbrella can be deployed across hundreds of devices with a single configuration in the Cisco SD-WAN vManage dashboard. For additional security and more granular controls, Umbrella's secure web gateway and cloud-delivered firewall capabilities can be deployed through a single IPsec tunnel. Our integrated approach can efficiently protect your branch users, connected devices, and application usage from all DIA breakouts.

For more information

Contact your Cisco sales representative for more information on the Umbrella SIG Essentials package.

"Umbrella enables us to allow branches to access the internet locally and securely instead of being backhauled to the data center."

IT Director,
Professional Services Company

https://www.techvalidate.com/tvid/3E6-9DA-F77

"With Umbrella, the risk of security breaches is less likely and mitigated across our user base. The solution allowed us to utilize broadband internet local at the branch which improved internet access speeds without compromising security."

IT Director,
Professional Services Company

https://www.techvalidate.com/tvid/B6E-142-D48

1: ESG Research, Market Dynamics Impacting Remote and Roaming User Security Requirements, Jan 2019

© 2019 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)