atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

FIREWALL APPLIANCE TECHNICAL SHEET

ATLANTIC.NET'S FIREWALL APPLIANCE

Technical Sheet

- Filtering by source and destination IP - IP protocol, source and destination port for TCP and UDP traffic.
- Able to limit simultaneous connections on a per-rule basis.
- Atlantic.Net's Firewall Appliance utilizes p0f, an advanced, passive OS/network fingerprinting utility, to allow you to filter by the Operating System initiating the connection.
- Atlantic.Net's Firewall Appliance has the option to add-on an Intrusion Detection system (IDS), which goes beyond and below firewall filtering. It goes beyond by looking at the pattern of network connections and recognizing port scans, specific threat signatures and denial of service attacks. It goes below by looking at the actual content of each packet, recognizing executable code, badly formed packets, buffer overflow attempts, and things like plain-text credit card numbers.
- Highly flexible policy routing possible by selecting gateway on a per-rule basis (for load balancing, failover, multiple WAN, etc).
- Aliases allow grouping and naming of IPs, networks and ports. This helps keep your firewall rule set clean and easy to understand, especially in environments with multiple public IPs and numerous servers.
- Capable of transparent layer 2 firewalling - can bridge interfaces and filter traffic between them, even allowing for an IP-less firewall (though you probably want an IP for management purposes).
- Packet normalization - Description from the AN scrub documentation: "'Scrubbing' is the normalization of packets so there are no ambiguities in interpretation by the ultimate destination of the packet. The scrub directive also reassembles fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that have invalid flag combinations."
    - Enabled in Atlantic.Net's Firewall Appliance by default.
    - Can disable, if necessary. This option causes problems for some NFS implementations, but is safe and should be left enabled for most installations.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net
sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

FIREWALL APPLIANCE TECHNICAL SHEET

STATE TABLE

The firewall's state table maintains information on your open network connections. Atlantic.Net's Firewall Appliance is a stateful firewall; by default, all rules are stateful. Most firewalls lack the ability to finely control your state table, but Atlantic.Net's Firewall Appliance has numerous features allowing granular control of your state table, thanks to the abilities of OpenBSD's pf.

On a per-rule basis:

- Limit simultaneous client connections
- Limit states per host
- Limit new connections per second
- Define state timeout
- Define state type

State types - Atlantic.Net's Firewall Appliance offers multiple options for state handling:

- Keep state - Works with all protocols. Default for all rules.
- Modulate state - Works only with TCP. Atlantic.Net's Firewall Appliance will generate strong Initial Sequence Numbers (ISNs) on behalf of the host.
- Synproxy state - Proxies incoming TCP connections to help protect servers from spoofed TCP SYN floods. This option includes the functionality of "keep state" and "modulate state" combined.
- None - Does not keep any state entries for the traffic. This is very rarely desirable, but is available because it can be useful under some limited circumstances.

State table optimization options - Atlantic.Net's Firewall Appliance offers four options for state table optimization:

- Normal - The default algorithm.
- High latency - Useful for high latency links, such as satellite connections. Expires idle connections later than normal.
- Aggressive - Expires idle connections more quickly. Uses hardware resources more efficiently, but can drop legitimate connections.
- Conservative - Tries to avoid dropping legitimate connections at the expense of increased memory usage and CPU utilization.

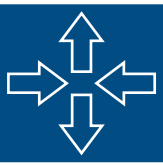
440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net
sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

FIREWALL APPLIANCE TECHNICAL SHEET



NETWORK ADDRESS TRANSLATION (NAT)

- Port forwards, including ranges and the use of multiple public IPs
- 1:1 NAT for individual IPs or entire subnets.
- Outbound NAT
  - Default settings NAT all outbound traffic to the WAN IP. In multiple WAN scenarios, the default settings NAT outbound traffic to the IP of the WAN interface being used.
  - Advanced Outbound NAT allows this default behavior to be disabled, and it enables the creation of very flexible NAT (or no NAT) rules.
- NAT Reflection - in some configurations, NAT reflection is possible so services can be accessed by public IP from internal networks.

REDUNDANCY

CARP from OpenBSD allows for hardware failover. Two or more firewalls can be configured as a failover group. If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active. Atlantic.Net's Firewall Appliance also includes configuration synchronization capabilities, so you make your configuration changes on the primary firewall and they automatically synchronize on the secondary.
pfsync ensures the firewall's state table is replicated to all failover configured firewalls. This means your existing connections will be maintained in the case of failure, which is important for preventing network disruptions.

LOAD BALANCING

Outbound Load Balancing

Outbound load balancing is used with multiple WAN connections to provide load balancing and failover capabilities. Traffic is directed to the desired gateway or load balancing pool on a per-firewall rule basis.

Inbound Load Balancing

Inbound load balancing is used to distribute load between multiple servers. This is commonly used with web servers, mail servers, and others. Servers that fail to respond to ping requests or TCP port connections are removed from the pool.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

FIREWALL APPLIANCE TECHNICAL SHEET

VPN

Atlantic.Net's Firewall Appliance offers three options for VPN connectivity: IPsec, OpenVPN, and PPTP.

IPSEC

IPsec allows connectivity with any device that supports standard IPsec. This is most commonly used for site-to-site connectivity with other Atlantic.Net Firewall Appliance installations and most commercial firewall solutions (Cisco, Juniper, etc.). It can also be used for mobile client connectivity.

PPTP SERVER

PPTP is a popular VPN option because nearly every OS has a built-in PPTP client, including every Windows release since Windows 95 OSR2.

The Atlantic.Net's Firewall Appliance PPTP Server can utilize a local user database or a RADIUS server for authentication. RADIUS accounting is also supported. Firewall rules on the PPTP interface control traffic initiated by PPTP clients

REPORTING AND MONITORING

The RRD graphs in Atlantic.Net's Firewall Appliance maintain historical information on the following:

- CPU utilization
- Total throughput
- Firewall states
- Individual throughput for all interfaces
- Packets per second rates for all interfaces
- WAN interface gateway(s) ping response times
- Traffic shaper queues on systems with traffic shaping enabled

Find Out More?

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at **www.atlantic.net**, call **888-618-DATA (3282)**, or email us at **sales@atlantic.net.**

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS