Florianópolis/SC, 11 de fevereiro de 2022

PREGÃO ELETRÔNICO/SRP Nº. 012/2022 – TJAM

ANEXO III – Formulário de Proposta de Preços

RAZÃO SOCIAL: IPTRUST ADVANCE TECNOLOGIA DA INFORMAÇÃO LTDA - EPP		
CNPJ: 18.753.084/0001-08	**TELEFONE(S):** 48 3333-1551 / 48 99143-0967	
E-MAIL: alessandro@iptrust.com.br | financeiro@iptrust.com.br		
ENDEREÇO: Rua Presidente Gama Rosa, nº 54 – andar 3, CEP 88036-260, Trindade, Florianópolis/SC		
BANCO: 341 - Itaú	**AGÊNCIA: 1575**	**CONTA CORRENTE: 22525-3**

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Balanceamento de Carga com Firewall de Segurança Avançada de Aplicações WEB Integrado, conforme especificações no Termo de Referência. Fabricante: F5 Networks Produtos: BIG-IP i5800 com licenciamento Best Bundle + IP Intelligence + Suporte Premium por 36 meses	Conjunto	1 conjunto de equipamentos e de licenças de software que atendam às especificações em sua integralidade (cluster)	2	R$ 4.058.000,00	R$ 8.116.000,00
2	Solução para tráfego SSL Fabricante: F5 Networks Produtos: BIG-IP SSL Orchestrator + Suporte Premium por 36 meses	Conjunto	1 conjunto de licenças de software que atendam às especificações em sua integralidade (cluster)	2	R$ 576.000,00	R$ 1.152.000,00
3	Serviços de instalação e configuração do Firewall de Segurança Avançada de Aplicações WEB solicitado no item 1	Serviços	1	2	R$ 212.000,00	R$ 424.000,00
4	Serviços de instalação e configuração para tráfego SSL solicitado no item 2	Serviços	1	2	R$ 44.000,00	R$ 88.000,00
5	Serviços de Treinamento	Serviços	2	4	R$ 75.000,00	R$ 300.000,00
6	Serviços de Consultoria e Suporte Técnico	Horas Técnicas	600 Horas	2	R$ 317.000,00	R$ 634.000,00
					Valor Total	**R$ 10.714.000,00**
Valor Total por extenso: Dez milhões, setecentos e quatorze mil.						

Observações:

a) Validade da proposta: 60 (sessenta) dias.
b) Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Florianópolis, 11 de fevereiro de 2022.

ipTrust Advance Tecnologia da Informação Ltda – EPP
Alessandro Kern Fernandes
Sócio-Administrador
CPF: 656.202.910-49

Alessandro Kern Fernandes (11 de February de 2022 11:27 GMT-3)

18.753.084/0001-08
IPTRUST ADVANCE TECNOLOGIA DA INFORMAÇÃO LTDA - ME
Rua Presidente Gama Rosa nº 54 Andar 3
Trindade - CEP 88.036-260
Florianópolis – SC

PROPOSTADEPRECOSFINAL

Relatório de auditoria final 2022-02-11

Criado em:	2022-02-11
Por:	Valéria Santana (financeiro@iptrust.com.br)
Status:	Assinado
ID da transação:	CBJCHBCAABAAkPfhT0afoP3HDG5wpnKZKGAO-msUB8oS

Histórico de "PROPOSTADEPRECOSFINAL"

Documento criado por Valéria Santana (financeiro@iptrust.com.br)
2022-02-11 - 14:25:04 GMT- Endereço IP: 186.249.193.70

Documento enviado por email para Alessandro Kern Fernandes (alessandro@iptrust.com.br) para assinatura
2022-02-11 - 14:25:29 GMT

Email visualizado por Alessandro Kern Fernandes (alessandro@iptrust.com.br)
2022-02-11 - 14:27:20 GMT- Endereço IP: 186.249.193.70

Documento assinado eletronicamente por Alessandro Kern Fernandes (alessandro@iptrust.com.br)
Data da assinatura: 2022-02-11 - 14:27:43 GMT - Fonte da hora: servidor- Endereço IP: 186.249.193.70

Contrato finalizado.
2022-02-11 - 14:27:43 GMT

Pregão Eletrônico/SRP: 012/2022 TJAM

Licitante: ipTrust Advance Tecnologia da Informação Ltda - EPP
CNPJ: 18.753.084/0001-0
Lote Único
Item 1

Maximize the Value of Your Enterprise Application Delivery

To make it easier and more affordable to get the capabilities your organization needs, F5 provides three offerings: Good, Better, Best.

With the F5 Good, Better, Best options, you receive:

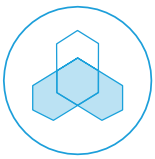
- Flexibility—Choosing from available modules makes it easier to adopt advanced F5 functionality.
- Simplicity—Having a standardized image and fewer configurations can help simplify operations.
- Best Value—You can save up to 65% vs. buying as components.

Select your right fit

Get advanced traffic management, optimization, and security services on one F5® BIG-IP® platform with the right offering for your organization.

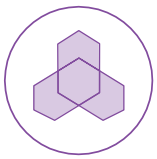
GOOD

Provides intelligent local traffic management for increased operational efficiency and peak network performance of applications.



BETTER

All the benefits of "Good" plus advanced application delivery optimization.



BEST

"Better" plus advanced access management and application security. Delivers optimal security, performance, and availability for your applications and network.

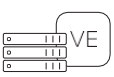
Choose the right platform for your organization

Virtual

Get flexible deployment options for virtual environments and the cloud.

Hardware

Achieve high performance with specialized and dedicated hardware.



Hybrid

Combine virtual and physical editions for flexibility and performance.

Features and Capabilities	Good	Better	Best
BIG-IP® Local Traffic Manager™			
Load balancing and monitoring	●	●	●
Application visibility and monitoring	●	●	●
L7 intelligent traffic management	●	●	●
Core protocol optimization (HTTP, TCP, HTTP/2, SSL)	●	●	●
SSL proxy and services	●	●	●
IPv6 support	●	●	●
Programmability (iRules®, iCall™, iControl®, iApps®)	●	●	●
ScaleN™ (on-demand scaling of performance and capacity)	●	●	●
BIG-IP® APM® Lite (user authentication, SSL VPN for 10 concurrent users)	●	●	●
SYN flood DDoS protection	●	●	●
Software Services			
Advanced routing (BGP, RIP, OSPF, ISIS, BFD)	Optional	●	●
BIG-IP® DNS			
Global server load balancing		●	●
DNS services		●	●
Real-time DNSSEC solution		●	●
Global application high availability		●	●
Geolocation		●	●
DNS DDoS attack prevention		●	●
BIG-IP® Advanced Firewall Manager™			
High-performance ICSA firewall		●	●
Network DDoS protection		●	●
Application-centric firewall policies		●	●
Protocol anomaly detection		●	●
BIG-IP® Application Security Manager™			
PCI-compliant web application firewall			●
Web scraping prevention			●
Integrated XML firewall			●
Violation correlation and incident grouping			●
Application DDoS protection			●
BIG-IP® Access Policy Manager®			
500 concurrent user sessions; scalable up to 200,000			●
BYOD enablement			●
Full proxy for VDI (Citrix, VMware)			●
Single sign-on enhancements (identity federation with SAML 2.0)			●

SDN services are automatically included with all iSeries appliances. BIG-IP Application Acceleration Manager (AAM) is end-of-sale.

To learn more about F5 market-leading technologies, visit f5.com.

DC1217 | OV-X-PILLAR-197719376

DATA SHEET

Pregão Eletrônico/SRP: 012/2022 TJAM

Licitante: ipTrust Advance Tecnologia da Informação Ltda - EPP
CNPJ: 18.753.084/0001-0
Lote Único
Item 1

BIG-IP System

WHAT'S INSIDE

Gain Agility with the Most Programmable Cloud-Ready ADC

F5's next-generation, cloud-ready Application Delivery Controller (ADC) platform provides DevOps-like agility with the scale, security depth, and investment protection needed for both established and emerging apps. The new F5® BIG-IP® iSeries appliances deliver quick and easy programmability, ecosystem-friendly orchestration, and record breaking, software-defined hardware performance. As a result, customers can accelerate private clouds and secure critical data at scale while lowering total cost of ownership (TCO) and future proofing their application infrastructure.

KEY BENEFITS

Obtain the lowest TCO
Reduce TCO and the infrastructure footprint by consolidating app and security services on to a unified, high-performance platform.

Protect critical data
Deliver the SSL capacity required to protect critical data—including offload of elliptical curve cryptography (ECC) processing to hardware—enabling forward secrecy scaling. Simplify operations and improve customer confidence with the fastest way to an SSL Labs A+ rating.

Secure applications
Deliver the most effective protection with integrated, one-pass, full stack (L3—L7) security, including an ICSA Certified firewall, high-capacity distributed denial-of-service (DDoS) mitigation, contextual access management, and more.

Ensure the easiest deployment
In cloud or container environments, save time with a simple, out-of-the-box native integration with leading private cloud, interconnects, and container environments.

Maximize investment protection
The iSeries' software-defined hardware includes unique F5 TurboFlex™ FPGA technology that enables on-demand optimized performance for specific use cases such as DDoS protection or UDP traffic processing. Eliminate forklift upgrades and extend the lifecycle of app delivery hardware with software-upgradeable performance.

Maximize uptime
Ensure your critical infrastructure is built on reliable, carrier-grade hardware with hot-swappable components, redundant power supplies and fans, and always-on management integrated with a full baseboard management controller (BMC) with IPMI support.

IPv6 READY

ICSA labs CERTIFIED SSL VPN FIREWALL - CORPORATE WEB APPLICATION FIREWALL

STANDARDIZE YOUR APP DELIVERY SERVICES

BIG-IP ADC appliances can simplify your network and reduce TCO by offloading servers, providing a consistent set of comprehensive application services, and consolidating devices, saving management, power, space, and cooling costs in the data center.

The massive performance and scalability of the BIG-IP platform reduces the number of ADCs needed to deliver even the most demanding applications. By offloading computationally intense processes, you can significantly reduce the number of application servers needed.

INTELLIGENT PERFORMANCE WHERE IT MATTERS

Traditional performance measurements in terms of throughput don't accurately represent the complex needs of delivering modern web applications. Connection capacity and L7 transactions per second are critical. For instance, ADCs must be able to process high levels of layer 4 and layer 7 connections and make application-layer decisions such as removing sensitive information or transforming application-specific payloads. BIG-IP appliances have the intelligence and performance to handle application layer decisions while securing your data and infrastructure.

THE ADVANTAGES OF F5 BIG-IP HARDWARE

The BIG-IP iSeries platform perfectly blends software and hardware innovations that balance the need for performance, scalability, and agility. The F5 TMOS® operating system provides total visibility, flexibility, and control across all application delivery services. With TMOS, organizations can intelligently adapt to the diverse and evolving requirements of applications and networks. Other unique or patented hardware and software innovations enable the BIG-IP iSeries platform to offer unmatched capabilities:

- F5 TurboFlex™ optimization technology: Field-programmable gate arrays (FPGAs), tightly integrated with CPUs, memory, TMOS, and software, provide specific packet-flow optimizations, L4 offload, support for private cloud tunneling protocols, and denial-of-service (DoS) protection. These hardware optimizations not only improve performancebut free CPU capacity for other app delivery and security tasks. Only BIG-IP iSeries appliances feature TurboFlex performance profiles–user-selectable, pre-packaged optimizations that provide different performance characteristics depending on the business need:
    - L4 offload enables unsurpassed throughput and reduced loads on software.

    - Unique per-virtual-IP/application SYN flood protection ensures that if one application is under attack, others are not affected. Only F5 ADCs implement hardware-based SYN cookies in L4 and full proxy L7 mode.
    - More than 100 types of DoS attacks can be detected and mitigated in hardware, hugely increasing the attack size that can be absorbed compared to software-only implementations.
    - Network virtualization and overlay protocol processing (such as VXLAN and NVGRE tunneling) increases traffic processing capacity.
    - UDP traffic processing increases throughput and reduces both latency and jitter, improving VoIP or streaming media performance.
- Best-in-market SSL performance accelerates SSL/TLS adoption by offloading costly SSL processing and speed key exchange and bulk encryption. BIG-IP iSeries solutions include hardware acceleration of ECC ciphers, enabling forward secrecy. In addition, the ability to achieve an SSL Labs A+ rating with a few simple steps reduces SSL configuration complexity and errors.
- BIG-IP platforms offer maximum hardware compression, enabling cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization.
- Enterprise class SSD (solid state drive) technology on select BIG-IP platforms improves performance and reliability, saves power, and reduces heat generation and noise.
- Efficiency features include 80 Plus Platinum certified power supplies as well as front-panel touchscreen LCD management, remote boot and multi-boot support, and USB support.

F5 ScaleN

F5 ScaleN® technology enables organizations to scale performance, virtualize, or horizontally cluster multiple BIG-IP devices, creating an elastic Application Delivery Networking infrastructure that can efficiently adapt as needs change.

- **On-demand scaling**–Increase capacity and performance with on-demand scaling, simply adding more power to your existing infrastructure instead of adding devices. Some BIG-IP appliance models can be upgraded to the higher performance model within each series through on-demand software licensing, which enables organizations to support growth without new hardware.
- **Operational scaling**–Virtualize ADC services with a multi-tenant architecture that

supports a variety of BIG-IP versions and product modules on a single device. F5 Virtual Clustered Multiprocessing™ (vCMP) technology enables select hardware platforms to run multiple BIG-IP guest instances. Each guest instance acts like a physical BIG-IP device, with a dedicated allocation of CPU, memory, and other resources. vCMP offers per-guest rate limiting for bandwidth, enabling different performance levels for each guest.

Further divide each vCMP guest using multi-tenant features such as partitions and route domains, which can isolate configuration and networks on a per-virtual-domain basis. Within each virtual domain, you can further isolate and secure configuration and policies, with a role-based access system for administrative control. When route domains/ partitions are combined with vCMP guests, F5 provides the highest density multi-tenant virtualization solution, which can scale to thousands of virtual ADC (vADC) instances. This ability to virtualize BIG-IP ADC services means service providers and enterprise users can isolate based on BIG-IP version, enabling departmental or project-based tenancy as well as performance guarantees, consolidated application delivery platform management, and increased utilization.

- **Application scaling**–Increase capacity by adding BIG-IP resources through an all-active approach, and scale beyond the traditional device pair to eliminate idle and costly standby resources. Application scaling achieves this through two forms of horizontal scale. One is Application Service Clustering, which focuses on application scalability and high availability. The other is Device Service Clustering, designed to efficiently and seamlessly scale BIG-IP application delivery services and sync application policies.

  Application Service Clustering delivers sub-second failover and comprehensive connection mirroring for a highly available cluster of up to eight devices at the application layer, providing highly available multi-tenant deployments. Workloads can be moved across a cluster of devices or virtual instances without interrupting other services and can be scaled to meet business demand.

  Device Service Clustering can synchronize full device configurations in an all-active deployment model, enabling consistent policy deployment and enforcement across devices–up to 32 active nodes. This ensures a consistent device configuration, with syncing of hardened firewall and access policies to simplify operations and reduce attack surfaces.

GAIN AGILITY AND CONTROL IN PRIVATE CLOUDS

Enterprises are migrating to private clouds to achieve agility and speed time to market for applications while maintaining control. Regardless of the chosen cloud stack, typically only basic networking and app services like load balancing are provided. Advanced application delivery and security services are required to optimize and protect applications. Highly scalable BIG-IP platforms, with programmatic interfaces and service delivery templates, enable integration and automation with orchestration systems and deliver right-sized services aligned to specific app needs.

F5 solutions integrate with the leading private cloud technology stacks, including OpenStack, VMware, and Microsoft. For OpenStack, F5 provides native orchestration with Heat templates to automate the end-to-end deployment of advanced app and security services, reducing deployment times from days to minutes. Integration with VMware vRealize Orchestrator through the Blue Medora vRO plug-in reduces configuration time, enables self-service of F5 application services by app owners, and automates complex, multi-step workflows. F5 iWorkflow™ enables integration of F5 devices with software-defined networking (SDN) orchestration systems providing a single point of contact between the orchestrator and F5 devices.

Two-tier architecture

For enterprises deploying a private cloud, a two-tier architecture provides an optimized design that takes best advantage of both hardware and software app delivery services. The first tier provides services such as L4 traffic management, distributed denial-of-service (DDoS) firewall, or SSL offloading, which are centralized and shared for all north-south traffic entering the network, enforcing consistent app policies. These services, which deal with high-volume traffic and incur heavy CPU loads, require high performance, scalability, and guaranteed service-level agreements (SLAs). Dedicated, purpose-built hardware such as BIG-IP iSeries appliances meet those requirements and, depending on the environment and app requirements, can be more cost efficient than commodity servers.

Tier 2—the tenant or app tier—includes emerging, cloud-native applications that can be hosted in containers or disaggregated into microservices. The apps require specific services addressing intra-app traffic (east-west traffic). Those services, which can include basic load balancing to web app firewall or web performance optimizations, can be delivered on a per-application basis through highly scalable, flexible software such as virtual editions of BIG-IP products. This two-tier architecture model, standardized on F5 application services, offers flexibility, a strategic point of control where proven app policies can be enforced, and complete visibility of all traffic, taking advantage of hardware where it's needed and software agility near the app.

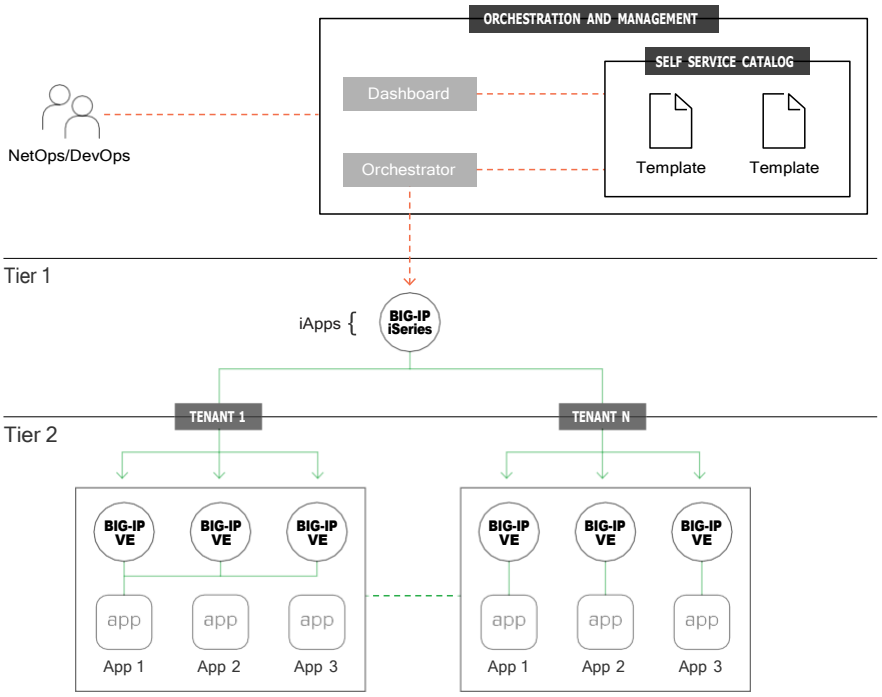


Figure 1: Orchestrated and automated deployment of app services in a two-tier private cloud architecture.

