SOLUTION BRIEF

A High-performance Secure Web Gateway and Much More

A10 Thunder SSLi and CFW are Future-proof, Feature-rich Secure Web Gateways that Deliver Additional Security Capabilities

Overview

A Secure Web Gateway (SWG) protects users from external threats on the internet, leading to stronger security and improved productivity.

An SWG helps companies overcome many of the challenges introduced by the growth in internet traffic and by the rise of modern, feature-rich cloud applications and workloads such as Office 365 applications. SWGs must deliver the ability to scale for increased traffic often with long-lived, persistent connections to cloud applications while also coexisting and enhancing existing security infrastructure

A10 Thunder® SSLi® and A10 Thunder CFW appliances are high-performance Secure Web Gateways with a true full proxy architecture that supports comprehensive protocol suites and dedicated hardware for extraordinary SSL performance. Both solutions support explicit or transparent deployment modes and provide additional features such as URL filtering, threat intelligence and ICAP support. With many form factors and capacities to choose from A10 devices offer flexible deployment options with extensive security and compliance features that can scale with growing enterprise needs.

Challenge

A high-performance Secure Web Gateway is an absolute must to overcome the complex challenges associated with growing modern cloud workloads. A future-proof, purpose-built solution is required to preserve the performance and scale amid growing demands.

Solution

A10's Thunder Series Secure Web Gateways are high-performance proxies that provide excellent scalability and many advance features for the growing demands of SaaS applications.

Benefits

- Identity and access management (IAM)
- URL filtering service
- ICAP compatibility to leverage DLP & AV solutions
- Security and compliance
- Flexible deployment in transparent or explicit mode
- SSL inspection at high-performance levels
- Optional up-to-date threat intelligence

