AT&T Network Based Firewall for AT&T NetBond®

User Guide

Revision: 5.0
11/11/2016
Table of Contents

AT&T Network Based Firewall for AT&T NetBond® User Guide ........................................ 1
Table of Contents .................................................................................................................. 2
Legal Disclaimer .................................................................................................................. 3
1. Product overview: Network Based Firewall for AT&T NetBond ............................... 4
   1.1 Feature overview: NBFW for AT&T NetBond ......................................................... 4
2. Getting Started ................................................................................................................. 5
   2.1. Implementation Planning and Access Requirements ........................................... 5
   2.2. Access to Manage Firewalls .................................................................................. 5
   2.3. Manage Firewalls ................................................................................................ 6
   2.4. Modify Location .................................................................................................... 7
   2.5. Modify VPN Rule .................................................................................................. 9
   2.6. Disconnect Firewall .............................................................................................. 9
   2.7 Data Gathering and Technical Interview ............................................................... 11
3. Installation ....................................................................................................................... 11
   3.1. Milestone Notification ......................................................................................... 11
   3.2. Service Completion Notice ................................................................................... 11
4. Billing ............................................................................................................................. 11
5. Maintenance ..................................................................................................................... 12
   5.1. AT&T Global Client Support Center (GCSC) Managed Security Service (MSS)
        Operations ............................................................................................................. 12
   5.2. Change Request Process ...................................................................................... 12
6. Nearest Exit Routing (NER) .......................................................................................... 12
   7.1. NER Feature Overview ....................................................................................... 12
   7.2. NER Requirements ............................................................................................... 12
   7.3. NER Use Case ...................................................................................................... 12

January 4, 2017
© 2016 AT&T Intellectual Property. All rights reserved. AT&T, the Globe logo, Mobilizing Your World and other marks are trademarks and service marks of AT&T Intellectual Property. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.
Legal Disclaimer

The information contained in this document should not be duplicated, transmitted, or disclosed, in whole or in part without the expressed written consent of AT&T. Information in this document is subject to change without notice. AT&T assumes no responsibility for any errors or omissions in this document. Use of this document and the information is pursuant to the terms and conditions of your service agreement with AT&T.

AT&T IS PROVIDING THE INFORMATION TO YOU “AS IS” AND “WITH ALL FAULTS.” AT&T DOES NOT WARRANT, BY VIRTUE OF THIS DOCUMENT, OR BY ANY COURSE OF PERFORMANCE, COURSE OF DEALING, USAGE OF TRADE OR ANY COLLATERAL DOCUMENT HEREUNDER OR OTHERWISE, AND HEREBY EXPRESSLY DISCLAIMS, ANY REPRESENTATION OR WARRANTY OF ANY KIND WITH RESPECT TO THE INFORMATION, INCLUDING, WITHOUT LIMITATION, ANY REPRESENTATION OR WARRANTY OF DESIGN, PERFORMANCE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, OR ANY REPRESENTATION OR WARRANTY THAT THE INFORMATION IS APPLICABLE TO OR INTEROPERABLE WITH ANY SYSTEM, DATA, HARDWARE OR SOFTWARE OF ANY KIND. AT&T DISCLAIMS AND IN NO EVENT SHALL BE LIABLE FOR ANY LOSSES OR DAMAGES OF ANY KIND, WHETHER DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, SPECIAL OR EXEMPLARY, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF GOODWILL, COVER, TORTIOUS CONDUCT OR OTHER PECUNIARY LOSS, ARISING OUT OF OR IN ANY WAY RELATED TO THE PROVISION, NON-PROVISION, USE OR NON-USE OF THE INFORMATION, EVEN IF AT&T HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES.
1. Product overview: Network Based Firewall for AT&T NetBond®

AT&T Network-Based Firewall (NFW) Private for AT&T NetBond is an optional service for current and new NetBond customers who want to better understand how to extend their AT&T VPN to their cloud providers without any auditing or firewall capabilities.

NFW for AT&T NetBond provides logical separation by creating two VPNs: Trusted corporate VPN and Extranet Cloud Provider VPN. The FW is located in between the two VPNs providing redundant, stateful firewall, Unified Threat Management (UTM) functions and automated network provisioning along with scalability for AT&T customers as their business needs change.

As part of the automated orchestration process, two VLANs (Trusted and Untrusted) are built with burstable bandwidth up to 5GB each, from the firewall edge routers to the trusted VPN.

The firewall edge routers receive routes from the trusted VPN and redistribute them into the CSP VPN via the untrusted VPN and vice versa. The security edge routers do not inject or filter any prefixes advertised by the customer or CSP. The traffic from the trusted VPN must flow through the firewall to/from the CSP VPN after customer has configured the security policy based on their needs. Since the traffic is private to each cloud provider, there is no need to translate the customer’s private IPv4 address space to a Public IP. This feature is only available in US at the Washington DC and Los Angeles IPE nodes.

Overall, the security policy and the selection and use of security features provided by AT&T is the responsibility of the customer and end user. AT&T does not guarantee that use of the security features that AT&T provides will prevent unauthorized access to customer systems or data.

1.1 Feature overview: NFW for AT&T NetBond

There are two service levels available for the AT&T NFW for AT&T NetBond service. These levels are:

- Primary Service Level
- Enhanced Service Level

Primary: Common Customer Security Policy allowing both inbound and outbound traffic flow based on the configuration. The Primary Level includes a basic set of
reports and certain self-administration capabilities via BusinessDirect®. With this service level, the customer is provided with burstable bandwidth up to 5GB which is also available on an on-demand basis.

**Enhanced:** This service level provides the option to upgrade to more add-features in addition to the Primary features described above. Included features are:
- Basic or Advanced Web Filtering
- Basic or Advanced Malware Filtering
- IDS Logging or Active IDS/IPS
- Nearest Exit Routing: Allows customers to have more than one firewall on a single VPN

For additional information about the features, please refer to the AT&T Secure Network Gateway (SNG) Service Guide.

---

2. **Getting Started**

2.1. **Implementation Planning and Access Requirements**

Following are some general points to consider when planning and provisioning your NBFW:
- You must be enabled with AT&T NetBond
- You must be a Multi-Protocol Label Switched (MPLS) customer on the AT&T VPN Network.
- You are essential to the delivery of the service by providing the security policy information prior to test and turn up

If you need assistance with application testing, security audits, etc., please consult with your AT&T Account Team to utilize AT&T Network Professional Services, an AT&T Alliance Channel partner or another third party to provide this capability.

2.2. **Manage Firewalls**

Everything about NBFW service can be found on Cloud Portal
Cloud Portal → My Services -› AT&T NetBond → Manage Firewalls

This will take you to a screen that will allow you to:
- Request a new Firewall
- Modify an existing Firewall
- Delete a Firewall in its entirety
2.3. Request Firewall

AT&T NetBond customers can initiate a NBFW order on the Cloud Portal. Manage Firewalls → Request Firewall

When you hit “Request Firewall”, a window will open which will allow you to select the desired firewall locations per VPN.

1. You may select one or more firewall locations but no more than two in the United States.
2. Select the VPN that you wish to add Firewall(s) by checking the box(es) associated with the Firewall location you desire. **Note:** In order to get Firewalls in more than one location you need to subscribe to NBFW Enhanced Service Level
3. Repeat step 2 for each AT&T VPN you wish to establish a firewall.
Once you have completed your selection(s), click on “Submit” and the order will be received by AT&T.  

Note: If you have selected more than one FW location and you have “Primary” service level, a pop-up screen will appear reminding you that you will need to subscribe to the “Enhanced” service level.

- An AT&T Account Manager and/or your Solution Implementation Manager (SIM) will contact you to proceed with requirements as explained in Data Gathering and Technical Interview sections.

2.4. Modify Location

This screen will allow an existing NBFW customer to:

- Add a second FW location in the United States (assumes you have one US location existing)
- Move a FW from one location to another
- Delete a Firewall Location (Only if you have MORE THAN ONE FW location)

2.4.1. Add a second Firewall location

A. Select the VPN for which you would like to add the second location. You should see one FW location with a checkmark and a status of COMPLETE.

B. Click on Modify Location. A new screen will appear with the check boxes activated.

C. Check the second location that you would like to have a FW established.

NOTE: DO NOT UNCHECK THE EXISTING FW LOCATIONS ALREADY CHECKED OR IT WILL BE DELETED
D. Click on Save. Your request is now being processed. The new FW location will now appear with a checkmark and IN PROGRESS status.
E. When the FW has completed installation, this status will change to COMPLETE.

2.4.2. Move a FW from one location to another
- Select the VPN for which you would like to move the FW location. You should see one FW location with a checkmark and a status of COMPLETE.
- Click on Modify Location. A new screen will appear with the check boxes activated.
- Check the new location that you would like to have a FW established and UNCHECK the location that you are moving FROM.
  NOTE: UNCHECKING THE EXISTING FW LOCATION WILL RESULT IN IT BEING DELETED
- Click on Save. Your request is now being processed. The new FW location will now appear with a checkmark and IN PROGRESS status. The old FW location will now appear with a checkmark and DELETING status.
- When the FW has completed installation, the new FW location will now appear with a checkmark and COMPLETE status. The old FW location will now appear WITHOUT a checkmark and NOT REQUESTED status.