Programmability

Enabling automation and orchestration is key to achieving the benefits of cloud and software-defined architectures and to scaling application services on demand. F5 platforms offer many ways to program the application services fabric and network, enabling organizations to automate deployment, react to events in real time, and easily integrate into orchestration systems. F5 iRules® scripting has long provided granular traffic control and visibility, enabling customization, rapid response to code errors and security vulnerabilities, and support for new protocols. New F5 iRules LX™ lowers costs and speeds deployments by extending iRules to JavaScript developers and providing access to, and easier integration with, over 250,000 community Node.js packages. In addition, with F5 iApps® templates, organizations can automate deployment and configuration of application services in minutes. F5 iControl® REST APIs and SDKs provide integration with leading open source and commercial orchestration systems, VMware, OpenStack clouds, and configuration management systems such as Puppet, Chef, and Ansible.

BIG-IQ Centralized Management

F5 BIG-IQ® Centralized Management is F5's management and orchestration platform. It provides a central point of control for F5 physical and virtual devices and the app delivery and security services that run on them. BIG-IQ Centralized Management is available both as a virtual edition and an F5 appliance. It simplifies management, helps ensure compliance, and gives you the visibility and reporting you need to troubleshoot and respond to issues and security attacks.

BIG-IQ Centralized Management manages policies, licenses, SSL certificates, images, and configurations for F5 devices and the following BIG-IP software modules:

- BIG-IP® Local Traffic Manager™ (LTM)
- BIG-IP® Application Security Manager™ (ASM)
- BIG-IP® Advanced Firewall Manager™ (AFM)
- BIG-IP® Access Policy Manager® (APM)
- F5 Secure Web Gateway Services
- BIG-IP® DNS
- F5 WebSafe™ and F5 MobileSafe® (monitoring only)

BIG-IQ Centralized Management supports BIG-IP appliances, VIPRION chassis/blades, and BIG-IP virtual editions (VE), whether they are running locally or in the cloud. It is ideal for organizations that require central management of F5 devices and modules, license management of BIG-IP VEs, or central reporting and alerting on application availability, performance, and security.

Simplified and enhanced diagnostics and troubleshooting

BIG-IP iSeries appliances include a baseboard management controller (BMC) and support for the Intelligent Platform Management Interface (IPMI) protocol. With the BMC and Always-On Management (AOM) firmware, F5 customers can have deeper access to internal sensor data for system monitoring, including multiple thermal, airflow, and voltage readings. Out-of-band alerts for hardware-level problems are possible without a running TMOS instance. Gain remote system console access to the BMC and AOM functions through the same IP address of the TMOS management port, eliminating the need for a special or separate network. BIG-IP iSeries appliances also can show system information, such as sensor values for troubleshooting, on their color touchscreen LCD displays.

FIPS compliance at scale

The Federal Information Processing Standards (FIPS) specify requirements for cryptographic modules. FIPS compliance is required for many government agencies and industries such as financial services and healthcare that demand the highest standards in information, application, and data security. F5 offers a broad range of FIPS-certified hardware appliances that support a FIPS 140-2 Level 2 implementation for RSA cryptographic key generation, use, and protection (when running validated versions of TMOS). For additional protection, the BIG-IP 10350v-F/i7820-DF/i5820-DF supports a FIPS 140-2 Level 3 implementation of the Internal HSM (PCI card). BIG-IP Hardware FIPS appliances include integrated HSMs that have

tamper-evident seals with a hardened-epoxy cover which, if removed, will render the card useless. Keys generated on or imported into a BIG-IP system hardware security module (HSM) are not extractable in a plain-text format. This security rating means the 10350v-F/i7820-DF/i5820-DF HSM card adds tamper-resistance, which is an additional means of detection to the tamper-evident methods of Level 2, as well as a response to physical access attempts, or to cryptographic module use or tampering.

THE BIG-IP ISERIES: F5'S NEXT-GENERATION ADC SOLUTION

The new BIG-IP iSeries solutions unify application delivery for established and emerging apps in data center and cloud environments. The iSeries appliances provide leading performance, control, and versatility. With this platform, enterprises and service providers can efficiently standardize on a single platform to offload SSL processing and deploy comprehensive application and security services anywhere, in any architecture and development model, while reducing TCO. In addition, F5 provides tools such as the F5 iHealth® Upgrade Advisor and BIG-IP Migration Assistant to simplify and guide upgrades to the latest TMOS release or configuration migration to the new iSeries platform.

Specifications	i15800/i15820-DF	i15600/i15600-N
Intelligent Traffic Processing:	L7 requests per second: 10M L4 connections per second: 4.2M L4 HTTP requests per second: 35M Maximum L4 concurrent connections: 300M Throughput: 320 Gbps/160 Gbps L4/L7 (160 Gbps/140 Gbps L4/L7 in i15820-DF)	L7 requests per second: 5M L4 connections per second: 2.4M L4 HTTP requests per second: 28M Maximum L4 concurrent connections: 300M Throughput: 320 Gbps/160 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 100K TPS (250k TPS in i15820-DF) (ECDSA P-256) RSA: 160K TPS (320K TPS in i15820-DF) (2K keys) 50 Gbps bulk encryption (80/100G Gbps bulk encryption (AES-CBC/AES-GCM) in i15820-DF*)	ECC†: 60K TPS (ECDSA P-256) RSA: 80K TPS (2K keys) 50 Gbps bulk encryption*
FIPS SSL:	35K (RSA) in i15820-DF 8.5K (ECDSA P-256) in i15820-DF	N/A
Hardware Compression:	60 Gbps (120 Gbps in i15820-DF)	N/A
Hardware DDoS Protection:	210M SYN cookies per second (105M SYN CPS in i15820-DF)	140M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3 (4x BW)	N/A
Software Compression:	N/A	30 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	56 (28 in i15820-DF)	N/A
Processor:	Two 14-Core Intel Xeon processors (total 56 hyperthreaded logical processor cores)	Two 14-Core Intel Xeon processors (total 56 hyperthreaded logical processor cores)
Memory:	512 GB DDR4	512 GB DDR4
Hard Drive:	1x 1.6 TB Enterprise Class SSD (2x 1.6 TB Enterprise Class SSD in i15820-DF)	1x 1.6 TB Enterprise Class SSD
Ethernet and Fiber CU Ports:	N/A	N/A
40 Gigabit Fiber Ports (QSFP+):	8 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	8 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
100 Gigabit Fiber Ports (QSFP28):	4 SR4/LR4 (sold separately) QSFP28	4 SR4/LR4 (sold separately) QSFP28
Power Supply:	2x1500W Platinum AC PSU (i15800) or DC (i15800-N)	2x1500W Platinum AC PSU (i15600) or DC (i15600-N)
Typical Consumption:	885W (dual power supply, 48V DC or 110V AC input)** (815W in i15820-DF)	885W (dual power supply, 48V DC or 110V AC input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz (i15800) -48 to -60 VDC Minimum. Start up voltage: -44 VDC (i15800-N)	100-240 VAC +/- 10% auto switching, 50/60hz (i15600) -48 to -60 VDC Minimum. Start up voltage: -44 VDC (i15600-N)
Typical Heat Output:	3020 BTU/hour (2785 BTU/hour in i15820-DF) (dual power supply, 48V DC or 110V AC input)**	3020 BTU/hour (dual power supply, 48V DC or 110V AC input)**
Dimensions:	3.45" (8.76 cm) H x 17.9" (45.47 cm) W x 30.2" (76.71 cm) D2U industry standard rack-mount chassis	3.45" (8.76 cm) H x 17.9" (45.47 cm) W x 30.2" (76.71 cm) D 2U industry standard rack-mount chassis
Weight:	76 lbs. (34.47 kg) (Dual power supply)	76 lbs. (34.47 kg) (Dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40º C
Safety Agency Approval:	ANSI/UL 60950-1-2014*** CSA 60950-1-07, Including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, Including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012/AC:2013 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; As Information Technology Equipment (ITE) Class A per (as applicable): EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A NEBS Level 3 compliant	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A NEBS Level 3 compliant

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.

*Maximum throughput.

**Please refer to the Platform Guide: i15000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

***This equipment complies with these requirements of the Low Voltage Directive 2014/35/EU:EC Type Examination Certificates: Master Contract 252302 CB Scheme

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i11800	i11600
Intelligent Traffic Processing:	L7 requests per second: 5.5M L4 connections per second: 2.1M L4 HTTP requests per second: 25M Maximum L4 concurrent connections: 140M Throughput: 160 Gbps/80 Gbps L4/L7	L7 requests per second: 2.5M L4 connections per second: 1.1M L4 HTTP requests per second: 22M Maximum L4 concurrent connections: 140M Throughput: 160 Gbps/80 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 48K TPS (ECDSA P-256) RSA: 80K TPS (2K keys) 40 Gbps bulk encryption*	ECC†: 30K TPS (ECDSA P-256) RSA: 37K TPS (2K keys) 40 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	40 Gbps	N/A
Hardware DDoS Protection:	130M SYN cookies per second	70M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3 (2x bandwidth)	N/A
Software Compression:	N/A	25 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	32	N/A
Processor:	One 18-Core Intel Xeon processor (total 36 hyperthreaded logical processor cores)	One 18-Core Intel Xeon processor (total 36 hyperthreaded logical processor cores)
Memory:	256 GB DDR4	256 GB DDR4
Hard Drive:	1x 960 GB Enterprise Class SSD	1x 960 GB Enterprise Class SSD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	6 SR4/LR4 (sold separately); QSFP + optical breakout cable assemblies available to convert to 10 gigabit ports	6 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
Power Supply:	2x 650W Platinum AC PSU (2x 650W DC PSU Optional)	2x 650W Platinum AC PSU (2x 650W DC PSU Optional)
Typical Consumption:	455W (dual power supply, 110V input)**	455W (dual power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1555 BTU/hour (dual power supply, 110V input)**	1555 BTU/hour (dual power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis
Weight:	36 lbs. (16.3 kg) (dual power supply)	36 lbs. (16.3 kg) (Dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40º C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i11800, i11600, i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i10800	i10600
Intelligent Traffic Processing:	L7 requests per second: 3.5M L4 connections per second: 1.5M L4 HTTP requests per second: 22M Maximum L4 concurrent connections: 100M Throughput: 160 Gbps/80 Gbps L4/L7	L7 requests per second: 2.1M L4 connections per second: 1M L4 HTTP requests per second: 11M Maximum L4 concurrent connections: 100M Throughput: 160 Gbps/80 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 48K TPS (ECDSA P-256) RSA: 80K TPS (2K keys) 40 Gbps bulk encryption*	ECC†: 30K TPS (ECDSA P-256) RSA: 37K TPS (2K keys) 40 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	40 Gbps	N/A
Hardware DDoS Protection:	130M SYN cookies per second	70M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3 (2x bandwidth)	N/A
Software Compression:	N/A	25 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	16	N/A
Processor:	One 8-Core Intel Xeon processor (total 16 hyperthreaded logical processor cores)	One 8-Core Intel Xeon processor (total 16 hyperthreaded logical processor cores)
Memory:	128 GB DDR4	128 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD Model with dual SSDs in RAID 1 also available	1x 480 GB Enterprise Class SSD Model with dual SSDs in RAID 1 also available
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	6 SR4/LR4 (sold separately); QSFP + optical breakout cable assemblies available to convert to 10 gigabit ports	6 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10 gigabit ports)
Power Supply:	2x 650W Platinum AC PSU (2x 650W DC PSU Option)	2x 650W Platinum AC PSU (2x 650W DC PSU Option)
Typical Consumption:	415W (dual power supply, 110V input)**	415W (dual power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1420 BTU/hour (dual power supply, 110V input)**	1420 BTU/hour (dual power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis
Weight:	36 lbs. (16.3 kg) (dual power supply)	36 lbs. (16.3 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i11800, i11600, i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i7800	i7600
Intelligent Traffic Processing:	L7 requests per second: 3M L4 connections per second: 1.1M L4 HTTP requests per second: 14M Maximum L4 concurrent connections: 80M Throughput: 80 Gbps/40 Gbps	L7 requests per second: 1.8M L4 connections per second: 750K L4 HTTP requests per second: 7M Maximum L4 concurrent connections: 80M Throughput: 80 Gbps/40 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 25K TPS (ECDSA P-256) RSA: 40K TPS (2K keys) 20 Gbps bulk encryption*	ECC†: 15K TPS (ECDSA P-256) RSA: 22K TPS (2K keys) 20 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	20 Gbps	N/A
Hardware DDoS Protection:	70M SYN cookies per second	50M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3	N/A
Software Compression:	N/A	12 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	12	N/A
Processor:	One 6-Core Intel Xeon processor (total 12 hyperthreaded logical processor cores)	One 6-Core Intel Xeon processor (total 12 hyperthreaded logical processor cores
Memory:	96 GB DDR4	96 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD Model with Dual SSDs in RAID 1 also available	1x 480 GB Enterprise Class SSD Model with Dual SSDs in RAID 1 also available
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
Power Supply:	2x 650W Platinum AC PSU (2x 650W DC PSU Option)	2x 650W Platinum AC PSU (2x 650W DC PSU Option)
Typical Consumption:	310W (dual power supply, 110V input)**	310W (dual power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1060 BTU/hour (dual power supply, 110V input)**	1060 BTU/hour (dual power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis
Weight:	30 lbs. (13.6 kg) (dual power supply)	30 lbs. (13.6 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40° C	5% to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i5800	i5600
Intelligent Traffic Processing:	L7 requests per second: 1.8M L4 connections per second: 800K L4 HTTP requests per second: 12M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 Gbps L4/L7	L7 requests per second: 1.1M L4 connections per second: 500K L4 HTTP requests per second: 6M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 20K TPS (ECDSA P-256) RSA: 35K TPS (2K keys) 20 Gbps bulk encryption*	ECC†: 13K TPS (ECDSA P-256) RSA: 20K TPS (2K keys) 15 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	20 Gbps	N/A
Hardware DDoS Protection:	50M SYN cookies per second	25M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3	N/A
Software Compression:	N/A	12 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	8	N/A
Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processing cores)	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
Memory:	48 GB DDR4	48 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD	1x 480 GB Enterprise Class SSD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR or LR (sold separately); Optional 10G copper direct attach	8 SR or LR (sold separately); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
Power Supply:	1x 650W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)	1x 650W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)
Typical Consumption:	265W (single power supply, 110V input)**	265W (single power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	905 BTU/hour (single power supply, 110V input)**	905 BTU/hour (single power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis
Weight:	26 lbs. (11.8 kg) (dual power supply)	26 lbs. (11.8 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40° C	5% to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012 Class A; EN 61000-3-2:2014; EN 61000-3-3:2013; EN 55024:2010; FCC Class A (Part 15), IC Class A; VCCI Class A	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012 Class A EN 61000-3-2:2014; EN 61000-3-3:2013 EN 55024:2010 FCC Class A (Part 15); IC Class A; VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i4800	i4600
Intelligent Traffic Processing:	L7 requests per second: 1.1M L4 connections per second: 450K L4 HTTP requests per second: 2M Maximum L4 concurrent connections: 28M Throughput: 20 Gbps L4/L7	L7 requests per second: 650K L4 connections per second: 250K L4 HTTP requests per second: 1M Maximum L4 concurrent connections: 28M Throughput: 20 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 10K TPS (ECDSA P-256) RSA: 20K TPS (2K keys) 15 Gbps bulk encryption*	ECC†: 6.5K TPS (ECDSA P-256) RSA: 10K TPS (2K keys) 10 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	10 Gbps	N/A
Hardware DDoS Protection:	N/A	N/A
TurboFlex Performance Profiles:	Tier 2	N/A
Software Compression:	N/A	6 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	N/A	N/A
Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
Memory:	32 GB DDR4	32 GB DDR4
Hard Drive:	1 TB Enterprise Class HDD	1 TB Enterprise Class HDD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	8 SX or LX (sold separately)	8 SX or LX (sold separately)
10 Gigabit Fiber Ports (SFP+):	4 SR/LR (sold separately); optional 10G copper direct attach	4 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	N/A	N/A
Power Supply:	1x 250W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)	1x 250W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)
Typical Consumption:	130W (single power supply, 110V input)**	130W (single power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	445 BTU/hour (single power supply, 110V input)**	445 BTU/hour (single power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 22.5" (57.15 cm) D 1U industry standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 22.5" (57.15 cm) D 1U industry standard rack-mount chassis
Weight:	20 lbs. (9.07 kg) (single power supply)	20 lbs. (9.07 kg) (single power supply)
Operating Temperature:	32°F to 104°F	32°F to 104°F
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40º C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.

*Maximum throughput.

**Please refer to the Platform Guide: i2000/i4000 Series for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i2800	i2600
Intelligent Traffic Processing:	L7 requests per second: 650K L4 connections per second: 250K L4 HTTP requests per second: 1M Maximum L4 concurrent connections: 14M Throughput: 10 Gbps L4/L7	L7 requests per second: 350K L4 connections per second: 125K L4 HTTP requests per second: 600K Maximum L4 concurrent connections: 14M Throughput: 10 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 3.5K TPS (ECDSA P-256) RSA: 4.3K TPS (2K keys) 8 Gbps bulk encryption*	ECC†: 2.1K TPS (ECDSA P-256) RSA: 2.5K TPS (2K keys) 5 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	5 Gbps	N/A
Hardware DDoS Protection:	N/A	N/A
TurboFlex Performance Profiles	Tier 1	N/A
Software Compression:	N/A	3 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	N/A	N/A
Processor:	One 2-Core Intel Pentium processor (total 4 hyperthreaded logical processor cores)	One 2-Core Intel Pentium processor (total 4 hyperthreaded logical processor cores)
Memory:	16 GB DDR4	16 GB DDR4
Hard Drive:	1 TB Enterprise Class HDD	1 TB Enterprise Class HDD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	4 SX or LX (sold separately)	4 SX or LX (sold separately)
10 Gigabit Fiber Ports (SFP+):	2 SR or LR (sold separately); Optional 10G copper direct attach	2 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	N/A	N/A
Power Supply:	1x 250W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)	1x 250W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)
Typical Consumption:	95W (single power supply, 110V input)**	95W (single power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	325 BTU/hour (single power supply, 110V input)**	325 BTU/hour (single power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 22.5" (57.15 cm) D 1U industry standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 22.5" (57.15 cm) D 1U industry standard rack-mount chassis
Weight:	20 lbs. (9.07 kg) (single power supply)	20 lbs. (9.07 kg) (single power supply)
Operating Temperature:	32°F to 104°F	32°F to 104°F
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40º C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005; A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A: EN 61000-3-2:2014 EN 61000-3-3:2013: EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.

