ACC Business Network-Based Firewall (NBFW) Sales Guide

Marsha Gilbert
ACC Business Offer Manager
816-995-4639
mg3424@att.com

Contents

1.0 ACC Business

ACC Business offers a focused set of AT&T Internet Protocol (IP) Services under the brand name of ACC Business, targeted to small to mid size domestic business customers.

ACC Business MIS/PNT customers are acquired through an external agent sales channel and are offered a modestly lower price in exchange for a different customer experience.

2.0 What is Network-Based Firewall Service

Network-Based Firewall (NBFW) is also known as AT&T Managed Security Service – Network-Based (MSS-NB). It is available to new and existing ACC Business MPLS PNT customers.

NBFW provides:

- a cost effective method to access the internet using PNT circuits, without the need for separate MIS facilities.
- NBFW centralized security management reduces the cost and complexity associated with managing multiple premise based devices.
- Security policies are applied globally to all outbound, inbound, and bi-directional internet traffic. Simple or sophisticated security policies for outbound, inbound and bi-directional Internet access and e-commerce applications.
- Customers can tailor the service to meet their needs by choosing from the offered Service Levels (Levels 1 - 5) and available optional features.

3.0 Product Overview

Network-Based Firewall provides customers with a Network-Based, fully managed solution with the following capabilities:

- Requires no additional equipment at customer premises. Customers subscribe to, rather than purchase, network security. This reduces capital expenditure, risk of technological obsolescence and the need for additional staff. AT&T owns and manages all service assets which are located in AT&T Security Data Centers (SDC).
- Traffic is routed directly to the Internet, not to a customer-administered central security location only to be re-routed back to the Internet.
- Provides 24×7 monitoring and attack management of the service. Customers are released from the responsibility of managing Internet traffic, constructing and administering firewalls, applying patches, managing hardware and running screening applications. All of these are required to enable secure Internet access in today's wide-open environment.

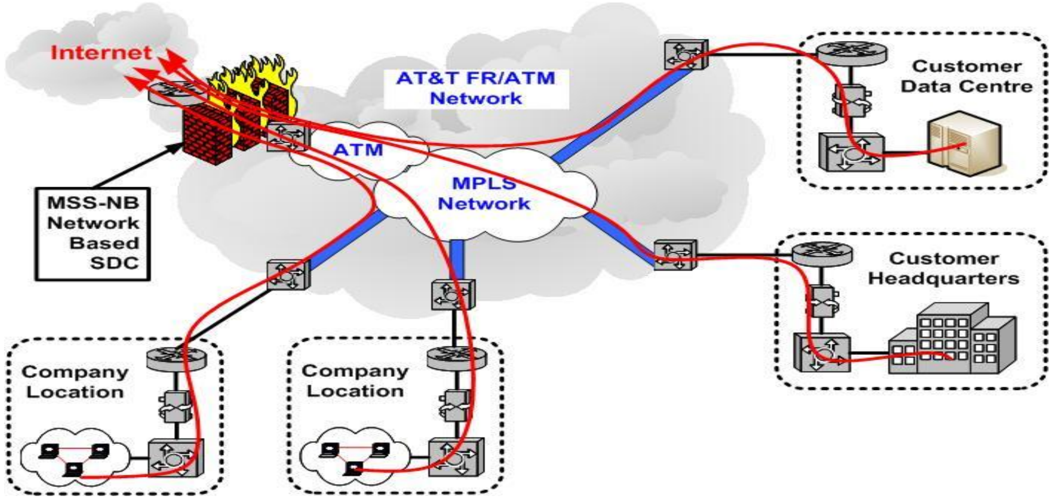
SLAs (Service Level Agreements) are not available as a part of the offer.

3.1 How Does It Work?

Sophisticated security features are installed directly into the network. This allows customers to access the Internet via their existing PNT network without rehoming remote traffic to a customer-administered central security location for re-routing back to the Internet.

This takes place via a MPLS based arrangement in the AT&T network. Once Internet-bound traffic reaches the NBFW, it is governed by a customer defined Security Policy.

3.1.1 Service Overview Diagram



A high level view of the way traffic flows from Customer sites through NBFW to the Internet.