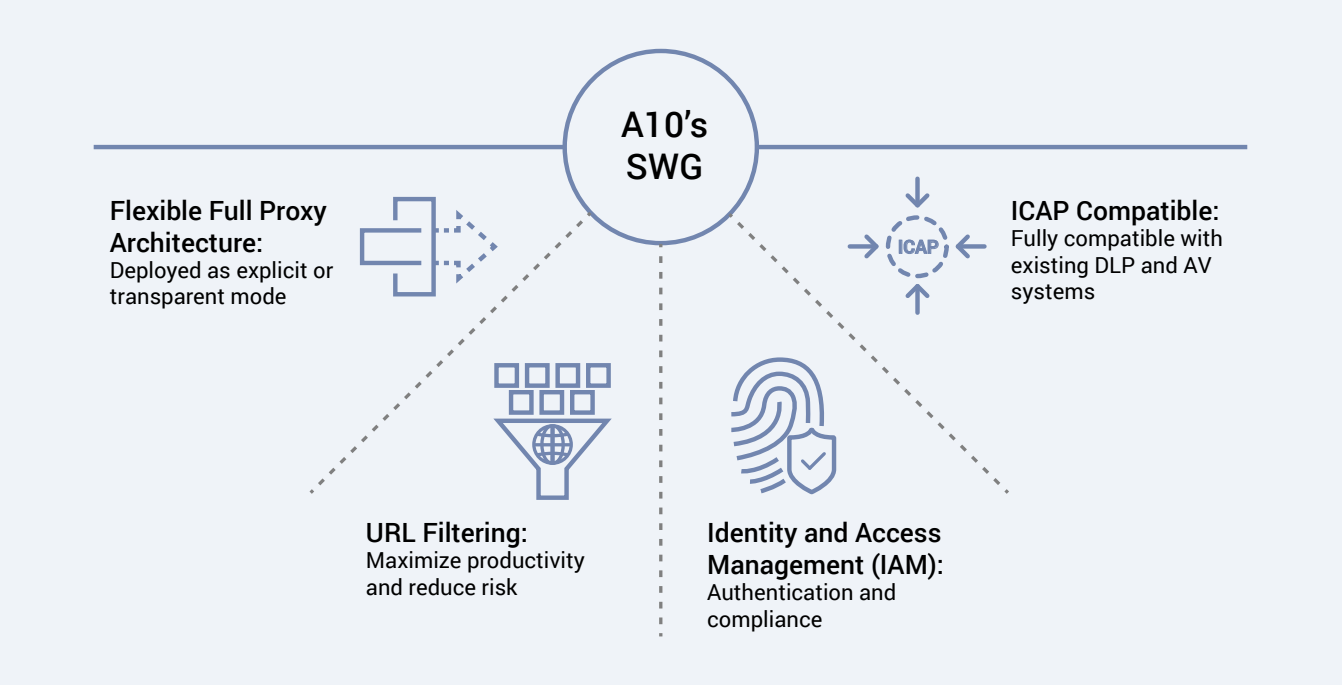

Figure 1: A10 Thunder device features

The Challenge

The meteoric rise in web traffic puts significant strain on Secure Web Gateways, which are often tasked to perform both end user security and policy enforcement. However, the many threats originating from the internet hiding under the veil of encrypted traffic, coupled with the multifold increase in cloud application traffic, has given rise to critical scalability and security concerns.

High throughput in a SWG is not the only performance criteria for accelerating modern cloud application traffic, as it vastly differs from the way traditional web traffic behaves. Dozens of long-lived connections from each employee and their many devices can quickly victimize proxies causing significant performance degradation and loss of productivity.

Similarly, security is an evolving challenge that SWGs must overcome. Threat intelligence, SSL inspection and ICAP compatibility are needed for protection through policy enforcement and compliance, and can also augment and enhance the performance of existing security solutions.

Along with unique challenges raised by modern web traffic patterns, there is a delicate balance between performance and security fueling the need for high-performance, purpose-built solutions that are future proof and can outpace the constantly evolving threat landscape.

A10's Secure Web Gateway

A10 Thunder solutions are designed from the ground up for unmatched scalability and performance, and can meet demanding enterprise requirements.