*Maximum throughput.

**Please refer to the Platform Guide: i2000 for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i11800-DS	i11600-DS
Intelligent Traffic Processing:	L7 requests per second: 5.5M L4 connections per second: 2.1M L4 HTTP requests per second: 25M Maximum L4 concurrent connections: 140M Throughput: 80 Gbps/70 Gbps L4/L7	L7 requests per second: 2.5M L4 connections per second: 1.2M L4 HTTP requests per second: 13M Maximum L4 concurrent connections: 140M Throughput: 80 Gbps/70 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 200K TPS (ECDSA P-256) RSA: 280K TPS (2K keys) 70 Gbps bulk encryption*	ECC†: 100K TPS (ECDSA P-256) RSA: 135K TPS (2K keys) 40 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	70 Gbps	70 Gbps
Hardware DDoS Protection:	130M SYN cookies per second	130M SYN cookies per second
TurboFlex Performance Profiles	Tier 3	Tier 3
Software Compression:	N/A	N/A
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	N/A
Virtualization (Maximum Number of vCMP Guests)	16	12
Processor:	One 18-Core Intel Xeon processor*** (total 36 hyperthreaded logical processor cores)	One 18-Core Intel Xeon processor*** (total 36 hyperthreaded logical processor cores)
vCPU Numbers:	32 vCPUs	24 vCPUs
Memory:	256 GB DDR4	256 GB DDR4
Hard Drive:	Dual SSD 2x 960GB Enterprise Class SSD	Dual SSD 2x 960GB Enterprise Class SSD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	6 SR4/LR4 (sold separately); QSFP + optical breakout cable assemblies available to convert to 10 gigabit ports	6 SR4/LR4 (sold separately); QSFP + optical breakout cable assemblies available to convert to 10 gigabit ports
Power Supply:	2x 650W Platinum AC PSU (2x 650W DC PSU Optional)	2x 650W Platinum AC PSU (2x 650W DC PSU Optional)
Typical Consumption:	455W (dual power supply, 110V input)**	455W (dual power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1485 BTU/hour (dual power supply, 110V input)**	1485 BTU/hour (dual power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis
Weight:	36 lbs. (16.3 kg) (dual power supply)	36 lbs. (16.3 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40º C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012/AC:2013 EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012/AC:2013 EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i11800, i11600, i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

***This is number of physical CPU cores, vCPU cores may vary depending on the type of licenses. Please upgrade using PAY-G licenses to increase the number of vCPU cores.

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i11400-DS	i7820-DF
Intelligent Traffic Processing:	L7 requests per second: 1.8M L4 connections per second: .75M L4 HTTP requests per second: 12.5M Maximum L4 concurrent connections: 140M Throughput: 80 Gbps/70 Gbps L4/L7	L7 requests per second: 3M L4 connections per second: 1.2M L4 HTTP requests per second: 14M Maximum L4 concurrent connections: 80M Throughput: 80 Gbps/40 Gbps
Hardware Offload SSL/TLS:	ECC†: 55K TPS (ECDSA P-256) RSA: 63K TPS (2K keys) 25 Gbps bulk encryption*	ECC†: 25K TPS (ECDSA P-256) RSA: 40K TPS (2K keys) 20 Gbps bulk encryption*
FIPS SSL:	N/A	13k TPS (FIPS 140-2 Level 3)***
Hardware Compression:	70 Gbps	20 Gbps
Hardware DDoS Protection:	130M SYN cookies per second	70M SYN cookies per second
TurboFlex Performance Profiles	Tier 3	Tier 3
Software Compression:	N/A	N/A
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	N/A
Virtualization (Maximum Number of vCMP Guests)	8	12
Processor:	One 18-Core Intel Xeon processor**** (total 36 hyperthreaded logical processor cores)	One 6-Core Intel Xeon processor**** (total 12 hyperthreaded logical processor cores)
vCPU Numbers:	16 vCPUs	N/A
Memory:	256 GB DDR4	96 GB DDR4
Hard Drive:	Dual SSD 2x 960GB Enterprise Class SSD	Dual SSD 2x 480GB Enterprise Class SSD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	6 SR4/LR4 (sold separately); QSFP + optical breakout cable assemblies available to convert to 10 gigabit ports	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
Power Supply:	2x 650W Platinum AC PSU (2x 650W DC PSU Optional)	2x 650W Platinum AC PSU (2x 650W DC PSU Option)
Typical Consumption:	455W (dual power supply, 110V input)**	310W (dual power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1485 BTU/hour (dual power supply, 110V input)**	1165 BTU/hour (dual power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis
Weight:	36 lbs. (16.3 kg) (dual power supply)	30 lbs. (13.6 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40º C	5% to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012/AC:2013 EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012/AC:2013 EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i11800, i11600, i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i11000 Series or Platform Guide: i7000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

***vCMP guest access to FIPS resources not supported.

****This is number of physical CPU cores, vCPU cores may vary depending on the type of licenses. Please upgrade using PAY-G licenses to increase the number of vCPU cores.

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	i5820-DF	10350v-N/10350v-F
Intelligent Traffic Processing:	L7 requests per second: 2M L4 connections per second: 800K L4 HTTP requests per second: 7M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 Gbps L4/L7	L7 requests per second: 3M L4 connections per second: 1.2M L4 HTTP requests per second: 14M Maximum L4 concurrent connections: 80M Throughput: 84 Gbps/40 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 20K TPS (ECDSA P-256) RSA: 35K TPS (2K keys) 20 Gbps bulk encryption*	Included: 42K TPS (2K keys) Maximum: 42K TPS (2K keys) 24 Gbps bulk encryption*
FIPS SSL:	8k TPS (FIPS 140-2 Level 3)	FIPS 140-2 Level 3 (10350v-F only)*** 35,000 TPS (2K keys) (10350v-F only) 24 Gbps bulk encryption (10350v-F only)
Hardware Compression:	20 Gbps	Included: 24 Gbps; Maximum: 24 Gbps
Hardware DDoS Protection:	50M SYN cookies per second	80M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3	N/A
Software Compression:	N/A	N/A
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	N/A
Virtualization (Maximum Number of vCMP Guests):	8	20
Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processing cores)	One 10-Core Intel Xeon processor (total 20 hyperthreaded logical processor cores)
Memory:	48 GB DDR4	128 GB
Hard Drive:	Dual SSD 2x 480GB Enterprise Class SSD	800 GB SSD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR or LR (sold separately); Optional 10G copper direct attach	16 SR or LR (sold separately, 2 SR included); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	2 SR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10 gigabit ports)
Power Supply:	1x 650W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)	Dual 850W included (80+Platinum efficiency), DC (10350v-N)
Typical Consumption:	265W (single power supply, 110V input)**	320W (dual supply, 48V DC**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	Operating range: 44 to 72 VDC Minimum start up voltage: 44 VDC
Typical Heat Output:	1215 BTU/hour (single power supply, 110V input)**	1095 BTU/hour (dual supply, 48V DC**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis	3.45" (8.76 cm) H x 17.3" (43.94 cm) W x 21.4" (54.36 cm) D 2U industry standard rack-mount chassis
Weight:	26 lbs. (11.8 kg) (dual power supply)	43 lbs. (19.5 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40° C	10% to 90% at 40º C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	UL 60950-1 2nd Edition; CAN/CSA C22.2 No. 60950-1-07 EN 60950-1:2006, 2nd Edition; IEC 60950-1:2006, 2nd Edition Evaluated to all CB Countries
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012/AC:2013 EN 61000-3-2:2014; EN 61000-3-3:2013; EN 55024:2010; FCC Class A (Part 15), IC Class A; VCCI Class A	EEN 300 386 V1.5.1 (2010-10); EN 55022:2006+A1:2007 EN 61000-3-2:2006; EN 61000-3-3:1995+A1:2000+A2:2005 EN 55024: 2010; USA FCC Class A; NEBS compliant; VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

**Please refer to the Platform Guide: i5000 Series or Platform Guide: 10000 Series for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

***vCMP guest access to FIPS resources not supported.

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

Specifications	10150v-N
Intelligent Traffic Processing:	L7 requests per second: 1.5M L4 connections per second: 609K L4 HTTP requests per second: N/A Maximum L4 concurrent connections: 80M Throughput: 84 Gbps/40 Gbps L4/L7
Hardware Offload SSL/TLS:	Included: 34K TPS (2K keys) Maximum: 34K TPS (2K keys) 24 Gbps bulk encryption*
FIPS SSL:	N/A
Hardware Compression:	N/A
Hardware DDoS Protection:	N/A SYN cookies per second
TurboFlex Performance Profiles:	N/A
Software Compression:	N/A
Software Architecture:	64-bit TMOS
On-Demand Upgradable:	N/A
Virtualization (Maximum Number of vCMP Guests):	12
Processor:	One 10-Core Intel Xeon processor (total 12 hyperthreaded logical processor cores)
Memory:	128 GB
Hard Drive:	800 GB SSD
Gigabit Ethernet CU Ports:	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP (SX or LX)
10 Gigabit Fiber Ports (SFP+):	16 SR or LR (sold separately, 2 SR included); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	2 SR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10 gigabit ports)
Power Supply:	Dual 850W included (80+Platinum efficiency), or DC (10150v-N)
Typical Consumption:	320W (dual supply, 48V DC**
Input Voltage:	Operating range: 44 to 72 VDC Minimum start up voltage: 44 VDC
Typical Heat Output:	1095 BTU/hour (dual supply, 48V DC**
Dimensions:	3.45“ (8.76 cm) H x 17.3” (43.94 cm) W x 21.4” (54.36 cm) D 2U industry standard rack-mount chassis
Weight:	43 lbs. (19.5 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	10% to 90% at 40º C
Safety Agency Approval:	UL 60950-1 2nd Edition; CAN/CSA C22.2 No. 60950-1-07 EN 60950-1:2006, 2nd Edition; IEC 60950-1:2006, 2nd Edition Evaluated to all CB Countries
Certifications/ Susceptibility Standards:	EEN 300 386 V1.5.1 (2010-10); EN 55022:2006+A1:2007 EN 61000-3-2:2006; EN 61000-3-3:1995+A1:2000+A2:2005 EN 55024: 2010; USA FCC Class A; NEBS compliant; VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.

*Maximum throughput.

**Please refer to the Platform Guide: 10000 Series or Platform Guide: i15000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

SIMPLIFIED LICENSING

It's never been easier to consolidate application services in data center and cloud environments. F5's Good-Better-Best licensing provides the flexibility to provision advanced F5 modules on-demand at the best value.

- Discover the right set of F5 solutions for your application environment.
- Procure the Better or Best modules for your applications.
- Implement comprehensive application services on a virtual or physical platform.

F5 GLOBAL SERVICES

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/support.

MORE INFORMATION

To learn more about BIG-IP, visit f5.com to find these and other resources:

Data sheets

BIG-IP Local Traffic Manager
BIG-IP DNS
BIG-IP Advanced Firewall Manager
BIG-IP Advanced WAF
BIG-IP Access Policy Manager
BIG-IP Carrier-Grade NAT
BIG-IP Policy Enforcement Manager
F5 Container Ingress Services

White papers

Build a Unified Application Delivery Architecture for Your Data Center and Cloud
Software-Defined Hardware: Enabling Performance and Agility with the BIG-IP iSeries Architecture
ScaleN: Elastic Infrastructure
Application Delivery Hardware: A Critical Component
Virtual Clustered Multiprocessing (vCMP)

DC0122 | DS-CORE-832415433

Pregão Eletrônico/SRP: 012/2022 TJAM

Licitante: ipTrust Advance Tecnologia da Informação Ltda – EPP
CNPJ: 18.753.084/0001-0
Lote Único
Item 1 e 2

What's Inside

Maintain Your F5 Solution with Fast, Reliable Support

In a world where change is the only constant, you rely on your F5® technology to deliver, no matter what turns your business takes. As challenges arise, quickly finding the best solution for your business can mean the difference between IT crisis and IT agility.

Both F5 Standard (10x5) and Premium (24x7) support include remote assistance both online and over the phone, proactive support for planned maintenance, advance Return Materials Authorization (RMA) replacement, software upgrades, and help with F5 iRules®. You can upgrade either Standard or Premium support with Expedited RMA Services and Maintenance Add-On Packages. In addition, F5 provides many free, self-service resources to help you get the most from your F5 investment.

Key benefits

Keep your business running

Receive fast, knowledgeable help with questions or issues regarding your F5 technology, so you can keep delivering the services on which your business depends.

Prepare for known events

Fast-track support for scheduled maintenance to minimize time spent opening a new case.

Increase flexibility

Make the most of the flexibility provided by iRules scripts to customize your F5 devices. With Standard and Premium support, F5 experts provide iRules assistance in troubleshooting, checking syntax, and validating logic.

Enhance ROI

Get more value from your investment by using the resources on F5.com to search the knowledge base, expand your skill set, and interact with the F5 developer community.

Standard and Premium Support Features

From F5-trained Network Support Engineers to online tools and software downloads, you'll find a range of F5 resources to provide the right level of support for your organization.

The difference between Standard and Premium support levels is in support hours.

Expert Assistance When You Need It

Count on F5 Support to provide the help you need, when you need it. F5's worldwide customer support organization has implemented an ISO 9001:2015–compliant Quality Management System that ensures F5 adheres to documented processes and procedures and continues to improve its delivery of customer support. With ISO compliance, you can be confident you'll receive consistently excellent service.

Network Support Centers

F5 Network Support Centers are strategically located for partners and customers in APAC, Japan, EMEA, and North America. Globally dispersing Network Support Centers allows F5 to provide support in a number of languages through native-speaking support engineers who are available when you are, during your business day.

- Standard support hours are Monday through Friday, 8:00 a.m. to 6:00 p.m., your local time.
- Premium support hours are around the clock, 365 days a year.

Network Support Engineers

F5 Network Support Engineers have extensive knowledge of F5 technology and receive continuous training in the latest features and updates to F5 products. When you contact Support, your call will be routed to the best subject matter expert for your case.

WebSupport Portal

F5's WebSupport Portal provides you with more flexibility and fast access to F5 Network Support Centers, at any time. Quickly create new support cases, receive an automated case number, read case details and updates, upload troubleshooting attachments, and more. Online help is always available.

Proactive Case Management

With Proactive Case management, you can alert F5 Support of upcoming scheduled maintenance on your F5 devices. That way, if you do need assistance, you'll save the time spent opening a new case and providing diagnostic files, and F5 Network Support Engineers can be quickly assigned to your case.

iRules Support

F5 will provide basic support for existing iRules to:

- Check iRule syntax
- Assist in troubleshooting iRules
- Validate iRule logic against functional requirements to F5's reasonable effort

The iRule must have been operating prior to contacting F5 support. F5 Support Services will not provide concept, design, authoring, or creation of the iRule. Additional assistance is available through DevCentral and F5 consulting services.

Software Upgrades and Updates

New software releases are available at no charge for support units.

Self-Service Resources

To get the most value from your F5 solution investment, explore the resources provided by the AskF5™ Knowledge Base and the F5 DevCentral online community.

AskF5 Knowledge Base

Consider AskF5 as your first source for answers. Visit the AskF5 website for software downloads, licensing tools, product guides, release notes, solutions to known issues, and how-to information. You can also sign up to receive security email alerts and product-specific RSS feeds.

F5 DevCentral

Join an online, developer community of more than 300,000 F5 users worldwide who collaborate and share innovations, including code samples, new techniques, and other tips.

Expedited RMA Services

Expedited RMA Services include options for Next Business Day delivery, 4-hour delivery, and for a technician to install the product for you. All levels include advance replacement.

Customers with Standard or Premium support can upgrade to Expedited RMA Services. RMA requests can be submitted only during supported hours, in accordance with the unit's base maintenance contract.

Maintenance Add-On Packages

Maintenance Add-On Packages offer an opportunity for you to proactively improve your IT infrastructure and better align IT with business goals on an ongoing basis.

Customers with Standard or Premium support levels can purchase Add-On Packages.

Service Delivery Manager

The Service Delivery Manager add-on provides a Service Delivery Manager (SDM) to assist in facilitating communication between your business owners and F5 technical resources to identify and anticipate issues. During escalation, your SDM serves as a single point of contact and conducts calls for Severity 1 (site down) priority case management until the issue is resolved.

Premium Plus

The highest level of support, Premium Plus provides a dedicated team of F5 Network Support Engineers who become familiar with your unique business environment and objectives, an SDM, and a dedicated phone line for your calls. Weekly status meetings and quarterly in-depth reviews provide an opportunity for you to work with your F5 team to address current issues and help you reach future goals. For immediate needs, your calls receive the highest priority status.

You can purchase a Premium Plus Add-On to your Premium support agreements.

Standard and Premium Support Level Comparison

Maintenance Agreement Features	Standard	Premium
10x5 support availability (M–F, 8am–6pm, your local time)	✓	
24x7 support availability		✓
AskF5 Knowledge Base access	✓	✓
WebSupport Portal access	✓	✓
Response to site-down calls within 30 minutes (phone only)	✓	✓
RMA advance replacement*	✓	✓

*Upgrade to Expedited RMA Services available

Add-On Packages Comparison

Add-On Package Features	SDM	Premium Plus
Severity 1 priority case management	✓	✓
Priority placement in the Support phone queue	✓	✓
Immediate Support Manager notification upon case creation	✓	✓
Regularly scheduled case generation and status reports	✓	✓
Quarterly onsite review	✓	✓
Top priority in case escalation path	✓	✓
Dedicated senior Technical Support team familiar with your environment		✓

F5 is committed to helping you keep your F5 technology in peak performance. If your organization requires a level of support not included in Standard or Premium support, or the Maintenance Add-On Packages, contact services@f5.com to find out about additional services and custom consulting.

