الحكومة الذكية
mgovernment

United Arab Emirates

The Federal Electronic Network
FEDnet Service Catalog

Contents

Introduction

The purpose of this document is to outline the FEDnet program service offering to the Federal Governments Entities. In line with the broader context of UAE Smart Government initiatives and FEDnet Program capabilities, this document incorporates the FEDnet Service Catalogue and the Service Level Agreements (SLAs) associated to the Services.

Each Service Category is described and contains a list of Services on offer to Government Entities. Any Entity that is on boarded to FEDnet will automatically enroll and be covered under the Master Services Agreement and SLAs. Future Services will be added as the Service demand develops. The Telecomms Regulatory Authority will issue further revisions of this document to reflect service additions and improvements.

STRATEGIC ALIGNMENT

In coordination with the Prime Minister's Office, the UAE Smart Government has developed a national plan to guide the UAE toward further growth and prosperity by transforming into a globally recognized Smart Government. The National Plan for UAE Smart Government Goals aligns to the UAE Vision 2021, UAE National Agenda, and ICT 2021 Strategy through an ambitious roadmap of smart technology initiatives that will enable the UAE Government to achieve key goals.

Fednet As A Strategic Smart Government Initiative

The National Plan vision, mission, and strategic objectives are realized through seven identified Priority Areas that span the entire Smart Government Program requirements:

1. **Smart Infrastructure**
2. **Smart Identity**
3. **Engagement and Outreach**
4. **Governance and Policy**
5. **Human Capital**
6. **Smart Data Analytics**
7. **Smart Service Modernization**

Background to the National Plan

Active Initiative
New Initiative

Smart Infrastructure
National Network Infrastructure

Smart Identity
National Trusted Srvice Manager
National KPI Expansion
National Identity Assurance Service
Constituent Box

Engagement and Outreach
Public Awareness Campaign
Smart Community Centers
Government Online
National CRM System

Governance and Policy
Federal CIO Model
Smart Gov. Regulatory Framework
Service Modernization Criteria
Smart Service Performance Measurement
National Government EA Guidelines
National UX Guidance and Tools

Human Capital
Center of Digital Innovation

Smart Data Analytics
Smart Analytics
National Smart Data
National Spacial Data Infrastructure

Smart Service Modernization
Service Modernization
Smart Health
National ePayment Service

Introduction to FEDnet

FEDnet was launched in line with the National Plan and provides a common infrastructure for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources for all Federal Government Entities.

The primary objectives of the FEDnet program is to firstly connect all Federal Government related Entities with each other and to then provide seamless, safe, durable and ongoing connectivity between Entities using a private common infrastructure.

By promoting communication between various Federal entities across the UAE using a single secure common architecture, the TRA is laying the foundation for subsequent Smart Government initiatives defined within the National Plan.

The FEDnet Cloud Compute (IaaS) environment is specifically designed for virtualization and automation, and enables on-demand provisioning from shared pools of infrastructure across physical and virtual environments in a simpler and more cost-effective approach. Utilizing this approach, the applications will no longer need to map to a physical server and storage device, instead Federal Entities can leverage pools of compute and storage resources to optimize the underlying infrastructure; hence improving 'speed to market' and cost efficiency.

Establishing a federal network is a fundamental milestone in integrating and offering government services. FEDnet will enable Entities to publish services to consumers from the privacy of the FEDnet cloud.

H.E. Hamad Al Mansoori
TRA Director General, United Arab Emirates

Three key FEDnet objectives are to achieve integration of services through secured private network, enable government services through cloud services and consolidate the effort to secure government electronic services.

FEDnet Mission

The overarching mission of FEDnet is to provide an efficient and secure means of delivering Smart Government services to entities and citizens in the UAE.

The TRA has implemented a technology infrastructure that increases efficiencies, reliability and security to enable common services and solutions for both Federal Entities and consumers of the UAE. Additionally, FEDnet aims to provide operational benefit to the UAE Government as a whole by supporting existing and future Government Services.

