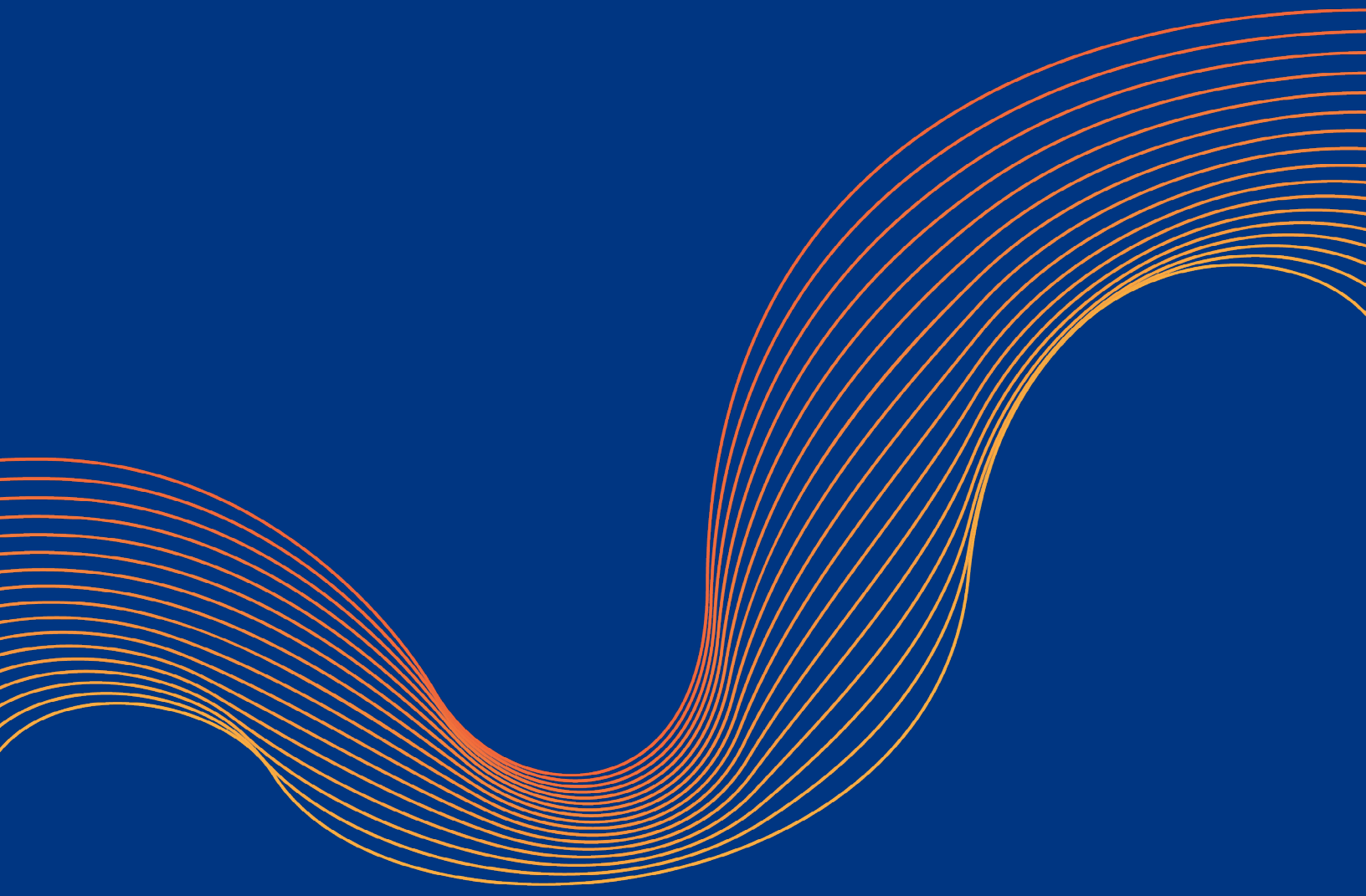
CLOUDFLARE

Trusted Internet Connections (TIC) 3.0



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Cloudflare Overlay Guidance

In late November 2007, the U.S. federal government announced the Trusted Internet Connections (TIC) initiative to migrate network services to a common solution for the federal government. The goal of the TIC initiative was to reduce external connections to the Internet and route network traffic through approved devices at approved access points. By routing that traffic through approved gateways, the federal government could apply consistent filtering and logging.

While the U.S. government formalized the TIC (also known as TIC 2.0), agencies inside of the government began to produce guidance around cloud computing usage. The government could reduce cost and complexity by migrating to software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) options, but had to first understand security risks and vendor approaches. In 2010, the Office of Management and Budget (OMB) issued a "Cloud First" directive to help the government realize economic and flexibility benefits and shortened procurement/certification timelines.