2.4.3. Delete a Firewall Location
Note: This option can only be used for a partial disconnect. To perform a full DISCONNECT of the ENTIRE FW, see section 2.6 below.
A. Select the VPN for which you would like to delete the Firewall location. You should see more than one FW location with a checkmark and a status of COMPLETE.
B. Click on Modify Location. A new screen will appear with the check boxes activated.
C. Uncheck the location that you would like to have a FW Deleted.
  (NOTE: THE UNCHECKED FW LOCATION(S) WILL BE DELETED)
D. Click on Save. Your request is now being processed. The FW location will now appear with a checkmark and DELETING status.
E. When the FW has completed deletion, box will be unchecked and the status will change to NOT REQUESTED.
2.5. Disconnect Firewall

Note: This is for a full disconnect of your Firewall order.

A. Select the VPN for which you would like to “Disconnect” the Firewall in its entirety. You should see one or more FW location(s) with a checkmark and a status of COMPLETE.

B. Click on “DISCONNECT FIREWALL” button immediately beneath the VPN name. You will be redirected to a website where you can process the disconnect request.
C. When the FW has been completely disconnected, the check boxes for all locations will be unchecked and the status will change to NOT REQUESTED.

2.6. Modify VPN Rule

To modify your VPN rule, you can select the VPN that has NBFW and change the status of “Firewall Required Before VNC” to either Yes or No. To complete the change, hit “Done”.

2.7. Manage Firewall Policy

For existing NBFW customers, this link will take you to the “Security Center” where you can:

- Generate and monitor your security reports
- View and download a company security policy and associated profiles
- Manage your NBFW rules and policies on-demand
- Request MACD tickets for NBFW policy changes
3. New Order Installation

3.1. Data Gathering and Technical Interview

- You will receive a Technical Provisioning Document (TPD) from your Solution Implementation Manager (SIM) to document all Firewall configuration requirements. You should review the TPD with the SIM and resolve any questions related to completing this document. Note that your participation in this process is crucial. Failure to participate and provide information in a timely manner will negatively impact your target service ready date.
- A SIM will contact you to schedule a call to discuss your order and document technical requirements in detail. The technical interview will cover questions related to completing the TPD.
- You will forward the completed TPD to the SIM via email for review and approval by AT&T Security Engineers prior to the start of the provisioning process.

3.2. Milestone Notification

- Once the TPD has been approved by the AT&T Security Engineer, the target provisioning interval can take up to 20 business days. This estimate will vary for complex orders including new access or if more than one Secure Network Gateway service is ordered.
- Your SIM will coordinate schedules and provide target dates for each step of service implementation, including the date and time of the final test and turn up (service ready date). It is incumbent for you to be familiar with your company’s planned projects and anticipate any conflicts that might interfere with the proposed service ready date. A customer’s inability to turn up the service on the mutually agreed upon service ready date could result in unnecessary charges.
- AT&T engineers will ensure that predecessor/successor projects (such as implementing new eVPN circuits) are coordinated with the milestones of this project.

3.3. Service Completion Notice

- An e-mail from the Managed Security Operations Center (MSOC) will confirm your site is in maintenance. The e-mail will include information for contacting the MSOC and details on AT&T support of your Managed Security Service.
- Your Firewall status on cloud portal will be “Complete” and you can start using the service.

4. Billing
For US Customers, your bill will be sent to the AT&T BusinessDirect® Portal (eBill). For Most of World (MOW) Customers, your Bills will be mailed to the billing address on the first of the month after turn up.
For billing questions, please call the toll-free number that appears on your bill.

5. Maintenance

5.1. AT&T Global Client Support Center (GCSC) Managed Security Service (MSS) Operations

This team is responsible for integrating new customers into the AT&T MSS lifecycle process, managing change requests via MAC’s (moves, adds, or changes) and providing answers to general questions regarding your managed security service.

The team will provide initial notification of non-scheduled impact events such as network and hardware failures. Additionally, they support MSS customers and notify about any fault management issues if they are encountered with your managed security service.

The team also provides written notification in either automated or manual formats for events of varying severity. The notification is for monitored traffic and is reported per the level contract. In the event of a potential compromise, the customer will be engaged via phone and a qualified analyst will aid in mitigation.

United States - GCSC Managed Security Services (MSS) Operations Help Desk:

The Managed Security Service (MSS) team access number for our support centers is available through your AT&T Account Representative.

- The MSS team access number is: 877-677-2881
- You will then be prompted for your customer PIN
- Prompt
  ⇒ Secure Email and Network Gateway Services

5.2. NBFW Change Request Process

Change Request:

- Normal Operating Hours for processing change requests are 24x7x365, including holidays.
- Change requests are processed within 24 normal operating hours