FEDnet Provides a Multi-layered Security Environment. This ensures security at all layers of the infrastructure to promote user adoption and information sharing by connecting entities to the FEDnet Secured Private MPLS Cloud.

The Federal Government cost of ownership is reduced through the consolidation of Shared Government Services. Cost savings will realized through the reduction of the internet and the MPLS footprint within the UAE.

Secured infrastructures

FEDnet has been implemented with a secure architecture that Leverages multi-layered zoning for security segregation. The zoned design contains a number of security measures that include firewalls, IPS, DDOS, Threat Management, Anti-Virus, SPAM filtering, encryption, PKI infrastructure and Application firewalls. A Security Information and Event Management (SIEM) system is operated by a dedicated 24x7x365 Security Operations Center (SOC) to manage all Security events within the Government Network.

Cloud Computing

The FEDnet program will deliver a Cloud environment with scalable on demand network, compute and storage capacity. Each Entity can provision its own Virtual Data Centers and Virtual Machines (VMs) within the FEDnet Cloud that is supported by a 24x7x365 Cloud Command Center.

Central Hosting

FEDnet will be built around a central hosting concept whereby Smart Government services and applications can be provisioned quickly using latest cloud orchestration and automation technologies.

High Availability

High availability is a fundamental principal of the FEDnet Design. The consequential benefit of this design is that there are no single points of failure within the FEDnet network topology.

Disaster Recovery

FEDnet is operated in an Active – Passive DC mode with the production Data Center (DC) located in Dubai and the Disaster Recovery (DR) DC located in Abu Dhabi. The FEDnet architecture has the capability to support the Active-Active mode of operation in future phases.

Fednet Communications Flow

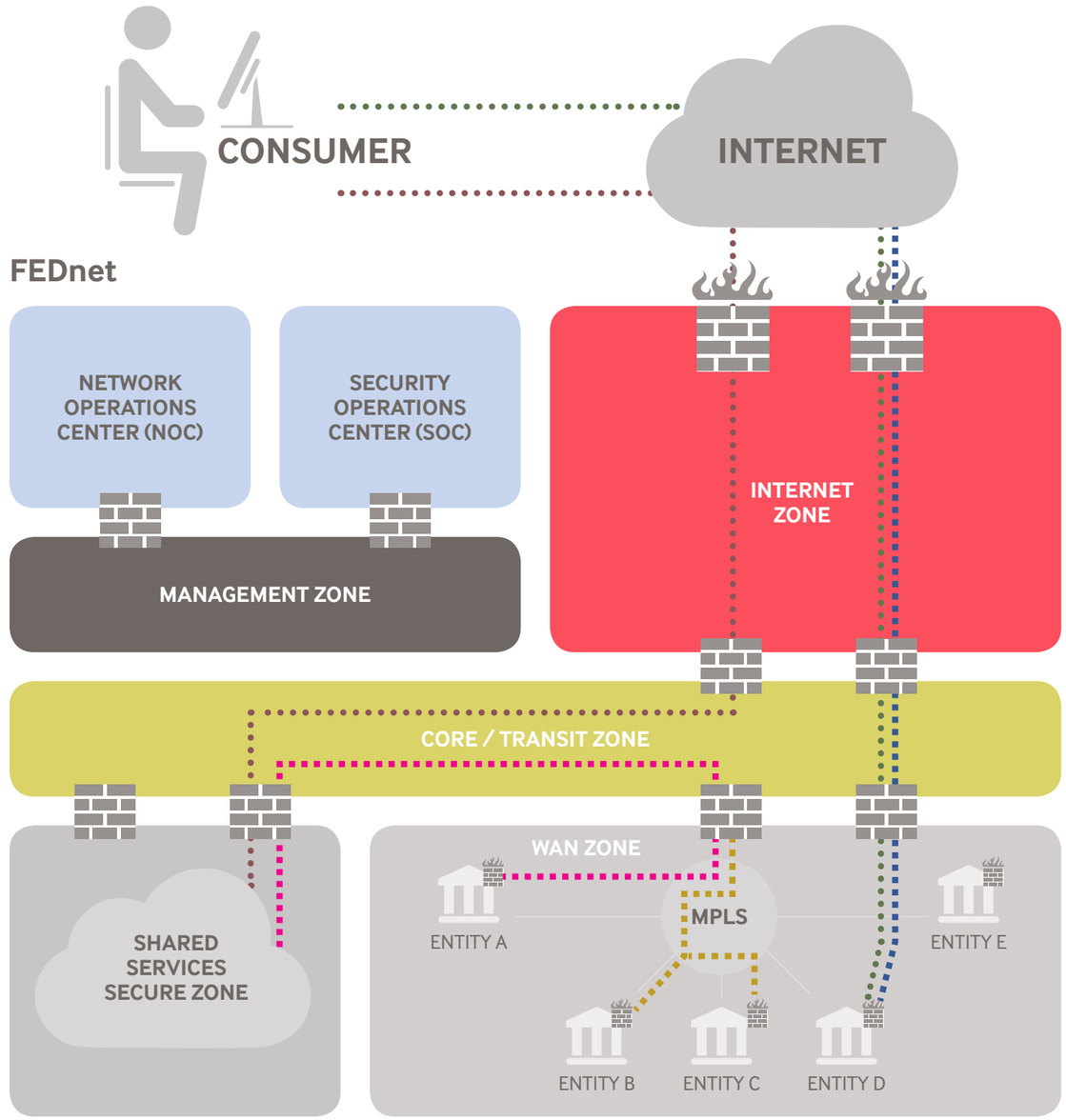
With FEDnet's high speed and robustly secured infrastructure capabilities, the communication flows between the various stakeholders are seamless and secure as outlined in the exhibit below:

