6AOSCG0039-29B
September 2012

ADTRAN

Configuration Guide

Security Best Practices for AOS Products

This configuration guide provides the best security practices for ADTRAN Operating System (AOS) products. Included in this guide are descriptions of the recommendations, detailed steps with examples, and a summary of all recommendations. The configuration instructions in this guide use the command line interface (CLI).

This guide consists of the following sections:

Overview

The technical recommendations in this guide are intended to help network administrators improve the security of their networks when configuring AOS products. The guidelines presented consist of recommended security best practices and as such should be implemented within the context of an organization's own security policies. Following the recommendations in this guide does not guarantee against security breaches. It is up to customers and their responsible department(s) to determine which, if any, of these practices to implement depending on their network configuration and access.

This document explains best practices for the following areas:

Each section of this document begins with a list of the best practices, which are then discussed in detail with examples in the rest of the section.

System security relies on the proper configuration of many AOS features and network configurations. It is not the goal of this guide to fully document all available options for these features and configurations. Refer to *Additional Resources on page 36* for a list of helpful documents that provide additional information on the topics covered in this guide.

For your convenience, *Appendix A. Security Configuration Summary on page 38* contains a summary of all the recommendations in this document.

Hardware and Software Requirements and Limitations

The security features discussed in this document apply to AOS products as outlined in the *AOS Feature Matrix* available from the ADTRAN Support Community (https://supportforums.adtran.com). Some commands are interface specific and may not be available on all platforms listed. Use the online help (? in the CLI) to determine if a command is supported by your hardware platform.

The commands used in this document are based on R10.1.0. If you are using a different version, use the appropriate commands for that version. In addition, this document addresses only IPv4 functionality.

CLI Access

The configuration instructions in this guide use the CLI. To access the CLI on your AOS unit, follow these steps:

1. Boot the unit.
2. Connect to the unit via Secure Shell (SSH) or the console port. If using the console port, skip to Step 4.
3. Enter your user name and password at the prompt.

> NOTE *If you have not changed the AOS default user name (**admin**) and password (**password**), please do so now. Refer to Local User Accounts on page 24 for information on changing the default password.*

4. Enter Enable mode on your unit by entering **enable** at the prompt as follows:

```
>enable
```

5. Enter your Enable mode password at the prompt.

> NOTE *If you have not done so, change the Enable mode password from the default (**password**). Refer to Enable Mode Password on page 25 for information on setting a password for Enable mode.*

6. Enter the unit's Global Configuration mode as follows:

```
#configure terminal
(config)#
```

Data Security

Recommendations for improved data security include:

1. Enable the firewall. (Refer to *Firewall Configuration Steps on page 9*.)
2. Ensure that all access control lists (ACLs) in the access control policy (ACP) are defined and not empty. (Refer to *Access Control Lists and Access Control Policies on page 6*.)
3. Use unique ACPs for the private, public, demilitarized zone (DMZ), and any other zones. Refer to *Example Configuration - Firewall with DMZ on page 16* for an example configuration with unique ACPs for private, public, and DMZ zones.
4. Define ACP entries to allow only the most specific and narrow range of traffic necessary. (Refer to *Access Control Lists and Access Control Policies on page 6*.)
5. Define ACP entries to specify a destination ACP. (Refer to *Access Control Lists and Access Control Policies on page 6*.)
6. Specify the smallest range of traffic possible when it is necessary to disable stateful processing. (Refer to *Stateful Inspection on page 6*.)

7. Apply ACPs to an interface. (Refer to *Step 5: Applying the ACP to an Interface on page 15*.)
8. Use the default event message display priority level. (Refer to *Firewall Event Messages on page 17*.)
9. For units on which the default route goes out the public interface, specify a high administrative distance route that routes to null 0 for any private subnets to which a static route exists. (Refer to *High Administrative Distance Route for Statically Routed Private Subnets on page 20*.)
10. Specify a Domain Name System (DNS) server when IP domain lookup is enabled. (Refer to *DNS Lookup and Proxy on page 20*.)
11. Ensure that the DNS proxy is disabled if it is not needed. (Refer to *DNS Lookup and Proxy on page 20*.)

> **NOTE** *NetVanta switches and the NetVanta 600 Series gateways either do not have or do not support the firewall. For these products, all security recommendations apply except those relating to the firewall and ACPs.*

For a list of all security recommendations, including a command summary and the default settings, refer to *Appendix A. Security Configuration Summary on page 38*.

Firewall Features

A firewall provides a first line of defense against potential security threats by enforcing access control parameters between an internal (trusted) network and any other (untrusted) network such as the Internet. When enabled, the firewall performs attack checking and stateful inspection on traffic destined to and routed through the unit. Refer to *Attack Checking on page 4* and *Stateful Inspection on page 6* for more information on these features.

The firewall filters inbound packets to ensure that only matching packets pass. The firewall can filter packets at several Open System Interconnection (OSI) levels and uses ACLs and ACPs to enforce complex, customized policies. Refer to *Access Control Lists and Access Control Policies on page 6* for more information.

The AOS firewall is disabled by default. Refer to *Firewall Configuration Steps on page 9* for a list of the basic steps to enable and configure the firewall, including creating ACLs and ACPs.

For an in-depth discussion of the IPv4 firewall, refer to the configuration guide *IPv4 Firewall Protection in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).

Attack Checking

Through attack checking, the firewall detects and blocks traffic that matches profiles of known networking exploits and attacks. If the firewall detects an attack, the unit generates an attack log message and blocks the attack. Refer to *Appendix B. Attack Log Messages on page 47* for more information on attack log messages.

Table 1 outlines the types of traffic blocked by the firewall. Since many attacks use similar invalid traffic patterns, attacks other than the examples listed in the table could also be blocked by the firewall.

Table 1. Traffic Blocked by IPv4 Firewall Attack Protection Engine

Invalid Traffic Pattern	AOS IPv4 Firewall Response	Common Attacks
Larger than allowed packets	Any packets that are larger than those defined by standards will be dropped.	Ping of Death
Fragmented IP packets that produce errors when attempting to reassemble	The firewall intercepts all fragments for an IP packet and attempts to reassemble them before forwarding to the destination. If any problems or errors are found during reassembly, the fragments are dropped.	SynDrop, TearDrop, OpenTear, Nestea, Targa, Newtear, Bonk, Boink
Smurf Attack	The firewall drops any Internet Control Message Protocol (ICMP) ping and User Datagram Protocol (UDP) echo responses that are not part of an active session.	Smurf Attack
IP Spoofing	The firewall drops any packets with a source IPv4 address that appears to be spoofed. The IPv4 route table is used to determine if a path to the source address is known (out of the IP interface from which the packet was received). For example, if a packet with a source IPv4 address of 10.10.10.1 is received on interface FR 1.16 and no route to 10.10.10.1 (through interface FR 1.16) exists in the route table, the packet is dropped. Traffic that bypasses spoofing checks includes packets from the router itself, Dynamic Host Configuration Protocol (DHCP) traffic, multicast and routing protocol traffic, and Virtual Router Redundancy Protocol (VRRP) traffic. Spoofing detection can be turned off on individual ACPs to allow policy-based routing (PBR) or for any other case in which it would drop traffic that should not be dropped.	IP Spoofing
ICMP Control Message Floods and Attacks	The following types of ICMP packets are allowed through the firewall: echo, echo-reply, timestamp, timestamp reply, time to live (TTL) expired, dest unreachable, and quench. These ICMP messages are only allowed if they appear to be in response to a valid session. All others are discarded.	Twinge
Attacks that send Transmission Control Protocol (TCP) URG packets	Any TCP packets that have the urgent (URG) flag set are discarded by the firewall.	WinNuke, TCP XMAS Scan
Falsified IP Header Attacks	The firewall verifies that the packet's actual length matches the length indicated in the IPv4 header. If it does not, the packet is dropped.	Jolt/Jolt2
Land Attack	Any packets with the same source and destination IPv4 addresses are discarded.	Land Attack
Broadcast Source IP	Packets with a broadcast source IPv4 address are discarded.	
Invalid TCP Initiation Requests	Initial TCP synchronize (SYN) packets that have acknowledge (ACK), URG, reset (RST), or finished (FIN) flags set are discarded.	

Table 1. Traffic Blocked by IPv4 Firewall Attack Protection Engine *(Continued)*

Invalid Traffic Pattern	AOS IPv4 Firewall Response	Common Attacks
Invalid TCP Segment Number RST	The sequence numbers for active TCP sessions are maintained in the firewall session database. If the firewall receives an RST segment with an unexpected (or invalid) sequence number, the packet is dropped.	
IP Source Route Option	All packets containing the IP source route option are dropped.	

Stateful Inspection

When enabled, the AOS firewall performs stateful inspection on traffic destined to and routed through the unit. The stateful inspection firewall creates an association for each session and stores this information in an internal database, providing the firewall with detailed information about the current state of every session flowing through the unit. When the firewall receives the first packet in a unique stream, it calculates the appropriate action to perform on the packet. Through the use of firewall associations, the AOS device can simply look at subsequent packets in a stream, note that the packets look the same as the first, and perform the calculated action upon them. Firewall associations increase the speed of packet throughput because the AOS device does not have to perform the matching process for every packet that comes through the firewall.

Using the **stateless** keyword on an ACL in an ACP bypasses the stateful firewall processing and application-level gateways (ALGs) for traffic that matches that ACL. With stateless processing, each packet is processed independently from previous packets (except that attack checks might be performed). If stateful processing must be disabled, do so for only smallest range of traffic possible.

