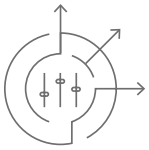
SOLUTION BRIEF

PROTECT NETWORKS AND IMPROVE SUBSCRIBER EXPERIENCE WITH A10 SECURITY SOLUTIONS

Cyberattacks are difficult to identify because attack methods and source locations vary greatly, and on-premise security solutions cannot take investigative action until organizations have been struck by malicious traffic. Identifying and correctly analyzing threats, and proactively classifying known malicious threats to take preemptive action requires prolonged exposure to the threat, significant computing power and extensive personnel resources.

Service providers need to reduce security risks by restricting and blocking access to malicious and undesirable websites, including malware, spam and phishing sources to ensure business continuity and protect networks from existing and future threats. To remain profitable, service providers are constantly looking for service monetization options and ways to improve efficacy of their security infrastructure.



A10 NETWORKS SECURITY SOLUTIONS

A10 URL CLASSIFICATION SERVICE

A10 URL Classification Service blocks accesses to specific URL categories and protect users against web threats. The service offers comprehensive website coverage and classification over 460 million domains in more than 45 languages into 83 categories to correctly identify and categorize websites. Highly accurate website categorization with advanced machine learning classifies websites at a rate of over 5000+ URLs per second.

CHALLENGE

Service providers need to proactively stop known bad actors to ensure availability of business services and to provide a safer internet experience with improved subscriber quality of experience (QoE).

SOLUTION

A10 URL Classification Service for URL filtering, is available in A10 Thunder appliances, allowing customers to restrict access to specific URL categories and websites. And A10 Threat Intelligence Service enables service providers to leverage global knowledge of threat sources to block traffic from known bots and attack sources.

BENEFITS

- Protect your network from existing and future threats
- Provide safer internet experience for your subscribers with efficient access control for web content
- Drive revenue streams with new service monetization options

A10 Thunder® appliances can be configured to leverage A10 URL Classification Service in two modes:

Static Mode: The A10 Thunder appliance maintains static domain-lists to block access to specific URL categories.

Dynamic Mode: The A10 Thunder appliance can automatically download new URL updates and optionally perform cloud-based lookups for unknown URLs.

A10 THREAT INTELLIGENCE SERVICE

A10 Threat Intelligence Service augments the application security portfolio of A10 Thunder appliances to identify and block traffic from known bots and attack sources. The service combines and enhances reputation data from dozens of security intelligence sources, including DShield, abuse.ch and Shadowserver, to instantly recognize and block traffic from known attack sources.

A10 Threat Intelligence Service also catches security threats such as spam or phishing sources, blocks command-and-control computers from communicating with your network and prevents zero-day attacks.

USE CASES

The following are some key use cases service providers can leverage with A10 URL Classification Service and A10 Threat Intelligence Service:

(1) URL FILTERING FOR WEB ACCESS CONTROL

ENFORCE REGULATORY CONTROL

Service providers can leverage A10 URL Classification Service to enforce government mandates by selectively allowing or denying traffic to maintain compliance standards. For example, enforce anti-terrorism laws by taking down offending or suspected terrorism websites or comply with government policies for anti-child pornography by blocking access to web-pages with child abuse content, for e.g., enforce filtering of Internet Watch Foundation (IWF) URL list.