1. Consumer to Entity
2. Consumer to the Shared Services Secure Zone
3. Government to the Internet
4. Government Entity to Government Entity
5. Government to the Shared Services Secure Zone

Private Government Mpls Network

Each government entity will connect to both the FEDnet Production and DR DCs through a pair of routers. The routers will be configured with multiple virtual circuits, depending on the Entity DR requirements.

FEDnet Architecture Overview



1. Consumer to Entity
(Example: Public facing mGov services hosted at Entity)

2. Consumer to Secuire Zone
(Example: Public facing mGov services hosted at FEDnet)

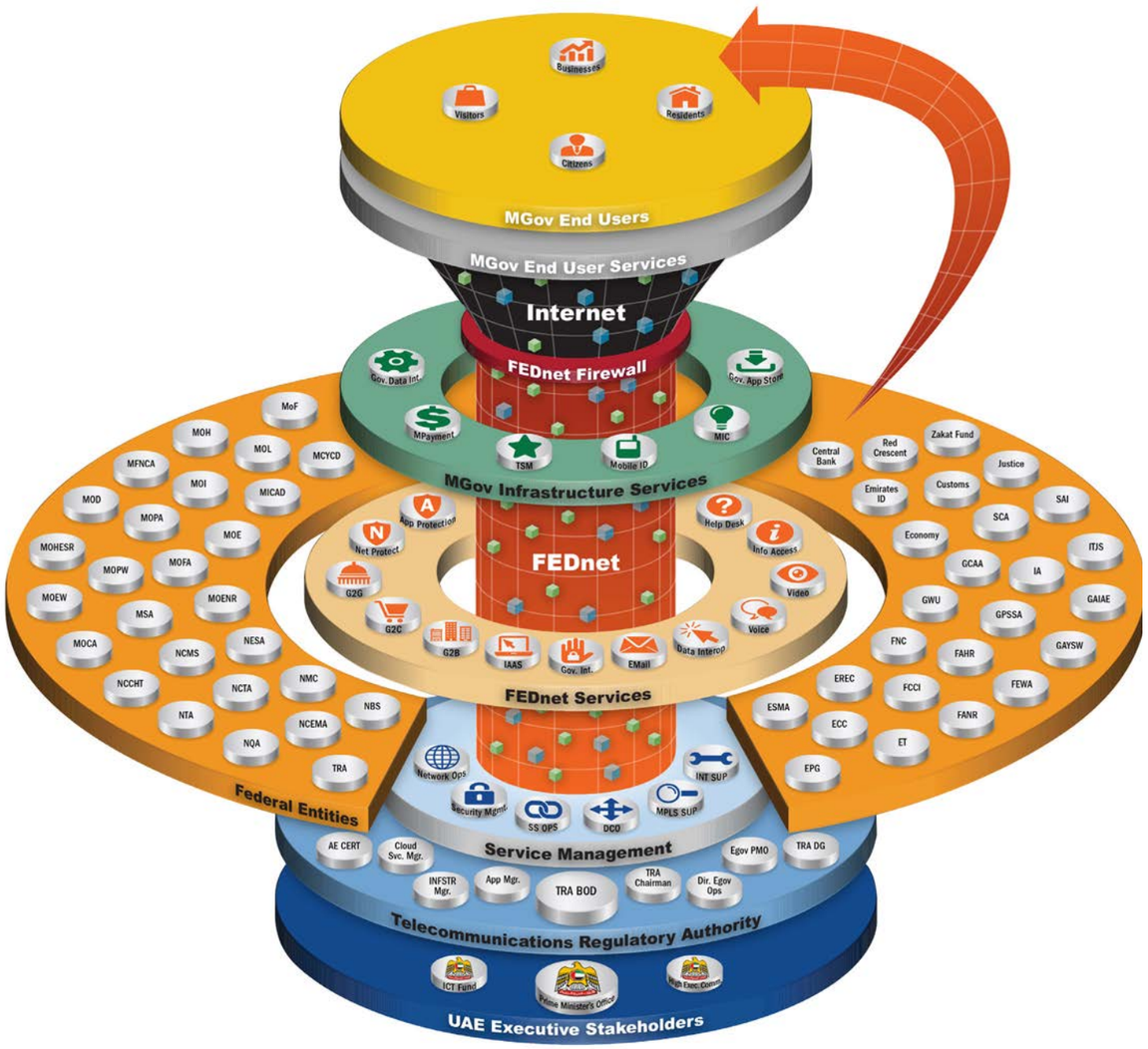
3. Government to Internet
(Example: User at Government premises browsing web

4. Government to Government
(Example: Entity B accessing a service from Entity C

5. Government to Secuire Zone
(Example: Public facing mGov services hosted at FEDnet)

UAE Federal Network (FEDnet) Community Model

Federal Entities provide services to mGov End Users via FEDnet



Master Services Agreement

Leveraging the combined negotiating power of the UAE Federal Entities, the TRA has executed a class leading Master Services Agreement (MSA) with du and Etisalat for the provision of FEDnet Services.

The MSA is for a 5 year period and has been constructed in a modular format to incorporate the detailed Service Catalogue, competitive commercials and clear Service Level Agreements (SLAs) all under the governance of favorable terms and conditions.

Federal Entities will automatically receive all the benefits of the MSA as they are migrated into the FEDnet Environment, including enhanced Service Levels.

MSA Structure

The MSA is a modular contract.
The MSA incorporates 13 schedules detailing Service and Change Management process, Governance and Escalation, Charges, Service Levels, Employee terms, as well as detailed Service Catalogues, all under the governance of favorable terms and conditions.

The MSA has in-built mechanisms (including continuous improvement) to drive du and Etisalat to deliver Service Excellence throughout the 5 year terms.

MSA has built mechanisms to drive Service Excellence

Service Management

Whilst day to day 'operational execution' will be undertaken by du and Etisalat, the TRA will retain overall accountability for FEDnet Services and Service Management.

The TRA have dedicated 'Service Managers and Contract Administrators' who have technical and contractual knowledge as well as service management experience to drive towards Service Excellence.
TRA Service Managers will conduct regular service performance reviews against the Service Levels KPIs.
Where a Service does not meet a KPI, the TRA Service Managers will initiate service improvement plans and where necessary, request Service Credits from the suppliers.

SLAS

FEDnet has a number of SLAs that include Service Availability, Service Resolution and Service Request fulfilment.

