Virtual Network Functions (VNFs)

Deploy Network Functions in Just a Few Days – in Software

Today's digital economy requires your business to move fast. There's no longer the luxury of taking months to complete IT and network deployments needed to quickly support new business initiatives.

You might already be saving significant time using software as a service (SaaS) and other cloud computing options. Now, you can dramatically speed up your network infrastructure deployments and changes, too.

AT&T has virtualized key network infrastructure functions, so they can be deployed quickly in software. By using virtual appliances instead of standalone physical appliances, you eliminate the time and labor associated with buying, installing, configuring, testing, and maintaining router hardware and other network devices. Many of which are proprietary and typically require different types of expertise at a higher cost.

Virtual Network Functions (VNF's) run on an industry-standard X86-based server from AT&T we call universal customer premises equipment (uCPE). Your VNF's are automatically configured on your uCPE by AT&T to match your company's policy.

Your equipment investment shifts from proprietary and vendor-specific to open and able to support multiple VNF functions on a single hardware platform for simplicity and cost savings.

VNF Services Available

Available with AT&T Virtual Private Network MPLS service with Ethernet access (EaVPN). Rides on x86 uCPE capable of supporting multiple VNFs. Supports service chaining so you can logically connect VNFs to one another. Choose from a standard set of templates or build your own. Includes AT&T-provided configuration, monitoring, fault management, maintenance, reporting, billing, and changes.

Available VNFs

Virtual Router (vRouter)
- Juniper

Virtual Firewall (vFirewall)
- Fortinet

Potential Benefits for Virtual Network Functions

- Faster network function deployment; you're up and running in days
- Reduced number of router appliances (hardware) to buy and manage
- Streamlined network operations and management
- Simplified vendor management
- Decreased break-fix downtime
- Lower capital and operational expenses for improved total cost of ownership (TCO)

Virtual Router (vRouter)

Features
- Static Routing
- Routing Policy
- RIP, OSPF, IS-IS, and BGP Routing Protocols
- Dynamic Host Configuration Protocol (DHCP) Relay
- Proxy Address Resolution Protocol (ARP)
- Logging, Reporting and Monitoring
- Licensing – AT&T

Resource Requirements

VNF	vCPU	RAM (GB)	Storage (GB)
Juniper vSRX 15xx	2	4	8

To learn more about AT&T Network Functions on Demand (NFoD) Virtual Network Functions (VNFs), visit www.att.com/nfv or have us contact you.

Share this with your peers

Virtual Firewall (vFirewall) & Fortinet Fortigate

vFirewall is a software instance of the Fortigate security solution from Fortinet, an industry-leading security provider. The vFirewall – a security virtual network function (VNF) – handles all the capabilities of a traditional, premises-based firewall hosted on dedicated hardware. But unlike a traditional firewall, the virtual, software-based firewall is low-cost, dynamically configured, and up and running fast. And you can make configuration changes quickly via the standard management console from Fortinet, the Fortimanager.

The vFirewall and uCPE architecture ensures that all traffic is inspected by the vFirewall VNF so granular policies can be written based on your organization's specific needs.

AT&T Management Functions

- Single point of contact (24x7x365)
- Configuration
- Proactive fault management
  - Hardware/software fault monitoring
  - Fault recognition
  - Trouble isolation
  - Problem resolution
  - Issue tracking
  - Interface with maintenance vendors
- Maintenance
  - Equipment repair/replacement
  - Break/Fix SLA - 24x7x4
- SLA Reporting-Business Center
- Change management

3 Network Architecture Options

1. **Classic AVPN Ethernet access**
   AVPN access circuit with VLANs for VPNs only
2. **Classic AVPN Ethernet with vNIC (virtual Network Interface, now called Multi-Port)**
   AVPN access circuit with VLANs for VPN and Internet
3. **Classic AVPN with third-party Internet**
   The first circuit is an AVPN access circuit with VPNs only

AT&T vFirewall Security Features

Feature	Description
Layer 4 Stateful Firewall	Support for standard L4 5-tuple firewall policies. It includes a source IP address/port number, destination IP address/port number and the protocol in use.
Intrusion Prevention (IDS/IPS)	Signature-based Intrusion Detection and Prevention (IDS/IPS). Administrator has the ability to enable this inspection on a per-firewall rule basis.
Web Filtering	Controls web browsing based on web category or through customized white or blacklists. Administrator has the ability to select categories, whitelist/blacklists on a per-firewall rule basis.
Antivirus/ Antispyware	A mix of signature-based and heuristic engines for the detection and blocking of malware. Administrator has the ability to enable this inspection on a per-firewall rule basis.
Application Control	Provides application-specific firewall rules above and beyond standard 5-tuple rules. Protects against tunneling through other protocols and traffic behavior within an application. Administrator has the ability to create both L4 and application-specific firewall rules and to configure directory services to identify individual users.

AT&T vFirewall Options, Requirements, and Support

FortiGate Software Version	vCPU	RAM (GB)	Storage (GB)	Virtual Domains	Throughput (Mbps)
Fortinet FortiGate VM00	1	1	2	1	50
Fortinet FortiGate VM01	1	2	2	10	~50
Fortinet FortiGate VM02	2	4	2	25	250
Fortinet FortiGate VM04	4	6	2	50	500
Fortinet FortiGate VM08	8	12	2	250	1000

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/nfv

To learn more about AT&T Network Functions on Demand (NFoD) Virtual Network Functions (VNFs), visit www.att.com/nfv or have us contact you.

06/06/16 AB-3135