Managed Firewall Service

SERVICE DESCRIPTION

[deft]

v22.11

Service Overview

Deft's Managed Firewall Service provides customers with Deft managed physical (hardware) or virtual (software) Firewalls. This Service provides a barrier between the Deft-provided uplink to the public Internet and Customer's equipment, permitting only designated traffic to pass between the networks.

Each Managed Firewall Service is tailored to the Customer's needs. All Managed Firewall Services include configuration management, firmware patching and updates, on-site hardware sparing (for physical and virtual configurations) maintenance and support provided by Deft Deft's Service Desk and 24x7x365 monitoring by Deft systems.

Reporting and documentation are provided to Customers through Deft's Customer Portal.

The Deft Managed Firewall Service is offered in Standard and High-Availability configurations to ensure always-on protection for your network, applications, and data.

This Service is available to all Deft customers located in a Deft-managed data center utilizing services including Colocation, Managed VMware Cloud or Dedicated Servers.

Service Performance & Tiers

Deft's Managed Firewall Service offers four Performance Tiers. Within each Performance Tier, Customers may select the Firewall Services applicable for their business including Standard, Threat Prevention or DNS/URL.

Firewall Performance Tiers				**Firewall Service Tiers**		
Firewall Performance (Traffic Throughput)	**Threat Prevention Performance** (Traffic Throughput)	**VPN Performance** (Traffic Throughput)	**Maximum Number of Concurrent Sessions**	**Standar Tier** (Pro)	**Threat Prevention Tier** (IDS/IPS) (Max)	**DNS/URL Tier** (Ultra)
2Gbps	1Gbps	1Gbps	250k	X	N/A	N/A
4Gbps	2Gbps	1.8Gbps	800k	X	X	N/A
8Gbps	4Gbps	4Gbps	2M	N/A	X	X
16Gbps	8Gbps	6Gbps	10M	N/A	X	X

Support Tiers

Deft's Managed Firewall Service offers two support tiers for customers to choose from including Standard Support Services and Enhanced Support & Engineering Services.

Standard Support Services

Standard Support Services are included for all Managed Firewall Service Customers. Standard Support Services include:

- 24x7x365 System Monitoring & Error Handling
- Outage Management & Remediation
- 24x7x365 Service Desk Suport
- 1 - 4 Hours Monthly Engineering Time (Dependent Upon Performance Tier Selection)

Monthly Engineering Time

Each Managed Firewall Service Tier includes a monthly allocation for Engineering Time. The number of hours included is dependent upon the Customer's Managed Firewall Configuration, as follows:

Managed Firewall Service Monthly Engineering Time			
Standard Engineering Support	**Firewall Service Tier**		
Engineering Hours	**Standard**	**IDS/IPS**	**DNS/URL**
2GB	1	2	3
4GB	1	2	3
8GB	2	3	4
16GB	2	3	4

* Additional Engineering support is available in 4-hour blocks. Please contact your Account Executive if you have questions regarding additional Engineering support hours pricing.

Enhanced Support & Engineering Services

Enhanced Support & Engineering Services are optional, and available for all Performance Tiers as follows:

- Custom Design Services
- Proactive Capacity Management
- New Configurations, Configuration Updates, Tunnels
- Comprehensive Troubleshooting
- Tuning IDS/IPS/DNS/URL Rules
- Log Shipping to Customer

Enhanced Support & Engineering Services Tiers

Enhanced Support & Engineering Services are available in three tiers: Gold, Silver and Bronze.

Enhanced Support & Engineering Service Tiers				
Tier	**Engineering Hours Included / Month**	**Uplift Cost (Standard)**	**Uplift Cost (IDS/IPS)**	**Uplift Cost (DNS/URL)**
Bronze	4	Please contact your account executive or Deft's Sales Team for pricing information.		
Silver	10			
Gold	50			

* Additional Engineering support is available in 4-hour blocks. Please contact your Account Executive if you have questions regarding additional Engineering support hours pricing.

Day To Day Service Management

Change Management
Managed Firewall Service provides simple and efficient means to make controlled changes to Client environments. System changes are serviced by the Managed Services Team through support requests. Changes follow a well-defined approval process, and most changes can be executed quickly by Deft's Managed Services Team.

Incident Management
Managed Firewall Service includes the monitoring of the overall health of the platform and the handling of the daily activities of investigating and resolving alarms or incidents. Deft creates pre-defined playbooks that are used to rectify alarms and incidents in a way that minimizes disruption to each Client's environment.