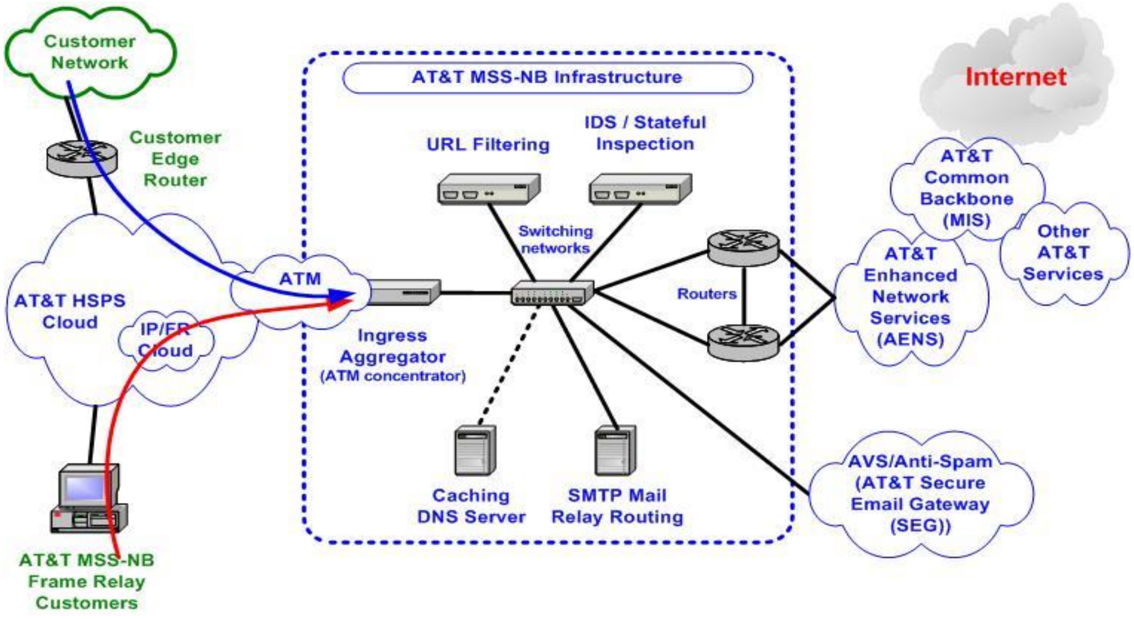
3.2 Service & Transport Types

- Transport
- NBFW is offered to ACC Business MPLS PNT customers only. Customers that have only MIS service are not candidates for Network-Based Firewall.
- PNT service is only available in the United States
- One (1) PNT network per firewall
- Service
- NBFW for ACC Business is available with service levels 1-5 and with all the bandwidth options (1.5mb- 45mb) and optional features.
- The ACC Business Network-Based Firewall offer will support all AT&T Network-Based Firewall capabilities except multiple VPN segments.
- There can only be 1 PNT network per firewall – each PNT network must have its own secure network (Secnet) and firewall.