More Information

To learn more about F5 Technical Support Services, visit f5.com or contact services@f5.com. For additional assistance with iRules development, contact F5 Professional Services at consulting@f5.com.

Pregão Eletrônico/SRP: 012/2022 TJAM

Licitante: ipTrust Advance Tecnologia da Informação Ltda – EPP
CNPJ: 18.753.084/0001-0
Lote Único
Item 1

IP Intelligence Service

DATA SHEET

What's Inside

Defend Against Malicious Traffic

Organizations today are exposed to a variety of potentially malicious attacks from rapidly changing IP addresses. Inbound and outbound botnet traffic such as distributed denial-of-service (DDoS) and malware activity can penetrate security layers and consume valuable processing power.

F5® IP Intelligence incorporates external, intelligent services to enhance automated application delivery with better IP intelligence and stronger, context-based security. By identifying IP addresses and security categories associated with malicious activity, the IP Intelligence service can incorporate dynamic lists of threatening IP addresses into the F5 BIG-IP® platform, adding context to policy decisions. IP Intelligence service reduces risk and increases data center efficiency by eliminating the effort to process bad traffic.

Key benefits

Ensure IP threat protection

Deliver contextual awareness and analysis to block threats from a dynamic set of high-risk IP addresses.

Improve visibility into threats from multiple sources

Detect malicious activity and IP addresses with help from a global threat-sensor network and IP intelligence database.

Enable granular threat reporting and automated blocking

Reveal communication with malicious IP addresses to create more effective security policies.

Optimize protection with real-time updates

Automatically refresh the threat database as often as every five minutes to keep the organization safe.

Contextual Awareness and IP Threat Protection

Using a frequently updated list of threat sources and high-risk IP addresses, IP Intelligence delivers contextual awareness and analysis of IP requests to identify threats from multiple sources across the Internet. The service draws on the expertise of a global threat-sensor network to detect malicious activity and IP addresses. Even when the BIG-IP device is behind a content delivery network (CDN) or other proxies, the IP Intelligence service provides protection by looking at the real client IP addresses as logged within the X-Forwarded-For (XFF) header. You can easily configure alarms or block traffic from a CDN with threatening IP addresses.

Deliver key contextual awareness

IP Intelligence:

- Updates the list of threatening IP addresses as frequently as every five minutes.
- Identifies and blocks the sources of known bad IP addresses.
- Identifies and blocks communications with new threatening IP addresses.

Protection Categories

The IP Intelligence service identifies and blocks IP addresses associated with a variety of threat sources, including:

Windows exploits: Includes active IP addresses offering or distributing malware, shell code, rootkits, worms, or viruses.

Web attacks: Includes cross-site scripting, iFrame injection, SQL injection, cross domain injection, or domain password brute force.

Botnets: Includes botnet command and control channels and infected zombie machines controlled by the botnet controller.

Scanners: Includes all reconnaissance, such as probes, host scan, domain scan, and password brute force.

Denial of service: Includes DoS, DDoS, anomalous SYN flood, and anomalous traffic detection.

Reputation: When enabled, denies access to IP addresses currently known to be infected with malware or to contact malware distribution points.

Phishing: Includes IP addresses hosting phishing sites or other kinds of fraud activities, such as click fraud or gaming fraud.

Proxy: Includes IP addresses providing proxy and anonymization services, as well as The Onion Router (TOR) anonymizer addresses.

Granular Threat Reporting and Automated Blocking

Armed with the latest intelligence and predictive risk analyses, IP Intelligence reveals inbound and outbound communication with malicious IP addresses and enables granular threat reporting and automated blocking. This increased visibility can reveal IP-based threats such as phishing attacks, attackers using anonymous proxies, the TOR network for online attacker anonymity, and even outbound communication with botnet command and control channels, exposing malware residing within the enterprise. Once identified, these threats can be mitigated by automatically blocking traffic through selected IP categories.

Sophisticated Threat Detection and Analysis

IP Intelligence incorporates a data set of threatening IP addresses and assigns threat categories. Network traffic and behavioral data from all IP addresses is also collected,

analyzed, and assigned to threat categories, providing visibility into threats based on IP addresses as they evolve.

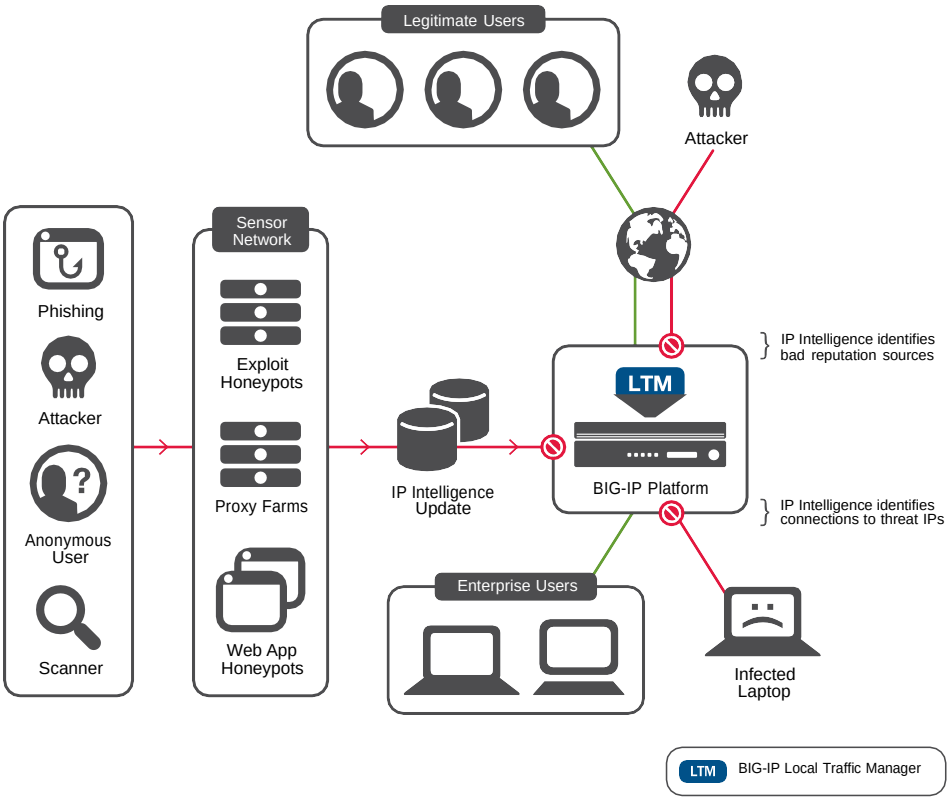


Figure 1: IP Intelligence identifies IP addresses, compares them to the global IP Intelligence database, and allows or blocks connections based on current known risks.

Threat Expertise from an Evolving IP Intelligence Database

When deployed on the F5 BIG-IP system, IP Intelligence uses insight about the Internet's most threatening IP addresses to block connections to and from those addresses. This evolving database of addresses is refreshed from the cloud as frequently as every five minutes to keep threat data current, minimize the threat window, and protect the organization and its reputation.

By detecting and blocking undesirable traffic, IP Intelligence offloads a significant percentage of the server workload. Emerging threats are continuously captured and published, while IP addresses that are no longer a threat are removed from the threat data. IP Intelligence augments visibility for all BIG-IP platforms without compromising access to legitimate IP addresses.

Real-Time Updates for Continuous Protection

Authenticated access to global threat data in the cloud enables IP Intelligence to update the BIG-IP system as frequently as every five minutes. BIG-IP products are easily configured to receive these real-time updates, delivering convenient security management while providing additional context during IP requests.

BIG-IP Platforms for Flexible Deployment

IP Intelligence is a subscription-based service that may be configured with the BIG-IP® Application Security Manager™ (ASM) user interface or incorporated into any BIG-IP platform with the F5 iRules® scripting language. For instance, IP Intelligence can be deployed with BIG-IP® Local Traffic Manager™ (LTM) in front of an e-commerce or financial website to mitigate phishing attacks. Add IP Intelligence to BIG-IP ASM to increase contextual awareness of Internet sites and protect requested applications from IP addresses with known malware or viruses. See the BIG-IP Platform Data Sheet for hardware details.

VIPRION Platforms

The IP Intelligence service is also available on the modular F5 VIPRION® system. The IP Intelligence service may be configured with the BIG-IP ASM user interface or incorporated with iRules into any BIG-IP product on the VIPRION platform. See the VIPRION Data Sheet for hardware details.

F5 Services

F5 Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Services can help you achieve IT agility. For more information about F5 Services, contact consulting@f5.com or visit f5.com/services.

More Information

To learn more about IP Intelligence, use the search function on f5.com to find this and other resources.

Data sheets

BIG-IP Platform

VIPRION

White paper

IP Intelligence

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.

Pregão Eletrônico /SRP 012/2022 - TJAM

Licitante: ipTrust Advance Tecnologia da Informação Ltda - EPP
CNPJ: 18.753.084/0001-08

Documento (planilha) em atendimento ao item - 8.1.2 do Termo de Referência

IDs	Description	Link
8.2	Solução para Alta Disponibilidade e Segurança Avançada de Aplicações	
8.2.1	Características de alta disponibilidade, otimização e balanceamento de carga para serviços locais	
8.2.1.1	Suportar todas as aplicações comuns de um Switch Layer 7, como:	
8.2.1.1.1	Server Load-Balancing	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-local-traffic-management-profiles-reference/introduction-to-local-traf
8.2.1.1.2	Firewall Load-Balancing	https://www.f5.com/services/resources/white-papers/load-balancing-101-firewall-sandwiches
8.2.1.1.3	Proxy Load-Balancing	https://support.f5.com/csp/article/K25523645
8.2.1.2	Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-local-traffic-manager-implementations-14-0-0/configuring-npath-routi
8.2.1.3	A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-local-traffic-manager-implementations/configuring-layer-3-npath-rout
8.2.1.4	Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede	https://support.f5.com/csp/article/K13392
8.2.1.5	Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação	https://www.f5.com/services/resources/white-papers/load-balancing-101-nuts-and-bolts
8.2.1.6	A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/_jcr_content/pdf
8.2.1.7	Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade de forma a não afetar o serviço	https://support.f5.com/csp/article/K13392
8.2.1.8	Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/_jcr_content/pdf
8.2.1.9	Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/14.html#unique_1626356
8.2.1.10	Suportar os seguintes métodos de balanceamento:	
8.2.1.10.1	Round Robin	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/6.html#unique_10065107
8.2.1.10.2	Least Connections	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/6.html#unique_10065107
8.2.1.10.3	Weighted Percentage (por peso)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/6.html#unique_10065107
8.2.1.10.4	Servidor ou equipamento com resposta mais rápida baseado no tráfego real	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/6.html#unique_10065107
8.2.1.10.5	Weighted Percentage dinâmico (baseado no número de conexões)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/6.html#unique_10065107
8.2.1.10.6	Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/6.html#unique_10065107
8.2.1.11	A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web	https://support.f5.com/csp/article/K14784?sr=43758715
8.2.1.12	Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:	
8.2.1.12.1	Por cookie: inserção de um novo cookie na sessão	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.2	Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.3	Por endereço IP destino	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.4	Por endereço IP origem	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.5	Por sessão SSL	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.6	Através da análise da URL acessada	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.7	Através da análise de qualquer parâmetro no header HTTP	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.8	Através da análise do MS Terminal Services Session (MSRDP)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.9	Através da análise do SIP Call ID ou Source IP	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.12.10	Através da análise de qualquer informação da porção de dados (camada 7)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/4.html
8.2.1.13	A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH	https://support.f5.com/csp/article/K11362
8.2.1.14	O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:	

8.2.1.14.1	Layer 3 – ICMP	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/15.html#conceptid
8.2.1.14.2	Conexões TCP e UDP pela respectiva porta no servidor	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-monitors-reference-11-5-0/3.html
8.2.1.14.3	Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-monitors-reference-11-5-0/3.html
8.2.1.15	Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/9.html#unique_17738392
8.2.1.16	Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/3.html#unique_11392574
8.2.1.17	Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/3.html#unique_11392574
8.2.1.18	Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/3.html#unique_11392574
8.2.1.19	Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/3.html#unique_11392574
8.2.1.20	Realizar Network Address Translation (NAT)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/16.html#conceptid
8.2.1.21	Realizar Proteção contra Denial of Service (DoS)	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-13-0-0/1.html
8.2.1.22	Realizar Proteção contra Syn flood	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-local-traffic-manager-implementations-14-0-0/mitigating-denial-of-ser
8.2.1.23	Realizar Limpeza de cabeçalho HTTP	https://clouddocs.f5.com/api/irules/HTTP__header.html
8.2.1.24	A solução deve permitir o controle da resposta ICMP por servidor virtual	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-11-5-1/48.html
8.2.1.25	Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/7.html#conceptid
8.2.1.26	Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-local-traffic-management-profiles-reference/introduction-to-local-traf
8.2.1.27	Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-local-traffic-manager-implementations/load-balancing-to-ipv6-nodes.h
8.2.1.28	Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/8.html#unique_21857374
8.2.1.29	Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/8.html#unique_21857374
8.2.1.30	Possuir capacidade para definir compressão especificamente para certos tipos de objetos	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/8.html#unique_21857374
8.2.1.31	Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-system-ssl-traffic-management-14-1-0-1/
8.2.1.32	Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados sejam realizadas com aceleração em hardware, para não onerar o sistema	https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf
8.2.1.33	Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo "man in the middle", ou seja, descriptografar, otimizar e criptografar novamente o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough	https://support.f5.com/csp/article/K14783
8.2.1.34	A solução deve possuir a funcionalidade de espelhamento de conexões SSL	https://support.f5.com/csp/article/K17391
8.2.1.35	A solução deve possuir a capacidade de redirecionar o SSL offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-system-ssl-administration/implementing-external-cryptographic-servei
8.2.1.36	Possuir recursos para configurar o equipamento para criptografar novamente em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-12-1-0/6.html
8.2.1.37	Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:	
8.2.1.37.1	Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS	https://support.f5.com/csp/article/K14783
8.2.1.37.2	Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS	https://support.f5.com/csp/article/K12140946
8.2.1.38	Ambas as autenticações acima mencionadas ocorrendo de forma simultânea	https://support.f5.com/csp/article/K15137?sr=57449070 #configure
8.2.1.39	Ao realizar inspeção, proteção, offload e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:	
8.2.1.39.1	Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS	https://support.f5.com/csp/article/K95338243
8.2.1.39.2	Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS	https://support.f5.com/csp/article/K5171
8.2.1.40	A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web	https://support.f5.com/csp/article/K14784
8.2.1.41	Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPS e SMTPS são enviadas aos servidores sem criptografia	https://support.f5.com/csp/article/K7415

8.2.1.42	A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:	
8.2.1.42.1	SSL session cache Timeout	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-13-0-0/_jcr_co
8.2.1.42.2	Session Ticket	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-13-0-0/_jcr_co
8.2.1.42.3	OCSP (Online Certificate Status Protocol) Stapling	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-13-0-0/_jcr_co
8.2.1.42.4	Dynamic Record Sizing	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-13-0-0/_jcr_co
8.2.1.42.5	ALPN (Application Layer Protocol Negotiation)	https://support.f5.com/csp/article/K04412053
8.2.1.42.6	Perfect Forward Secrecy	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-13-0-0/_jcr_co
8.2.1.43	Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores	https://support.f5.com/csp/article/K14903
8.2.1.44	Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados	https://support.f5.com/csp/article/K14903
8.2.1.45	Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos	https://support.f5.com/csp/article/K13878
8.2.1.46	Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor	https://support.f5.com/csp/article/K29377715
8.2.1.47	A solução deve suportar Internet Content Adaptation Protocol (ICAP)	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-12-1-0/_jcr_cont
8.2.1.48	Deve ser capaz de realizar DHCP relay	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-12-1-0/_jcr_cont
8.2.1.49	Deve possuir relatórios em tempo real das aplicações, com pelo menos os seguintes gráficos:	
8.2.1.49.1	Tempo de resposta da aplicação	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/avr-implementations-11-6-0/1.html#uniqu
8.2.1.49.2	Latência	
8.2.1.49.3	Conexões para conjunto de servidores, servidores individuais	
8.2.1.49.4	Por URL	
8.2.1.50	A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:	
8.2.1.50.1	Servidores virtuais	
8.2.1.50.2	Servidores balanceados	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/avr-implementations-11-6-0/1.html#uniqu
8.2.1.50.3	URLs	
8.2.1.50.4	Países de origem, baseados em geolocalização (GEOIP)	
8.2.1.50.5	Dispositivos de origem do cliente (user agent)	
8.2.1.51	Deve possuir framework unificado para configuração da aplicação	https://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf
8.2.1.52	Deve possuir criptografia IPSEC para comunicação entre os balanceadores	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-tunneling-and-ipsec-14-1-0/configuring-ipsec-in-tunnel-mode-be
8.2.1.53	Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.1.54	A Solução deve ter a capacidade de permitir a criação de MIBs customizadas	https://support.f5.com/csp/article/K13596
8.2.1.55	A Solução deve ter suporte a sFlow	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-
8.2.1.56	A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-tmos-routing-administration-14-0-0/09.h
8.2.1.57	A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-tmos-routing-administration-14-0-0/11.h
8.2.1.58	A solução deve suportar Equal Cost Multipath (ECMP)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-tmos-routing-administration-14-0-0/11.h
8.2.1.59	A solução deve realizar Bidirectional Forward Detection (BFD)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-tmos-routing-administration-14-0-0/11.h
8.2.1.60	A solução deve ter suporte a Stream Control Transmission Protocol (SCTP)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-service-provider-administration-13-0-0/1.
8.2.1.61	Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-system-ssl-administration-14-1-0/05.htm