Patch Management
Managed Firewall Service takes care of all infra- structure system patching activities to help keep resources current and secure. When updates or patches are released from infrastructure vendors, Deft applies them in a timely and consistent manner to minimize the impact on Client business.

Access Management
Managed Firewall Service enables clients to securely connect to the Service in the manner they require – be it API access, HTTPS, Cross Connects or Dedicated Physical Connectivity. Our team will make sure that the connection is maintained.

Security Management
Managed Firewall Service protects Client information assets and helps keep all Managed Firewall Service infrastructure secure. All systems are logically separated and only available to the appropriate Managed Firewall/VPN Service environment.

Continuity Management
Deft can provide redundant services as an additional option. In the event of a failure or outage that impacts the Client's business, or at their request, Deft can bring the additional Managed Firewall infrastructure online. Deft also offers comprehensive Disaster Recovery as a Service capabilities which introduces formal SLA and automation to the restore / recover processes for environments dependent upon the Managed Switch and Router Service.

Monitoring and Reporting
All Deft Managed Firewall Service environments include comprehensive Health and Performance Monitoring.

Initial Configuration & Additional Modifications

Collaborating with the Customer, Deft's Managed Service and Engineering teams will configure the baseline parameters for initial operation of the Managed Firewall Service.

The variables will include, but not necessarily be limited to:

Port Configuration

- Descriptions to match hardware for inventory purposes
- Logical setup to match network requirements

Traffic Filtering Configuration

- IP addresses and ports to open
- Network and port address translation as required
- Higher-level URL and application rulesets

VLAN Configuration

- Includes switch, local, and private VLANs
- Includes Trunked (802.1Q) connections to other destinations

IP Addressing

- Public addresses whether provided by Deft or the Customer
- Private (RFC1918) addresses

IP Routing

- Includes simple connectivity to Deft network
- Includes complex routing to Third Party
- Providers for both Public (BGP) and private (L3VPN)

Cable Management

- All physical cables associated with physical Managed Firewall Service deployments will be deployed by Deft personnel
- With prior approval, cabling may be deployed by the customer. Please note, Deft personnel will be required to enable ports

Customer Success & Service Operations

The foundation of every Deft Managed Firewall Service is collaboration. All customer success and service operations workflows have been designed to minimize response time, mitigate risk, and optimize collaboration so knowledge transfer occurs when and where necessary.

We recognize your business, and your customers, operate 24x7x365. We have designed and operate our business to be here for you, whenever and however necessary to ensure your success.

Customer Success Team

Deft provides each customer with comprehensive resources to deliver ongoing service and support for your cloud environment. From sales, solution architecture and certified engineer support on our Service Desk, to customer success and executive management sponsor- ship, you will have experts with you every step of the way.

How to Contact Deft Support

Deft uses cases to identify incidents and provide support to our clients until the incident is resolved. Case identification and review is conducted using the Deft Customer Portal. Each Deft client is supplied with accounts that are permissioned to create, update and view their cases.

Case Creation – Customer Portal

Support cases submitted to Deft are submitted using the Deft Customer Portal, accessible at https://portal.deft.com

To create a support case:

- Log into the Deft Customer Portal.
- Select "Create Case".
- You receive an automatic confirmation of the successful case creation, including the case number.
- Deft Service Desk staff review the case for accuracy, confirm the Severity Level, and send acknowledgement of case receipt to you.
- Deft Service Desk agent & Network Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Creation – Customer Portal

We recognize there may be times when a support case required the immediacy only a phone call can provide. Support cases may be created by calling the Deft Service Desk at +1 (312) 829-1111, Ext. 2. Telephone submitted support cases utilize a similar support operation, with a few modifications.

To create a support case:

- Call the Deft Service Desk at +1 (312) 829-1111, Ext. 2.
- Deft Service Desk Agent verifies caller identity, captures relevant information, creates the support case, and assigns a Severity Level.
- Deft Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Escalation Paths

Deft provides several, formal options for support case escalation. Escalations occur to set a support case to a desired Severity Level, as outlined below.

Primary Escalation Paths

This method is preferred as it is the most ecient method for raising the Severity Level of a case. To create a support case, you will:

- Log into the Deft Customer Portal.
- Navigate to the appropriate case.
- Click the "Escalate Case" link.
- Select the desired Severity Level and submit.