The FEDnet Service Levels are defined in the next table and act as a primary mechanism for achieving Service Excellence.

The Service Level Agreement KPIs ensure the Service performs to Government Expectations and promotes continuous Service improvement'

SLA	Service Level	Required Service Level	Service Credit
MPLS Link Availability	For each Service Recipient (Government Entity), Availability of connectivity for Resilient Dual Links from Entity to the Shared Government Data Centre.	99.99%	Yes
Internet Link Availability	For each Service Recipient (Government Entity), Availability of connectivity for Resilient Dual Links from the Shared Government Data Centre to the Internet.	99.95%	Yes
Data Center Interconnectivity Availability	Availability of connectivity for Resilient Dual Links from the Shared Government Data Centre to the Disaster Recovery Data Center.	99.99%	Yes
Incident Management	Percentage of Severity 1 Incidents successfully Resolved within 4 hours from the creation of the Incident Log. Time spent waiting for the Entity will not be counted i.e. Stopwatch will be temporarily stopped.	99.00%	Yes
	Percentage of Severity 2 Incidents successfully Resolved within 8 hours from the creation of the Incident Log. Time spent waiting for the Entity will not be counted i.e. Stopwatch will be temporarily stopped.	99.00%	Yes
	Percentage of Severity 3 Incidents successfully Resolved within 4 calendar days from the creation of the Incident Log. Time spent waiting for the Entity will not be counted i.e. Stopwatch will be temporarily stopped.	99.00%	No
	Percentage of Severity 4 Incidents successfully Resolved within 5 calendar days from the creation of the Incident Log. Time spent waiting for the Entity will not be counted i.e. Stopwatch will be temporarily stopped.	99.00%	No
	Initial Root Cause Analysis competed within 24 hours of incident resolution, with full analysis within 5 days for Severity 1 Incidents.	100%	No
Change Management	Percentage of Standard Service Requests successfully fulfilled within 3 days from the creation of the Service Request Log. Time spent waiting for the Entity will not be counted i.e. Stopwatch will be temporarily stopped. Additionally, If an Entity requires a response quicker than the Standard times then they will become an Emergency Change.	99%	Yes
	Minimum 98% successful deployment of planned & approved changes, (i.e. changes that have been reviewed and scheduled through the formal Change Procedure), each calendar month.	98%	No
	Minimum 85% successful deployment of all Emergency Change requests, each calendar month.	85%	No
	Emergency Change requests to be commenced within 1 hour of receipt. The Time taken to obtain approvals for Emergency Changes will not be counted within this measure.	100%	No
	No unauthorised Changes to be deployed, where unauthorised means a Change being deployed by the Supplier's Outsourced Services team has not been approved within the Change Procedure or a Change being carried out by the wider Supplier engineering/delivery teams has not been communicated to the Customer 5 working days in advance.	Zero Unauthorized Changes	No
	100% of FEDNET infrastructure & security components patched up to date on a quarterly basis as detailed in the FEDNET Maintenance Release Plan; so that no infrastructure component has software fix/patch/release levels (for applicable software modules) that are more than 6 months older than the stable manufacture recommended version. All Critical updates will be applied immediately following the Change Procedure. Exceptions agreed in advance with the TRA Service. Manager during the quarterly Infrastructure Software Review.	100%	No
Service Desk	Percentage of calls to the Help Desk answered within 30 seconds by a NOC technical analyst.	95%	No
	Maximum Acknowledgement Time for Incidents and Service Requests by phone and web.	20 minutes	No
Backup/Restore	No more than 2 Backup failures within each calendar month.	<3 Backup Failures	No

FEDnet Service Catalogue

G2G CONNECTIVITY

Service Description

FEDnet provides connectivity between Government Entities, which will enable a seamless and secure interconnected network where Government entities can share data over the encrypted Federal Government Private MPLS Cloud. Government Entities can securely publish and consume services from each other once connected.

List of Services

- Enable new G2G connectivity
- Connect other FEDnet entities to the G2G hosting entity
- Incident & Request Handling
- Major Incident Handling Triage
- Monthly SLA reporting to Business Owner
- Upgrade MPLS Link
- Add/Remove Firewall rule

Service Dependencies

G2G connectivity is dependent on the FEDnet WAN Zone, MPLS and DC Interconnect.

Service Operating Hours

24x7x365

Disaster Recovery

A disaster recovery site will available from May 2015

Service Customers

All approved Federal Government Entities

Service Custodian

FEDnet Network Operations Center

Service Desk

800 FEDNET

Business Owner

TRA Director of eGovernment Operations

Escalation Point

TRA Senior Infrastructure Manager

SHARED GOVERNMENT INTERNET

Service Description

FEDnet provides Secure Internet Connectivity to Federal Government entities through a dual Internet Service Provider (ISP) Solution allowing for high throughput and redundancy.

The Internet Service provides a consolidation of internet connections across Federal Entities. This reduces the perimeter against intruder attacks by limiting the public vulnerability point to just one Internet Gateway.

List of Services

- Internet Connectivity to Entity hosted services
- Assign Public IPs for Entity Internet hosted services
- Upgrade Internet Bandwidth
- Blocking Websites, Services as per entity requirements
- Add/Remove Firewall rules
- Secure Inbound connection for entity to their internal hosted services (VPN)
- Incident Management
- Service Request fulfilment
- Monthly Entity internet utilization report
- Monthly SLA reporting to Business Owner

Service Dependencies

The Shared Government Internet Service is dependent on the FEDnet MPLS, WAN Zone, Core Zone, DC Interconnect and Internet Zone.

Service Operating Hours

24x7x365

Disaster Recovery

A disaster recovery site will available from May 2015

Service Customers

All approved Federal Government Entities

Service Custodian

FEDnet Network Operations Center

Service Desk

800 FEDNET

Business Owner

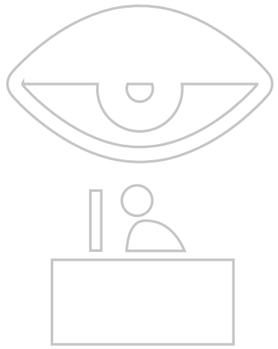
TRA Director of eGoverment Operations

Escalation Point

TRA Senior Infrastructure Manager

INFRASTRUCTURE EVENT MANAGEMENT

Service Description



A suite of IT Service Management tools have been deployed for automated monitoring and alerting.

FEDnet Infrastructure events are monitored 24x7x365 by the NOC and appropriate measures are taken once faults occur or events breach any set thresholds.

List of Services
- Monitoring and Alerting
- Configuration, change, availability, capacity and problem management
- Incident & Request Handling
- 24x7 Monitoring the Network & Compute Environment
- Level 1 incident monitoring & event management
- Monthly SLA reporting to Business Owner
- Web Portal for Incident and Requests logging for Entities
- Call logging and forwarding to level 2 Support teams

Service Dependencies
Dependency on Management Zone and all FEDnet Infrastructure

Service Operating Hours
24x7x365

Disaster Recovery
A disaster recovery site will available from May 2015

Service Customers
All approved Federal Government Entities

Service Custodian
FEDnet Network Operations Center

Service Desk
800 FEDNET

Business Owner
TRA Director of eGovernment Operations

Escalation Point
TRA Cloud Manager

SOFTWARE AS A SERVICE
SHARED GOVERNMENT EMAIL

Service Description

The first Software as a Service that will be offered to Government Entities is the Shared Government email service, which provides a centralized government email environment based on Microsoft Exchange 2013.

Future Services will be added as the Service Catalogue grows.

List of Services Active Directory/DNS
- Account Management
- Group Management
- Access policy management
- Tenant Management Exchange
- Provisioning of mailbox
- De-provisioning of mailbox
- Mailbox quota management
- Email access through Internet (Outlook Web Access)
- Email access through Phone devices (ActiveSync) Backup
- Exchange Backup and Recovery
- Granular Exchange Recovery
- Mailbox Recovery

Service Dependencies
The Shared Government Email Service is dependent on the FEDnet MPLS, WAN Zone, Core Zone, DC Interconnect, Internet Zone and the Secure Zone.