8.2.1.62	A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-local-traffic-manager-monitors-reference
8.2.1.63	A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash	https://support.f5.com/csp/article/K97098157
8.2.1.64	A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA	https://support.f5.com/csp/article/K45130957
8.2.1.65	A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-12-1-0/_jcr_cont
8.2.1.65.1	Deve ser possível configurar o tamanho máximo da fila	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-12-1-0/_jcr_cont
8.2.1.65.2	Deve ser possível configurar o tempo máximo de permanência na fila	https://techdocs.f5.com/content/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-12-1-0/_jcr_cont
8.2.1.66	A solução deve realizar controle de banda estático para grupos de aplicações e rede	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/7.html#concepti
8.2.1.67	A solução deve realizar controle de banda dinâmico por aplicação e usuário	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/7.html#concepti
8.2.1.68	A solução deve realizar controle de banda baseado em domínio de roteamento	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/7.html#concepti
8.2.1.69	Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/7.html#concepti
8.2.1.70	Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/7.html#concepti
8.2.1.71	A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/7.html#concepti
8.2.1.72	A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-tmos-tunnels-ipsec-13-0-0/1.html
8.2.1.73	A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-tmos-tunnels-ipsec-13-0-0/1.html
8.2.1.74	Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0/about-nodes.html#GUID-955E
8.2.1.75	Possuir suporte ao protocolo SPDY e HTTP 2.0	https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-concepts-11-6-0/16.htmlhttps://support.f
8.2.1.76	O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL	https://support.f5.com/csp/article/K84303332
8.2.1.77	O equipamento deverá permitir a sincronização das configurações:	
8.2.1.77.1	De forma automática	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-device-service-clustering-admin-11-5-0/7
8.2.1.77.2	Manualmente, forçando a sincronização apenas no momento desejado	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-device-service-clustering-admin-11-5-0/7
8.2.1.78	Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:	https://support.f5.com/csp/article/K14135?sr=47651690
8.2.1.78.1	Compartilhar a rede de heartbeat com a rede de dados	https://support.f5.com/csp/article/K14135?sr=47651690
8.2.1.78.2	Utilizar uma rede exclusiva para o heartbeat	https://support.f5.com/csp/article/K14135?sr=47651690
8.2.1.79	Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-irules-concepts-11-6-0/1.html
8.2.1.80	A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens	https://support.f5.com/csp/article/K16221101?sr=54663987
8.2.1.81	Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts	https://community.f5.com/t5/technical-articles/getting-started-with-irules-lx-part-1-introduction-conceptual/ta-p/27622
8.2.1.82	Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-basics-11-6-0/6.html?sr=47652246
8.2.1.82.1	GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version	
8.2.1.83	Deve ser possível tomar as seguintes ações através dessas políticas:	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-basics-11-6-0/6.html?sr=47652246
8.2.1.83.1	Bloqueio de tráfego	
8.2.1.83.2	Reescrita e manipulação de URL	
8.2.1.83.3	Registro de tráfego (log)	
8.2.1.83.4	Adição de informação no cabeçalho HTTP	
8.2.1.83.5	Redirecionamento do tráfego para um membro específico	
8.2.1.83.6	Selecionar uma política específica para Aplicação Web	
8.2.1.84	A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:	
8.2.1.84.1	Endereço IP de origem	

8.2.1.84.2	Porta TCP ou UDP de origem	
8.2.1.84.3	Endereço IP de destino	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-
8.2.1.84.4	Porta TCP ou UDP de destino	
8.2.1.84.5	Protocolo de camada 4 (TCP ou UDP)	
8.2.1.84.6	Data e hora da mensagem	
8.2.1.84.7	URL acessada	
8.2.1.85	A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory	https://support.f5.com/csp/article/K15497?sr=57454690
8.2.1.86	A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas	https://support.f5.com/csp/article/K4423?sr=57454710
8.2.1.87	A solução deve ser capaz de analisar a performance de aplicações web	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-0-0/1.html
8.2.1.88	A solução deve possuir relatórios das aplicações	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-0-0/1.html
8.2.1.89	Deve prover métricas de aplicações como: Transações por segundo	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-0-0/1.html
8.2.1.90	A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-0-0/1.html
8.2.1.91	As informações coletadas deverão permitir a análise dos dados por aplicações, por URLs, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/logging-application-security-events.html#GUID-1068D52E-42B0-4FFA-BFBE-C81944432B12
8.2.1.92	A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-0-0/1.html
8.2.1.93	A geração de informações históricas deverá permitir:	
8.2.1.93.1	O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-0-0/5.html
8.2.1.93.2	Permitir a correlação de métricas de uso de rede com o comportamento das aplicações	http://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf
8.2.2	Características de alta disponibilidade entre Datacenters e proteção DNS:	
8.2.2.1	A solução deve operar em, no mínimo, a seguintes formas:	
8.2.2.1.1	DNS autoritativo	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.1.2	DNS secundário	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.1.3	DNS resolver	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.1.4	DNS cache	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.1.5	Balanceamento de DNS servers	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.1.6	DNSSEC	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.2	A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/4.ht
8.2.2.3	Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/5.ht
8.2.2.4	A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário	https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf
8.2.2.5	A solução deve servir as respostas às requisições onde o DNS é o autoritativo a partir da memória RAM	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/7.ht
8.2.2.6	A solução deve possuir proteções contra ataques DNS, no mínimo:	
8.2.2.6.1	Inspeção de protocolo	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.6.2	Validação de protocolo	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.6.3	UDP flood	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.6.4	Pacotes mal formados	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.6.5	Ataque thwarting teardrop	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.6.6	Ataque ICMP	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.7	Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.8	A solução deve ser capaz de realizar balanceamento dos servidores DNS	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.9	A solução deve ser capaz de realizar filtragem de pacotes	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.10	A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN, reflexão e ampliação DNS	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.11	A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.12	A solução deve realizar stateful inspection	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.13	A solução deve possuir base de Geolocalização IP	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.14	A solução deve implementar DNS64	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-dns-services-implementations-13-0-0/10.

8.2.2.15	A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV,TXT	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-dns-services-implementations-13-0-0/14.l
8.2.2.16	Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/12.h
8.2.2.17	Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/7.ht
8.2.2.18	Deve prover as respostas a queries DNS da própria RAM CACHE	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/7.ht
8.2.2.19	A solução deve ser capaz de realizar IP Anycast	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.20	A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.21	A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-implementations-12-1-0/12.html
8.2.2.22	A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.23	A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.24	Deve ser possível ajustar quantos endereços são enviados em uma única resposta	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.25	Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.26	Suportar pelo menos os seguintes algoritmos de balanceamento:	
8.2.2.26.1	Round Robin	
8.2.2.26.2	Global Availability	
8.2.2.26.3	Ratio	
8.2.2.26.4	LDNS Persist	
8.2.2.26.5	Geografia	
8.2.2.26.6	Disponibilidade da Aplicação	
8.2.2.26.7	Capacidade do Virtual Server	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.26.8	Least Connections	
8.2.2.26.9	Pacotes por segundo	
8.2.2.26.10	Round trip time	
8.2.2.26.11	Hops	
8.2.2.26.12	Packet Completion Rate	
8.2.2.26.13	QoS definido pelo usuário	
8.2.2.26.14	Kilobytes per Second	
8.2.2.27	Implementar persistência da conexão do usuário entre aplicações ou data centers	https://techdocs.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm-concepts-11-5-0/4.html#unique_3024960
8.2.2.28	A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.29	A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.30	A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.31	A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6)	https://www.f5.com/pdf/products/big-ip-global-traffic-manager-ds.pdf
8.2.2.32	Possuir suporte a IPv6 no balanceamento global entre datacenters	https://support.f5.com/csp/article/K62640222
8.2.2.33	Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6	https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf
8.2.3	Características de segurança de firewall e DoS camada 4	
8.2.3.1	A solução deve atuar como firewall de datacenter	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.2	A solução deve possuir certificação ICSA	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.3	A solução deve permitir a criação de logs customizados por aplicação	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.4	A solução deve terminar as conexões SSL com a finalidade de inspecioná-las	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.5	A solução deve proteger de ataques DDoS nas camadas de rede e de sessão	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.6	A solução deve permitir a criação de regras com, no mínimo, os seguintes parâmetros:	
8.2.3.6.1	Endereço IP destino	

8.2.3.6.2	Endereço IP de origem	
8.2.3.6.3	Porta de destino	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-network-firewall-policies-and-implement
8.2.3.6.4	Porta de origem	
8.2.3.6.5	VLAN	
8.2.3.6.6	Protocolo	
8.2.3.6.7	Ação	
8.2.3.6.8	Horário	
8.2.3.6.9	Log	
8.2.3.7	A solução deve permitir definir agendamento para ativação da regra	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-network-firewall-policies-and-implement
8.2.3.8	A solução deve permitir definir, no mínimo, as seguintes ações no tráfego:	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-network-firewall-policies-and-implement
8.2.3.8.1	Permitir: os pacotes são aceitos e passam pelo firewall	
8.2.3.8.2	Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego	
8.2.3.8.3	Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego	
8.2.3.9	Deve ser possível criar regras que sejam aplicadas de diferentes contextos:	
8.2.3.9.1	Global	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-network-firewall-policies-and-implement
8.2.3.9.2	Domínio de Roteamento	
8.2.3.9.3	Virtual Server	
8.2.3.9.4	Mitigar, no mínimo, os seguintes tipos de ataques:	
8.2.3.9.5	ICMP/UDP/TCP FloodS	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-system-dos-protection-and-protocol-firev
8.2.3.9.6	TCP Flag Abuses	https://support.f5.com/csp/article/K11809419
8.2.3.9.7	GET/POST FloodS	https://support.f5.com/csp/article/K14235020https://support.f5.com/csp/article/K44230544
8.2.3.9.8	SYN Floods	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-network-firewall-policies-and-implement
8.2.3.9.9	Smurfing	https://www.f5.com/services/resources/glossary/icmp-flood-ping-flood-smurf-attack
8.2.3.9.10	DNS Attacks	https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/dns-dos-firewall-implementations-11-5-0/4.htm
8.2.3.9.11	NTP Reflection Attacks	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.9.12	Fragging Attack	https://support.f5.com/csp/article/K17102
8.2.3.9.13	Slowloris	https://support.f5.com/csp/article/K10260
8.2.3.9.14	Connection Attacks	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf
8.2.3.9.15	Botnet	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/configuring-bot-defense.html
8.2.3.9.16	Fragmentation attacks	https://support.f5.com/csp/article/K49869231#link_06_04
8.2.4	Características de segurança de firewall de aplicação e DDoS de camada 7	
8.2.4.1	O equipamento oferecido deverá proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7)	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.2	Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, aprendizado e analíticos de big data	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/1.html
8.2.4.3	Deve possuir proteção de DoS através de análise comportamental, de assinaturas de robôs e baseado no nível de estresse do servidor de aplicação	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/1.html
8.2.4.4	A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/releasenotes/product/relnote-asm-12-1-0.html
8.2.4.5	A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.6	Permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-getting-started-13-1-0/1.html
8.2.4.7	Possuir política de segurança de aplicações web pré-configurada na solução	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.8	Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/34.html?sr=5745
8.2.4.9	Permitir a criação de políticas diferenciadas por aplicação	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/34.html?sr=5745

8.2.4.10	Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies	https://support.f5.com/csp/article/K12312?sr=57455154
8.2.4.11	A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.12	A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-getting-started-12-1-0/4.html
8.2.4.13	A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-13-1-0/32.html
8.2.4.14	Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus	https://support.f5.com/csp/article/K70941653
8.2.4.15	Deve se integrar com o software de Antivírus existente no ambiente da CONTRATANTE	https://support.f5.com/csp/article/K70941653
8.2.4.16	Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-irules-concepts-11-6-0/1.html
8.2.4.17	Permitir a integração com Firewall de Database de outros fabricantes	https://www.f5.com/pdf/deployment-guides/oracle-database-firewall-asm-dg.pdf
8.2.4.18	A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes	https://www.f5.com/products/ecosystem-integrationshttps://www.f5.com/pdf/solution-center/splunk-asm-sb.pdf
8.2.4.19	O fabricante da solução deve disponibilizar também a comercialização como serviço na nuvem (WAFaaS), incluindo o serviço de migrar as regras/políticas existentes do Datacenter para a nuvem	https://www.f5.com/pdf/products/f5-silverline-web-application-firewall-datasheet.pdf
8.2.4.20	Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.21	A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto, o sistema não precisa usar recursos para mitigar tráfego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.22	A solução deve suportar e fazer a proteção do tráfego em cima do protocolo WebSocket	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.23	A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto deve ser possível por exemplo logar as requisições válidas num servidor de SIEM e as inválidas em outro servidor de SIEM de outra marca e modelo	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/14.html
8.2.4.24	A solução deverá possuir funcionalidade de proteção positiva e segura, como:	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.24.1	Acesso por Força Bruta	
8.2.4.24.2	Ameaças Web AJAX/JSON	
8.2.4.24.3	DoS e DDoS camada 7	
8.2.4.24.4	Buffer Overflow	
8.2.4.24.5	Cross Site Request Forgery (CSRF)	
8.2.4.24.6	Cross-Site Scripting (XSS)	
8.2.4.24.7	SQL Injection	
8.2.4.24.8	Parameter tampering	
8.2.4.24.9	Cookie poisoning	
8.2.4.24.10	HTTP Request Smuggling	
8.2.4.24.11	Manipulação de campos escondidos	
8.2.4.24.12	Manipulação de cookies	
8.2.4.24.13	Roubo de sessão através de manipulação de cookies	
8.2.4.24.14	Sequestro de sessão	
8.2.4.24.15	Força bruta no browser	
8.2.4.24.16	XML bombs/DoS	
8.2.4.24.17	Checagem de consistência de formulários	
8.2.4.24.18	Checagem do cabeçalho do "user-agent" para identificar clientes inválidos	
8.2.4.25	A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/21.html
8.2.4.26	Deverá ser capaz de identificar e bloquear ataques através de:	
8.2.4.26.1	Assinaturas, com atualização periódica da base pelo fabricante	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.27	As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições deve fazer parte da solução de WAF ofertada	https://support.f5.com/csp/article/K82512024
8.2.4.28	Regras de verificação personalizadas – política de segurança configurada	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-asm-getting-started/creating-a-simple-security-policy.html#GUID-FD3
8.2.4.29	Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/protecting-sensitive-data-with-data-guai
8.2.4.30	Permitir a customização da resposta de bloqueio	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-11-5-0/25.html
8.2.4.31	Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/preventing-dos-attacks-on-applications.html#GU

8.2.4.32	Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/preventing-dos-attacks-on-applications.html#GU
8.2.4.33	Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/4.htmlhttps://tec
8.2.4.34	Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/preventing-dos-attacks-on-applications.html#GU
8.2.4.35	A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.36	Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/changing-security-policy-settings.html#GUID-E3
8.2.4.37	Deverá implantar, no mínimo, as seguintes funcionalidades:	
8.2.4.37.1	Proteção contra Buffer Overflow	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.37.2	Checagem de URL	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.37.3	Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT)	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.37.4	Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection)	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.37.5	Proteção contra Cross-site Scripting	https://support.f5.com/csp/article/K94326043
8.2.4.37.6	Funcionalidade de Cookie Encryption	https://support.f5.com/csp/article/K14784
8.2.4.37.7	Checagem de consistência de formulários	https://support.f5.com/csp/article/K74535942
8.2.4.37.8	Checagem do cabeçalho "user-agent" para identificar clientes inválidos	https://support.f5.com/csp/article/K00736342
8.2.4.38	Implementar as seguintes funcionalidades:	
8.2.4.38.1	Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/protecting-sensitive-data-with-data-guar
8.2.4.38.2	Esconder qualquer mensagem de erro HTTP dos usuários	https://support.f5.com/csp/article/K52325602
8.2.4.38.3	Remover as mensagens de erro às páginas que serão enviadas aos usuários	https://support.f5.com/csp/article/K52325602
8.2.4.38.4	Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios	https://support.f5.com/csp/article/K13050156#link_03_06
8.2.4.39	Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF)	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/changing-security-policy-settings.html#GUID-E3
8.2.4.40	Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s)	https://support.f5.com/csp/article/K79414542
8.2.4.41	Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/refining-security-policies-with-learning.h
8.2.4.42	O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação	https://support.f5.com/csp/article/K75376155
8.2.4.43	O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado	https://support.f5.com/csp/article/K75376155
8.2.4.44	O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral	https://support.f5.com/csp/article/K8866
8.2.4.45	As atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-11-5-0/39.html
8.2.4.46	O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/preventing-dos-attacks-on-applications.html#GU
8.2.4.47	O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/preventing-dos-attacks-on-applications.h
8.2.4.47.1	Número de requisições por segundo enviados a uma URL específica	
8.2.4.47.2	Número de requisições por segundo enviados de um IP específico	
8.2.4.47.3	Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots)	https://support.f5.com/csp/article/K54335130
8.2.4.47.4	Número máximo de transações por segundo (TPS) de um determinado IP	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/preventing-dos-attacks-on-applications.h
8.2.4.47.5	Aumento de um determinado percentual do número de transações por segundo (TPS)	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/preventing-dos-attacks-on-applications.h
8.2.4.47.6	Aumento do tempo de resposta (latência de aplicação) de uma determinada URL	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/preventing-dos-attacks-on-applications.h
8.2.4.48	O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável	https://support.f5.com/csp/article/K54335130

8.2.4.49	O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente	https://support.f5.com/csp/article/K02212345
8.2.4.50	O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-13-1-0/7.html
8.2.4.51	O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-bot-and-attack-signatures-13-0-0/5.html
8.2.4.52	Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.52.1	IBM Lotus Domino	
8.2.4.52.2	Microsoft ActiveSync v1.0, v2.0	
8.2.4.52.3	Microsoft OWA in Exchange 2003, 2007, 2010	
8.2.4.52.4	Microsoft SharePoint 2003, 2007, 2010	
8.2.4.52.5	Oracle 10g Portal	
8.2.4.52.6	Oracle Application 11i	
8.2.4.52.7	Oracle PeopleSoft Portal	
8.2.4.52.8	SAP NetWeaver	
8.2.4.53	O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation)	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.54	Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
8.2.4.55	Implementar a segurança de serviços web, através dos seguintes métodos:	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-11-5-0/17.html
8.2.4.55.1	Criptografar/Decriptografar partes das mensagens SOAP	
8.2.4.55.2	Assinar digitalmente partes das mensagens SOAP	
8.2.4.55.3	Verificação de partes das mensagens SOAP	
8.2.4.56	Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/protecting-sensitive-data-with-data-gua
8.2.4.57	Prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário	https://support.f5.com/csp/article/K52325602
8.2.4.58	Deverá ter integração, via ICAP, com servidor de antivírus para verificação dos arquivos a serem carregados nos servidores	https://support.f5.com/csp/article/K70941653
8.2.4.60	Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/40.html
8.2.4.60.1	Determinar os comandos FTP permitidos	
8.2.4.60.2	Requisições FTP anônimos	
8.2.4.60.3	Checar compliance com o protocolo FTP	
8.2.4.60.4	Proteger contra ataques de força bruta nos logins	
8.2.4.61	Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/41.html
8.2.4.61.1	A comunicação deve ser aderente a RFC 2821	
8.2.4.61.2	Limitar o número de mensagens	
8.2.4.61.3	Validar registro SPF do DNS	
8.2.4.61.4	Determinar quais métodos SMTP podem ser utilizados	
8.2.4.62	Deverá armazenar os logs localmente ou exportar para Syslog server	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-
8.2.4.63	Deverá proteger contra ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas	https://support.f5.com/csp/article/K11930
8.2.4.64	Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal	https://support.f5.com/csp/article/K64208044
8.2.4.65	A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, ataques DoS, ataques de força bruta, ataques de robôs, violações, URL, endereços IP, países, severidade e PCI Compliance	https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/13.html
8.2.4.66	Deverá permitir o agendamento de relatórios a serem entregues por email	https://techdocs.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-1-0/3.html
8.2.4.67	Fornecer os seguintes Gráficos de alertas por:	
8.2.4.67.1	Política de segurança	
8.2.4.67.2	Tipos de ataques	
8.2.4.67.3	Violações	
8.2.4.67.4	URL	
8.2.4.67.5	Endereços IP	
8.2.4.67.6	Países	
8.2.4.67.7	Severidade	
8.2.4.67.8	Código de resposta	
8.2.4.67.9	Métodos	

