Traditional model

Network:
Centralized

Security:
Single place to enforce policies and protection
Today’s model

Network:
Decentralized

Security:
Protect at data center, cloud, and branch edge
4 out of 5 orgs are shifting to direct internet access (DIA)

76% of orgs use SD-WAN extensively or selectively

DIA & SD-WAN pervasive in branch offices

Source: ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019
Challenges you face

- Malware and ransomware
- Gaps in visibility and coverage
- Volume and complexity of security tools
- Limited security resources
Deliver protection everywhere

Internet / SaaS

Branch DIA

Transform edge security

HQ

Boost existing security

Roaming/Mobile

Enable off-network

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
What is Umbrella?
Where does Umbrella fit?

Benefits

- Block malware before it hits the enterprise
- Contains malware if already inside
- Internet access is faster
- Provision globally in minutes
Enterprise-wide deployment in minutes

On-network coverage
With one setting change
Integrated with Cisco ISR 1K and 4K series and Cisco WLAN controllers

Off-network coverage
With AnyConnect VPN client integration
Or with any VPN using lightweight Umbrella client
Data centers co-located at major IXPs

31 data centers worldwide
<table>
<thead>
<tr>
<th>DNS name</th>
<th>Query Speed</th>
<th>0</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
<th>100</th>
<th>120</th>
<th>140</th>
<th>160</th>
<th>180</th>
<th>200</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>10.02 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenDNS/Umbrella</td>
<td>16.19 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSFilter</td>
<td>22.98 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norton</td>
<td>23.03 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>23.09 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neustar</td>
<td>23.32 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SafeDNS</td>
<td>25.01 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NuSEC</td>
<td>25.17 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VeriSign</td>
<td>25.52 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quad9</td>
<td>33.06 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yandex</td>
<td>45.77 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Less is better

**Information**

- All DNS providers are tested every minute from 200+ locations around the world.
- Only IPv4 is used.
- A 1 second timeout is set. If a query takes longer, it's marked as timeout.
- The data is updated once per hour. Contact us if you need real-time data.
- "Raw Performance" is the speed when querying each nameserver directly.
- "Resolver Simulation" simulates the algorithm of public DNS resolvers and shows the performance from the resolver's point of view.
- "Uptime" shows the real uptime of DNS provider. A provider is marked as down only if all nameservers go down at the same time. (in the select location)
- "Quality" shows the uptime of nameservers. For example, if a provider has 4 NS and 1 fails, then quality is 75% for that location and benchmark. This means even though the provider is marked as down a real user could still get an answer thanks to the round robin algorithm.
1. DNS-layer enforcement

- Umbrella provides:
  - Connection for safe requests
  - Prevention for user and malware-initiated connections
  - Proxy inspection for risky domains
2. Intelligent Proxy

Cisco Umbrella enables proxy for requests based on threat, intelligence and policy.

Requests for “risky” domain requests

URL inspection

Feeds from Cisco Talos, Cisco WBRS, and partners
Block lists of custom URLs

AV engines
Cisco AMP

File inspection

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco’s intelligence
“Security controls are only as good as the breadth and quality of the threat intelligence behind them...”

“..the ability to apply threat intelligence correctly and at scale is the ‘magic of true protection’”
To stop more, you have to see more. More telemetry from cloud to core, more partnerships, and more insight into how threats work.

- The expansive Cisco security portfolio creates the broadest contextual data set
- 185 intelligence partnerships
- At least one vulnerability disclosed for every working day of the year
DNS entries processed daily

Cisco Umbrella

Talos
Cisco Security Research

180B

Palo Alto
100M

InfoBlox
1.2B

Trend Micro
8B
Umbrella on Cisco
<table>
<thead>
<tr>
<th><strong>Cisco IT’s deployment of Umbrella</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.6b</strong></td>
<td><strong>22m</strong></td>
</tr>
<tr>
<td>DNS queries per day off sourced from the Cisco network and endpoints</td>
<td>DNS blocks per day</td>
</tr>
<tr>
<td><strong>30 min</strong></td>
<td></td>
</tr>
<tr>
<td>Average time of the change requests to enable enterprise wide policy changes</td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td><strong>110k</strong></td>
</tr>
<tr>
<td>End client installation cases from AnyConnect bootstrap deployment</td>
<td>Umbrella clients installed via AnyConnect VPN bootstrap in 2 weeks</td>
</tr>
</tbody>
</table>
The Future
Transformation to the Secure Internet Gateway

- DNS-layer security
- Web gateway
- Firewall
- Data loss prevention

On-premises security converges in the cloud for more effective protection of branch offices
Secure web gateway: full web proxy
Deep inspection and control of web traffic

- URL logging and blocking
- Content control
- App discovery & control
- File inspection & blocking

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
APP DISCOVERY & BLOCKING

CASB functionality to address Shadow IT and enable secure cloud adoption

- Ability to easily block unapproved apps
- Status of discovered apps
- Summary of high risk categories
- Visibility into cloud app usage by risk with links to app details
Cisco SD-WAN integration
Simple, effective protection across your Cisco SD-WAN fabric

Quickly deploy DNS-layer security as first line of defense
Add deeper inspection and control with cloud-delivered firewall and secure web gateway capabilities
Easily scale security with future SaaS and web traffic growth

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

- Full URL visibility and blocking (black, white, category)
- HTTPS decryption
- File inspection/Threat protection
- PAC, IPSec Tunnel, Proxy Chaining
- Remote Clients