The shift to a cloud first policy began to highlight the limitations of TIC 2.0. As more and more government services moved to the cloud, they were being forced through the expensive TIC-authorized access points. The TIC access points could not scale to support the increased bandwidth, encryption, and perimeter defense requirements. Because of these limitations, the U.S. government released TIC 3.0 guidance in September 2019.

TIC 3.0 seeks to allow U.S. federal agencies flexibility in creating security architectures that make sense for their network architecture rather than using a perimeter-based approach.

Cloudflare has been building a network for years to solve this problem. The Cloudflare network delivers the security filtering of the TIC 3.0 requirements without asking departments to compromise on performance. We have built one of the world's largest networks, running 200+ cities across 100+ countries. Our network interconnects with 9,800+ networks globally (major ISPs, cloud services, and enterprises). Cloudflare was built from the ground up to support the convergence of networking and security. While available as a standalone product, the Cloudflare vision for Zero Trust networking is to deliver a natively integrated service with secure web gateway, remote browser isolation, firewall as a service, cloud access security broker, data loss protection, and SD-WAN functionality with single-pass inspection — all managed from the same UI.

We apply the same Zero Trust policies to all access decisions no matter where and how globally distributed users access the corporate environment — at home, on the road, or in the office.

Cloudflare brings security filtering closer to where users operate. Every service in the Cloudflare security stack runs in every data center, giving the U.S. government the ability to provide comprehensive security control without slowing down user connectivity. By enforcing security rules closer to the user, Cloudflare reduces the performance hit of backhauling traffic and lets users connect to the Internet without added delay.

The Cloudflare network improves performance in more ways than just data center distribution. Cloudflare monitors connectivity around the Internet, constantly measuring performance based on traffic passing through Cloudflare every day. The network uses that data to accelerate connections, including through our own global private backbone, to beat performance on the regular Internet.

We have selected a few of the TIC 3.0 Policy Enforcement Point (PEP) overlays and mapped them to current Cloudflare product offerings. We are constantly innovating by building our services on our serverless developer platform, Workers, so if you have a specific requirement that you do not see mapped below, do not hesitate to reach out to us via publicsector@cloudflare.com.

TRUSTED INTERNET CONNECTIONS (TIC) 3.0

TIC Security Capability	Cloudflare Product(s)	Complementary Product(s)	Service Description	Configuration Guidance
WEB PEP Security Capabilities				
Break & Inspect	WAF, Spectrum, Gateway		Cloudflare acts as a proxy in the data stream from client to server. WAF can inspect all payload information on common HTTP and HTTPS ports. Our SSL configurations can decrypt and then re-encrypt the traffic before sending back to the origin. Spectrum is a reverse proxy product that extends Cloudflare protections to all TCP/UDP applications. Gateway, a secure web gateway product, can conduct break and inspect to enforce L4 and L7 HTTP and DNS rules.	https://developers.cloudflare.com/cloudflare-one/
Active Content Mitigation	Gateway, WAF	Browser Isolation	Gateway, a secure web gateway product, can block malicious active content utilizing AV scanning or by using our browser isolation technology to execute, process, and render untrusted or malicious active content on our edge network far away from the customer's devices and networks. Our Web Application Firewall (WAF) contains active content mitigation, which contains categories such as "Data Loss Prevention" that search for specific patterns within network traffic and blocks or allows based on those patterns.	
Certificate Denylisting	All Products		All Cloudflare products support Online Certificate Status Protocol (OCSP) and certificate revocation lists (CRLs).	https://developers.cloudflare.com/ssl/ssl-for-saas/certificate-validation-methods https://blog.cloudflare.com/high-reliability-ocsp-stapling/
Content Filtering	Gateway		Gateway allows administrators to create DNS and HTTP filtering policies to block or allow requests based on various selectors such as destination host, URL, URL query, URL path, HTTP method, HTTP response, uploaded/downloaded file extension, uploaded/downloaded MIME type, content categories, and applications.	https://developers.cloudflare.com/cloudflare-one/policies
Authenticated Proxy	Access		Access supports authenticating via supported identity providers.	https://developers.cloudflare.com/cloudflare-one/identity

