TECHNICAL SUPPORT NOTE
Configuring Access Policies in AOS

Introduction

Packet filtering is the process of determining the attributes of each packet that passes through a router and deciding to forward or block traffic based on a list of packet filtering rules. Packet filtering provides the basic protection mechanism for a routing firewall host, allowing you to determine what traffic passes through it based on the contents of the packet, thereby potentially limiting access to each of the networks controlled by the firewall. Stateful inspection adds some intelligence to packet filtering. With stateful inspection, the firewall keeps track of a session so it knows if the session is already active. It uses this information plus a list of rules to determine if a packet should be blocked or forwarded.

Concepts

Packet Filtering using the ADTRAN OS firewall has two fundamental parts:

Access Control Lists (ACLs)

- ACLs are used as packet selectors by other ADTRAN OS systems.
- ACLs have no function without an Access Policy Class.

Access Policy Classes (ACPs)

- ACPs consist of a *selector* (ACL) and an *action* (permit, deny, NAT).
- ACPs integrate both permit and deny policies with NAT.
- ACPs have no effect until they are assigned to a network interface.

Both ACLs and ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed. They both have an implicit ‘deny’ at the end of the list.

The internal ACP engine is stateful, and is closely integrated with the stateful inspection firewall. If a packet is allowed through the ACPs, it creates a session. Then associations are created that allow all traffic related with that session through.

It is important to point out the differences between the operation of **stateful** policies in the ADTRAN OS versus **stateless** filters. For example, consider an application where a host located behind a firewall device initiates an outbound session to a server on the Internet. If the firewall is configured to use stateless filters, two or more filters must be defined: one that allows the outbound traffic from the host to the Internet, and a second that allows inbound traffic (responses from the initiated session). Typically, the inbound filter list needs to reject sessions initiated from the Internet, while allowing other responses to sessions initiated from the private network. Because the filter lists have no knowledge of the state of the session (sequence numbers, inactivity time, etc) there is a possibility that an attacker will be able to "fool" the configured filter lists and direct malicious traffic through the firewall. With stateful policies, however, a single policy is configured that permits the traffic from the host to be initiated to the Internet. The ADTRAN OS stateful inspection firewall creates an association for this session and stores it in an internal database. When the server on the Internet sends a response back to the host, the ADTRAN OS stateful inspection firewall recognizes that this traffic is associated with an allowed session and permits the traffic. Since the firewall has detailed knowledge about the current state of every session flowing through the device, it is much more difficult for an attacker to generate traffic that is not blocked by the firewall.

The ACP engine also has Application Level Gateways (ALGs) that are aware of protocols not easily integrated with NAT or firewalls that create associations that allow these protocols to work transparently.

For example, the FTP ALG will not only create the associations to allow the control session (port 20) to pass data, but will also create associations to allow the server initiated data sessions to work(port 21). This allows FTP clients to pass through the ADTRAN OS firewall and ACPs without using passive mode.

Packet Flow

Case 1: Packets from interfaces with a configured policy-class to any other interface:

ACPs are applied when packets are received on an interface. If an interface has not been assigned a policy-class, by default, it will allow all received traffic to pass through. If an interface has been assigned a policy-class but the firewall has not been enabled with the **IP firewall** command, traffic will flow normally from this interface with no ACP processing.

Case 2: Packets that travel in and out a single interfaces with a configured policy-class:

These packets are processed through the ACPs as if they are destined for another interface (identical to Case 1). Again note that the IP Firewall command must be enabled for ACP processing.

Case 3: Packets that travel from interfaces without a configured policy-class to interfaces that do:

These packets are routed normally and are not processed by the ACP.

Case 4: Packets that travel from interfaces without a configured policy-class to other interfaces without a configured policy-class:

This traffic is routed normally. The **IP firewall** command has no effect on this traffic other than to prevent attacks entering the interface.