For more information on configuring and using ACLs and ACPs, refer to *Access Control Lists and Access Control Policies on page 6*.

Access Control Lists and Access Control Policies

ACLs and ACPs regulate traffic through the routed network. When designing your traffic flow configuration, it is important to keep the following in mind:

- An ACL serves as a packet selector.
- An ACP defines the action to take on the packets selected by the ACL.
- An ACL is inactive until it is assigned to an active ACP.
- An ACP is inactive until it is assigned to an interface and the firewall is enabled.
- Both ACL and ACP entries are processed from the top down; typically, the most specific entries should be at the top and the most general at the bottom.

ACLs

ACLs compare IP traffic to a list of specified criteria and determine if that traffic matches the criteria. ACLs are used for packet matching in many AOS filtering and security features, including the firewall, virtual private network (VPN), and quality of service (QoS). ACLs allow these features to logically inspect each IP packet, compare it to the set of criteria listed in the ACL, and then take the appropriate action with the packet.

Each ACL entry begins with either a **permit** or **deny** keyword. The **permit** keyword allows packets meeting the specified pattern to be processed by the feature using the ACL (in the case of the firewall, an ACP). The **deny** keyword causes packets meeting the specified pattern to advance to the next ACP entry until a match is made.

When an ACL is being used to inspect an IP packet, the entries in the ACL are processed from top-to-bottom, in the order in which the entries were added to the ACL. If an IP packet does not match the criteria specified by a certain entry, then it is compared to the criteria in the next entry. If a packet does not match any of the entries, it is implicitly denied.

*An empty ACL with no **permit** or **deny** entries will implicitly permit everything. Therefore, ensure that all ACLs in the ACP are defined and not empty.*

There are two types of ACLs:

- **Standard ACL -** The only field in the packet inspected by standard ACLs is the source address. Packets sent from specific subnets or specific hosts can be specified as either **permit** or **deny**. The **any** keyword is used to specify either a **permit** or a **deny** of all packets. For standard ACLs (but not extended), an ACL cache is created to speed up the packet matching process.
- **Extended ACL -** An extended ACL can inspect a number of fields in the packet. These include protocol, source and destination addresses, source and destination ports, and most fields in the TCP and ICMP headers. The **any** keyword can be used in reference to the packet's source, destination, or both.

For detailed steps to create and define ACLs, refer to *Step 3: Creating an ACL and Defining Permissions on page 9*.

See also *SIP Access Class on page 22*, *Management Interface Access Classes on page 27*, and *SNMP Groups and Users on page 29* for additional uses of ACLs.

For more information on ACLs in general, refer to the configuration guides *IP ACLs in AOS* and *IPv4 Firewall Protection in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).

ACPs

When a packet is received on an interface, the configured ACP is applied to determine what action to take on the packet. Each ACP consists of an action (**allow**, **discard**, **nat**) and a selector (ACL). In addition, an

ACP entry can specify a destination ACP to match as part of its rule. After inspecting traffic, the ACP performs one of four actions:

- The **allow** keyword permits traffic through the firewall without changing the IP packet's source or destination IPv4 addresses or Layer 4 ports.
- The **discard** keyword drops the traffic.
- The **nat source** keyword translates the source IPv4 address to a specified IPv4 address (or to the primary IPv4 address of the specified interface) and creates an association in the firewall.
- The **nat destination** keyword translates the destination IPv4 address to a specified IPv4 address and creates an association in the firewall.

ACPs are order dependent. When an IPv4 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. Typically, the most specific entries should be at the top and the more general at the bottom.

Every inbound interface can have only one associated ACP. Typically, an ACP is configured on the internal interface that permits hosts to initiate traffic to the Internet, often by using network address translation (NAT). A second ACP is configured on the public interface that discards all unnecessary traffic initiated from the Internet. When the device on the Internet sends a response back to the host, the AOS stateful inspection firewall recognizes that this traffic is associated with an allowed session and allows the traffic to pass through. 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.

There are several types of ACPs:

- **Self** - The self ACP handles traffic whose source or destination is the router itself. This ACP is unique and cannot be deleted.
- **Default** - The default ACP is applied to every interface that does not have a user-defined ACP applied and allows all traffic while performing stateful checks with **ip firewall** enabled. It will allow all traffic while performing stateless checks if **ip crypto** is enabled while **ip firewall** is disabled. The default ACP is unique and cannot be deleted.
- **User-defined** - A user-defined ACP is defined by the user. AOS supports up to 20 user-defined ACPs.

When defining ACPs, observe the following guidelines:

- Define ACP entries to allow only the most specific and narrow range of traffic necessary.
- Use unique ACPs for the private, public, DMZ, and any other zones. Refer to *Example Configuration - Firewall with DMZ on page 16* for an example configuration file with unique ACPs for private, public, and DMZ zones.

Referencing an ACP that doesn't exist denies all traffic, but referencing an ACL that doesn't exist matches all traffic. In addition, an empty ACP implicitly denies all traffic.

For detailed steps to create and define ACPs, refer to *Step 4: Creating and Defining an ACP on page 11*.

Firewall Configuration Steps

The following section provides the basic steps necessary to enable the firewall and create ACLs and ACPs through the CLI.

Step 1: Accessing the CLI

Access the CLI as described in *CLI Access on page 3*.

Step 2: Enabling the Firewall

From the Global Configuration mode, use the **ip firewall** command to enable the AOS firewall, which provides security features including ACPs, NAT, and stateful inspection. The firewall is disabled by default. For example:

(config)**#ip firewall**

Step 3: Creating an ACL and Defining Permissions

Create an IPv4 ACL and configure it to permit or deny specific traffic. This step determines whether you are creating a standard ACL (matching on source information) or an extended ACL (matching on multiple criteria). This step also enters the configuration mode for the IPv4 ACL.

IPv4 ACPs must use IPv4 ACLs. You cannot apply an IPv4 ACL to an IPv6 ACP, or vice-versa. In addition, all IPv4 ACLs and IPv4 ACPs must have a different name than any configured IPv6 ACLs or IPv6 ACPs.

Create an ACL

From the Global Configuration mode, use the **ip access-list** command to create either a standard or extended IPv4 ACL and enter the IPv4 Access Control List Configuration mode. For example:

(config)**#ip access-list [extended | standard]** <*ipv4 acl name*>

The <*ipv4 acl name*> parameter names the configured IPv4 ACL using an alphanumeric descriptor that will be referenced within an ACP.

Define Permissions

To configure a **standard** IPv4 ACL, specify the packet source information and decide whether the feature using the IPv4 ACL will **permit** or **deny** matching traffic using the following command:

(config-std-nacl)**#[permit | deny]** <*source*> **[log] [track** <*name*>**]**

To configure an **extended** IPv4 ACL, specify whether the feature using the ACL will **permit** or **deny** matching traffic based on protocol, source information, and destination information using the following command:

(config-ext-nacl)#**[permit | deny]** <*protocol*> <*source*> <*source port*> <*destination*> <*destination port*> **[log] [track** <*name*>**]**

Each ACL has an implicit deny any as the last criteria if there are other entries within the ACL. An empty ACL is an implicit permit any.

The <*protocol*> parameter specifies the data protocol used by the packet. Valid entries are **ip**, **icmp**, **tcp**, **udp**, **ahp**, **esp**, **gre**, or a specific protocol. Range is **0** to **255**.

The <*source*> parameter specifies the source used for packet matching. Sources can be expressed in one of four ways:

- Using the keyword **any** to match any IPv4 address.
- Using the **host** <*ipv4 address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
- Using the <*ipv4 address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are also expressed in dotted decimal notation (for example, **0.0.0.255**) and they work in reverse logic from subnet masks. When broken out into binary form, a **0** indicates which bits of the IPv4 address to consider, and a **1** indicates which bits are disregarded. For example, specifying 255 in any octet of the wildcard mask equates to a *don't care* for that octet in the IPv4 address. Additionally, a 30-bit mask would be represented with the wildcard string **0.0.0.3**, a 28-bit mask with **0.0.0.15**, a 24-bit mask with **0.0.0.255**, and so forth.
- Using the keyword **hostname** <*hostname*> to match traffic based on a DNS name. The unit must be configured with DNS servers using the Global Configuration mode command **name-server** <*ipv4 address*> for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VPN routing and forwarding (VRF) with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source. The command in this case would appear:

  (config-ext-nacl)#**[permit | deny] hostname** <*hostname*> **[vrf** <*name*>**] [track** <*name*>**] [log]**

The <*source port*> parameter is optional, and allows you to specify the matched traffic source port. The source port is used only when the <*protocol*> is specified as **tcp** or **udp**. The following selections are available for specifying source port information:

- Using the keyword **any** matches any port.
- Using the keyword **eq** <*port number/name*> matches only packets equal to a specified source port number.
- Using the keyword **gt** <*port number/name*> matches only packets with a source port number greater than the specified number.
- Using the keyword **lt** <*port number/name*> matches only packets with a source port number less than the specified number.

- Using the keyword **neq** <*port number/name*> matches only packets that are not equal to the specified source port number.
- Using the keyword **range** <*starting port number/name*> <*ending port number/name*> matches only packets that contain a source port number in the specified range.

  The <*port number/name*> parameter specifies the port number or name used by TCP or UDP to pass information to upper layers. The valid range for port numbers is from **0** to **65535**. All ports below **1024** are considered well-known ports, and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above **1024** are dynamically assigned ports that include registered ports for vendor-specific applications. Some UDP and TCP ports can also be entered by port name. If the **range** keyword is used, two port values must be entered. For a list of valid entries, refer to the *AOS Command Reference Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).

The <*destination*> parameter specifies the destination used for packet matching. Destinations can be expressed in the same four ways as the source information.

The <*destination port*> parameter is optional, and allows you to specify the monitored traffic destination port. The destination port is used only when the <*protocol*> is specified as **tcp** or **udp**. The same selections available for source port selection are available for destination port selection.

The optional **track** <*name*> parameter associates the IPv4 ACL entry with a particular track. This track can be used to disable the entry in case of certain events specified by the track.

The optional **log** parameter specifies that any entries that match the IPv4 ACL criteria will be logged.

For more information on ACLs, refer to the configuration guide *IP ACLs in AOS* or the *AOS Command Reference Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).

Step 4: Creating and Defining an ACP

Create ACPs to allow, discard, or NAT traffic for each routable IP interface. To create an IPv4 ACP, enter the following command from the Global Configuration mode and enter the IPv4 Access Control Policy Configuration mode:

```
(config)#ip policy-class <ipv4 acp name>
(config-policy-class)#
```

The <*ipv4 acp name*> parameter identifies the configured IPv4 ACP using an alphanumeric descriptor (maximum of 50 characters). All ACP names are case sensitive.

Once the ACP is created, configure the action(s) to take when traffic has been received on the interface. Traffic can be permitted to enter the interface by using the **allow list** command or discarded by using the **discard list** command. The source or destination address and port can be translated to a specified address by using the **nat source list** or **nat destination list** commands, respectively.

These commands are covered in detail in the following sections:

- *Allow Traffic Based on IPv4 ACL Entries on page 12*
- *Discard Traffic Based on IPv4 ACL Entries on page 12*
- *Apply NAT to the Destination IPv4 Address on page 13*
- *Apply NAT to the Source IPv4 Address on page 14*

Allow Traffic Based on IPv4 ACL Entries

Use the **allow list** command from the IPv4 Access Control Policy Configuration mode to specify an IPv4 ACL to determine which IP packets are allowed to enter the interface to which the IPv4 ACP is assigned, and create a policy session in the IPv4 firewall. All firewall policy sessions are subject to the built-in firewall timers. Additional conditions further define how the traffic is handled and are explained in the following paragraphs.

(config-policy-class)**#allow list** <*ipv4 acl name*> **[self | policy** <*ipv4 acp name*>**] [stateless]**

The **allow reverse list** command is identical in function to the **allow list** command, except the **reverse** keyword instructs the firewall to use the source information as the destination information and vice versa when attempting matches against the specified IPv4 ACL. This command is most useful when the IPv4 ACP is applied to an interface terminating a VPN tunnel. The **allow reverse list** allows the reuse of the IPv4 ACL defined as the VPN selector.

(config-policy-class)**#allow reverse list** <*ipv4 acl name*> **[self | policy** <*ipv4 acp name*>**] [stateless]**

The **self** parameter allows all IP packets matched by the IPv4 ACL and destined for any local IP address on the unit to enter the router system. These packets are terminated by the unit and are not routed or forwarded to other destinations. Using the **self** parameter is helpful when opening remote administrative access to the unit (Telnet, SSH, ICMP, Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), etc.).

The **policy** <*ipv4 acp name*> parameter specifies the destination IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the IP packet's egress interface as determined by the routing table or PBR configuration. This allows configurations to permit packets routed out interfaces in specific security zones, but not the entire system.

The **stateless** parameter is optional and enables bypassing stateful firewall processing and ALGs. It is used for trusted traffic or traffic that the firewall is incorrectly blocking as a perceived attack. Stateless processing is helpful when passing traffic over VPN tunnels. Traffic sent over VPN tunnels is purposely selected and encrypted; there is usually no need for additional inspection of the traffic by the firewall. VPN configurations created using the VPN Wizard in the GUI use stateless processing by default. If voice quality monitoring (VQM) is being used over VPN, the selectors cannot be stateless.

The following example configures the IPv4 ACP named **UNTRUSTED** to allow any traffic that matches the IPv4 ACL named **INWEB** to enter the router system:

(config)**#ip policy-class UNTRUSTED**
(config-policy-class)**#allow list INWEB**

Discard Traffic Based on IPv4 ACL Entries

Use the **discard list** command to specify an IPv4 ACL to determine which IPv4 packets are discarded after being received on the interface to which the IPv4 ACP is assigned. IP packets matched by the IPv4 ACL

will be discarded, and no further ACP entries will be inspected. All IP packets not matched by the IPv4 ACL are processed by the next ACP entry or implicitly discarded if no further ACP entries exist.

(config)#**discard list** <*ipv4 acl name*> **[self | policy** <*ipv4 acp name*>**]**

The **self** parameter discards IPv4 packets that are matched by the IPv4 ACL and destined for any local interface on the unit. These packets, had they been allowed, would be terminated by the unit and not routed or forwarded to other destinations. Using the **self** keyword is helpful when forbidding certain access to the unit.

The **policy** <*ipv4 acp name*> parameter specifies the destination IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the IP packet's egress interface as determined by the routing table or PBR configuration. The **policy** parameter causes all IP packets matched by the IPv4 ACL and destined for the interface using the specified IPv4 ACP to be discarded. If there is no match, the firewall will process the IPv4 packet based on the next ACP entry or implicitly discard it if no further ACP entries exist.

The following example configures the IPv4 ACP named **UNTRUSTED** to discard any traffic that matches the IPv4 ACL named **BLOCK**:

(config)#**ip policy-class UNTRUSTED**
(config-policy-class)#**discard list BLOCK**

*The IPv4 ACL named **BLOCK** in this example would have to use **permit** statements to specify the matched traffic that will be discarded in the ACP. If **deny** statements were used in the IPv4 ACL, it would cause the next rule in the ACP to be processed instead of dropping the desired traffic.*

Apply NAT to the Destination IPv4 Address

Use the **nat destination list** command to translate the destination IPv4 address to a specified IPv4 address, and create a firewall policy session. The translation is applied only to those IP packets permitted by the specified IPv4 ACL and entering the interface to which the IPv4 ACP is assigned. All firewall policy sessions are subject to the built-in firewall timers.

(config-policy-class)#**nat destination list** <*ipv4 acl name*> **address** <*ipv4 address*> **[vrf** <*name*> **|**
port <*port number*>**] [no-alg]**

The **address** <*ipv4 address*> parameter specifies the address of the internal IP host to which the translated IPv4 packets are destined. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

The optional **port** <*port number*> parameter translates the original destination port to a user-specified port.

The optional **vrf** <*name*> parameter specifies the VRF instance. The VRF does not have to be the same VRF from which the IPv4 packet originated. VRF on an AOS product allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Therefore, executing the above mentioned commands without specifying a VRF indicates that the specified IPv4 address corresponds to the default unnamed VRF. For more information, refer to *Configuring IPv4 Multi-VRF in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).

The optional **no-alg** parameter allows IP packets matching the IPv4 ACP entry to traverse the firewall without being processed by the ALGs. This parameter, along with the appropriate IPv4 ACL, prevents specific traffic from being processed by the ALGs.

The following example enables NAT for traffic that matches the ACL **INWEB** and changes the destination IPv4 address to **192.168.0.253**:

```
(config)#ip policy-class UNTRUSTED
(config-policy-class)#nat destination list INWEB address 192.168.0.253
```

The **nat destination list** <*ipv4 acl name*> **pool** command is used in conjunction with NAT pools. NAT pools are used to translate IPv4 addresses between a specified internal range and a specified public range for a static one-to-one mapping of addresses. NAT pools is a feature that is outside the scope of this document.

```
(config-policy-class)#nat destination list <ipv4 acl name> pool <pool name> [no-alg]
```

For more information on NAT pools, refer to the configuration guide NAT Pools in AOS available from the ADTRAN Support Community (https://supportforums.adtran.com).

Apply NAT to the Source IPv4 Address

Use the **nat source list** command to translate the source IPv4 address to a user specified IPv4 address (or to the primary IPv4 address of the specified interface) and create a firewall policy session. The NAT is applied only to IP packets permitted by the specified IPv4 ACL, and entering the interface to which the IPv4 ACP is assigned. This function is commonly referred to as a many:1 and is typically used to enable Internet access for hosts on a privately addressed subnet. All firewall policy sessions are subject to the built-in firewall timers.

```
(config-policy-class)#nat source list <ipv4 acl name> [address <ipv4 address> | interface
<interface>] overload [policy <ipv4 acp name>] [no-alg]
```

The **address** <*ipv4 address*> parameter specifies the IPv4 address the translated IP packets should be sourced from. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

The **interface** <*interface*> parameter specifies the interface from which the translated packets will be sourced. The primary IPv4 address of an interface is used as the source IPv4 address for translated packets. Specify an interface in the format <*interface type* [*slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id*]>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **nat source list** <*ipv4 acl name*> **interface ?** for a list of valid interfaces.

The **overload** parameter allows multiple source IPv4 addresses to be replaced with the single IPv4 address specified or the primary IPv4 address of the specified interface. This conceals internal IPv4 addresses from outside the local network. The **overload** parameter is required when using the **nat source list** command with a single IPv4 address or interface.