8.2.4.67.10	Protocolos	
8.2.4.67.11	Vírus	
8.2.4.67.12	Usuário	
8.2.4.67.13	Sessão	
8.2.4.68	Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental	https://www.f5.com/pdf/products/F5_advanced_WAF_overview.pdf
8.2.4.69	A solução deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação	
8.2.4.70	Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação	
8.2.5	Proteção avançada de web application firewall e Anti-bot para mobile SDK	
8.2.5.1	Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS	
8.2.5.2	Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação	
8.2.5.3	Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque	
8.2.5.4	Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário	
8.2.5.5	Deve proteger esses dados criptografados de malwares e keyloggers	
8.2.5.6	Deve possuir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning	
8.2.5.7	Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las	
8.2.5.8	Deve ajudar a prevenir contra ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web	
8.2.5.9	Proteger contra ataques automatizados direcionados a aplicações móveis disponibilizadas tanto na App Store quanto Google Play	
8.2.5.10	Proteger API Mobile contra ataques do tipo: Content scraping, Denial of service e API ataques	
8.2.5.11	Prover proteção robusta contra robôs para aplicações móveis para proteger contra: Scanners de vulnerabilidade, robôs e outros vetores de ataques automatizados	
8.2.5.12	A solução de proteção de apps móveis deve ser capaz de distinguir o tráfego proveniente de um app legítimo de demais scripts automatizados ou apps não certificados	
8.2.5.13	Deve ser possível mesclar o código da aplicação ao software SDK que irá proteger a aplicação móvel de forma simples	
8.2.5.14	Solução de segurança para a proteção de aplicativos móveis, contra ataques de bots e ataques automatizados, que obedecem às seguintes características:	
8.2.5.15	A solução deve ter um SDK para o processo de fusão com os binários.apk e .ipa dos aplicativos móveis	
8.2.5.16	A solução deve ter uma plataforma sem código para executar o processo de fusão com o aplicativo automaticamente, incluindo a assinatura dos Aplicativos, e enviá-lo nos repositórios públicos da App Store como um aplicativo confiável	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-implementations-14-1-0/working-with-the-anti-bot-mobile-applic
8.2.5.17	Capacidade de detecção de bots e ataques automatizados destinados a aplicativos móveis expostos aos clientes	
8.2.5.18	A solução deve suportar análise comportamental e impressão digital para garantir que a transação seja feita por um ser humano	
8.2.5.19	Dentro do processo de fusão, as seguintes funcionalidades de devem ser suportadas:	
8.2.5.19.1	Ofuscação	
8.2.5.19.2	Proteção contra adulterações	
8.2.5.19.3	Validação Checksum	
8.2.5.19.4	Verificação de integridade do aplicativo	
8.2.5.19.5	Anti-reversão	
8.2.5.20	Suportar a detecção de dispositivos comprometidos através de Jailbroken ou Rooted com a capacidade de permitir ou bloquear o acesso destes para a aplicação	
8.2.5.21	A solução deve suportar a detecção Man-in-the-middle	
8.2.5.22	A solução deve ter a capacidade de registrar eventos que incluam informações sobre a solicitação, ação realizada, nome do aplicativo, versão ou se o dispositivo sofreu Jailbroken ou acesso Root	
8.2.5.23	A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas:	
8.2.5.23.1	Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF)	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/changing-security-policy-settings.html#GUID-E3
8.2.5.23.2	Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy	https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf

8.2.6	Características de controle de acesso remoto e VPN SSL	
8.2.6.1	Deverá implementar as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.1.1	Deve possuir o modo “Túnel por aplicação” onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.1.2	Deve possuir o modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.1.3	Deve possuir o modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.1.4	Deve possuir suporte a split tunneling	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.1.5	Deve possuir suporte à compressão HTTP	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.1.6	Deve permitir estabelecimento de conexão segura de acesso remoto sem a necessidade de instalação de um software cliente na máquina do usuário	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-portal-access/overview-of-portal-access.html#
8.2.6.1.7	Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento D-TLS (Datagram TLS)	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-secure-web-gateway-13-0-0/4.html
8.2.6.1.8	Deve permitir possibilidade de compressão de dados antes de sua criptografia	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.1.9	Deve possibilitar utilização de área de trabalho protegida, onde os arquivos de trabalho devem ser criptografados e, ao fim de cada sessão, removidos automaticamente para garantir o máximo nível de segurança	https://support.f5.com/csp/article/K93235017
8.2.6.1.10	Deve possibilitar a customização da interface gráfica da página de Login e mensagens de apresentação ao usuário	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-access-policy-manager-customization-14-0-0/customizing-the-apm-log
8.2.6.1.11	Deve oferecer acesso remoto seguro à rede inteira para qualquer aplicação baseada em IP (TCP ou UDP)	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.2	Suporte a Single-Sign-On (SSO), com os seguintes recursos:	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.2.1	Deverá ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.2.2	Deve ser capaz de realizar single-sign-on utilizando kerberos	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.2.3	O equipamento deverá ser capaz de fazer cache das credenciais do usuário e utilizar a credencial correta para cada sistema	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.2.4	O equipamento deverá ser capaz de implementar SSO mesmo quando conectado via modo “Network”, quando o usuário chama o portal digitando o site diretamente no browser (sem clicar pelo portal)	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/28.html
8.2.6.3	Deverá implementar suporte a validação da estação do usuário para, no mínimo, os seguintes recursos:	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.3.1	Versão do Sistema Operacional	
8.2.6.3.2	Firewall ativado	
8.2.6.3.3	Antivírus instalado	
8.2.6.3.4	Antivírus atualizado	
8.2.6.3.5	Processos em execução	
8.2.6.3.6	Certificados digitais instalados na máquina	
8.2.6.3.7	Deverá ser possível configurar uma ação dependendo da validação da estação do usuário	
8.2.6.3.8	A configuração dessas ações deverá ser através de interface gráfica	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-visual-policy-editor/visual-policy-editor.html#G
8.2.6.4	Deverá permitir conferência do endereço IP quanto à origem geográfica, permitindo a criação de regras de acesso de acordo com o país ou estado de origem. A base de dados de endereços IP deverá estar presente no equipamento, e deverá ser atualizada periodicamente pelo fabricante da solução sem custo adicional	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.5	Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.6	Deverá ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Directory	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-authentication-methods.html
8.2.6.7	A solução deverá suportar a utilização de cliente stand-alone, e cliente deverá ser capaz de fazer Roaming inteligente, onde a mudança de endereço IP não implica na re-autenticação manual do usuário	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-client-configuration-13-1-0/2.html
8.2.6.8	Deve possuir capacidade para definir diversos métodos para acesso remoto	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.9	Deve possuir capacidade para suportar múltiplos navegadores	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-clientcompatmatrix-16-0-0.html
8.2.6.10	Deve possuir capacidade para definir autenticação e autorização web dos usuários para acesso ao virtual server (access sessions)	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.11	Deve possuir capacidade para definir perfis de acesso à rede através de wizard	https://support.f5.com/csp/article/K21215234
8.2.6.12	Deve possuir capacidade para definir o tempo de inatividade antes de encerrar a sessão do usuário	https://support.f5.com/csp/article/K12300
8.2.6.13	Deve possuir capacidade para definir o tempo máximo de conexão para sessão do usuário	https://support.f5.com/csp/article/K12300

8.2.6.14	Deve possuir capacidade para definir a quantidade máxima de usuários por servidor virtual	https://support.f5.com/csp/article/K23402746
8.2.6.15	Deve possuir capacidade para definir a quantidade máxima de sessões por usuário	https://support.f5.com/csp/article/K23402746
8.2.6.16	Deve possuir capacidade para definir os recursos de DNS, WIN e NTP	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-portal-access/configuring-access-profiles-for-p
8.2.6.17	Deve possuir capacidade para definir os recursos de AAA	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.18	Deve possuir capacidade para realizar múltiplos métodos de autenticação remotos [RADIUS | LDAP | ACTIVE DIRECTORY | SECUREID | HTTP | TACACS+ | KERBEROS]	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/1.html
8.2.6.19	Deve possuir capacidade para finalizar a sessão do usuário com base em número X de tentativa com erro	https://support.f5.com/csp/article/K18650749https://support.f5.com/csp/article/K13315545
8.2.6.20	Deve possuir capacidade para permitir a troca da senha dos usuários que tenham expirado	https://support.f5.com/csp/article/K16806
8.2.6.21	Deve possuir capacidade para definir lease pool que contenha endereços IP a serem designados aos usuários com acesso a rede (endereço do cliente PPP)	https://support.f5.com/csp/article/K63118490
8.2.6.22	Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL padrão	https://support.f5.com/csp/article/K14783
8.2.6.23	Deve possuir capacidade de redirecionar tráfego HTTP para HTTPs para um determinado servidor virtual	https://support.f5.com/csp/article/K26312346
8.2.6.24	Deve possuir capacidade para realizar compressão GZIP para tráfego VPN	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.25	Deve possuir capacidade para definir que todo tráfego seja tunelado	https://support.f5.com/csp/article/K62501251
8.2.6.26	Deve possuir capacidade para definir ACLs estáticas e dinâmicas	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-implementations/configuring-dynamic-acls.htm
8.2.6.27	Deve possuir capacidade para definir segmentação do tráfego tunelado baseado em lista de endereços IP/máscara	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-network-access-13-0-0/1.html#guid-831e
8.2.6.28	Deve possuir capacidade para definir mapeamento de drivers para clientes Windows	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-access-policy-manager-network-access-14-0-0/configuring-network-ac
8.2.6.29	Deve possuir capacidade para iniciar automaticamente uma aplicação no cliente quando o túnel for estabelecido	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-access-policy-manager-network-access-14-0-0/configuring-network-ac
8.2.6.30	Deve possuir capacidade para definir perfil de acesso ao portal através do wizard	https://support.f5.com/csp/article/K21215234
8.2.6.31	Deve possuir capacidade para realizar proxy reverso com a finalidade de "ofuscar" a URL promovendo assim o acesso seguro às aplicações web internas	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-12-1-0/17.html
8.2.6.32	Deve possuir capacidade para personalizar as páginas de login/logout para determinados usuários e grupos de usuários	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-access-policy-manager-customization-14-0-0/personalizing-access-pro
8.2.6.33	Deve possuir capacidade para realizar Single Sign On (SSO) [NTLM v1 & v2 | BASIC | HTTP FORMS BASED | KERBEROS | OAM]	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-single-sign-on-concepts-configuration/single-si
8.2.6.34	Deve possuir capacidade para mapear qualquer variável da sessão para o SSO da sessão do usuário (Credential Mapping)	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.35	Deve possuir capacidade para personalizar a página de SSO	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-customization/configuring-settings-in-basic-cus
8.2.6.36	Deve possuir capacidade para exibir múltiplas páginas de SSO baseadas em recursos individuais ou de grupo	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-single-sign-on-11-5-0/25.h
8.2.6.37	Deve possuir capacidade para descobrir dentro do web browser do usuário qual idioma designado	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-customization/customization-basics.html
8.2.6.38	Deve possuir capacidade para, graficamente, criar e manter as políticas de acesso como diagrama de fluxo (Visual Policy Editor)	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor.html
8.2.6.39	Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes de conceder acesso [ANTI-VIRUS | FIREWALL | FILE/PROCESS | REGISTRY ENTRY | MACHINE CERTIFICATE]	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.40	Deve possuir capacidade para realizar verificações e validações no servidor antes de conceder acesso [OS DETECTION | GEOLOCATION IP | CLIENT APPLICATION]	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.41	Deve possuir capacidade para conceder acesso a usuários autorizados os recursos específicos ou grupo de recursos	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.42	Deve possuir capacidade para definir bookmark para páginas web externas (Webtop Links)	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-application-access/configuring-webtops-2.html

8.2.6.43	Deve possuir capacidade para prover cliente RDP baseado em Browser para acesso RDP ou Windows Terminal Servers para clientes Microsoft Windows	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.44	Deve possuir capacidade para criar Application Tunnels, que permitirão acesso às aplicações internas	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-application-access/configuring-app-tunnel-acce
8.2.6.45	Deve possuir capacidade para utilizar compressão nas aplicações pré-determinadas	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-application-access/configuring-app-tunnel-acce
8.2.6.46	Deve possuir capacidade para iniciar automaticamente uma aplicação no cliente no momento do estabelecimento do túnel	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-access-policy-manager-network-access-14-0-0/configuring-network-ac
8.2.6.47	Deve possuir capacidade para atribuir a qualquer aplicação com front-end web autenticação e autorização de usuários sem alteração do código da aplicação	https://www.f5.com/pdf/products/access-policy-manager-apm-overview.pdf
8.2.6.48	Deve possuir capacidade para definir web perfil de acesso a aplicação através de wizard	https://support.f5.com/csp/article/K21215234
8.2.6.49	Possibilitar utilização de encapsulamento D-TLS (Datagram TLS)	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.50	Deverá prover acesso remoto através de VPN SSL para Microsoft Windows, Linux, dispositivos baseados em Android e iOS e MAC OSX	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-clientcompatmatrix-16-0-0.html
8.2.6.51	Suportar autenticação de usuários em AAA	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.52	O sistema deve inspecionar se no cliente existem antivírus e firewall instalados antes de prover o acesso remoto. Essa verificação deverá ocorrer em sistemas operacionais de desktops	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.53	Com base na análise do cliente, o sistema deverá conceder dinamicamente o acesso ao usuário: se o cliente estiver adequado com as políticas de segurança poderá acessar os recursos definidos em sua autenticação, caso contrário deverá ter acesso limitado definidos pelo administrador	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-visual-policy-editor/access-policy-item-referen
8.2.6.54	O sistema deverá forçar a limpeza do cache do navegador ao término da sessão	https://support.f5.com/csp/article/K93235017
8.2.6.55	Deve suportar acesso a serviços de terminais através de:	https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf
8.2.6.55.1	Citrix XenApp	
8.2.6.55.2	Citrix XenDesktop	
8.2.6.55.3	Microsoft RDP	
8.2.6.55.4	Java RDP	
8.2.6.55.5	VMware Horizon View	
8.2.7	Características gerais e de acesso a gerência	
8.2.7.1	Suportar e garantir a instalação em ambiente de alta disponibilidade	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-12-1-0/4.html
8.2.7.2	Assegurar que o equipamento deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento da mesma marca e modelo	https://support.f5.com/csp/article/K8665
8.2.7.3	Fornecer uma solução que opere no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-device-service-clustering-administration-14-1-0/creating-an-active-act
8.2.7.4	Assegurar que a operação da solução de 2 ou mais equipamentos, quando implementada em ambiente redundante, suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-device-service-clustering-administration-14-1-0/creating-an-active-act
8.2.7.5	Fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais	https://support.f5.com/csp/article/K8665
8.2.7.6	A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes	https://support.f5.com/csp/article/K8665
8.2.7.7	Fornecer recurso de agregação de portas baseado no protocolo LACP	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-0-0/3.html
8.2.7.8	Deve possuir suporte a LACP em modo passivo e ativo	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-0-0/3.html
8.2.7.9	Fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-0-0/3.html
8.2.7.10	Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s)	https://support.f5.com/csp/article/K9796
8.2.7.11	Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-tmos-routing-administration-14-0-0/03.h
8.2.7.12	Possuir suporte a IPv6	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-13-1-0/26.html#guid-9a7
8.2.7.13	A solução deve suportar múltiplas tabelas de rotas independentes	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-11-6-0/8.html
8.2.7.14	O equipamento, quando habilitado para mais de uma função (SLB, GSLB, Aceleração Web, etc), deverá permitir a definição da importância da função, determinando quanta CPU e memória será alocada para cada tipo de funcionalidade	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-essentials-11-6-0/7.html
8.2.7.15	~~Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, Aceleração~~ Web, etc	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-essentials-11-6-0/7.html
8.2.7.16	A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-essentials-11-6-0/7.html
8.2.7.17	Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas	https://support.f5.com/csp/article/K44841551https://ihealth.f5.com
8.2.7.18	Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network)	https://www.f5.com/services/resources/white-papers/vxlan-and-the-big-ip-platform
8.2.7.20	Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento	https://support.f5.com/csp/article/K15040
8.2.7.21	Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol)	https://support.f5.com/csp/article/K3122
8.2.7.22	Permitir acesso in-band via SSH	https://support.f5.com/csp/article/K17333

8.2.7.23	Manter internamente múltiplos arquivos de configurações do sistema	https://support.f5.com/csp/article/K4423
8.2.7.24	Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional	https://support.f5.com/csp/article/K175
8.2.7.25	Possuir auto-complementação de comandos na CLI	https://clouddocs.f5.com/cli/tmsh-reference/v13/general/tmsh.html
8.2.7.26	Possuir ajuda contextual	https://clouddocs.f5.com/cli/tmsh-reference/v13/general/tmsh.html
8.2.7.27	Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos	https://clouddocs.f5.com/cli/tmsh-reference/v13/general/tmsh.html
8.2.7.28	Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-user-account-administration-12-0-0/4.htm
8.2.7.29	Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-13-0-0/10.html
8.2.7.32	A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfix sem o uso da linha de comando	https://support.f5.com/csp/article/K34745165
8.2.7.33	A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot	https://support.f5.com/csp/article/K34745165
8.2.7.34	Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps)	https://support.f5.com/csp/article/K15235
8.2.7.35	Suportar a rollback de configuração e imagem	https://support.f5.com/csp/article/K34745165
8.2.7.36	Possuir e fornecer MIBs compiláveis na plataforma HP Open View Network Node Manager	https://www.f5.com/pdf/white-papers/managing-big-ip-hp-microsoft-wp.pdf
8.2.7.37	Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema	https://support.f5.com/csp/article/K13080
8.2.7.38	Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog	https://support.f5.com/csp/article/K13080
8.2.7.39	Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-
8.2.7.40	A interface Gráfica deverá permitir a reinicialização do equipamento	https://support.f5.com/csp/article/K7369
8.2.7.41	Reinicialização do equipamento por comando na CLI	https://support.f5.com/csp/article/K7369
8.2.7.42	Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-
8.2.7.44	Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-
8.2.7.45	Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-
8.2.7.46	Implementar Debugging: CLI via console e SS	https://support.f5.com/csp/article/K97244114
8.2.7.47	Deve possuir suporte a Link Layer Discovery Protocol (LLDP)	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-13-0-0/5.html
8.2.7.48	Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-13-0-0/5.html
8.2.7.49	A Solução deve ter a capacidade de permitir a criação de MIBs customizadas	https://support.f5.com/csp/article/K13596
8.2.7.50	A Solução deve ter suporte a sFlow	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-
8.2.8.3	Características da Solução para tráfego SSL	
8.2.8.3.1	Características de visibilidade do tráfego SSL	
8.2.8.3.1.1	Deve implementar SSL offload, ou seja, realizar a encriptação e decriptação das sessões SSL	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.2	Aceleração SSL/Troca de chaves/criptografia deverá ser feita com aceleração em hardware	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.3	Deve suportar modo Explicit Proxy	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.4	Deve suportar modo Transparent Proxy	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.5	Deve dar a opção de ações caso o certificado original do servidor expire	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.6	Deve dar a opção de ações caso o certificado original do servidor não seja confiável	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.7	Deve dar a opção de fazer o bypass do tráfego caso falhe o TLS handshake	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU

8.2.8.3.1.8	Deve suportar Dynamic Domain Bypass	https://techdocs.f5.com/kb/en-us/products/ssl-orchestrator/manuals/product/f5-herculon-ssl-orchestrator-setup-13-0-0
8.2.8.3.1.9	Deve suportar implantação em linha em Layer 2	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.10	Deve suportar implantação em linha em Layer 3	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.11	Deve suportar o envio de tráfego para dispositivos em linha em Layer 2 ou 3, conectando-se diretamente ao dispositivo de descriptografia e também através de um switch. Desacoplando o dispositivo de segurança da interface física, porta ou VLAN	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html
8.2.8.3.1.12	Deve suportar o envio de tráfego ICAP para dispositivos	https://clouddocs.f5.com/sslo-deployment-guide/chapter3/page3.4.html
8.2.8.3.1.13	Deve ser capaz de enviar tráfego para dispositivos passivos, como DLPs	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/what-is-f5-ssl-orchestrator.html#GUID-38F7B595-20C
8.2.8.3.1.14	Deve ser capaz de balancear tráfego entre dispositivos de inspeção	https://clouddocs.f5.com/sslo-deployment-guide/chapter3/page3.4.html
8.2.8.3.1.15	Deve ser capaz de enviar o tráfego original para dispositivos de inspeção	https://clouddocs.f5.com/sslo-deployment-guide/chapter3/page3.4.html
8.2.8.3.1.16	Deve ser capaz de monitorar a integridade de dispositivos por meio de sondagem (probes)	https://clouddocs.f5.com/sslo-deployment-guide/chapter3/chapter3.html
8.2.8.3.1.17	Deve ser capaz de fazer direcionamento do tráfego descriptografado baseado em políticas	https://clouddocs.f5.com/sslo-deployment-guide/chapter4/page4.3.html
8.2.8.3.1.18	Deve ser capaz de criar múltiplos Service Chains	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.19	Deve suportar mais de 10 dispositivos	https://techdocs.f5.com/kb/en-us/products/ssl-orchestrator/manuals/product/ssl-orchestrator-setup-14-0-0-4-0/02.htm
8.2.8.3.1.20	Deve ser capaz de fazer bypass da inspeção com base em categoria ou URL	https://clouddocs.f5.com/sslo-deployment-guide/chapter4/page4.3.html
8.2.8.3.1.21	Deve implementar a renegociação de sessão	https://support.f5.com/csp/article/K13512
8.2.8.3.1.22	Deve implementar geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/terminology-for-herculon-ssl-orchestrator-ct.html#GU
8.2.8.3.1.23	Deve implementar autenticação, autorização e registro das operações dos administradores através dos protocolos TACACS+ e RADIUS	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-user-account-administration-12-0-0/6.htm
8.2.8.3.1.24	Deve possuir MIB SNMP	https://support.f5.com/csp/article/K13322
8.2.8.3.1.25	Deve possuir redundância ativo/standby com sincronismo dos estados das conexões dos usuários assim como suas características de atribuição de servidores	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/setting-up-f5-ssl-orchestrator-in-a-high-availabil.html#
8.2.8.3.1.26	Deve permitir que ferramentas de segurança recebam o tráfego descriptografado da solução e tomem decisões para mitigar ataques	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.27	Deve otimizar a infraestrutura SSL, provendo visibilidade para variadas soluções de segurança sobre o tráfego SSL/TLS	https://techdocs.f5.com/kb/en-us/products/ssl-orchestrator/manuals/product/f5-herculon-ssl-orchestrator-setup-13-0-0
8.2.8.3.1.28	Deve maximizar o uso dos investimentos de segurança atuais do CONTRATANTE	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.29	Deve suportar fazer “traffic steering” para as soluções de segurança	https://techdocs.f5.com/kb/en-us/products/ssl-orchestrator/manuals/product/f5-herculon-ssl-orchestrator-setup-13-0-0
8.2.8.3.1.30	Deve possuir inteligência baseada em contextos para tratar o tráfego criptografado	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf

8.2.8.3.1.31	Deve centralizar as operações de criptografia/descriptografia, provendo a mais moderna tecnologia de encriptação SSL com grande variedade de cifras e protocolos	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.32	Deve permitir a descoberta de ameaças ocultas em transações e prevenir ataques em diferentes estágios	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.33	Deve permitir maior flexibilidade e escalabilidade de diferentes soluções de segurança	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.34	Deve ser possível distribuir carga, utilizando técnicas de balanceamento para as soluções de segurança como por exemplo Firewalls	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.35	Deve-se realizar checagem de saúde para identificar se as soluções de segurança estão funcionando sem problemas. Caso haja alguma falha em determinada solução deve ser possível fazer o by-pass e não passar o tráfego para essa solução, não prejudicando o acesso do cliente	https://clouddocs.f5.com/sslo-deployment-guide/chapter3/chapter3.html
8.2.8.3.1.36	Deve ser possível reduzir o custo administrativo com o uso de políticas inteligentes baseado em contextos, permitindo maior eficiência no envio de tráfego para as soluções relevantes e maior efetividade no uso dos diversos equipamentos de segurança	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.37	Deve utilizar métodos de classificação como por exemplo categoria, geolocalização, domínio, reputação IP, etc, para definir se o tráfego deve ser descriptografado e enviado para um serviço ou outro, ou se ainda de ser feito o by-pass desse tipo de tráfego direto para Internet	https://clouddocs.f5.com/sslo-deployment-guide/chapter4/page4.3.html
8.2.8.3.1.38	Através de políticas baseadas em contextos, deve ser possível reduzir custos administrativos, removendo o gerenciamento de chaves e certificados dos equipamentos de segurança	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.39	Deve ser possível ainda reduzir a latência de inspeção SSL atual que é realizada em diversos equipamentos de segurança, centralizando essa operação de criptografia/descriptografia num dispositivo único	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.40	Deve permitir enviar o tráfego descriptografado para análise de diversos equipamentos de segurança como por exemplo: Firewalls, DLP, antimalware, IPSs, ferramentas forenses, etc	https://techdocs.f5.com/en-us/bigip-16-1-1/ssl-orchestrator-setup/what-is-f5-ssl-orchestrator.html#GUID-38F7B595-20C
8.2.8.3.1.41	Deve suportar equipamentos de seguranças de diversos fabricantes	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.42	Deve suportar uma grande diversidade de cifras SSL	https://support.f5.com/csp/article/K86554600
8.2.8.3.1.43	Deve ser possível melhorar a utilização e disponibilidade dos equipamentos de segurança através de técnicas de balanceamento e monitoração	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.44	Deve realizar descriptografia de SSL/TLS independente da porta TCP	https://techdocs.f5.com/kb/en-us/products/ssl-orchestrator/manuals/product/ssl-orchestrator-setup-14-0-0-4-0/05.htm
8.2.8.3.1.45	Deve suportar pelo menos as seguintes cifras e protocolos: TLS 1.2, SHA2, AES-GCM, DTLS 1	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
8.2.8.3.1.46	Deve suportar ECDHE, RSA e DHE com suporte a Forward Secrecy	https://techdocs.f5.com/content/kb/en-us/products/ssl-orchestrator/manuals/product/ssl-orchestrator-architecture-14-

8.2.8.3.1.47	Deve oferecer controle a nível de Proxy nas cifras e protocolos	https://clouddocs.f5.com/sslo-deployment-guide/chapter4/page4.4.html
8.2.8.3.1.48	Deve permitir ser implementado pelo menos com dispositivos: Roteados (L3) e inline (L2), via protocolo ICAP e dispositivos que apenas recebem o tráfego, como por exemplo IDSs	https://clouddocs.f5.com/sslo-deployment-guide/chapter3/chapter3.html
8.2.8.3.1.49	Deve suportar integração com Network HSM	https://clouddocs.f5.com/sslo-deployment-guide/chapter4/page4.4.html
8.2.8.3.1.50	Deve possuir filtro de URL para classificação de tráfegos que não deverão ser descriptografados e nem inspecionados	https://www.f5.com/pdf/products/ssl-orchestrator-datasheet.pdf
.		

Florianópolis/SC, 11 de fevereiro de 2022

PREGÃO ELETRÔNICO/SRP Nº. 012/2022 – TJAM

ANEXO III – Formulário de Proposta de Preços

RAZÃO SOCIAL: IPTRUST ADVANCE TECNOLOGIA DA INFORMAÇÃO LTDA - EPP		
CNPJ: 18.753.084/0001-08	**TELEFONE(S):** 48 3333-1551 / 48 99143-0967	
E-MAIL: alessandro@iptrust.com.br | financeiro@iptrust.com.br		
ENDEREÇO: Rua Presidente Gama Rosa, nº 54 – andar 3, CEP 88036-260, Trindade, Florianópolis/SC		
BANCO: 341 - Itaú	**AGÊNCIA: 1575**	**CONTA CORRENTE: 22525-3**

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Balanceamento de Carga com Firewall de Segurança Avançada de Aplicações WEB Integrado, conforme especificações no Termo de Referência. Fabricante: F5 Networks Produtos: BIG-IP i5800 com licenciamento Best Bundle + IP Intelligence + Suporte Premium por 36 meses	Conjunto	1 conjunto de equipamentos e de licenças de software que atendam às especificações em sua integralidade (cluster)	2	R$ 4.060.000,00	R$ 8.120.000,00
2	Solução para tráfego SSL Fabricante: F5 Networks Produtos: BIG-IP SSL Orchestrator + Suporte Premium por 36 meses	Conjunto	1 conjunto de licenças de software que atendam às especificações em sua integralidade (cluster)	2	R$ 577.894,73	R$ 1.155.789,46
3	Serviços de instalação e configuração do Firewall de Segurança Avançada de Aplicações WEB solicitado no item 1	Serviços	1	2	R$ 212.000,00	R$ 424.000,00
4	Serviços de instalação e configuração para tráfego SSL solicitado no item 2	Serviços	1	2	R$ 45.000,00	R$ 90.000,00
5	Serviços de Treinamento	Serviços	2	4	R$ 76.000,00	R$ 304.000,00
6	Serviços de Consultoria e Suporte Técnico	Horas Técnicas	600 Horas	2	R$ 348.000,00	R$ 696.000,00
					Valor Total	**R$ 10.789.789,46**
Valor Total por extenso: Dez milhões, setecentos e oitenta e nove mil, setecentos e oitenta e nove reais e quarenta e seis centavos.						

Observações:

a) Validade da proposta: 60 (sessenta) dias.
b) Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Florianópolis, 11 de fevereiro de 2022.

ipTrust Advance Tecnologia da Informação Ltda – EPP
Alessandro Kern Fernandes
Sócio-Administrador
CPF: 656.202.910-49

18.753.084/0001-08
IPTRUST ADVANCE TECNOLOGIA
DA INFORMAÇÃO LTDA - ME
Rua Presidente Gama Rosa nº 54 Andar 3
Trindade - CEP 88.036-260
Florianópolis – SC

DATA SHEET

Pregão Eletrônico/SRP: 012/2022 TJAM

Licitante: ipTrust Advance Tecnologia da Informação Ltda - EPP
CNPJ: 18.753.084/0001-0
Lote Único
Item 2

F5 SSL Orchestrator

WHAT'S INSIDE

Keys to Encrypted Threat Protection: Visibility into and Orchestration of Encrypted Traffic

The ever-increasing volume of encrypted traffic is hampering the ability of IT and security operations (SecOps) teams to protect their applications, customer data, and intellectual property. Traditional security gateways, network firewalls–even next-generation firewalls (NGFWs)–and intrusion prevention systems (IPS) are increasingly running blind to SSL/TLS traffic. Attackers commonly hide threats within links to encrypted websites or encrypted payload attachments in phishing and spear phishing attacks, and they use encrypted channels to evade detection during data exfiltration and command-and-control (C2) communications.

They will select specific cipher primitives based on known security product gaps to force bypass of encrypted malicious traffic. The growth in SSL/TLS encryption is a challenge for enterprises, because without security tools able to inspect inbound and outbound SSL/TLS traffic efficiently at scale, encrypted attacks go undetected and expose your applications and data to breaches.

Visibility into and inspection of SSL/TLS traffic only scratches the security surface, though. Most organizations lack the ability to centrally control and implement decryption policies across the multiple existing and deployed security inspection devices commonly found in an organization's security stack. Many organizations resort to daisy-chaining devices or tedious, manual configurations to support inspection across the security stack–increasing latency, complexity, and risk.

F5® SSL Orchestrator® is designed and purpose-built to enhance SSL/TLS infrastructure, provide security solutions with visibility into SSL/TLS encrypted traffic, and optimize and maximize your existing security investments. SSL Orchestrator delivers dynamic service chaining and policy-based traffic steering, applying context-based intelligence to encrypted traffic handling to allow you to intelligently manage the flow of encrypted traffic across your entire security stack, ensuring optimal availability. Designed to easily integrate with

existing architectures and to centrally manage the SSL/TLS decrypt/re-encrypt function, F5 SSL Orchestrator delivers the latest SSL encryption technologies across your entire security infrastructure. With SSL Orchestrator's high-performance encryption and decryption capabilities, your organization can quickly discover hidden threats and prevent attacks at multiple stages, leveraging your existing security solutions.

SSL Orchestrator ensures encrypted traffic can be decrypted, inspected by security controls, then re-encrypted—delivering enhanced visibility to mitigate threats traversing the network. As a result, you can maximize your security services investment for malware, data loss prevention (DLP), ransomware, and next-generation firewalls (NGFW), thereby preventing inbound and outbound threats, including exploitation, callback, and data exfiltration.

KEY BENEFITS

Enables visibility into SSL/TLS traffic with centralized decryption/encryption function for inspection across multiple security tools.

Provides high-performance decryption of inbound and outbound encrypted traffic, enabling security inspection to expose threats with greater efficiency and stop attacks such as phishing, spear phishing, and ransomware.

Dynamically chains security devices, independently monitors and scales them, and intelligently manages decryption across the entire security chain via a contextual classification engine, reducing administrative costs while utilizing security resources more efficiently.

Delivers a single platform for unified inspection of next-generation encryption protocols, providing unparalleled flexibility, minimizing architectural changes, and preventing new security blind spots.

Shortens the typically cumbersome, time-consuming and costly change management process by orchestrating the security stack, simplifying equipment changes, and mitigating their detrimental impact.

Flexibly integrates into even the most complex architectures, centralizing SSL decrypt/encrypt functions and delivering the latest encryption technologies across the entire security infrastructure.

Scales security services with high availability, leveraging F5's best-in-class load balancing, health monitoring, and SSL offload capabilities.

Figure 1: F5 SSL Orchestrator maximizes efficiency and performance for a wide range of inspection devices while maintaining optimal security.

CENTRALIZE SSL DECRYPTION ACROSS MULTIPLE SECURITY TOOLS

F5 SSL Orchestrator provides decryption and re-encryption of user traffic bound to the internet and web-based applications, enhancing security inspection. The solution supports policy-based management and steering of traffic flows to third-party security devices such as firewalls, IPSs, anti-malware, DLPs, secure web gateways (HTTP proxy services), and forensics tools. Centralizing the SSL/TLS decrypt/encrypt function enables you to realize the full value of your security investments. Our multi-vendor ecosystem approach simplifies and strengthens the inspection of all inbound and outbound encrypted traffic malware and exfiltration.

INSPECT NEXT-GENERATION ENCRYPTION PROTOCOLS

Next-generation encryption protocols are evolving with industry best practices for increased security and privacy. New emerging standards encourage rapid adoption of SSL forward secrecy for improved network security. The transition to next-generation encryption breaks passive SSL devices, bypassing your security controls and putting you, your network, your apps, and your data at risk. The diverse cipher support of F5 SSL Orchestrator prevents new blind spots by enabling greater flexibility without requiring architectural changes.

SIMPLIFY CHANGE MANAGEMENT THROUGH SECURITY STACK ORCHESTRATION

Making necessary equipment changes or swaps in daisy-chained security stacks are difficult and time-consuming. Changes or swaps increase operational and business costs, cause delays, and can create unintended encrypted traffic bypasses, expanding risks and the threat threshold for your applications and data. Security stack orchestration with F5 SSL Orchestrator simplifies equipment changes, lessens change time, cost, and impact, and alleviates prospective traffic bypass and potential exploitation.

IMPROVE SCALABILITY AND AVAILABILITY OF YOUR EXISTING SECURITY TOOLS

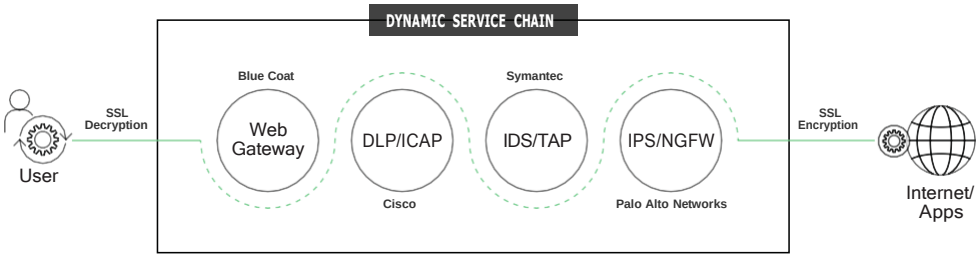
Enterprises with substantial traffic loads will optimize security deployments by leveraging the health monitoring, load-balancing, and SSL offload capabilities of F5 SSL Orchestrator. These capabilities enable your security investments to better scale and protect through multi-layered security, even in the most demanding environments. Scaling your existing, deployed security devices with failover protection achieves better utilization and service availability.

F5 SSL Orchestrator's high-availability design addresses synchronization delays caused by heavy loads and memory constraints, resulting in a reliable and low-latency auto-failover configuration. Additionally, enterprises can configure high-availability devices to synchronize automatically and incrementally.

CONFIGURE DYNAMIC SERVICE CHAINING BASED ON CONTEXT

SSL Orchestrator dynamically chains security services, including anti-virus/anti-malware products, intrusion detection systems (IDS), IPSs, NGFWs, secure web gateways (HTTP proxy services), and DLPs. It leverages classification metrics such as domain name, content category, geolocation, IP reputation, and other policies that determine whether to decrypt traffic and which services traffic should be sent to. The policy-based traffic steering capabilities of SSL Orchestrator also increase administrative efficiency and reduce administrative cost by removing key and certificate management from your security infrastructure.

Figure 2: SSL Orchestrator enables the creation of dynamic security service chains.



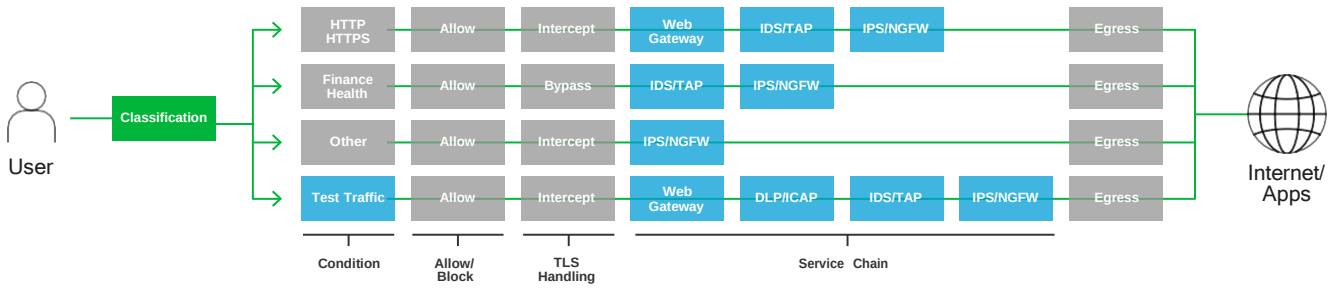


Figure 3: Leveraging its context-aware policy engine, SSL Orchestrator steers decrypted traffic to the appropriate security service chain and can perform an intelligent bypass on sensitive user traffic, such as financial or health-care related traffic.

DEPLOY WITH FLEXIBLE OPTIONS THAT EASE INTEGRATION

SSL Orchestrator supports multiple deployment modes, easily integrating into even the most complex of architectures. This centralizes SSL/TLS decrypt/re-encrypt services and delivers the latest encryption technologies across your entire security infrastructure. It eliminates your organization's need to re-architect the network to enable visibility into encrypted traffic, orchestrating and effectively routing traffic to the appropriate security services—in addition to dynamically chaining the appropriate security services. That helps to better utilize, preserve, and future-proof your security solution investments. In addition, SSL Orchestrator includes a step-by-step Guided Configuration to help your IT or SecOps teams logically walk through the deployment within your existing architecture and with your existing security solutions. The Guided Configuration simplifies deployment of SSL Orchestrator and enables you and your organization to be better protected, sooner, against the onslaught of encrypted threats.

INTEGRATE F5 SECURITY SOLUTIONS INTO YOUR SERVICE CHAIN

Use your F5 Secure Web Gateway (SWG) subscription within your SSL Orchestrator dynamic service chain for traffic classification and URL-based content filtering for outbound traffic. With F5 SWG, you can configure security policies to block or accept traffic based on over 150 granular URL categories intelligently classified by F5 SWG. F5 SWG processes traffic packets using powerful malware analytics tools, so you can detect patterns that indicate complex attack vectors and block the traffic from traversing your network.

PARTNERS

F5 has developed—and continues to develop—an ever-expanding security solution ecosystem for SSL Orchestrator. While SSL Orchestrator is vendor and product agnostic, F5 has optimized integration solutions for leading tools from partners such as Cisco, FireEye, Palo Alto Networks, and others.

The following Recommended Practices Guides, with reference architectures, provide granular, prescriptive guidance for deployment:

- Broadcom Symantec Data Loss Prevention (DLP)
- Cisco Firepower Threat Defense
- Cisco Web Security Appliance (WSA)
- FireEye NX
- McAfee Data Loss Prevention (DLP)
- McAfee Web Gateway
- Menlo Security Web Isolation Platform
- Palo Alto Networks NGFW

FEATURES

F5 SSL Orchestrator enables your security team to streamline security service deployment, delivering greater agility, control, and visibility into encrypted traffic.

SSL visibility

- High performance SSL/TLS decryption/re-encryption
- Inspection of inbound and outbound encrypted traffic
- Supports L3 (routed) and L2 (transparent) modes
- Forward and reverse proxy architecture
- SSL/TLS decryption independent of TCP port

Dynamic service chaining

- Policy-based steering of decrypted traffic
- Decoupled from physical interface, port, or VLANs
- Simplified security service insertion
- Service resiliency
- Service monitoring
- Load balancing of multiple security devices

Contextual policy engine

- Source and destination IP and subnet port
- Protocol
- Domain
- IP geolocation
- IP reputation (subscription)
- URL categorization (subscription)
- Policy-based block, bypass, and forward for inspection actions

Granular control

- Header changes
- Support for port translation

Robust cipher and protocol support

- TLS 1, 1.1, 1.2, 1.3
- Forward secrecy/perfect forward secrecy encryption
- RSA/ECDSA/DHE/ECDHE
- AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA/SHA2 (SHA256/384), Chacha20-Poly1305
- Proxy-level control over ciphers and protocols

Deployment modes

- Outbound layer 3 explicit proxy
- Outbound layer 3 transparent proxy
- Inbound layer 3 reverse proxy
- Outbound layer 2
- Inbound layer 2
- High availability with TCP session resiliency

Supported service types

- HTTP proxy services (including HTTP/2 support)
- Inline layer 3 services
- Inline layer 2 services
- ICAP/DLP services
- TAP services
- F5 Secure Web Gateway Services (SWG)

Reporting and logging

- On-board analytics dashboard

Network hardware security module (HSM)

- Thales (Gemalto, SafeNet)
- Atos
- AWS CloudHSM
- Equinix SmartKey (Fortanix)
- Entrust (nCipher)

Add-ons

- IP Intelligence Services (subscription feed)
- URL filtering
- Network HSM
- F5 BIG-IP Access Policy Manager (APM)
- F5 Secure Web Gateway Services (SWG)
- DTLS 2.0 mode for delivering and securing applications
- Support for dynamic split tunneling

Specifications	i15800	i11800/i11800-DS*
Processor:	Two 14-Core Intel Xeon processors (total 56 hyperthreaded logical processor cores)	One 18-Core Intel Xeon processor (total 36 hyperthreaded logical processor cores)
Memory:	512 GB DDR4	256 GB DDR4
Hard Drive:	1x 1.6 TB Enterprise Class SSD	1x 960 GB Enterprise Class SSD (i11800) Dual SSD 2x 960 GB Enterprise Class SSD (i11800-DS)
Gigabit Ethernet CU Ports:	N/A	Optional SFP
Gigabit Fiber Ports (SFP):	N/A	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	N/A	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	8 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	6 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
100 Gigabit Fiber Ports (QSFP28)	4 SR4/LR4 (sold separately) QSFP28	N/A
SSL Orchestrator Throughput (Maximum):		
Receive Only:	22.7 Gbps	18.9 Gbps (i11800); 30.5 Gbps (i11800-DS)
L3 Inline Service:	22.9 Gbps	19.1 Gbps (i11800); 31.5 Gbps (i11800-DS)
L3 Inline + (1) L2 Service:	22.9 Gbps	17.9 Gbps (i11800); 27.1 Gbps (i11800-DS)
L3 Inline + (2) L2 Services:	22.8 Gbps	16.9 Gbps (i11800); 13.2 Gbps (i11800-DS)
For each additional L2 service:	-1.3 Gbps	-1.9 Gbps (i11800); -5.1 Gbps (i11800-DS)
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
Receive Only:	41.8 K	24.7 K (i11800); 31.7 K (i11800-DS)
L3 Inline Service:	41.2 K	25.0 K (i11800); 30.9 K (i11800-DS)
L3 Inline + (1) L2 Service:	37.3 K	24.0 K (i11800); 27.2 K (i11800-DS)
L3 Inline + (2) L2 Services:	34.3 K	23.2 K (i11800); 24.5 K (i11800-DS)
For each additional L2 service:	-2.9 K	-2.9 K (i11800); -2.5 K (i11800-DS)
L3 Inbound Topology:		
Receive Only:	76.7 K	45.8 K (i11800); 57.5 K (i11800-DS)
L3 Inline Service:	74.0 K	45.5 K (i11800); 56.4 K (i11800-DS)
L3 Inline + (1) L2 Service:	65.4 K	45.2 K (i11800); 47.4 K (i11800-DS)
L3 Inline + (2) L2 Services:	57.8 K	39.4 K (i11800); 41.0 K (i11800-DS)
For each additional L2 service:	-7.0 K	-3.6 K (i11800); -5.9 K (i11800-DS)
SSL Orchestrator Concurrent Sessions:		
L3 Outbound	5500 K (5.5 M)	3100 K (3.1 M)
L3 Inbound	6200 K (6.2 M)	3400 K (3.4 M)

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System data sheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. Please refer to the Platform Guide: i15000 Series or Platform Guide: i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

*More information on additional dedicated cryptographic hardware on the DS Series is available in the BIG-IP System data sheet, which also provides complete specifications on all BIG-IP iSeries platforms.

Specifications	i10800	i7800
Processor:	One 8-core Intel Xeon processor (total 16 hyperthreaded logical processor cores)	One 6-core Intel Xeon processor (total 12 hyperthreaded logical processor cores)
Memory:	128 GB DDR4	96 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD Model with dual SSDs in RAID 1 also available	1x 480 GB Enterprise Class SSD Model with Dual SSDs in RAID 1 also available
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	6 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10 GB ports)	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
SSL Orchestrator Throughput (Maximum):		
Receive Only:	18.2 Gbps	10.9 Gbps
L3 Inline Service:	19.0 Gbps	11.1 Gbps
L3 Inline + (1) L2 Service:	16.2 Gbps	11.0 Gbps
L3 Inline + (2) L2 Services:	13.2 Gbps	9.1 Gbps
For each additional L2 service:	-2.2 Gbps	-1.3 Gbps
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
Receive Only:	17.0 K	12.1 K
L3 Inline Service:	16.7 K	13.0 K
L3 Inline + (1) L2 Service:	15.0 K	12.3 K
L3 Inline + (2) L2 Services:	13.6 K	11.1 K
For each additional L2 service:	-1.3 K	-0.9 K
L3 Inbound Topology:		
Receive Only:	36.1 K	23.0 K
L3 Inline Service:	35.2 K	23.0 K
L3 Inline + (1) L2 Service:	28.5 K	22.6 K
L3 Inline + (2) L2 Services:	24.3 K	19.7 K
For each additional L2 service:	-4.1 K	-2.0 K
SSL Orchestrator Concurrent Sessions:		
L3 Outbound	1400 K (1.4 M)	1000 K (1.0 M)
L3 Inbound	1600 K (1.6 M)	1200 K (1.2 M)

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System data sheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. SFP+ ports in i10800 are compatible with F5 SFP modules. Please refer to the Platform Guide for i5000/i7000/ i10000/i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

Specifications	i5800	i4800
Processor:	One 4-core Intel Xeon processor (total 8 hyperthreaded logical processing cores)	One 4-core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
Memory:	48 GB DDR4	32 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD	1x 500 GB Enterprise Class HDD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	8 SX or LX (sold separately)
10 Gigabit Fiber Ports (SFP+):	8 SR or LR (sold separately); optional 10G copper direct attach	4 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	N/A
SSL Orchestrator Throughput (Maximum):		
Receive Only:	10.1 Gbps	6.2 Gbps
L3 Inline Service:	10.7 Gbps	6.4 Gbps
L3 Inline + (1) L2 Service:	9.1 Gbps	5.9 Gbps
L3 Inline + (2) L2 Services:	7.6 Gbps	4.7 Gbps
For each additional L2 service:	-1.3 Gbps	-0.8 Gbps
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
Receive Only:	9.3 K	5.8 K
L3 Inline Service:	9.2 K	5.7 K
L3 Inline + (1) L2 Service:	8.2 K	4.7 K
L3 Inline + (2) L2 Services:	7.5 K	4.6 K
For each additional L2 service:	-0.8 K	-0.5 K
L3 Inbound Topology:		
Receive Only:	19.4 K	12.3 K
L3 Inline Service:	18.9 K	12.2 K
L3 Inline + (1) L2 Service:	15.4 K	8.3 K
L3 Inline + (2) L2 Services:	13.1 K	8.4 K
For each additional L2 service:	-2.3 K	-1.5 K
SSL Orchestrator Concurrent Sessions:		
L3 Outbound	500 K	300 K
L3 Inbound	610 K	375 K

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System data sheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. Please refer to the Platform Guide for i5000/i7000/i10000/i11000 Series or Platform Guide for i2000/i4000 for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

Specifications	i2800*
Processor:	One 2-core Intel Xeon processor (total 4 hyperthreaded logical processor cores)
Memory:	16 GB DDR4
Hard Drive:	1x 500 GB Enterprise Class HDD
Gigabit Ethernet CU Ports:	Optional SFP
Gigabit Fiber Ports (SFP):	4 SX or LX (sold separately)
10 Gigabit Fiber Ports (SFP+):	2 SR or LR (sold separately); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	N/A
SSL Orchestrator Throughput:	2.8 Gbps
SSL Orchestrator Transactions/ Second (TPS):	3800
SSL Orchestrator Concurrent Sessions:	150 K

*Supports a maximum of one additional service.

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System data sheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. Please refer to the Platform Guide for i2000/i4000 for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

Specifications	VIPRION 4450 Blade on VPR-4800 Chassis	VIPRION 2250 Blade on VPR-2400 Chassis
SSL Orchestrator Throughput: *		
With 1 blade:		
L3 inline service	44.5 Gbps	15.6 Gbps
L3 Inline + (1) L2 Service:	41 Gbps	13.3 Gbps
L3 Inline + (2) L2 Service:	33.5 Gbps	10.7 Gbps
For each additional L2 service:	- 5.1 Gbps	-1.9 Gbps
With 2 blades		
L3 inline service	74.5 Gbps	32 Gbps
L3 Inline + (1) L2 Service:	71.5 Gbps	24.5 Gbps
L3 Inline + (2) L2 Services:	59.5 Gbps	20 Gbps
For each additional L2 service:	-9.3 Gbps	-4.6 Gbps
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
With 1 blade:		
L3 inline service:	33.5K	10K
L3 Inline + (1) L2 Service:	30.1K	9.2K

Specifications	VIPRION 4450 Blade on VPR-4800 Chassis	VIPRION 2250 Blade on VPR-2400 Chassis
L3 Inline + (2) L2 Services:	27.6K	8.5K
For each additional L2 service	-2.4K	-0.7K
With 2 blades:		
L3 inline service:	51.2K	18.3K
L3 Inline + (1) L2 Service:	47.5K	16.6K
L3 Inline + (2) L2 Services:	44.6K	15.5K
For each additional L2 service:	-2.9K	-1.2K
L3 Inbound Topology:		
With 1 blade:		
L3 inline service:	64.6K	20.1K
L3 Inline + (1) L2 Service:	54.6K	17.3K
L3 Inline + (2) L2 Services:	47.5K	15K
For each additional L2 service	-6.8K	-2.0K
With 2 blades:		
L3 inline service:	79K	36.6K
L3 Inline + (1) L2 Service:	73.1K	30.7K
L3 Inline + (2) L2 Service:	66.6K	27K
For each additional L2 service:	-5.9K	-3.8K

*Throughput will increase at approximately 60% for each additional (non-vCMP) blade.

For complete specifications on all the VIPRION platforms, please refer to the VIPRION data sheet.

Notes: L2 virtual wire mode is only supported on the VIPRION 2250 and VIPRION 4450 blades. L2 virtual wire mode is not supported in any vCMP configuration. Inline layer 2 services are not supported in the following vCMP conditions: VIPRION 2250 blade on VIPRION 2400 chassis, VIPRION 4300 blade on VIPRION 4800 chassis, and VIPRION 4450 blade on VIPRION 4480 chassis.

HIGH PERFORMANCE VIRTUAL EDITION (VE)

Specifications	8vCPU/16 GB RAM	12vCPU/24 GB RAM	16vCPU/32 GB RAM	20vCPU/40 GB RAM	24vCPU/48 GB RAM
SSL Orchestrator Throughput: *	8.7 Gbps	10.7G Gbps	12.4 Gbps	13.6 Gbps	17 Gbps
SSL Orchestrator Transactions/ Second (TPS): *	4,800	6,500	8,200	9,100	12,700
SSL Orchestrator Concurrent Sessions: *	95,000	145,000	215,000	290,000	380,000

* Performance numbers for one inline L3 service. Expected drop in throughput per additional service added is -1.5 Gbps, based on the average throughput difference between 1 and 2 services for the 8vCPU VE and the 16vCPU VE.

High Performance VE tests were run on a single dedicated host with SR-IOV enabled.

MORE INFORMATION

To learn more about F5 SSL Orchestrator or other F5 resources, visit f5.com.

Web page

F5 SSL Orchestrator

Solution overview

F5 SSL Orchestrator

Recommended practices guides

Broadcom Symantec Data Loss Prevention
Cisco Firepower Threat Defense
Cisco Web Security Appliance (WSA)
FireEye NX
McAfee Data Loss Prevention (DLP)
McAfee Web Gateway
Menlo Security Web Isolation Platform
Palo Alto Networks NGFW

DC0621 | DS-SEC-694407980