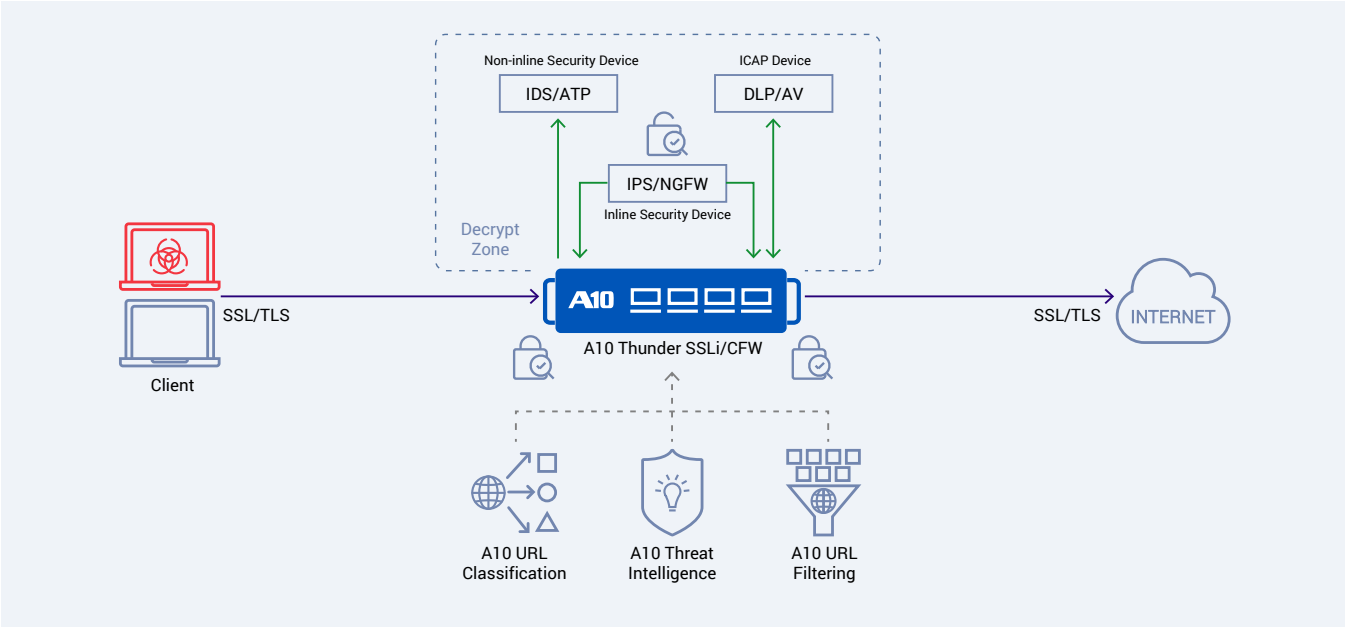

Figure 2: Thunder Secure Web Gateway architecture

Some of the benefits offered by A10's solutions are:

- **Identity and Access Management (IAM):**

  Identity and Access Management can be used to enforce authentication for security and compliance purposes. Users are redirected to existing authentication server and Thunder devices keep track of the user's sessions for logging and to monitor user activities.

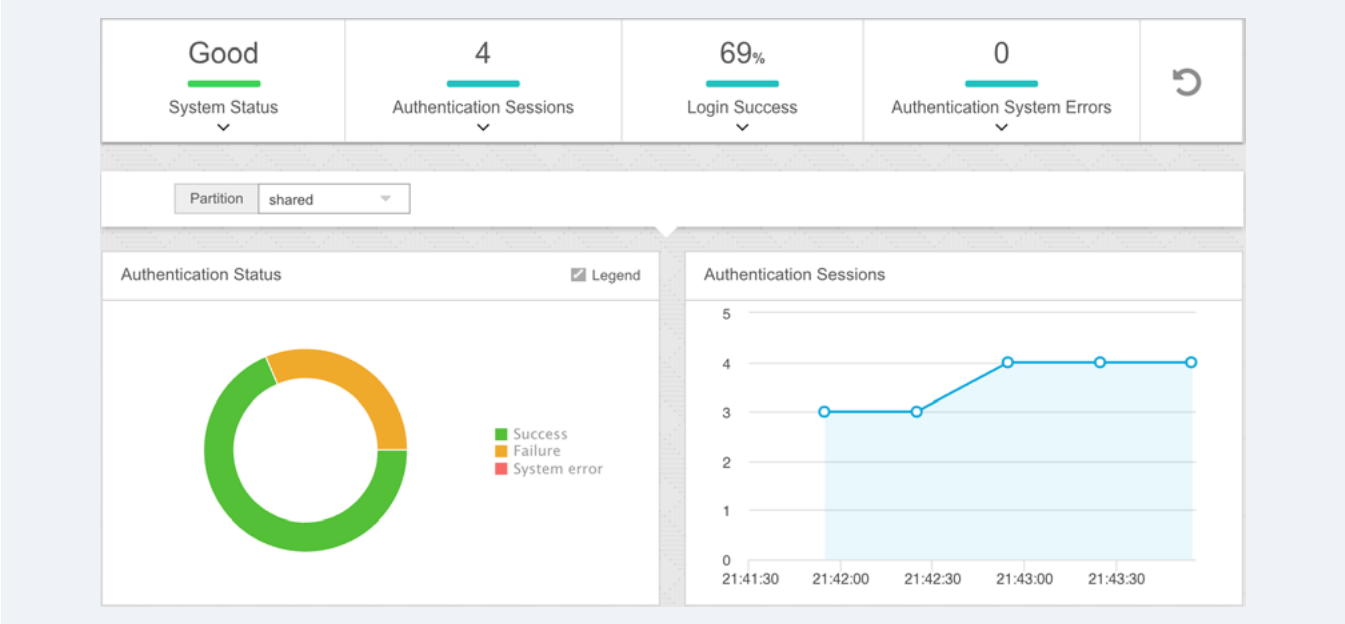

Figure 3: Authentication dashboard

- **URL filtering services:**

  URL filtering maximizes employee productivity and reduces risk by blocking non-business and malicious websites, including malware and phishing sources. URL filtering categorizes more than 13 billion URLs into 83 categories to block undesirable sites and shield users from threats. Users can be coached or denied access based on defined policies.