TRUSTED INTERNET CONNECTIONS (TIC) 3.0

TIC Security Capability	Cloudflare Product(s)	Complementary Product(s)	Service Description	Configuration Guidance
Data Loss Prevention	Gateway		DNS and HTTP rules can be created in Gateway that block or allow traffic based on various criteria (e.g. upload MIME type) that can control the flow of data.	https://blog.cloudflare.com/data-loss-prevention/ https://developers.cloudflare.com/cloudflare-one/policies/filtering/http-policies
Domain Resolution Filtering	Gateway		Gateway supports DNS over HTTPS (DoH) and will inspect all DNS queries, including DoH.	https://developers.cloudflare.com/cloudflare-one/policies/filtering/dns-policies-builder
Protocol Compliance Enforcement	WAF		Web Application Firewall allows customers to enable rules to block HTTP protocol anomalies and violations.	https://support.cloudflare.com/hc/en-us/articles/200172016-Understanding-the-Cloudflare-Web-Application-Firewall-WAF-#sJboboLurEVhipzWYJQnyz#sJboboLurEVhipzWYJQnyz
Domain Category Filtering	Gateway		Gateway supports filtering based on 13 DNS Security and 97 Content Categories.	https://developers.cloudflare.com/cloudflare-one/policies/filtering/dns-policies-builder/dns-categories
Domain Reputation Filtering	Gateway		Gateway supports filtering based on a number of criteria. Rules can be created to filter requests to categories with lower reputation such as newly seen domains, new domains, and Domain Generation Algorithm (DGA) domains. Customers can also define their own domain lists or import existing lists and set policies.	https://developers.cloudflare.com/cloudflare-one/policies/filtering/dns-policies-builder
Malicious Content Filtering	Gateway	Browser Isolation	Gateway, a secure web gateway product, can block malicious active content utilizing AV scanning or by using our browser isolation technology to execute, process, and render untrusted or malicious active content on our edge network far away from the customer's devices and networks.	https://developers.cloudflare.com/cloudflare-one/policies/filtering/dns-policies-builder https://support.cloudflare.com/hc/en-us/articles/200172016-Understanding-the-Cloudflare-Web-Application-Firewall-WAF-

TRUSTED INTERNET CONNECTIONS (TIC) 3.0

TIC Security Capability	Cloudflare Product(s)	Complementary Product(s)	Service Description	Configuration Guidance
Access Control	Access	Argo Tunnel	Access supports authenticating via one of the supported identity providers. Identity-based policies can be created to allow specific users or groups of users to access an internal application or cloud-based application.	https://developers.cloudflare.com/cloudflare-one/policies/zero-trust
Networking PEP Security Capabilities				
Access Control	Access, Magic Firewall	Magic Transit	Access supports authenticating via one of the supported identity providers. Identity-based policies can be created to allow specific users or groups of users to access an internal application or cloud-based application. Magic Firewall is a network-level firewall delivered through Cloudflare that allows Magic Transit customers to control network-based traffic with firewall rules.	https://developers.cloudflare.com/cloudflare-one/policies/zero-trust https://developers.cloudflare.com/magic-transit/magic-firewall
Internet Address Denylisting	Magic Transit, Magic Firewall, WAF, Gateway	Browser Isolation	Within our Magic Transit, Magic Firewall, WAF, and Gateway products, we provide the ability for customers to set their own allowlists or blocklists. A customer can scope out which IP addresses or IP CIDR spaces they wish to limit access to their services. This can be done on a per host or application basis.	https://support.cloudflare.com/hc/en-us/articles/217074967-Configuring-IP-Access-Rules
Host Containment	Access, Magic Firewall		Cloudflare Access has the ability to grant specific permissions to a host. Revocation of the authentication token issued on that host can be done at any time. The Magic Firewall product can block traffic from a different network to/from specific hosts behind the firewall.	https://developers.cloudflare.com/cloudflare-one/tutorials/rdp
Resiliency PEP Overlay				
Distributed Denial of Service Protections	Advanced DDoS, WAF, Spectrum, Magic Transit	Magic Transit	Cloudflare provides “always-on” DDoS protection for almost all of our products.	https://support.cloudflare.com/hc/en-us/articles/200172676-Understanding-Cloudflare-DDoS-protection
Elastic Expansion	All Products	Browser Isolation	Our unique architecture allows us to run all of our services on all globally distributed servers spread across 200+ data centers.	https://www.cloudflare.com/network/

TRUSTED INTERNET CONNECTIONS (TIC) 3.0

TIC Security Capability	Cloudflare Product(s)	Complementary Product(s)	Service Description	Configuration Guidance
Regional Delivery	All Products		Our regional services give customers the ability to accommodate regional restrictions while still using the Cloudflare global edge network.	https://blog.cloudflare.com/introducing-regional-services/
DNS PEP Overlay				
Domain Name Sinkholing	Gateway		Gateway allows administrators to create DNS filtering policies to "override" specific domain names. The override will forward all requests to a given destination to another destination the administrator sets.	https://www.cloudflare.com/resources/assets/slt3lc6tev37/6GcZqWjqsWB8TDdVWzlsgE/bb265042263263038d2fdba072365691/Cloudflare_Gateway_Datasheet.pdf
Domain Name Verification for Agency Clients	Gateway		We are a fully compliant Secure Resolver. We will obey all requests for DNSSEC-enabled domains.	
Domain Name Validation for Agency Domains	Managed DNS		We provide DNSSEC signatures through algorithm 13. We generate the associated DS key material and hand that off to the customer for implementation at the registrar. This builds the associated trust chain.	