Alternate Case Escalation Paths

Additional Case Escalation paths are also available. However, it is import- ant to note that Alternate Case Escalation Paths will not be as expedient as the Preferred Escalation Path.

Alternate Escalation – Case Response

You may submit a response to an existing case and simply request an escalation to the desired Severity Level. The Severity Level will be raised once a Service Desk Agent has reviewed and processed the request.

Alternate Escalation – Phone Support

- You may call the Deft Service Desk at +1 (312) 829-1111, Ext. 2.
- The Deft Service Desk Agent will verify the caller's identity and the support case number. You verbally request escalation to the desired Severity Level.
- The Deft Service Desk Agent updates the case accordingly.

Service Level & Response Time

All Deft Managed Firewall Service customers can set the severity level of their support cases. The severity level you select will determine the response time. You can select the following severity levels when submitting a support case:

Severity Level	Description	Response Time SLA
Critical / Level 1	Critical Issues include business-critical system outages or issues causing extreme business impact.	15-minute response time
High / Level 2	High Severity Level issues include the impairment of production systems, impaired application performance, and moderate business impact.	30-minute response time
Normal / Level 3	Normal Severity Level issues include standard service issue requests and minimal business impact.	1-hour response time
Low / Level 4	Low Severity Level issues include general information requests, questions and guidance from Deft MSP team members, arranging prescheduled maintenance activities.	4-hour response time
Informational / Level 5	Informational Issues include general questions, how-to style requests, or reports.	24-hour response time

As standard business practice, Deft's Service Desk acknowledges all support cases within 15 minutes of case creation. The response times identified in the table above represent the average time required to remediate such issues. Please note the response time to resolution of your issue may vary based upon circumstances and configurations unique to your business and your cloud architecture. Any support cases created without a severity level selected will be set to "Level 3 – Normal" by default.

Managed Firewall Service Key Featuers & Benefits

Deft's Managed Firewall Service delivers a comprehensive set of features and benefits for today's connected organizations. This fully managed service begins by providing granular control over the traffic allowed to access your network and expands to include:

Application-based policy enforcement (App-ID™)

Access control according to application type is far more effective when application identification is based on more than just protocol and port number. The App-ID service can block high risk applications, as well as high risk behavior, such as file-sharing, and traffic encrypted with the Secure Sockets Layer (SSL) protocol can be decrypted and inspected.

User identification (User-ID™)

The User-ID feature enables configuration and enforcement of firewall policies based on users and user groups instead of or in addition to network zones and addresses. The firewall can communicate with many directory servers, such as Microsoft Active Directory, eDirectory, SunOne, OpenLDAP, and most other LDAP-based directory servers to provide user and group information to the firewall. This information is used for secure application enablement that can be defined per user or group. Granular control of certain components of an application based on users and groups can also be configured.

Threat Prevention

Threat prevention services that protect your network from viruses, worms, spyware, and other malicious traffic. These services can be varied by application and traffic source to suit the needs of your network, end-users and your business.

URL Filtering

Outbound connections can be filtered to prevent access to inappropriate web sites.

Traffic Visibility

Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Service identifies the applications with the most traffic and the highest security risk so additional decisions can be made, and actions taken.

Networking Versatility and Speed

Multigigabit speeds and a single-pass architecture enable the Service to be provided with little or no impact on network latency.

GlobalProtect™

The GlobalProtect™ capabilities provides security for client systems, such as laptops that are used in the field, by allowing easy and secure login from anywhere in the world.

Key Featuers & Benefits (cont'd)

Fail-Safe Operation

High availability (HA) support provides automatic failover in the event of any hardware or software disruption.

Malware Analysis and Reporting

The WildFire™ cloud-based analysis service provides detailed analysis and reporting on malware that passes through the firewall. Integration with the AutoFocus™ threat intelligence service enables assessment of the risk associated with your network traffic at organization, industry, and global levels.

VM-Series Firewall

A VM-Series firewall provides a virtual instance of PAN-OS® positioned for use in a virtualized data center environment and is ideal for your private, public, and hybrid cloud computing environments.

About Deft

Deft offers managed cloud services, cloud consulting, business continuity solutions, and managed data center services. We work with companies, large and small, that see IT as their critical success factor.

Deft is a SOC 2 audited company and PCI-DSS compliant. We are proud to be an 8-time Inc. 5000 Honoree.

Learn more at www.deft.com or call us at +1 (312) 829-1111.