- **ICAP compatibility to leverage existing data leak prevention (DLP) and antivirus (AV) solutions:**

  Acting as an ICAP client, Thunder devices can co-exist with existing security infrastructure and help augment and enhance enterprise security needs. Thunder devices using ICAP can pass traffic to the network's existing DLP and AV systems without the need for extra solutions, while also providing SSL decryption functions.

- **Logging and compliance**:

  High-speed logging for all session activities in CEF format and per-rule statistics for SIEM integration are available. Authenticated sessions are tracked and used in logging for compliance purposes. In addition, the URL bypass feature selectively bypasses traffic from decryption to enforce privacy policies such as HIPAA, PCI-DSS and PII using a list of over 460 million domains.

- **AppCentric templates**:

  A10 Networks AppCentric templates (ACT) are intelligent configuration and monitoring templates. ACT helps reduce deployment times and simplify configuration, management and troubleshooting for IT.

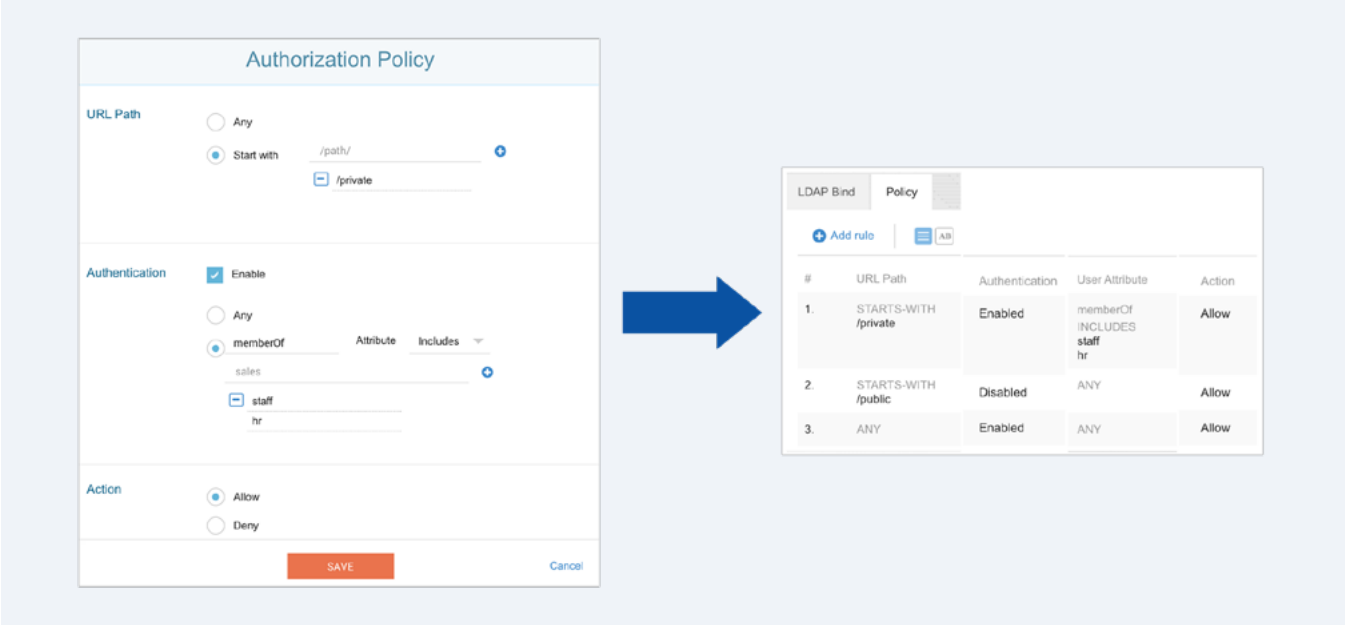

Figure 4: Authentication policy construct using ACT

- **Load balancing and steering:**

  Increase security capacity by load balancing multiple security devices and selective traffic steering based on fine-grained policies for unmatched scalability and efficiency.