Attack Protection

In order to configure access policies, the **IP firewall** must be enabled. Firewall attack protection is enabled with the **IP firewall** command. The ADTRAN OS blocks IP traffic (matching patterns of known networking exploits) from traveling through the device. For some of these attacks, the user may manually disable checking/blocking, while other attack checks are always on anytime the firewall is enabled. For more information on the function of the **IP firewall** command, refer to the document, IP Firewall Command Tech Note.

Policy Examples

A few examples are now presented to clarify the use of policies.

The first example demonstrates the NetVanta 3200 router configuration for a simple network that allows the LAN to get to the Internet, but blocks unwanted traffic from the Internet. The second example shows how to modify the configuration to allow traffic to a webserver from the Internet. The third example explains how to modify the configuration to do Network Address Translation (NAT) from the Internet.

* Before You Begin

Prior to configuring access-policies your NetVanta router, obtain all necessary IP address assignments from the network administrator and Internet Service Provider (ISP) if applicable. All circuits should be installed and tested prior to the installation of your router. Although the example shown here may differ than your configuration, all the basic concepts associated with policies are presented. For gaining access to the Configuration Mode of the Netvanta 3000 Series Router, see Netvanta 3000 Series Quick Start Guide Other documents that may be beneficial include: IP Firewall Command Tech

Note, NetVanta Command Reference Guide, and Configuring Network Address Translation for the NetVanta 3200. For additional assistance please contact ADTRAN Technical Support.

Simple configuration, no NAT

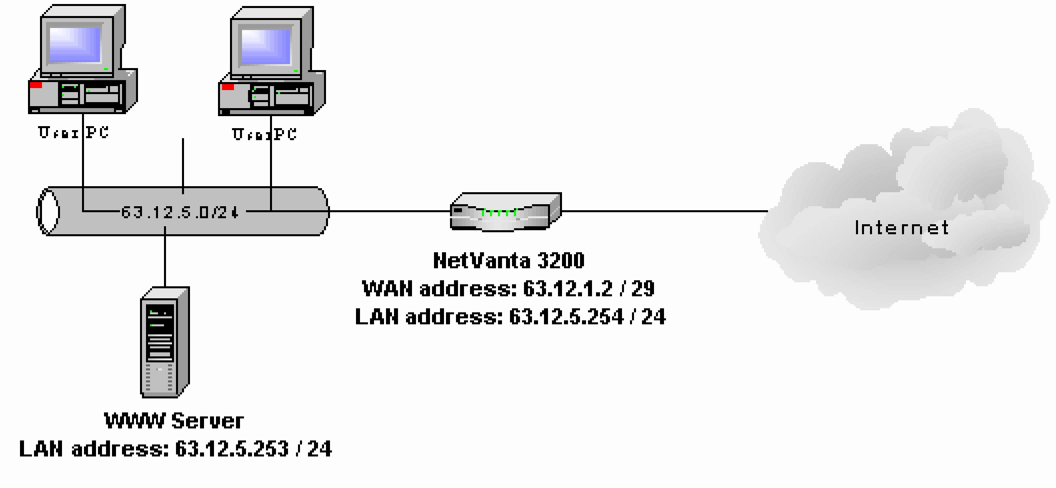
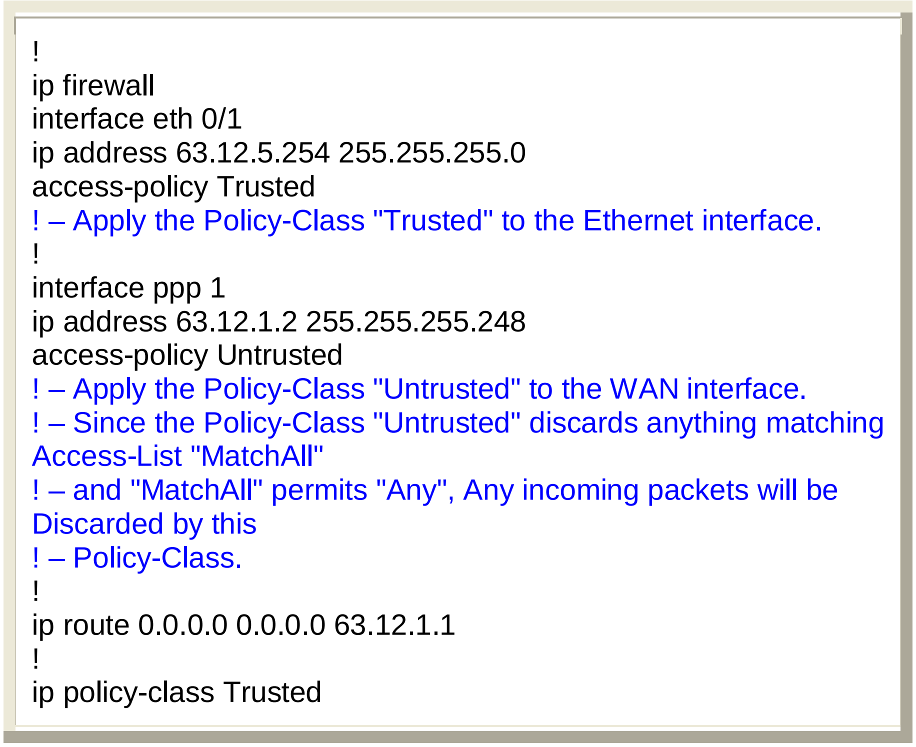