3.3 Solution Elements and Technical Details

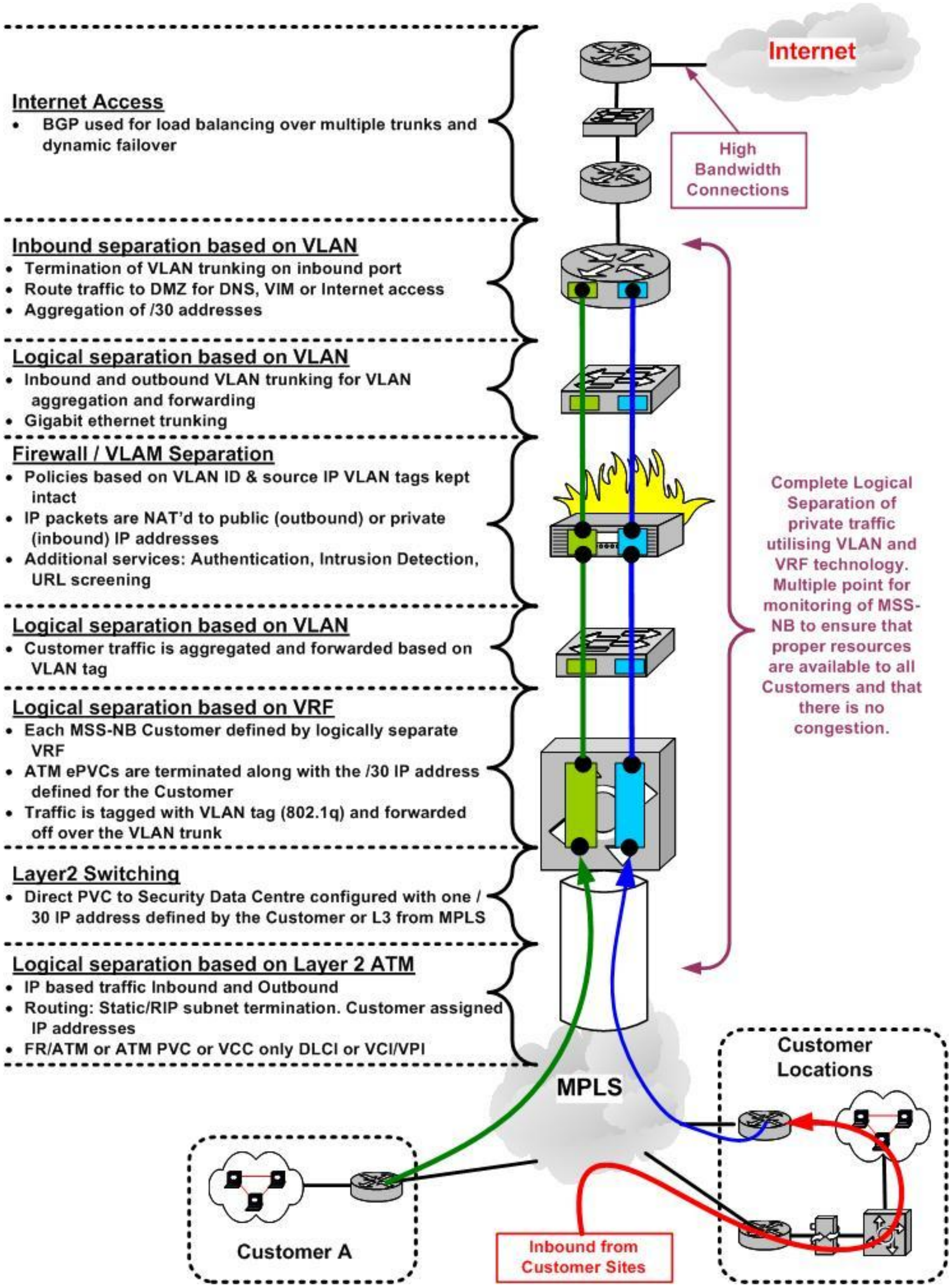
Element	Description
Security Data Center(s) (SDC)	SDCs are located in hardened, AT&T locations with access to high-capacity AT&T packet and IP networks. They contain the NBFW infrastructure and are managed remotely from the AT&T Security Network Operations Centers (S/NOC).
Connectivity Options	An Enterprise Permanent Virtual Circuit (ePVC) enables connection to an MPLS enabled customer VPN providing any to any connectivity between sites. Dual ePVCs are provisioned from the customer's primary AT&T SDC to the customer's MPLS VPN.
Security Network Operations Center (S/NOC)	The S/NOC is responsible for monitoring components and networks for security events as well as monitoring the hacker and response communities for the latest threats and defenses. They perform day-to-day administration and management of the technical components of the SDC, including component health, capacity planning, provisioning, configuration, troubleshooting and upgrading.
Network Address Translation (NAT)	NAT is used in the SDC crossover routers to translate unregistered IP addresses to a registered IP address for appropriate routing to NBFW. Port Address Translation (PAT) is used in NBFW to translate all unregistered clients to a registered IP address.

3.4 Security Data Center (SDC) Elements Diagram


Customer Network
Customer Edge Router
AT&T HSPS Cloud
IP/FR Cloud
AT&T MSS-NB Frame Relay Customers
ATM
AT&T MSS-NB Infrastructure
URL Filtering
IDS / Stateful Inspection
Switching networks
Routers
Ingress Aggregator (ATM concentrator)
Caching DNS Server
SMTP Mail Relay Routing
Internet
AT&T Common Backbone (MIS)
AT&T Enhanced Network Services (AENS)
Other AT&T Services
AVS/Anti-Spam (AT&T Secure Email Gateway (SEG))

A high level view of the elements located in the Security Data Center.

3.5 Traffic Routing Details



Internet
High Bandwidth Connections
Complete Logical Separation of private traffic utilising VLAN and VRF technology. Multiple point for monitoring of MSS-NB to ensure that proper resources are available to all Customers and that there is no congestion.
MPLS
Customer Locations
Customer A
Inbound from Customer Sites

Internet Access

- BGP used for load balancing over multiple trunks and dynamic failover

Inbound separation based on VLAN

- Termination of VLAN trunking on inbound port
- Route traffic to DMZ for DNS, VIM or Internet access
- Aggregation of /30 addresses

Logical separation based on VLAN

- Inbound and outbound VLAN trunking for VLAN aggregation and forwarding
- Gigabit ethernet trunking

Firewall / VLAM Separation

- Policies based on VLAN ID & source IP VLAN tags kept intact
- IP packets are NAT'd to public (outbound) or private (inbound) IP addresses
- Additional services: Authentication, Intrusion Detection, URL screening

Logical separation based on VLAN

- Customer traffic is aggregated and forwarded based on VLAN tag

Logical separation based on VRF

- Each MSS-NB Customer defined by logically separate VRF
- ATM ePVCs are terminated along with the /30 IP address defined for the Customer
- Traffic is tagged with VLAN tag (802.1q) and forwarded off over the VLAN trunk