- **SSL inspection with decrypt zone:**

  Thunder devices can decrypt traffic for security products simultaneously, including inline, non-inline (passive/TAP) and ICAP-enabled devices. Thunder SSLi boosts the performance of the security infrastructure by decrypting traffic and forwarding it to one or more third-party security devices, such as a firewall for deep packet inspection (DPI), then re-encrypts traffic and forwards it to the intended destination. Response traffic is inspected in the same way.

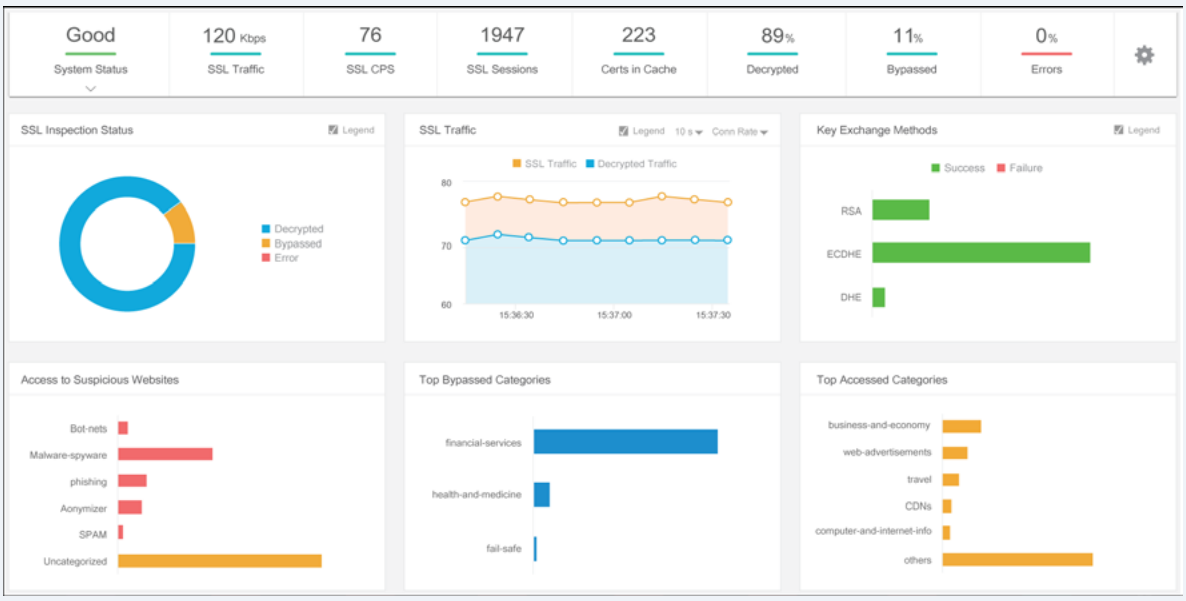

Figure 5: SSLi dashboard

- **Optional Up-to-the-minute threat intelligence:**

  The A10 Threat Intelligence Service leverages more than three dozen intelligence sources and provides an actionable list of known bad actors on the internet. A10's solutions leverage these lists to increase security efficacy by blocking traffic from and to bad destinations without the need to involve validation techniques.

Summary

A10's high-performance, future-proof and purpose-built Secure Web Gateways satisfy enterprise security needs by keep up with the speed at which modern SaaS applications and their myriad challenges. A10 Thunder SSLi and CFW provide superior performance and many advance features behind a true full proxy architecture at a fraction of the cost, making it a compelling, competitively priced choice for a Secure Web Gateway.

Next Steps

For more information, please contact your A10 representative and visit: A10networks.com/firewall.

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally. For more information, visit A10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-SB-19181-EN-03 OCT 2022