The optional **policy** <*ipv4 acp name*> parameter specifies the IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the IP packet's egress interface as determined by the routing table or PBR configuration. If there is a match, the firewall will process the packet. If there is no match, the firewall will process the packet based on the next ACP entry or implicitly discard it if no further ACP entries exist.

The optional **no-alg** parameter allows IP packets matching the IPv4 ACP entry to traverse the firewall without being processed by the ALGs. This parameter, along with the appropriate IPv4 ACL, prevents specific traffic from being processed by the ALGs.

The **nat source list** <*ipv4 acl name*> **pool** command is used in conjunction with NAT pools. NAT pools are used to translate IPv4 addresses between a specified internal range and a specified public range for a static one-to-one mapping of addresses. NAT pools is a feature that is outside the scope of this document.

(config-policy-class)**#nat source list** <*ipv4 acl name*> **pool** <*pool name*> **[policy** <*ipv4 acp name*>**] [no-alg]**

For more information on NAT pools, refer to the configuration guide NAT Pools in AOS available from the ADTRAN Support Community (https://supportforums.adtran.com).

Step 5: Applying the ACP to an Interface

Before applying an IPv4 ACP to an interface, verify your Telnet or SSH connection will not be affected by the policy. If an ACP is applied to the interface through which you are connecting and it does not allow Telnet or SSH traffic, your connection will be lost.

To assign an IPv4 ACP to an interface, enter the appropriate interface configuration mode, and apply the ACP to the interface:

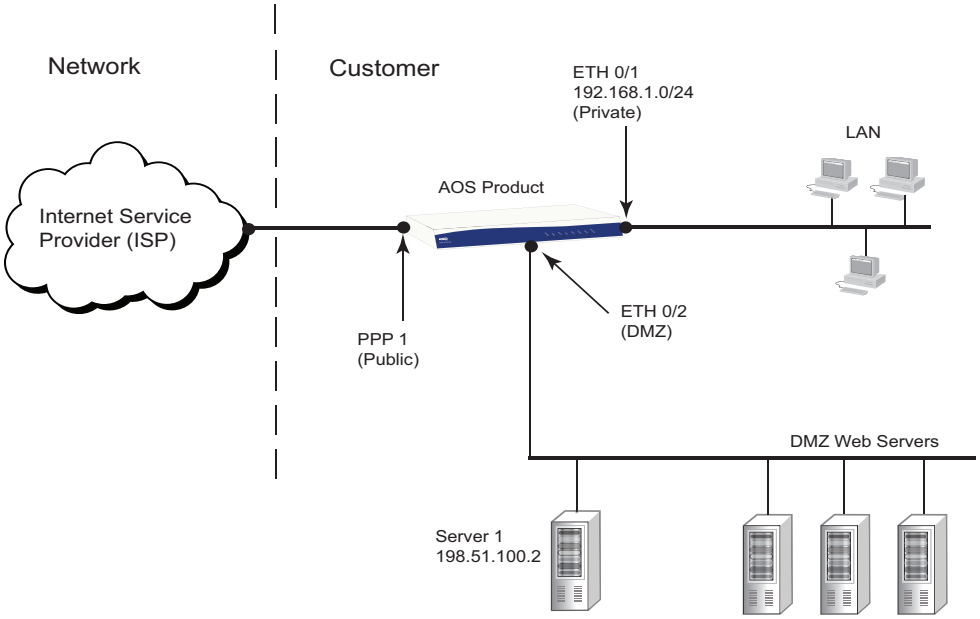
(config)**#interface** <*interface*>
(config-interface)**#ip access-policy** <*ipv4 acp name*>

The <*interface*> parameter specifies the physical or virtual interface on an AOS unit. For more information on using the **interface** command, refer to the *AOS Command Reference Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).

For information on all of the options available when configuring an IPv4 firewall, refer to the configuration guide *IPv4 Firewall Protection in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).

Example Configuration - Firewall with DMZ

The following example illustrates how you can quickly contain servers on a DMZ and ensure that infected servers cannot access your private network. This example describes typical hardware ACL applications in real-world settings. The configuration is done using the CLI. The configuration parameters entered in this example are a sample configuration only. You should configure these applications in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration example to provide you with a method of copying and pasting the configuration directly from this guide into the CLI. You should make the necessary adjustments to the configuration before adding it to your configuration to ensure it will function properly in your network.




```
!Example using policy classes Public, Private, and DMZ
!
ip access-list standard MATCHALL
  permit any
!
ip access-list extended DMZ_TRAFFIC
  permit tcp any 198.51.100.0 0.0.0.255 eq www
  permit tcp any 198.51.100.0 0.0.0.255 eq https

!
ip policy-class Private
  ! Allow traffic to the box from the trusted LAN
  allow list MATCHALL self
  ! Allow traffic to the DMZ
  !This rule only applies to traffic routed to an interface with policy class "DMZ"
  allow list MATCHALL policy DMZ
  ! NAT everything outbound to the Internet that uses the primary
  ! Internet connection (ppp 1)
  ! This rule only applies to traffic routed to an interface with policy class "Public"
  nat source list MATCHALL interface ppp 1 overload policy Public
```



```
  ! drop everything else
!
!
ip policy-class Public
  ! Allow all HTTP and HTTPS traffic to the DMZ
  allow list DMZ_TRAFFIC policy DMZ
  ! drop everything else
!
!
ip policy-class DMZ
  ! Allow everything outbound to the Internet that uses the primary
  ! Internet connection (ppp 1)
  allow list MATCHALL policy Public
  ! We do not want to allow traffic initiated from the DMZ to the
  ! Private policy class
  ! Since a policy class has an implicit discard at the end
  ! we do not have to do “discard list MATCHALL policy Private”
!
interface ppp 1
  ip address negotiated
  ip access-policy Public
!
interface eth 0/1
  ip address 192.168.1.254 255.255.255.0
  ip access-policy Private
!
interface eth 0/2
  ip address 198.15.100.254 255.255.255.0
  ip access-policy DMZ
!
```

Firewall Event Messages

There are multiple priority levels for event messages. You can manage these messages in several ways, based on their assigned priority level. The levels are listed below, from least critical to most critical.

Priority Level Number	Priority Level
5	Debug
4	Information
3	Notice
2	Warning
1	Error
0	Fatal

There are two management options for the event messages displayed on the console. The default behavior displays levels 0 to 4 (Fatal, Error, Warning, Notice, and Information level messages). Use the default event message display priority level. If levels have been disabled, use the **event-history priority** command to set the threshold for events stored in the event history. All events with the specified priority or higher will be kept for viewing in the local event log. The following example logs all events:

(config)**#event-history priority info**

To display events for all priority levels, issue the command **debug ip firewall**. Issue the **no debug ip firewall** command to stop displaying the events.

There are additional management options available for event history storage, email notification, and syslog forwarding. For more information on managing event message display, refer to the *IPv4 Firewall Protection in AOS* configuration guide available from the ADTRAN Support Community (https://supportforums.adtran.com).

Table 2. IPv4 Firewall Events

Event Message	Priority Level
All attack-log messages (Refer to *Appendix B. Attack Log Messages on page 47*.)	Error (1)
Service access request successful	Information (4)
No Access Policy matched, dropping packet	Information (4)
Deny Access Policy matched, dropping packet	Information (4)
Connection terminated. Bytes transferred: <*value*>	Information (4)
Connection closed. Bytes transferred: <*value*>	Information (4)
Connection timed out. Bytes transferred: <*value*>	Information (4)
Maximum number of global associations reached, dropping packet	Notice (3)
Maximum number of associations reached on <*policy-class name*> policy-class, dropping packet	Notice (3)
Available heap free does not allow for a new association, dropping packet	Notice (3)
Unable to initialize Association Protocol Info, deleting packet	Notice (3)
Unable to send SYNpacket	Notice (3)
Send final ACK to target failed	Notice (3)
Unable to get Port for Protocol <*protocol number*>	Notice (3)
ADFreeNatPort: Unable to get PortMap for NAT <*ip address:port*> Proto <*protocol number*> vrf <*name*>	Notice (3)
Unable to free Unknown Protocol NAT port for <*ip address:port*> vrf <*name*>	Notice (3)
Unable to free TCP NAT port for <*ipv4 address:port*> vrf <*name*>	Notice (3)
Unable to free UDP NAT port for <*ipv4 address:port*> vrf <*name*>	Notice (3)
Unable to free ICMP NAT port for <*ipv4 address:port*> vrf <*name*>	Notice (3)
Unable to free GRE NAT port for <*ipv4 address:port*> vrf <*name*>	Notice (3)
Unable to free Unknown Protocol NAT port for <*ipv4 address:port*> vrf <*name*>	Notice (3)
Attempt to de-register port map for unavailable NIP <*ipv4 address*><*ipv4 address*>	Notice (3)
ADLAddNatPort: Unable to get PortMap for NAT <*ipv4 address*> Proto <*protocol number*>	Notice (3)