Layer2 Switching

- Direct PVC to Security Data Centre configured with one /30 IP address defined by the Customer or L3 from MPLS

Logical separation based on Layer 2 ATM

- IP based traffic Inbound and Outbound
- Routing: Static/RIP subnet termination. Customer assigned IP addresses
- FR/ATM or ATM PVC or VCC only DLCI or VCI/VPI

3.6 Service Levels

Service Level	Standard Features of Service Levels	Description
1	Outbound Only with URL filtering One SDC One Secure Network (SecNet) Reports via AT&T Business Direct Customer is given a single public IP address (or PAT – Port Address Translation address). Choice of up to 8 ports/protocols: HTTP (80) DNS_TCP (53) DNS_UDP (53) TELNET (23) SSH (22) HTTPS (443) FTP (20/21) ICMP	One Size Fits all customers (at this level) Security Policy. Available for all Security Data Centers (SDC). Note: SMTP Mail Relay is not allowed at this Service Level as this assumes inbound as well as outbound mail traffic.
2	Outbound Only with URL filtering Custom Security Policy (up to 10 rules) Additional multiple egress SDCs may be bought Customer is given a single public IP address (or PAT – Port Address Translation address). If more public IP addresses are required for NAT these can be bought.	Outbound only Security Policy but allowing additional rules, egress points (SDC locations), SecNets, etc. Note: SMTP Mail Relay is not allowed at this Service Level as this assumes inbound as well as outbound mail traffic.
3	Outbound and Inbound traffic Custom Security Policy (up to 30 rules) /28 public IP address range allocated, giving 16 addresses in total. One address reserved for PAT, leaving 15 spare.	Outbound and Inbound Security Policy. In addition to Level 2 options, allows more rules and larger range of public IP addresses as standard.
4	Outbound & Inbound traffic Custom Security Policy (up to 50 rules) /27 public IP address range allocated, giving 32 addresses in total. One address reserved for PAT, leaving 31 spare. Support for up to aggregate bandwidth of up to 135Mbps, as standard Four hours of premium network engineering or security engineering time by telephone during implementation	Outbound and Inbound Security Policy. In addition to Level 3 options, has a larger range of public IP addresses as standard and support for higher bandwidths. Note: Any solutions over 135Mbps bandwidth require custom pricing due to additional possible costs.
5	Outbound and Inbound traffic Custom Security Policy (up to 99 rules) • All components are high availability with dual redundant access links to the Internet and private side Support for existing alternate ISP (failover) and/or advertising the Customer IP address space is included (minimum /24 of customer's own ARIN, APNIC, RIPE or other ICANN entity registered space) Eight hours of premium network engineering or security engineering time by telephone during implementation	Outbound and Inbound Security Policy. In addition to Level 4 options, has support for other ISP, engineering support, etc.

3.7 NBFW Standard Features

NBFW offers standard features for Firewall and Intrusion Detection for each Customer. AT&T deploys, monitors, and maintains customer defined inbound and outbound security policies for each Secure Network (SecNet).

3.7.1 Firewall

NBFW allows the customer to define the security policy enforced at the SDC. The standard security policy promotes a robust security implementation and enforcement, including:

- A customer defined security policy per Secure Network, at each location, with support for most TCP and UDP IP services, IPSEC (IKE/GRE/PPTP) pass-through and inbound relayed traffic to SMTP and external DNS caching from AT&T secure servers
- Stateful Inspection of allowed IP traffic through the firewall
- Changes to the customer security policy are managed through Business Direct

3.7.2 Network

- Aggregate bandwidth (i.e. total of all locations) subscriptions from 1.544Mbps to 45Mbps
- Support for customer source networks, using static route definitions within the firewall
- Static Network Address Translation (NAT) for customer servers (DNS, SMTP, etc.)
- Many-to-one outbound Network address translation of customer IP address space, with customer route isolation. This utilizes the NBFW Port Address Translation (PAT) facility.
- Resilient connections to AT&T's IP backbone and AT&T's packet services network (HSPS)

3.7.3 Intrusion Detection

Network-Based Firewall includes intrusion detection which scans all customer traffic for a number of defined categories of exploits, anomalies and attacks. Intrusion Detection is performed on the Security Data Center (SDC) infrastructure only, not on customer premises equipment.

3.7.4 DNS (Domain Name Service)

Network-Based Firewall service includes DNS caching.

A DNS service can be provided by AT&T-Enhanced Network Services (AENS) or customers can use their own DNS authority.

The DNS caching service provided by NBFW gives customers name resolution and protection services. All customer DNS queries will be sent to the MSS-NB DNS caching servers from the customers' specified internal primary DNS servers.

NBFW expects that customers have implemented some form of split DNS where internal resolution is done on a customer DNS server. These internal DNS servers are maintained and administered by the customer. External DNS queries will be sent from these servers to NBFW caching DNS servers for resolution.

NBFW does not support internal customer DNS resolution. This must be provided by the customer.

Customers will need to configure their DNS to use "forwarding’ to the NBFW caching DNS servers for unknown domains. This prevents non-recursive attempts at resolution. Most new versions of BIND on all platforms support a global "forwarders" statement.

3.7.5 Dynamic Load Balancing

Dynamic Load Balancing distributes traffic dynamically across the NBFW environment within an SDC. Benefits of this include:

- Optimized traffic flow
- Provide consistent performance
- Reduce impact of server failures

3.7.6 NAT (Network Address Translation)

NAT conceals the company's internal network IP addresses from the Internet, avoiding their disclosure as public information. NBFW uses NAT in the following way:

- Inbound and Outbound: Static mode of Network Address Translation (NAT) provides a one-to-one assignment between the published IP address and the company's internal IP address for services such as SMTP, DNS, FTP and Web servers.
- Outbound: Many-to-one outbound network address translation (also known as 'hide NAT') to the Internet for specific hosts that need internet access. This uses the Port Address Translation (PAT) function of NBFW.
- Published IP address (192.9.100.1) to the real IP address (192.168.1.1)

3.7.7 Peak Bandwidth Allocation

Customers select their company's required bandwidth allocation for Internet access through the firewall.

Customers are allocated the total bandwidth for all connections covered by the service rate.

Bursting above the allocated bandwidth is not allowed.

3.7.8 Same SDC Redundancy

Alternate paths through the SDC are used to eliminate single-points-of-failure.

Automatic failover using BGP is accomplished by provisioning a second ePVC as a backup link into the SDC from the customer's VPN.

Each component within a Security Data Center (SDC) is not only equipped, where possible, with backup power supplies, but is mirrored throughout the platform infrastructure with a duplicate component to give failover and redundancy support.

3.7.9 Alternate Site Redundancy (Fail Over)

Alternate site redundancy uses a 3rd ePVC to reroute traffic to an alternate SDC which has a duplicate security policy.

The site failover would be triggered in the event of primary and backup circuit failover into the first SDC or if there was a total failure of critical components of the network infrastructure leading into or out of the first SDC.

3.7.10 Reporting

Network-Based Firewall (MSS-NB) service reports are provided via the AT&T BusinessDirect Portal.

The available reports provide Top 20 details on Access, Denies, Traffic activity, URL activity, and IDS events for day, week and month periods. Reporting content and specific report availability (additions or deletions) may be changed by the NBFW service.

Firewall log data in syslog format can also be provided to a customer designated server.

A list of the reports follows:

- Connection Requests and Traffic Report
- Top 20 Accepts by Destination IP address
- Top 20 Accepts by Service
- Top 20 Accepts by Source IP Address
- Top 20 Denies by Cause
- Top 20 Denies by Destination IP Address
- Top 20 Denies by Service
- Top 20 Denies by Source IP Address
- Top 20 Denies by URL
- Top 20 Traffic by Destination IP Address
- Top 20 Traffic by Service
- Top 20 Traffic by Source IP Address
- Top 20 URL Offender
- Top 20 URL Denies by Category
- Top 20 Events by Destination IP Address

- Top 20 Events by Service
- Top 20 Events by Signature
- Top 20 Events by Source IP Address

3.7.11 Vulnerability Assessments

NBFW uses a periodic vulnerability assessment on the service to identify and remove vulnerabilities that could potentially be exploited by intruders to gain access to the environment.

Note: This security feature is performed on the SDC infrastructure only, not on customer premises equipment.

3.8 Optional Features

Available on Service Level	Optional Feature	Description
1,2,3,4,5	**URL Filtering**	Allows internet traffic to be filtered based on web site content. This option is licensed on the number of concurrent users (e.g. 100, 500, 1000, 3000, 5000, above). This option has the following features available: A number of pre-defined url categories (e.g. religion, sports, etc) which are selected to be allowed or denied The Whitelist / Blacklist function allows browsing to specific URL's to be permitted or denied. This function overrides any URL filtering options. It is possible to block web searches based on keywords URL blocking can also be done by IP address rather than URL name
2	**Additional SDC Egress** **(or Multiple Outbound Access Point)**	Allows outbound access from more than one SDC. Option allows 1, 2 or 3 additional SDCs. For each additional SDC there will be the following costs: Two additional ePVCs for each extra SDC. This is because the total bandwidth determines the access charges Policy setup and support costs for each extra SDC Each extra SDC includes a /30 range of public IP addresses. Each /30 block gives 4 usable IP addresses
3,4,5	**Additional Secure Networks (SecNets)**	Allows customer to have extra Secure Networks (SecNets) into a single SDC. The price includes the cost of ePVCs into a single SDC. A DMZ or other isolated MPLS network is considered to be another Secure Network.

3,4,5	**Additional Public IP Addresses**	If the customer needs more than the allocated number of IP addresses for that Service Level, they can buy extra IP addresses. This benefit of this option is additional NAT functionality. The IP addresses can be bought as listed below: Multiple blocks of /30 IP addresses – up to 32. Each /30 block gives 4 usable IP addresses. A single /30 IP address range must stay with each SDC (no individual IP addresses can be spread from a single /30 to multiple sites) Multiple blocks of /24 IP addresses – up to 10. Each /24 block gives 256 usable IP addresses. A single /24 IP address range cannot be broken into less than 32 IP addresses (i.e. a /27 subnet) for a single SDC.
3,4,5	**Additional Firewall Rules**	This option allows the customer to choose extra Firewall rules in addition to those provided at the Service Level. The rules can be bought in blocks of five.
3,4,5	**Premium Network Engineering or Security Consultant time**	The customer may request resource from AT&T to assist with issues related to their Wide Area Network operating with the AT&T MPLS network and the NBFW service. This option allows the customer to purchase Premium Network Engineering or Security Consultant telephone assistance in multiple blocks of 8 hours.
3,4,5	**Additional Site Egress & Ingress** **(or Multiple Gateway Access Point)**	This option allows the customer to have inbound and/or outbound access through more than one SDC. They can select 1, 2 or 3 additional SDCs. Since the total bandwidth used determines access charges, this option will assume that the cost includes 2 additional ePVCs for each additional SDC, For each additional SDC there will be the following costs: A /30 range of public IP addresses, this includes the PAT (overload) address. Each /30 block gives 4 usable IP addresses. Two additional ePVCs for each extra SDC. This is because the total bandwidth determines the access charges Policy setup and support costs for each extra SDC.
3,4,5	**Site Failover**	This option allows the customer to have a single alternate SDC to receive "failover traffic". A 3rd ePVC is provisioned from the alternate site to the customer's MPLS network. A duplicate security policy is maintained on the alternate SDC for a specified SecNet. If a customer has multiple SecNets, they must purchase Site Failover for a specific number of SecNets. Network-Based Firewall Failover Requirements: Customer must provide their own registered /24. Failover is provided in US from Secaucus to Mesa. Failover is not provided in the US from Mesa to Secaucus. No current MOW failover option. Cannot fail from EMEA or AP to the US. Failover will be available In EMEA and AP when the secondary sites of Sydney and Amsterdam are on-line.

4.0 Benefits

4.1 Why Does ACC Business Sell It?

To increase PNT customer acquisition and retention by leveraging the integrated VPN and internet access capabilities available with AT&T Network-Based Firewall.

Provide an advantage to ACC Business over smaller tier 2 and 3 service providers by delivering an advanced network security service.

4.2 Why Do Customers Buy It?

Network-Based Firewall is cost effective compared to purchasing and managing separate access facilities and hubs for internet access.

With Network-Based firewall customers gain improved control over their networks at a lower cost than centralized security management.

4.3 Customer Benefits

- Reduced total cost of ownership by reducing complexity and potentially the number of perimeter firewalls at branch locations
- Internet and PNT access from a single set of circuits and ports
- Eliminates need for PNT customers to purchase separate access facilities
- Centralized monitoring and reporting through Business Direct
- Centralized policy management gives a simplified change control process across the enterprise
- Highly redundant infrastructure in hardened AT&T data centers
- Traffic is routed directly to the Internet, not to a customer-administered central security location only to be re-routed back to the Internet
- Highly scalable with pre-provisioned bandwidth and security components
- Reduced cost, reliable performance and proactive security monitoring make NBFW a great value
- One-stop shopping for IP security and Internet connectivity.

5.0 Selling Strategy: Value Proposition

5.1 Why Network-Based Firewall?

NBFW is a managed security offering that enables appropriate security policies for Internet access. Customers have the ability to select from one of five flexible service levels which provide different levels of function, security policy complexity and support options

5.2 Price

NBFW is priced according to the bandwidth bought by the customer plus any selected options.

The customer can increase or decrease bandwidth levels and service options. The service price at the selected bandwidth includes redundant Internet access in a single data center, resilient Firewall and IDS hardware/software, redundant ports to the customer WAN and dual ePVC connectivity to the customers MPLS VPN.

5.3 Value

Three elements make NBFW a great value:

- Reduced expenses due to lower total cost of ownership. The customer avoids the expenses of hardware and software, hiring and training personnel and paying for unused bandwidth.
- Reliable performance from AT&T's position as a leading Internet Service Provider (ISP) with an award winning backbone
- Separate logical path to the Internet so that mission-critical applications run uninterrupted.