User PC
User PC
63.12.5.0/24
NetVanta 3200
WAN address: 63.12.1.2 / 29
LAN address: 63.12.5.254 / 24
Internet
WWW Server
LAN address: 63.12.5.253 / 24

Figure 1 Simple example

This is a simple network using public IP addresses on the LAN. The Netvanta 3200 configuration allows the LAN traffic to reach the Internet, but doesn’t allow traffic from the Internet to reach the LAN unless it matches the outbound sessions already created.



```
!
ip firewall
interface eth 0/1
ip address 63.12.5.254 255.255.255.0
access-policy Trusted
! – Apply the Policy-Class "Trusted" to the Ethernet interface.
!
interface ppp 1
ip address 63.12.1.2 255.255.255.248
access-policy Untrusted
! – Apply the Policy-Class "Untrusted" to the WAN interface.
! – Since the Policy-Class "Untrusted" discards anything matching
Access-List "MatchAll"
! – and "MatchAll" permits "Any", Any incoming packets will be
Discarded by this
! – Policy-Class.
!
ip route 0.0.0.0 0.0.0.0 63.12.1.1
!
ip policy-class Trusted
```

```
allow list MatchAll
! – Create the Policy-Class "Trusted".
! – For any interface using Policy-Class "Trusted" allow Access-
List "MatchAll".
! – Since the Policy-Class "Trusted" allows anything matching
Access-List "MatchAll"
! – and "MatchAll" permits "Any", Any incoming packets will be
Allowed by this
! – Policy-Class.
!
ip policy-class Untrusted
discard list MatchAll
! – Create the Policy-Class "Untrusted".
! – For any interface using Policy-Class "Untrusted" discard
Access-List "MatchAll".
!
ip access-list standard MatchAll
permit any
! – Create the Access-List "MatchAll".
! – Permit any IP address.
!
```

The next example adds inbound access to the Web server. Changes to the configuration are in bold.

```
!
ip firewall
interface eth 0/1
ip address 63.12.5.254 255.255.255.0
access-policy Trusted
!
interface ppp 1
ip address 63.12.1.2 255.255.255.248
access-policy Untrusted
!
ip route 0.0.0.0 0.0.0.0 63.12.1.1
!
ip policy-class Trusted
allow list MatchAll
!
ip policy-class Untrusted
allow list InWeb
```

```
discard list MatchAll
! – Allow any traffic that matches Access-List "InWeb",
! – Before discarding any traffic that matches Access-List
"MatchAll".
!
ip access-list standard MatchAll
permit any
!
ip access-list extended InWeb
permit tcp any host 63.12.5.253 eq 80
! – Create Extended Access-List "InWeb"
! – Permit any TCP traffic with a destination address of
63.12.5.253 and a destination port of 80 (HTTP).
!
```

Simple configuration with NAT and webserver access.