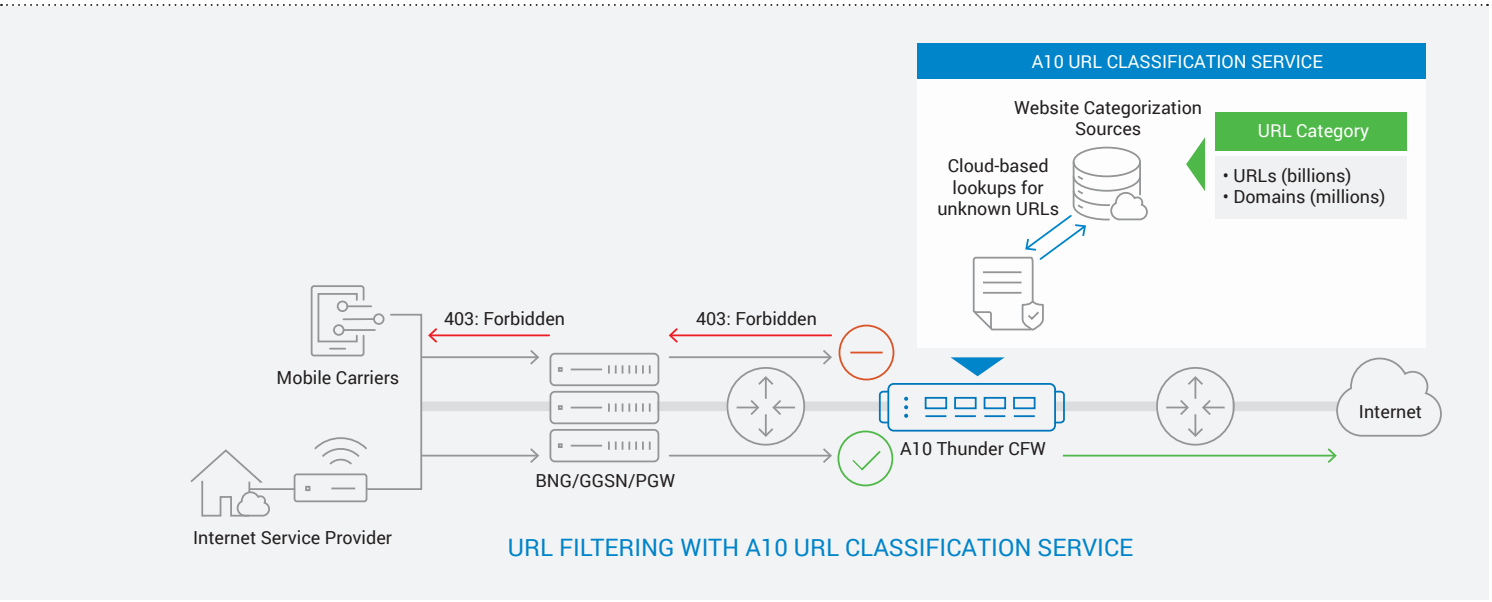


Figure 1: URL Filtering solutions for regulatory control

SERVICE MONETIZATION WITH SUBSCRIBER-AWARE PARENTAL CONTROL

Service providers can monetize web classification services by offering subscriber-aware access control options. A10 URL Classification Service is policy-based – different policies can apply based on subscriber profiles. Content filters with highly granular filtering and blocking capabilities lets service providers offer secure web access by restricting mature web content and allowing access to the content, for example, with a certain ratings category for teen subscribers.

Subscriber-aware parental controls let parents maintain full control over which websites their children can access by filtering out inappropriate sites from search results.

A10 Thunder appliances blocks access to potentially criminal URLs and malicious IP addresses based on national block-lists obtained from website categorization sources. URL filtering with A10 URL Classification Service selectively allows or drops requests based on URL category list, which includes botnets and malware sites.

A10 Thunder appliances can operate in static mode by maintaining static domain lists to block access to specific URL categories based on regional policies or operate in dynamic mode by automatically downloading new URL updates and optionally performing cloud-based lookups for unknown URLs.

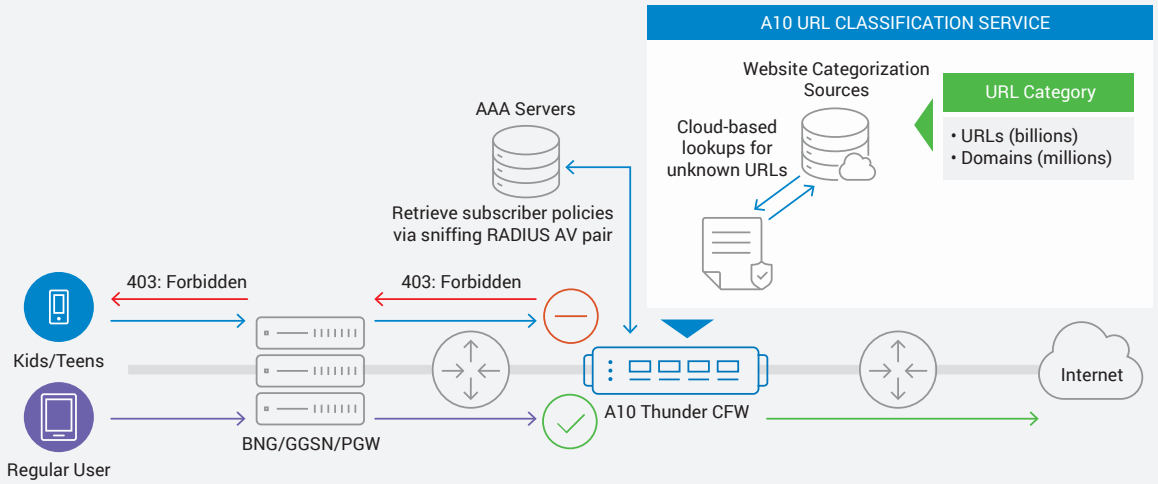


Figure 2: Subscriber-aware parental control solution for service providers

(2) BLOCK ACCESS BASED ON IP REPUTATION

SECURITY & DATA PROTECTION

Block non-DDoS threats like spam and phishing and protect your network with A10 Threat Intelligence Service. Threat intelligence data and IP reputation of over 31million malicious IPs from more than three dozen security intelligence sources, enables A10 Thunder appliances to instantly recognize and block traffic to and from known malicious IP sources.

A10 Threat Intelligence Service consistently updates malicious IP address list based on analysis from cloud services. A10 Thunder appliances use that data to block the malfunctioned access.

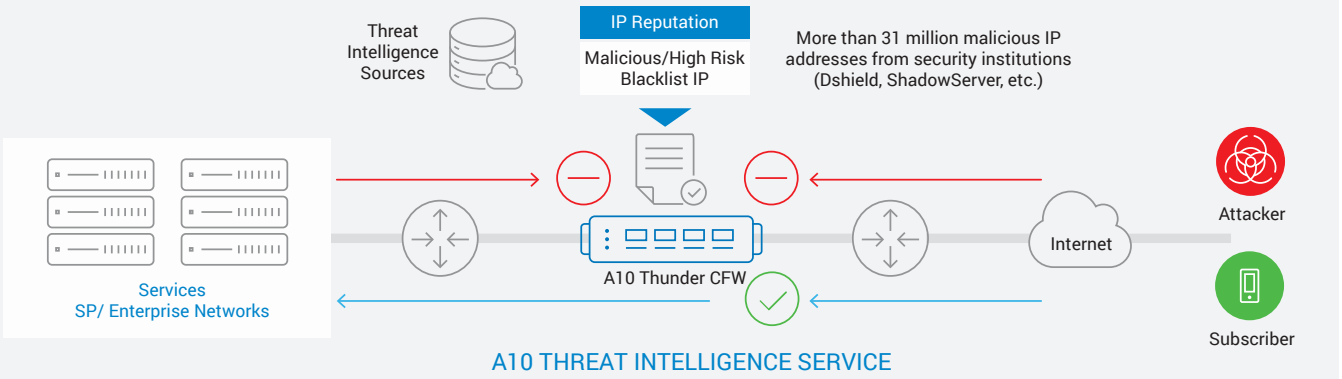


Figure 3: Blocking access based on threat intelligence service

SOLUTION COMPONENTS

- A10 Thunder CFW (also supported on Thunder ADC)
- aGalaxy® centralized management system
- A10 Threat Intelligence Service
- A10 URL Classification Service
- aXAPI® REST-based API

SUMMARY

Service providers can leverage URL classification and advanced threat monitoring security services to enhance threat visibility and improve security efficacy of your network infrastructure while providing efficient access control. These solutions empower service providers to drive revenue and profitability, and stay competitive with faster time to market of new security service offerings.

NEXT STEPS

For more information, please contact your A10 representative and visit www.a10networks.com/firewall.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19185-EN-01 OCT 2017