5.4 Simplicity

To the customer, NBFW is a simple solution to a complex security problem:

- A fully managed end-to-end security solution provides the security components (hardware and software), installation, day-to-day management and maintenance. Also, most importantly, the expert customer support and proactive network monitoring protect the customer's network perimeter.
- NBFW provides increased protection from the Internet by protecting the customer's WAN at high bandwidth network gateways. This is instead of protection at premises locations which may have bandwidth restrictions. Mitigation of broad scale Denial of Service attacks, Virus, and Worm outbreaks is more effectively performed at a high bandwidth gateway before these problems reach the customer's network edge.
- One-stop shopping with ACC Business is available for a Customers IP security and Internet connectivity.

5.5 Targeting Criteria

The target market for NBFW is any customer with a multi-site Private Network where centralized security management and enforcement at a single or few gateway locations is an effective solution for their business requirements.

5.6 Target Market

Target customers should have many, if not all, of the following characteristics:

- Customers that require their own outbound security policy, including the ability for their own inbound access as well
- Multi-site PNT installations
- Requirement to control employee access to Internet content by utilizing the add-on URL Filtering feature available within NBFW, or by adding on AT&T Web Security.
- Customers that want an Internet VPN implementation (i.e. secured inbound traffic with IPSEC pass-through) back to a designated IPSec VPN switch.
  Note: Termination of IPSEC traffic at NBFW is NOT provided, only pass-through of IPSEC traffic to customer premise VPN devices.

6.0 Offer Positioning

Customer Environment	Addressable?	Fit	Sales Positioning
Existing multi-site AT&T PNT customers without any dedicated IP access solution	Yes	Good	Position service for remote nodes, not headquarter (HQ). Position AT&T Dedicated IP and MFS (Managed Firewall Services) for HQ.
Existing multi site PNT network with Dedicated IP access at headquarter (HQ) location, backhauling remote nodes to HQ	Yes	Good	Position at remote locations to eliminate backhaul to HQ.
New PNT customers	Yes	Good	Position at remote locations and HQ for Internet Access
Existing multi-site frame relay customers with other carriers' dedicated IP access at headquarter (HQ) location, backhauling remote nodes to HQ	Yes	Good	Complimentary. Position for remote nodes. Potential win back of dedicated service.
Not a PNT customer	Yes	Good	Sell Customer a network service like EVPN in combination with NBFW
MIS only customer	No	Poor	

7.0 Pricing

NBFW pricing consists of a one-time setup charge and monthly-recurring charges (detailed below):

- One Time Charges – A one-time installation fee is charged for the initial setup and provisioning of NBFW and any selected options.
- Fixed Recurring Charges – Monthly recurring charges are calculated using some or all of the following solution elements:
    - Customer chosen service level of the service and the bandwidth selected
    - Optional features selected

7.1 Installation Charges

Installation Charge Per SDC			
United States – Mesa or Secaucus	**Optional SDC Fail-Over**	**Cross Connect - under 100Mbps**	**Cross Connect –equal to or over 100Mbps**
500	1500	1500	1500

7.2 Bandwidth Charges

Monthly Recurring Charges for PNT Access ONLY. Consult Technical Sales with questions on AVPN availability.

Bandwidth	**United States – Mesa SDC, Secaucus SDC**	**Optional SDC Fail-Over (in-region)
2 Mbps	1400	*1300*
5 Mbps	3600	*2600*
10 Mbps	6700	*4700*
15 Mbps	7700	*6900*
25 Mbps	11600	*11300*
30 Mbps	13800	*13400*
50Mbps	22800	*22100*
80 Mbps	36300	*35200*

7.3 Feature Pricing

Service Level	**Monthly**	**Install**	**Comment**
1	900	5000	
2	1400	7000	
3	2750	9000	
4	4600	10000	
5	8600	12000	
URL Filtering			
100 Users	300	500	
500 Users	1200	500	
1000 Users	1900	500	
3000 Users	4500	500	
5000 Users	6900	500	
Unlimited	ICB	500	
IDS/IPS			
IDS Only	N/A	N/A	
Active IDS/IPS – Basic	700	250	
Active IDS/IPS – Advanced	1000	500	
Application Filtering	750	500	
Additional Firewall Rules			
Block of 5 – each	400	500	Up to 10 blocks
Additional MACD's	200	N/A	Two MACD's per package
Additional Public IP Addresses			
Block of 4 (/30) – each	100	250	Up to 32 blocks
Block of 256 (/24) - each	2500	2500	Up to 10 Class C's (/24)

7.4 Discounts

Field Level Discounts are available for the following NBFW Service Elements:

- Service Level
- Bandwidth
- URL Filtering
- Application Filtering
- IDS/IPS Basic Advanced

NBFW Charges	For 1 year contract term	For 2 year contract term	For 3 year contract term
Installation charges (OTC):	**0%**	**0%-100%**	**0%-100%**
Monthly recurring charges (MRC)	**0%**	**0%-45%**	**0%-53%**

For all other NBFW Service Elements:

- Cross Connect
- Fail Over
- Additional Firewall Rules
- Additional MACD's
- Additional IP Addresses

NBFW Charges	For 1 year contract term	For 2 year contract term	For 3 year contract term
Installation charges (OTC):	**0%**	**0%-50%**	**0%-100%**
Monthly recurring charges (MRC)	**0%**	**0%-5%**	**0%-10%**

7.5 Promotions

Contact ACC Business Technical Sales for information on current promotions & qualifications. Or consult the Active Promotions Summary document at: https://businesssolutions.web.att.com/sites/ACC-Business/Pages/Products%20and%20Pricing.aspx#cross

8.0 ACC Business Technical Sales Support

ACC Business Technical Sales will assist to:

- Qualify opportunities
- Generate pricing
- Generate contracts
- Assist with the Technical Specification document
- Obtain the required pre-approval by the AT&T NBFW Review Board
- Approve the order for release

9.0 Pre-Sales Requirements Checklist

Function	Checklist
Contact / Qualify Customer	ACC Business Network-Based Firewall customers must have existing PNT service with the following recommended configuration Have a typical hub and spoke network topology or MPLS enabled WAN. Have a multi-site WAN installation
Complete Pre-Qualification Form	Engage ACC Business Technical Sales to obtain and complete Pre-Qualification form.
Submit Pre-Qualification form for review	ACC Business Technical Sales will submit the completed Pre-Qualification form to the MSS-NB Global Pre-Qualification Team (details are in the Pre-Qual document). The Team meets each week to review NBFW prospects.
Receive approval to proceed	Once approval is received, ACC Business can proceed with pricing , contracting, etc.

10.0 ICB Review Board Checklist and Process

When a sales opportunity deviates from the standard NBFW offer, the Individual Case Basis (ICB) Review Board must examine the proposed solution. The steps in this process are as follows:

- ACC Business Technical Sales confirms that it needs to be examined by the Review Board
- ACC Business Technical Sales will Email the documents listed below to the Review Board
- A customer requirements summary includes details of the business problem and the customer requirement.
- A Network Diagram
- A description of the solution and how it deviates from the standard offer

Once all of the above information has been received, ACC Business Technical Sales will schedule a conference call. The Board can review a limited number of cases each week and most decisions will be made at the time of the conference call.

11.0 Pricing Schedule

- NBFW contracts are available via AOW.
- The customer must sign the ACC Business NBFW Pricing Schedule, in addition to the PNT Pricing Schedule (if new PNT applicable).
- If sold with new PNT Network
- The countersign date for the NBFW contract will usually always be after the PNT countersign date
- The NBFW contract and billing start date will always be 1-2 months after the PNT contract & billing start date.
- However, the terms will be identical.

12.0 Provisioning

If the PNT Network is ordered at the same time as the NBFW, the PNT Network must be provisioned prior to the start of the provisioning of the NBFW. In this case, the ACC Business MIS Specialist will hold NBFW order until the PNT Network is installed.

The ACC Business MIS Specialist will project manage the order through to completion. Updates on the initial PNT network will also be provided by the MIS specialist, business as usual.

13.0 Billing

The following billing options are available:

- Standard invoicing with a single invoice per account number.
- Corporate Billing is also required to bill charges for service locations or affiliates of the parent company.
- MARC Billing.
- Network-Based Firewall charges should be generated on the same statement as MIS/PNT/COS charges.
- Network-Based firewall charges should be combined with PNT charges on a corporate billed account.
- For NBFW & new PNT sales, the NBFW contract and billing start date will always be 1 - 2 months after the PNT contract & billing start date (though the terms will be identical)

14.0 Moves, Adds and Changes

There are some change orders that the customer can do via BusinessDirect, such as a change of firewall rules or a change to filtering. Only non revenue effecting changes are allowed using BusinessDirect.

Revenue affecting orders must be submitted via a Pricing Schedule.

15.0 Customer Care / Technical Support / Maintenance

The AT&T Customer Care organization is continuously monitoring customers using Managed Firewall Services. They provide 24x7 monitoring and technical support.

If a customer is experiencing problems or would like to make changes to their existing service, the AT&T Customer Care group will assist.

New NBFW customers are provided information about the Customer Care Group via E-Mail during the installation process. This E-Mail will also provide contact information and the customer specific information to identify their network firewall.

The Helpdesk Contact information is also available at:
https://help.attbusiness.net/index.cfm?fuseaction=contact_us.viewHelpNumbers