Table 2. IPv4 Firewall Events *(Continued)*

ADLAddNatPort: Trying to add reference to unused port <*port*> for NAT <*ipv4 address*> Proto <*protocol number*>	Notice (3)
ADLAddNatPort: Trying to add reference to unreferenced port <*port*> for NAT <*ipv4 address*> Proto <*protocol number*>	Notice (3)
ADLDelNatPort: Port to free was not found for <*ipv4 address:port*>, vrf <*vrf id*>	Notice (3)
IGWGetPortByAlgId: Unable to get PortMap for NAT <*ipv4 address*> Proto <*protocol number*>	Notice (3)
IGWGetPortPairByAlgId: Unable to get PortMap for NAT <*ipv4 address*> Proto <*protocol number*>	Notice (3)
ADAlgRegisterNatPorts: Invalid Range StartPort <*port*> EndPort <*port*>	Notice (3)
ADAlgRegisterNatPorts: Trying to register twice. AlgId <*ALG id*> Protocol <*protocol number*>	Notice (3)
ADAlgRegisterNatPorts: Some ports in the specified Range already Registered AlgId <*ALG id*> Protocol <*protocol number*> StartPort <*port*> EndPort <*port*>	Notice (3)
NAT port pool helper cannot find pool for <*ipv4 address*> (vrf <*name*>) for deferred deletion	Notice (3)
Invalid FTP PASV cmd reply seen, dropping packet	Notice (3)
FTP Get port failed	Notice (3)
FTP PASV cmd response came without request, dropping packet	Notice (3)
H.323: Unable to get Nat port	Notice (3)
H.323: Failed to make H323_H245 Connection	Notice (3)
H.323: Failed to Allocate Nat Port	Notice (3)
H.323: Failed to make connection for H323T120	Notice (3)
H.323: Failed to make connection for H323RtpRtcp	Notice (3)
IRC: No of Messages are more than MAX_IRC_REQUESTS	Notice (3)
IRC: Size of Message is more than MAX_IRCSIZE	Notice (3)
IRC: Unable to create dynamic association for IRC	Notice (3)
Stored RPC transaction Id doesn't match server response, dropping packet	Notice (3)
RPC Server's response is undecipherable, dropping packet	Notice (3)
RTSP: Failed to Nat Port for RTSP connection	Notice (3)
RTSP: Failed to Create RTSP Data connection	Notice (3)
Not creating passive association with NAT port of zero	Notice (3)
ALGSipInit: Failed to set app process	Notice (3)
ALGSipProcess: Received non-SIP packet	Notice (3)
ALGSipProcess: Received unsupported SIP request (<*request*>)	Notice (3)
ALGSipProcess: ALGSipMangleMessage returned error	Notice (3)
ALGSipProcess: Failed to create association for RTP	Notice (3)
Unable to find Call-ID in message	Notice (3)
ALGSipMangleMessage: Unable to NAT Request-Line	Notice (3)
SIP ALG: Failed to add contact NAT port to RegPasv table	Notice (3)
ALGSipMangleMessage: Failed to add Undo information to NAT table	Notice (3)

Table 2. IPv4 Firewall Events *(Continued)*

ALGSipMangleMessage: Failed to add Call-Id Undo information to NAT table	Notice (3)
ALGSipMangleMessage: Failed to create association for RTP	Notice (3)
ALGSipMangleMessage: Failed to create association for RTCP	Notice (3)
ALGSipNewConnection: Failed to create association	Notice (3)
Security policy unavailable for policy-class, dropping packet	Warning (2)
IN bound Access Policy not found, dropping packet	Warning (2)

High Administrative Distance Route for Statically Routed Private Subnets

For units on which the default route goes out the public interface, use the **ip route** command to specify a high administrative distance route that routes to null 0 for any private subnets to which a static route exists.

(config)**#ip route** <*ip address*> <*subnet mask*> **null 0** <*administrative distance*>

The <*ip address*> parameter specifies the IPv4 address to add to the route table.

The <*subnet mask*> parameter specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host.

The **null 0** option specifies that traffic is routed to the null interface. Routing to null 0 in this case prevents traffic destined to private subnets from being sent out the default route if the link to that private network goes down.When traffic is routed to the null interface, the router drops all packets destined for that interface.

The <*administrative distance*> parameter is used to determine the best route when multiple routes to the same destination exist: the lower the administrative distance, the more preferable the route. The range for administrative distance is **1** to **255**.

The following example specifies an administrative distance of **255**, which means that any other route will override it:

(config)**#ip route 10.10.10.0 255.255.255.0 null 0 255**

You could use the null route in this example to discard traffic destined for the 10.10.10.0/24 subnet when the connection to 192.168.1.2 goes down if **ip route 10.10.10.0 255.255.255.0 192.168.1.2** is already configured.

DNS Lookup and Proxy

AOS includes DNS lookup and proxy services that can provide basic DNS functions for your network. DNS is an application layer protocol that allows computers and network devices to translate host names into IP addresses.

DNS lookup is the method of resolving a host name to an IP address. The DNS client sends a DNS query to a DNS server. The DNS server replies with a DNS response that either provides an error message or gives a resulting IP address. DNS lookup only provides DNS resolution for the AOS device.

> NOTE *If **domain-lookup** is enabled, which it is by default, one or more DNS servers should be configured using the **name-server** command to prevent DNS requests from being broadcast and possibly responded to by a third-party rogue DNS server.*

Follow these steps to configure DNS lookup and specify a domain server:

```
(config)#domain-lookup
(config)#name-server <primary-server-ip> [<secondary-server-ip>]
```

The <*secondary-server-ip*> parameter is optional, and you may enter one or more secondary name servers.

The DNS proxy service forwards DNS lookups from clients to a DNS server. DNS proxy in AOS also includes a statically defined host name feature, where host names defined in the configuration can be statically mapped to an IP address. If DNS proxy has been enabled but is not needed, disable it with the **no domain-proxy** command:

```
(config)#no domain-proxy
```

DNS clients can use the AOS device to resolve DNS queries. The AOS device first checks for static host name definitions. If a matching static host name entry is not found, the AOS device will forward (proxy) the DNS query to the configured DNS server and then forward the DNS response back to the DNS client.

Voice Security

Recommendations for improved voice security include:

1. Use a standard ACL to restrict Session Initiation Protocol (SIP) traffic to allow only trusted user agents. (Refer to *SIP Access Class on page 22*.)
2. Ensure that the SIP registrar is disabled if SIP voice users are not being used. (Refer to *SIP Registrar and Authentication on page 22*.)
3. Enable SIP REGISTER and INVITE authentication if SIP voice users are being used. (Refer to *SIP Registrar and Authentication on page 22*.)
4. Enable the Realtime Transport Protocol (RTP) symmetric filter. (Refer to *RTP Symmetric Filter on page 23*.)

For a list of all security recommendations, including a command summary and the default settings, refer to *Appendix A. Security Configuration Summary on page 38*.

SIP Call Leg Distribution Unit

The call leg distribution unit (CLDU) is used to match an inbound SIP call to one of the configured SIP trunks on the unit. If the SIP header information doesn't contain the fully qualified domain name (FQDN) or resolved IP address of the configured **sip-server** or **domain** on the SIP trunk, the unit will reject the call, which helps prevent unsolicited SIP traffic from being processed by the unit.

The CLDU follows a process when inspecting the received SIP packet. The search order is as follows in A4.05 and later:

- Via header
- From header
- To header
- Contact header
- Layer 3 source IP address

Prior to A4.05, the search order was as follows:

- From header
- To header
- Via header
- Contact header
- Layer 3 source IP address

SIP Access Class

It is possible for a malicious entity to gain unauthorized access to services or cause a denial of service (DoS) attack if the unit is not protected from untrusted SIP traffic. Creating an ACL that allows SIP traffic from only your SIP server can help prevent such attacks. Use the **ip sip access-class** <*name*> **in** command to limit the traffic allowed to reach the SIP stack by applying preconfigured standard ACLs to incoming connections:

(config)**#ip sip access-class** <*name*> **in**

The <*name*> parameter specifies a previously configured standard IPv4 ACL. By default, no ACL is configured or applied, and all traffic reaches the SIP stack.

For more information on configuring and using ACLs, refer to either *Access Control Lists and Access Control Policies on page 6* or the *IP ACLs in AOS* configuration guide available from the ADTRAN Support Community (https://supportforums.adtran.com).

SIP Registrar and Authentication

The SIP registrar is used to register user agents into the location database. If SIP voice users are not being used (i.e., SIP phones registering to a voice user), ensure that the SIP registrar is disabled by issuing the **no ip sip registrar** command:

(config)**#no ip sip registrar**

If SIP voice users are being used, the SIP registrar will have been enabled, and you will need to use the **ip sip authenticate** command to enable SIP INVITE authentication:

(config)**#ip sip authenticate**

In addition, use the **ip sip registrar authenticate** command to specify that authentication is required for registrations:

(config)**#ip sip registrar authenticate**

> NOTE *For more information on the use of voice user account passwords, please refer to your voice product's administrator's guide.*

RTP Symmetric Filter

The RTP symmetric filter resolves issues resulting from multiple RTP streams destined for the same UDP port being used by the Digital Signal Processor (DSP). This situation can occur, for example, when a call that has ended is still active somewhere in the network and the flow of RTP toward the unit has not stopped. Use the **ip rtp symmetric-filter** command to enable filtering of received nonsymmetric packets:

(config)**#ip rtp symmetric-filter**

When this option is enabled, any packets that don't match the source IP address and port in the received Session Description Protocol (SDP) will be dropped. By default, the RTP symmetric filter is disabled on some AOS platforms and enabled on others. You should always enable it except in rare cases in which some SIP devices send from a different port than the one on which they receive.

Management/Access Control

The following sections provide security recommendations for improved management and access control:

For a list of all security recommendations, including a command summary and the default settings, refer to *Appendix A. Security Configuration Summary on page 38*.