Service Operating Hours
24x7x365

Disaster Recovery
A disaster recovery site will available from May 2015

Service Customers
All approved Federal Government Entities

Service Custodian
FEDnet Cloud Command Center

Service Desk
800 FEDNET

Business Owner
TRA Director of eGoverment Operations

Escalation Point
TRA Cloud Manager

INFRASTRUCTURE AS A SERVICE

Service Description

FEDnet provides convenient, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers and storage).

With a centralized deployment model, compute and storage resources can be rapidly provisioned and released with minimal management effort or service provider interaction.

The overall objective is to create a more agile Federal enterprise where services can be provisioned on demand to meet government compute requirements.

List Of Services

Virtualization

- Commission a VM from Template (Windows/Linux)
- Modify Configuration of a VM e.g., CPU, Memory, Disk, NIC
- Decommission a VM
- Create/Delete/Restore a Snapshot of VM/Appliance
- Power on/off a VM/Appliance
- Reboot a VM/Appliance
- Add/ Modify/Delete
- License a Windows/Redhat server
- Performance and Monitor a VM (Alarms, Task & Events)
- Deploy/Modify/Delete OVF Template (Appliance)

Hosting

- Create Tenant/Modify Tenant/Remove Tenant
- Create/Modify/Remove Organization
- Create/Modify/Remove Virtual Data Centre

Firewall

- Add/Modify/Remove context in firewall
- Add/Modify/Remove firewall policies

Load balancer

- Add servers in load balancer
- Create service groups in load balancer
- Create VIP services for application in load balancer
- Create/Modify/Remove service in load balancer

Authentication

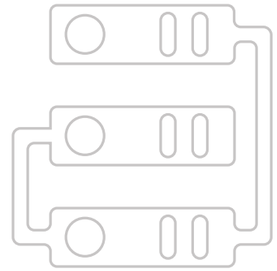
- Create/Modify authorization policies for users/ groups
- Create/Remove users/groups
- Add/Remove network devices

Network

- Create a VLAN/Remove a VLAN
- Create a VSAN/Remove a VSAN
- Assign IP subnet
- Assign IP address

Backup

- Complete VM Backup
- Database Backup
- File Level Recovery
- Database Recovery



Storage

- Create storage group
- Create Logical Unit Numbers (LUN)
- Register/Unregister hosts
- Assign/Remove LUNs to storage group
- Connect/Disconnect host to storage group

Service Dependencies

The Infrastructure as a Service is dependent on the FEDnet MPLS, WAN Zone, Core Zone, DC Interconnect, Internet Zone and the Secure Zone.

Service Operating Hours

24x7x365

Disaster Recovery

A disaster recovery site will available from May 2015

Service Customers

All approved Federal Government Entities

Service Custodian

FEDnet Cloud Command Center

Service Desk

800 FEDNET

Business Owner

TRA Director of eGovernment Operations

Escalation Point

TRA Cloud Manager

SECURITY EVENT MANAGEMENT

Service Description

A Security Information and Event Management (SIEM) system is operated by a dedicated 24x7x365 Security Operations Center (SOC) to manage all Security events within FEDnet.

FEDnet contains a number of security measures that include firewalls, IPS, DDOS, Threat Management, Anti-Virus, SPAM filtering, encryption, PKI infrastructure and Application firewalls.

The FEDnet Infrastructure events are monitored 24x7x365 by the SOC and appropriate measures are taken for events of interest.