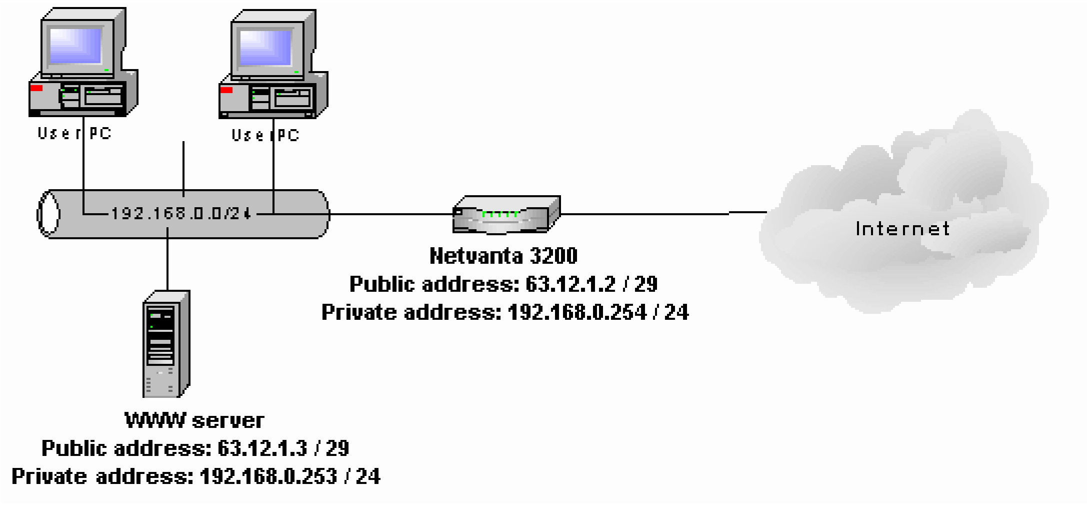

User PC
User PC
192.168.0.0/24
Netvanta 3200
Public address: 63.12.1.2 / 29
Private address: 192.168.0.254 / 24
Internet
WWW server
Public address: 63.12.1.3 / 29
Private address: 192.168.0.253 / 24

Figure 1 Simple example plus NAT

This is a simple network using private IP addresses on the LAN and providing NAT on the WAN interface to the Internet. The Netvanta 3200 configuration allows the LAN traffic to reach the Internet by doing NAT. Traffic from the Internet is discarded unless it matches the outbound sessions already created, or has a destination address and port that matches the webserver.

```
!
ip firewall
interface eth 0/1
ip address 192.168.0.254 255.255.255.0
access-policy Trusted
! – The IP address is changed to the private address scheme.
!
interface ppp 1
ip address 63.12.1.2 255.255.255.248
access-policy Untrusted
!
ip route 0.0.0.0 0.0.0.0 63.12.1.1
!
ip policy-class Trusted
nat source list MatchAll address 63.12.1.2 overload
! – Enable NAT for traffic that matches Access-List "MatchAll"
and change
! - the source address to 63.12.1.2
!
ip policy-class Untrusted
nat destination list InWeb address 192.168.0.253
discard list MatchAll
! – Enable NAT for traffic that matches Access-List "InWeb" and
change
! - the destination address 192.168.0.253
!
ip access-list standard MatchAll
permit any
!
ip access-list extended InWeb
permit tcp any host 63.12.1.3 eq 80
! – Create Extended Access-List "InWeb"
! – Permit any TCP traffic with a destination address of 63.12.1.3
and a destination port of 80 (HTTP).
!
```

If you experience any problems using your ADTRAN product, please contact ADTRAN Technical Support.

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.