Logins and Passwords

Recommendations for improved login and password security include:

1. Enable password encryption globally. (Refer to *Password Encryption on page 24*.)
2. Change the default user name and password on the AOS device. (Refer to *Local User Accounts on page 24*.)

3. Define local user names and passwords as needed. (Refer to *Local User Accounts on page 24*.)
4. Change the Enable mode password. (Refer to *Enable Mode Password on page 25*.)
5. Create and assign portal lists to restrict user access to services as necessary. (Refer to *Portal Lists on page 25*.)

Password Encryption

Password encryption displays the encrypted form of passwords in the running configuration, which keeps unauthorized persons from viewing passwords in the configuration file. The **service password-encryption** command turns on encryption for all currently configured passwords, as well as any newly created passwords:

(config)**#service password-encryption**

With this option enabled, password encryption applies to all passwords, including passwords for user name, Enable mode, Telnet/console, Point-to-Point Protocol (PPP), Border Gateway Protocol (BGP), and authentication keys. For platforms that support voice features, password encryption also applies to the following: voice user account login PIN, SIP authentication password, and voicemail PIN.

You cannot recover a lost encrypted password. You must bypass passwords from the console and set a new password.

Local User Accounts

Each AOS device has a default user name (**admin**) and password (**password**). Make sure to change the default password for the **admin** user. In addition, you will want to add additional local user names and passwords as needed. To change/create user names and passwords, use the **username** <*username*> **password** <*password*> command:

(config)**#username** <*username*> **password** <*password*>

For example, to change the **admin** password to **arGht43#6**, enter the following:

(config)**#username admin password arGht43#6**

To remove the **admin** user, enter the following:

(config)**#no username admin**

To create strong passwords, make sure that they contain the following:

- Both alphabetic and numeric characters
- Both uppercase and lowercase characters
- At least one symbol
- At least 7 characters (longer is better)

Enable Mode Password

By default, the Enable mode password is set to **password**. To prevent users from accessing the configuration functions for your device, change the Enable mode password:

(config)#**enable password** <*password*>

Refer to the recommendations in *Local User Accounts on page 24* for creating strong passwords.

Portal Lists

A portal list enables you to restrict user name access to specific portals (that is, system services such as HTTP, Telnet, SSH, FTP, and console). By creating and assigning a portal list to a user name, you restrict the user name to authenticating only the services in the portal list. For example, if you use phones that use FTP to download configuration files from the NetVanta 7000 Series, ADTRAN recommends that you restrict the **polycomftp** user name to use only FTP. Doing so requires creating a portal list that allows only FTP and assigning this portal list to the **polycomftp** user name.

To create a portal list, use the **portal-list** command from the Global Configuration mode:

(config)#**portal-list** <*name*> <*portal1 portal2 portal3...*>

The <*name*> parameter specifies the name of the portal list, and the list of portals after the name specifies which portal(s) to allow the user names associated with the portal list to access. The portal list may include one or more of the following portals: **console, ftp, http-admin, ssh,** and **telnet**. For example, the following assigns the **console**, **telnet**, and **ssh** portals to the portal list **ENGINEERS**:

(config)#**portal-list ENGINEERS console telnet ssh**

To assign a portal list to a user, use the **username portal-list password** command from the Global Configuration mode:

(config)#**username** <*username*> **portal-list** <*name*> **password** <*password*>

The <*username*> parameter specifies the user name. The <*name*> parameter specifies the name of the portal list, and the <*password*> parameter specifies the password. A single portal list can be assigned to multiple users. If a user has no portal list assigned, that user can access any portal.

Access Control

Security recommendations for improving access control include the following:

1. Disable Link Layer Discovery Protocol (LLDP) on untrusted interfaces. (Refer to *LLDP on page 26*.)
2. Enable secure services such as SSH and HTTPS as needed. (Refer to *Services on page 26*.)
3. Disable insecure services such as Telnet and HTTP. (Refer to *Services on page 26*.)
4. Use SSH instead of Telnet and HTTPS Secure Sockets Layer version 3.0 (SSLv3) instead of HTTPS SSLv2. (Refer to *Services on page 26*.)
5. Remove the default DHCP server pool. (Refer to *DHCP Server Pool on page 27*.)

6. Set session timeouts for HTTP/HTTPS, console, Telnet, and SSH to 15 minutes or less. (Refer to *Session Timeouts on page 27*.)
7. Use ACLs to limit the source IP addresses allowed to access the management interface. (Refer to *Management Interface Access Classes on page 27*.)

LLDP

Disable LLDP on untrusted interfaces. By default, all interfaces are configured to send and receive LLDP frames. Use the **no lldp send-and-receive** command to block LLDP packets on an interface.

The following example blocks sending and receiving LLDP frames on Ethernet interface 0/1:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#no lldp send-and-receive
```

Services

ADTRAN recommends enabling secure services and disabling less secure services as needed. All services are enabled by default. For executing commands on a remote host, SSH provides more security than Telnet. Therefore, ADTRAN recommends using SSH instead of Telnet. HTTPS provides for more secure transmission of content than HTTP. Therefore, ADTRAN recommends disabling HTTP and using HTTPS instead of HTTP. Refer to the following sections for information on enabling/disabling individual services.

SSH

If SSH has been disabled and needs to be re-enabled, enter the **no shutdown** command from the SSH Line Interface Configuration mode:

```
(config)#line ssh 0 4
(config-ssh0-4)#no shutdown
```

Telnet

To disable Telnet, enter the **shutdown** command from the Telnet Line Configuration mode:

```
(config)#line telnet 0 4
(config-telnet0-4)#shutdown
```

HTTP

To disable HTTP but not HTTPS, enter the **no http server** command from the Global Configuration mode:

```
(config)#no http server
```

HTTPS

If HTTPS has been disabled and needs to be re-enabled, enter the **http secure-server** command from the Global Configuration mode:

```
(config)#http secure-server
```

By default, SSLv2 is disabled; leave it disabled to use only SSLv3.

DHCP Server Pool

All units have a default DHCP pool named **Private**. Use the **no ip dhcp pool** command to remove this pool from the unit:

(config)**#no ip dhcp pool Private**

Session Timeouts

Long session timeouts can make it easier to compromise the system if a computer that is logged in is left unattended. Set session timeouts for HTTP/HTTPS, SSH, Telnet, and console to 15 minutes or less.

Use the **http session-timeout** <*value*> command from the Global Configuration mode to set the HTTP and HTTPS session timeout value in seconds:

(config)**#http session-timeout** <*value*>

The <*value*> parameter specifies the time in seconds and should be **900** seconds (15 minutes) or less.

Use the **line-timeout** <*value*> command in the appropriate line configuration mode to set the session timeouts for the console, Telnet, and SSH. The <*value*> parameter specifies the timeout value in minutes and should be set to **15** or less.

The following sets the console session timeout to **5** minutes:

(config)**#line console 0**
(config-con 0)**#line-timeout 5**

The following sets the Telnet session timeout to **5** minutes:

(config)**#line telnet 0 4**
(config-telnet0-4)**#line-timeout 5**

The following sets the SSH session timeout to **5** minutes:

(config)**#line ssh 0 4**
(config-ssh0-4)**#line-timeout 5**

Management Interface Access Classes

Use access classes to limit the source IP addresses allowed to access the management interface.

The following command restricts access to the HTTP server using the specified standard IPv4 ACL:

(config)**#http ip access-class** <*ipv4 acl name*> **in**

The following command restricts access to the HTTPS server using the specified standard IPv4 ACL:

(config)**#http ip secure-access-class** <*ipv4 acl name*> **in**

The following restricts access to Telnet using the specified standard IPv4 ACL:

(config)**#line telnet 0 4**
(config-telnet0-4)**#ip access-class** <*ipv4 acl name*> **in**

The following restricts access to SSH using the specified standard IPv4 ACL:

```
(config)#line ssh 0 4
(config-ssh0-4)#ip access-class <ipv4 acl name> in
```

For more information on configuring and using ACLs, refer to either *Access Control Lists and Access Control Policies on page 6* or the *IP ACLs in AOS* configuration guide available from the ADTRAN Support Community (https://supportforums.adtran.com).

Authentication, Authorization, and Accounting (AAA)

ADTRAN recommends the following for AAA: Configure the minimum number of local accounts on devices for emergency use in case of loss of connection to the Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) server.

Authentication, authorization, and accounting (AAA) is a security software system implemented on all AOS products. The main function of AAA is to govern which users are allowed network access, which services they are allowed to use, and to keep track of what users do while on the network. AAA is made up of three independent, configurable security measures:

- **Authentication** validates the identity of the user attempting to gain access to the device, most often through a user name and password.
- **Authorization** allows the connected user access to specified areas of the device, based on preconfigured parameters. In authorization, the information gained in authentication is checked against stored user parameters in a RADIUS server or in a TACACS+ server.
- **Accounting** collects data about user activities while logged into the device and compiles it into logs and reports that enable network administrators to see how the device is being used and by whom.

Most AAA services rely on the configuration of RADIUS or TACACS+ servers for their functionality, and all AAA services rely on method lists to take the appropriate actions for managing your network at the interface level. The servers play a role in storing and maintaining user information for authentication and authorization, and each server holds accounting information about user activity. AOS supports all three AAA services on TACACS+ servers, whereas only authentication is supported on RADIUS servers.

For information on configuring AAA, refer to the *Configuring AAA in AOS Configuration Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).

SNMP

Recommendations for using Simple Network Management Protocol (SNMP) include the following:

1. Enable the SNMP agent if needed.
2. If SNMP is needed, add SNMPv3 groups and SNMPv3 users using an ACL to restrict allowed hosts. (Refer to *SNMP Groups and Users on page 29*.)
3. Ensure the SNMP trap/inform hosts use SNMPv3 and are pointing only to those devices that are actively managing devices. (Refer to *SNMP Traps on page 30*.)
4. Enable all SNMP traps. (Refer to *SNMP Traps on page 30*.)

SNMP is the Internet Engineering Task Force (IETF) industry standard Application Layer protocol for remotely managing networks. SNMP provides management services that include automatic notification when unacceptable network conditions exist, status polling of network devices, and the ability to edit configuration settings. SNMP has three basic components:

- The **network manager** is the control program that collects, controls, and presents data pertinent to the operation of the network devices. The network manager runs on a server called a network management system (NMS).
- The **SNMP agent** is a control program that responds to queries and commands from the network manager and returns requested information, or invokes configuration changes initiated by the network manager. The SNMP agent resides in each AOS network device.
- A **management information base (MIB)** is an index to the organized data within a network manager that allows information exchange between the network manager and SNMP agent to operate efficiently. After installing the MIBs, the network manager is familiar with the operating parameters that can be controlled or monitored, and references the parameters with a numerical identification. The parameters are known as MIB object identifiers (OIDs) or MIB variables.

By default, the SNMP agent is disabled. If SNMP is needed, enable the SNMP agent:

(config)**#snmp agent**

Executing this command enables the SNMP agent within the product, which allows the product to respond to queries from the NMS if configured appropriately.

SNMP Groups and Users

SNMP groups are used to control access to SNMP information. SNMP server users are configured and attached to a specified group with an SNMP version. The SNMP version defines the security model of the group, with SNMP version 1 (SNMPv1) being the least secure and SNMP version 3 (SNMPv3) the most secure. SNMPv3 uses services, such as authentication, privacy, and ACLs to provide a higher level of security not present with v1 or v2.

If SNMP is needed, add an SNMPv3 group and an SNMPv3 user using an ACL to restrict allowed hosts.

To add an SNMPv3 group using privacy authentication and an IPv4 standard ACL, use the following command:

(config)**#snmp-server group** <*groupname*> **v3 priv ip access-class** <*ipv4 standard acl name*>

To add an SNMPv3 user to a specified SNMPv3 group using a specified IPv4 standard ACL and a specified password for either the HMAC-MD5-96 or HMAC-SHA-96 authentication level, use the following command:

(config)#s**nmp-server user** <*username*> <*groupname*> **v3 auth [md5 | sha]** <*authentication password*> **ip access-class** <*ipv4 standard acl name*>

For example, the following creates a new user named **BobbyW** and assigns the user to a group called **securityV3priv** using the version 3 security model and the message digest 5 (MD5) authentication method with a password of **passWORD#6243** and using the standard ACL **SNMP** to verify:

(config)**#snmp-server user BobbyW securityV3priv v3 auth md5 passWORD#6243 ip access-class SNMP**

The **group** and **user** commands should both use the SNMP access class and the SNMPv3 authentication and privacy authentication options.

SNMP Traps

Inform and trap messages are sent by the SNMP agent to report network conditions or status updates from the network device. Use the **snmp-server host** command to configure a host to receive SNMP notifications. The command allows you to enable all traps or to specify the following traps to enable individually: Border Gateway Protocols (BGP) traps, Frame Relay traps, SNMP traps, network monitor track traps, and voice traps.

When configuring a host to receive SNMP notifications, ensure the SNMP trap/inform hosts use SNMPv3 and are pointing only to those devices that are actively managing devices:

(config)**#snmp-server host** <*ip address*> **traps version 3 priv** <*community*> **[bgp | frame-relay | snmp | track | voice]**

If you do not use the option to specify individual traps to enable (**bgp**, **frame-relay**, **snmp**, **track**, or **voice**), all traps will be enabled. The **version 3 priv** option indicates that version 3 privacy and authentication is used. The <*ip address*> parameter specifies the IP address of the SNMP host that receives the SNMP traps. Ensure the SNMP trap/inform hosts are pointing only to those devices that are actively managing devices. The <*community*> parameter specifies the community string (used as a password) for authorized agents to obtain access to SNMP information.

Enable all SNMP traps to enable the SNMP authentication failure alarm:

(config)**#snmp-server enable traps**

For more detailed information on SNMP configuration, refer to the configuration guide *SNMP in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).

General

General recommendations for improving management access control security include the following:

1. Configure a Simple Network Time Protocol (SNTP) or a Network Time Protocol (NTP) server, time zone, and daylight savings time (DST) mode to ensure a valid time stamp on all system generated logs. (Refer to *Time Server on page 30*.)
2. Replace the default banner to define your company's policies. (Refer to *Banner on page 31*.)
3. Ensure there are no **run tcl** entries in the configuration file. (Refer to *Tcl Scripting on page 32*.)
4. Enable the AOS syslog feature and configure the syslog server IP address to log events. (Refer to *Logging Events on page 32*.)
5. Disable IP directed broadcasts on all interfaces. (Refer to *Directed Broadcasts on page 32*.)

Time Server

Configure a time server to ensure a valid time stamp on all system generated logs.

To configure an SNTP server:

(config)**#sntp server** <*hostname* or *ip address*>

Alternatively, to configure an NTP server:

(config)**#ntp server** <*hostname* or *ip address*>

Set a time zone on the unit using the **clock timezone** <*value*> command. The following example sets the time zone to Central Time:

(config)**#clock timezone -6-Central-Time**

For a complete list of time zone values, refer to the *AOS Command Reference Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).

Enable or disable updating the clock for DST using the **clock [no-]auto-correct-DST** command. The example below enables the unit to update the clock for DST:

(config)**#clock auto-correct-DST**

Banner

All AOS devices ship with a default banner. Replace this banner to define your company's policies. Banners appear in the following order:

- Message-of-the-day (MOTD) banner appears at initial connection.
- Login banner follows the MOTD banner.
- Exec banner appears after successful login.

To create a new banner, use the **banner** command:

(config)**#banner [exec | login | motd]** <*delimiter*> <*message*> <*delimiter*>

In the following example, leave the leading carriage return and the one before the final #; they are for spacing purposes when the banner is displayed:

```
(config)#banner motd #

**********************************************************************
ABC Company
555-555-5555 during Business Hours
555-555-1234 during Off-Business Hours
This system is restricted solely to ABC Company.

Authorized personnel only.
**********************************************************************

#
```


Tcl Scripting

Tcl is a scripting language used in a wide variety of applications. In AOS applications, Tcl is most commonly used for generating scripts that help automate tasks such as network configuration and network connectivity tests. Because scripts can alter the unit's configuration, ADTRAN does not recommend using them. Check the configuration file to ensure there are no **run tcl** entries.

Logging Events

Events should be logged by enabling syslog. Enable the AOS syslog feature with the following command:

```
(config)#logging forwarding on
```

Configure the syslog server IP address using the **logging forwarding receiver-ip** <*ip address*> command. For example:

```
(config)#logging forwarding receiver-ip 192.168.1.50
```

To capture logins, use the **logging forwarding priority-level** command. Set the priority level to **info** as shown in the following example:

```
(config)#logging forwarding priority-level info
```

Directed Broadcasts

A directed broadcast is a packet intended for all nodes on a nonlocal network. If **ip directed-broadcast** is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Enabling directed broadcasts can make an interface vulnerable to DoS attacks; therefore, ADTRAN recommends disabling **ip directed-broadcast** on all interfaces if it has been enabled. It is disabled on all interfaces by default. The following example disables **ip directed-broadcast** on the interface **ethernet 0/1**:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#no ip directed-broadcast
```

Wi-Fi Security

Recommendations for improved Wi-Fi security include:

1. Use WPA2 security mode.
2. Use a long and relatively unguessable key for the security mode.

For a list of all security recommendations, including a command summary and the default settings, refer to *Appendix A. Security Configuration Summary on page 38*.

The **security mode** command configures the security mode settings for a virtual access point (VAP). AOS devices support the 802.11 wired equivalent privacy (WEP), 802.1x, Wi-Fi protected access (WPA), and WPA2 security modes. By default, no security mode is defined. For the greatest security protection, ADTRAN recommends using the WPA2 security mode.

To specify using WPA2 with preshared keys (PSK), enter the following:

```
(config)#interface dot11ap 1/1.1
(config-dot11ap 1/1.1-bg)#security mode wpa aes-ccmp psk <key>
```

The <*key*> parameter specifies a security key. The security key must be 8 to 63 ASCII or 16 to 126 hexadecimal characters. For increased security, use a long and relatively unguessable key.

To specify using WPA2 with a RADIUS server, enter the following:

```
(config)#interface dot11ap 1/1.1
(config-dot11ap 1/1.1-bg)#security mode wpa aes-ccmp eap
```

For more information on wireless configuration, refer to the *Wireless Configuration Guide* available rom the ADTRAN Support Community (https://supportforums.adtran.com).

Auto-Link Security

For improved auto-link security, use HTTPS for auto-link communication.

For a list of all security recommendations, including a command summary and the default settings, refer to *Appendix A. Security Configuration Summary on page 38*.

ADTRAN's n-Command Managed Service Provider (MSP) is a management platform for AOS-based networks. The system provides the management tools necessary to aid IT administrators in daily network operation and configuration, allowing them to quickly adapt to networking changes, make better use of limited resources, evaluate network performance, and save time and money.

