For Business

Integrates with your existing security stack

Integrate iboss cloud with existing cybersecurity technology investments via standardized connectors and protocols

Web gateways are responsible for ensuring secure connectivity as users access a wide range of applications and resources in the cloud. The gateways have the ability to inspect traffic for unwanted content, malware and data loss. Because of the gateway's critical role of inspecting packets, files and data as it traverses to and from the cloud, the ability to feed that data into other systems for further analysis extends the overall efficacy of the platform.

Any file the iboss cloud inspects can be inspected by any other system as the cloud will forward the file to the external system and wait for a response before proceeding. Forwarding of files is performed by the industry standard ICAP protocol. In addition, any traffic the iboss cloud gateways inspect can be forwarded to any other system by forwarding that traffic to the external system instead of the original destination. This is typically performed via proxy forwarding or proxy chaining.

Traffic forwarding methods include proxy-chaining, DNS forwarding, or forwarding via the standard ICAP protocol. In addition, when forwarding traffic via ICAP, the gateways will respect the response from the ICAP service to block or adapt content before it is sent to the users. This allows infinite capability expansion as third-party cybersecurity services come to market. This ensures that organizations get the best-of-breed protection and leverage existing cybersecurity investments in addition to the advanced protection included with the iboss cloud.

The ability to send files and data to external systems for additional inspection allows limitless cybersecurity integration possibilities.

Learn more

Selectively forward traffic to third-party systems using proxy chaining and forwarding

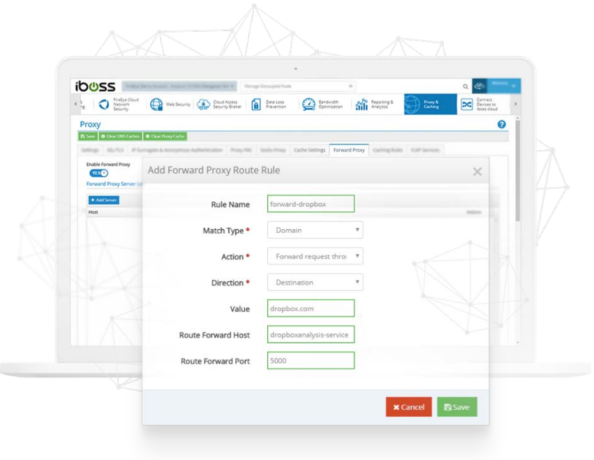
Stream real-time cloud data to external CASB systems

Use ICAP to automatically send inspected files to external security systems

Selectively forward traffic to third-party systems using proxy chaining and forwarding

The iboss cloud natively integrates with third-party vendors by feeding the data and files that traverse the cloud to any external system or service for additional protection. Data traffic can be forwarded selectively based on a variety of criteria including destination domain and request headers. Typically, third-party cybersecurity systems will provide additional capabilities or layered protection for data as it traverses to and from the cloud through the iboss cloud.

Proxy chaining and forwarding allows traffic streams to pivot through additional third party systems for inspection. Proxy chaining is easily configured within iboss cloud using various header and data matching options.



Add Forward Proxy Route Rule

Rule Name: forward-dropbox

Match Type *: Domain

Action *: Forward request thro

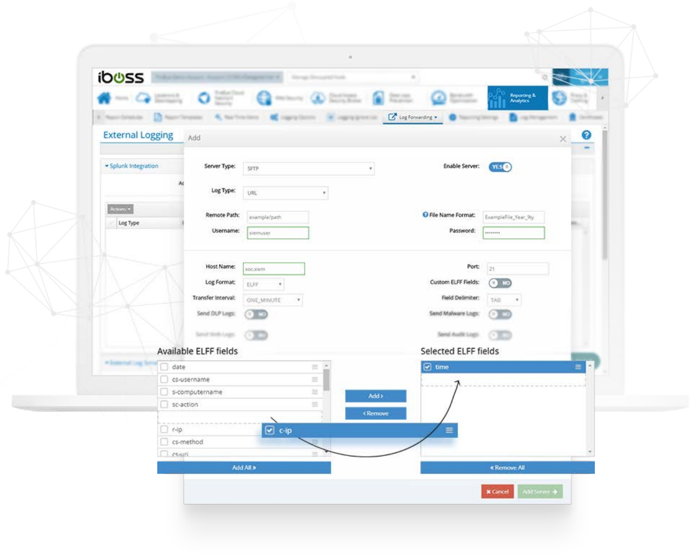
Direction *: Destination

Value: dropbox.com

Route Forward Host: dropboxanalysis-service

Route Forward Port: 5000

The receiving third-party service can perform security functions to the data prior to that data reaching its final cloud destination.


External Logging

Add

Server Type: SFTP

Enable Server: YES

Log Type: URL

Remote Path: example/path

File Name Format: ExampleFile_Year_%y

Username: siemuser

Password: ••••••••

Host Name: soc.siem

Port: 21

Log Format: ELFF

Custom ELFF Fields: NO

Transfer Interval: ONE_MINUTE

Field Delimiter: TAB

Send DLP Logs: NO

Send Malware Logs: NO

Available ELFF fields: date, cs-username, s-computername, sc-action, r-ip, cs-method, cs-uri

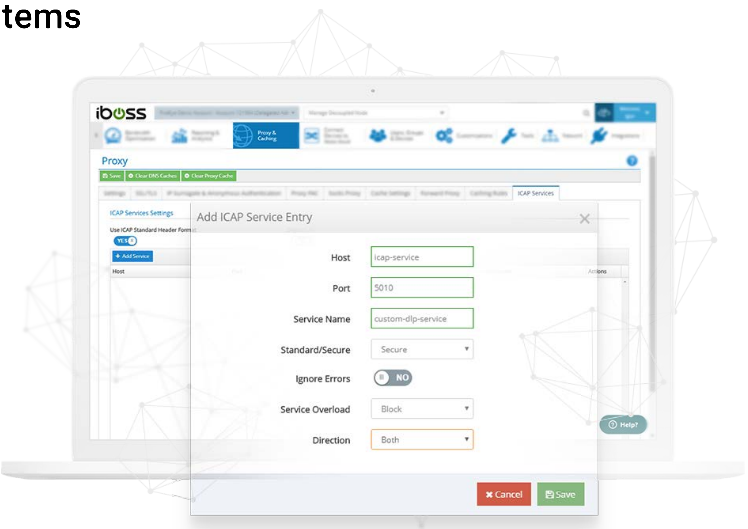
Selected ELFF fields: time, c-ip

Stream real-time cloud data to external CASB systems

The iboss cloud can natively forward traffic generated from users to any CASB system without complex coding or configuration. The logs can be sent in real-time so that they can be analyzed and enhanced by other CASB solutions to provide additional visibility and insight into cloud application use. Traffic is forwarded directly from iboss cloud to the CASB system without the need to deploy virtual appliances or external connectors. This ensures data streams in real-time to the CASB system for fast protection and visibility.

Use ICAP to automatically send inspected files to external security systems

ICAP is an industry-standard protocol for passing files from one system to another for inspection. The iboss cloud fully supports the ICAP protocol so that any file inspected by the iboss cloud can be forwarded to any other system for inspection and protection. The cloud will wait for the additional third-party system to make a determination on the file prior to passing the content along to its final destination. Selectively passing files through ICAP can also be achieved by highly extensible rules so that only files of interest are passed to the external system. ICAP is typically supported by external DLP systems as a standard way of receiving files for inspection making the iboss cloud an ideal choice for integration with third-party DLP platforms.


Proxy

ICAP Services Settings

Use ICAP Standard Header Format: YES

Add ICAP Service Entry

Host: icap-service

Port: 5010

Service Name: custom-dlp-service

Standard/Secure: Secure

Ignore Errors: NO

Service Overload: Block

Direction: Both

Buy Now

The iboss cloud can secure user Internet access on any device, from any location, in the cloud. Best of all, you can start using it immediately to protect your users instantly.

What you get

- In the cloud Internet security
- Advanced Internet malware protection that follows users
- Advanced cloud and SaaS controls
- Web filtering and compliance controls
- Internet security for in-office users without appliances
- Branch office Internet security without data backhaul
- And a lot more...

Buy now

Contact Us

Get in touch with a technical specialist
for a live demo.

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEIA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

Contact Us

CONTACT SUPPORT

Support Overview
Open a Ticket

North America Support:
877-742-6832 X3
support.na@ibosscloud.com

LATAM Support:
+52 (55) 41696270
support.latam@ibosscloud.com

EMEIA Support:
+44 (0) 203 7908289
support.emeia@ibosscloud.com

APAC Support:
+63 (45) 4571057
support.apac@ibosscloud.com

CONTACT SALES

Request Demo
Request Information

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEIA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

iboss

Copyright © 2020
iboss. All Rights Reserved.