List of Services

Security Event Validation and Escalation
- Security Incident/Event Analysis
- Security event log correlation report
- Building new correlation rules
- Reporting and building SIEM Dashboard
- Incident Handling, Notification and Escalation
- Device Reporting
- Connector Installation

SOC Report Request Management
- Security Incident reporting
- KPI Reporting
- Monthly Reporting to Business Owner

SOC Executive Dashboard Management
- Creating/Modify and Manage Dashboard

Security Log Integration
- Log Integration with SIEM

Vulnerability Assessment
- Reporting on vulnerable assets

SOC Capacity Management
- Utilization Trend Report – License constrain from EPS perspective

Service Dependencies
Dependency on Management Zone and all FEDnet Infrastructure

Service Operating Hours
24x7x365

Disaster Recovery
A disaster recovery site will available from May 2015

Service Customers
All approved Federal Government Entities

Service Custodian
FEDnet Network Operations Center

Service Desk
800 FEDNET

Business Owner
TRA Director of eGoverment Operations

Escalation Point
TRA Senior Infrastructure Manager

Frequently asked questions

Q: When will I be migrated to FEDnet?

A: An Adoption Roadmap will be sent to all Entities with start and finish dates for the migration.

Q: We require services which are not part of the service catalogue; can they be accommodated?

A: Any additional Services not published in the Service Catalogue should be requested through NOC Service desk 800 FEDnet or servicedesk@fednet.gov.ae. The request will then be forwarded to the TRA and a Service Manager will follow up to capture the requirement. Any new Services will be subject to approval by the FEDnet Steering Committee.

Q: How do I enroll onto the SLAs?

A: You are automatically enrolled and have access to FEDnet Services once you are migrated.

Q: What happens if an SLA is breached?

A: If an SLA is breached then a Service credit is issued to the TRA. This incentivizes the operators to meet SLA KPIs.

Q: There is an Entity I need to connect to and it's not on your roadmap?

A: An Entity can request for connectivity to Federal Entities that are not connected to FEDnet by contacting the FEDnet Service Desk. The request will then be forwarded to a TRA Service Manager that will capture the requirement. Any new connections to Entities will be subject to approval by the FEDnet Steering Committee.

Q: What OS does FEDnet support?

A: FEDnet provides Infrastructure as a Service. This does not include OS support. Any operating System that can be virtualized can be deployed by the Entity and will need to be licensed and supported by the Entity.

Q: How will I be notified of Emergency maintenance?

A: Emergency maintenance will only be requested in circumstances where the Service will be impacted if the maintenance is not carried out. Entities will be immediately notified of emergency changes impacting their service. These are not considered planned maintenance and reactive to an incident or security threat.

Q: When will the Disaster Recovery Service be available?

A: DR will be available from May 2015 onwards. A regular failover and maintenance schedule will be shared with Entities.

Q: How do I use IaaS?

A: Training will be provided from May 2015 onwards.

Q: Will FEDnet replace my branch/Inter Entity site connectivity?

A: FEDnet provides a single point of entry and does not provide inter Entity connectivity between Entity Sites. Only connectivity between Government Entities is provided.

Q: When I enroll, which set of default services will be available from FEDnet?

A: After MPLS Deployment, Entities will have access to G2G, IaaS, Shared Government Email, Infrastructure and Security Event Management. After Network Adoption Entities will have access to Shared Government Internet Service.

Q: Why should I use IaaS?

A: The Federal Government has invested in a secure private cloud compute environment. Future Services should be provisioned in the Entity VDC to maximize the benefit of this investment. FEDnet is an attractive offering when compared to a new DC and Infrastructure offering.

Q: How do I log an Incident or Change?

A: Incidents and Service Requests can be raised through the 24x7x365 FEDnet Service Desk on 800 FEDnet.

Q: Stability and Scalability for the service offerings?

A: FEDnet is a highly resilient environment without any Single Points of Failure. The solution is scalable as the demand for the Services grow.

Q: Where can I get more technical information?

A: Any additional information can be requested through the NOC Service desk 800 FEDnet.

Q: How do I escalate an issue?

A: The first escalation point is the Head of the NOC through the FEDnet service desk (800 FEDnet). The Second escalation point is a TRA Service Manager on FEDnet@tra.gov.ae.

Q: How will I be notified of scheduled maintenance?

A: The FEDnet Service Desk will communicate any planned maintenance outages 5 days in advance.

CONTACT US
800 FEDNET
servicedesk@fednet.gov.ae