ADTRAN products can be linked to and managed by the n-Command MSP server; these products communicate with the n-Command server using the AOS auto-link feature.

Auto-link can use HTTP or HTTPS for its communication with the n-Command MSP server. By default, auto-link uses HTTPS, which is more secure than HTTP. If auto-link has been changed to use HTTP, you can change it back to HTTPS by using the following command:

```
(config)#auto-link https
```

For detailed information on configuring auto-link, refer to the configuration guide *Configuring Auto-Link in AOS for n-Command MSP* available from the ADTRAN Support Community (https://supportforums.adtran.com).

Saving and Verification

Recommendations for saving and verification include:

1. Save changes made in the running configuration to the startup configuration file. (Refer to *Saving Configuration File Changes on page 34*.)
2. Use the security audit tool to identify possible security risks. (Refer to *Security Audit Tool on page 34*.)

Saving Configuration File Changes

When you are ready to save the changes made to the configuration, use the **write** command to copy your changes to the unit's NVRAM; for example:

```
#write
```

Once the save is complete, the changes are retained even if the unit is shut down or suffers a power outage.

Security Audit Tool

AOS products provide a security audit tool to aid in indentifying possible security risks. To run the security audit tool and save the log to flash memory, use the following command:

```
#run audit security log
```

The audit results save to a file named **securityAudit_**<*timestamp*>. The file name has the timestamp attached in the format yyyymmddhhmmss.

To find the exact name of your file, use the **show flash** command to list all files currently stored in flash memory:

```
#show flash
```

After finding the file name, use the **show file** <*filename*> command to view the file if your unit only has a flash file system; otherwise use the **show file flash** <*filename*> command:

```
#show file <filename>
```

Various configuration items could be identified as posing a security risk. Remember, it is up to the user to determine if the items found are truly issues that need to be addressed. The following table lists the items that are audited, their severity level, and a description to assist you in correcting the problem.

Table 3. Possible Security Risks

Violation Type	Severity	Description
Startup-Config	High	Indicates that the startup configuration file does not match the running configuration file. This is determined by comparing the message digest 5 (MD5) checksum of both files for a match.
Passwords/Keys	High	Identifies nonsecure passwords. If a password has MD5 encryption enabled, the tool tests for common password sequences, such as **qwerty**, **1234**, **abc**, **xyz**, etc. If MD5 is disabled, an alert is issued if the password: • Is less than seven characters. • Does not contain alphabetic and numeric characters. • Matches common sequences, such as **qwerty**, **1234**, **abc**, **xyz**, etc. • Matches the default passwords. • Matches another password in the system. • Service password encryption is not enabled.
Firewall	High	Indicates the firewall is disabled.

Table 3. Possible Security Risks *(Continued)*

Violation Type	Severity	Description
Policy-Class	High	Identifies any of the following ACP vulnerabilities: • Stateful inspection is disabled. • An undefined ACL exists in the ACP. • An interface with a private IP address (10.x.x.x, 172.16.x.x, 192.168.x.x) has an ACP assigned that does not have NAT configured. • An interface is enabled without an ACP assigned.
SNMP	High	Indicates the SNMP agent is enabled and configured to allow SNMPv1 or SNMPv2. Both of these versions are considered nonsecure. SNMPv3 group and SNMPv3 user are preferred.
Wi-Fi	High	Identifies any of the following wireless vulnerabilities: • Security mode is set to anything but WPA2 (including **none**). • Service set identifier (SSID) broadcast is enabled. • A weak key.
Network Protocols	High	Identifies any of the following network protocols are enabled and considered a security risk: • HTTP • HTTPS SSLv2 • File Transfer Protocol (FTP) • Trivial File Transfer Protocol (TFTP) • Telnet SSH is suggested as a replacement for Telnet and HTTPS SSLv3 instead of HTTPS SSLv2.
Session Timeout	High	Identifies the console, HTTP, SSH, or Telnet session timeout is set to a value greater than 15 minutes. Long session timeouts can compromise the system. The recommended setting is 15 minutes or less.
Time-Server	High	Indicates the time server NTP or SNTP is not configured. It can also indicate the time server is configured, but not synchronized. It is important to have a valid timestamp on all logs generated by the system.
Logging	Medium	Indicates user activity is not being logged. User activity should be logged either by enabling syslog or TACACs+ accounting. (The syslog can be enabled by using the **logging forwarding on** command.)
Domain Lookup	Medium	Indicates **ip domain-lookup** is enabled, but a DNS server has not been configured. This allows DNS requests to be broadcast.
Interfaces	Medium	Identifies the following interface vulnerabilities: • The **ip directed-broadcast** is enabled, which could make an interface vulnerable to DoS attacks. • A static ACL is assigned to an interface. A more secure option is to enable the firewall and assign an ACP.
Enable Password	Low	Indicates the Enable password is not set for MD5 encryption. MD5 encryption is more secure than standard password encryption.
Banner	Low	Indicates the default executive banner is still set. It is recommended that a custom banner be displayed when a user attempts to login. The banner warns of the legal consequences of unauthorized access to the unit.

Table 3. Possible Security Risks *(Continued)*

Violation Type	Severity	Description
Tcl Scripts	Low	Indicates Tcl scripting is enabled. Scripts could alter the unit's configuration.

Additional Resources

Configuring a secure network relies on the proper configuration of many AOS features and network configurations. The following table outlines additional documentation available for the features discussed in this document. These documents include detailed configuration information as well as troubleshooting tips and information. The documents are available from the ADTRAN Support Community (https://supportforums.adtran.com).

Table 4. Additional Documentation

Feature	Article Title/Description
AAA	*Configuring AAA in AOS* provides detailed configuration information for AAA.
ACLs	*IP ACLs in AOS* describes how ACLs are configured and used, as well as how to troubleshoot ACL configurations. *IPv4 Firewall Protection in AOS* provides detailed information on creating and defining ACLs.
ACPs	*IPv4 Firewall Protection in AOS* provides detailed information on creating and defining ACPs.
Administrative Route Distance	*AOS Command Reference Guide* provides technical and usage information for AOS commands.
Auto-Link	*Configuring Auto-Link in AOS for n-Command MSP* provides step-by-step configuration instructions.
CLI Commands	*AOS Command Reference Guide* includes documentation of all CLI commands for AOS products.
DHCP	*Configuring Dynamic Host Control Protocol (DHCP) in AOS* provides configuration and troubleshooting information on DHCP.
DNS Lookup and Proxy	*Configuring DNS Lookup and Proxy in AOS* provides configuration information on DNS lookup and proxy.
Firewall	*IPv4 Firewall Protection in AOS* provides step-by-step configuration instructions.
LLDP	*LLDP and LLDP-MED* describes general concepts with detailed command descriptions and troubleshooting information.
Multi-VRF	*Configuring IPv4 Multi-VRF in AOS* provides an overview of multi-VRF general concepts and step-by-step configuration instructions.
NAT Pools	*NAT Pools in AOS* provides an overview of general concepts with configuration instructions and troubleshooting information.
RTP Symmetric Filter	*AOS Command Reference Guide* provides technical and usage information for AOS commands.

Table 4. Additional Documentation *(Continued)*

Feature	Article Title/Description
Security Audit	*Understanding Security Audit Tools and PCI DSS in AOS Products Quick Configuration Guide* provides an overview of the security audit tool and guidance for interpreting the results.
Security Dashboard	*Configuring the Security Dashboard in AOS* provides information on accessing and using the Security Dashboard feature.
SIP	*AOS Command Reference Guide* provides technical and usage information for AOS commands.
SNMP	*SNMP in AOS* describes the use and configuration of SNMP in AOS.
Tcl Scripts	*Tcl Scripting in AOS* describes how to configure and use Tcl scripts in AOS.
Wi-Fi	*Wireless Configuration Guide* provides an overview of wireless technology, the elements of wireless local area networks (WLANs), methods for configuring AOS access points (APs), radios, and virtual access points (VAPs), as well as WLAN topography overviews. For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide.*

Appendix A. Security Configuration Summary

The following tables summarize the security best practices recommendations for each portion of the *Security Best Practices for AOS Products Configuration Guide*. For each recommendation, the tables provide the corresponding configuration command(s) and the default setting..

Table A-1. Data Security Recommendations

Recommendation	Command(s)	Default
1. Enable the firewall.	(config)**#ip firewall**	Disabled
2. Ensure that all ACLs in the ACP are defined and not empty.	To create a standard ACL: (config)**#ip access-list standard** <*ipv4 acl name*> (config-std-nacl)# To create an extended ACL: (config)**#ip access-list extended**<*ipv4 acl name*> (config-ext-nacl)#	No ACLs configured or applied
3. Use unique ACPs for the private, public, DMZ, and any other zones.	(config)**#ip policy-class** <*ipv4 acp name*> (config-policy-class)# Refer to *Example Configuration - Firewall with DMZ on page 16* for an example configuration file that defines unique private, public, and DMZ zones.	No ACPs configured
4. Define ACP entries to allow only the most specific and narrow range of traffic necessary.	(config)**#ip policy-class** <*ipv4 acp name*> (config-policy-class)**#allow list** <*ipv4 acl name*>	No ACPs configured
5. Define ACP entries to specify a destination ACP.	(config)**#ip policy-class** <*ipv4 acp name*> (config-policy-class)**#allow list** <*ipv4 acl name*> **policy** <*ipv4 acp name*>	No ACPs configured
6. Specify the smallest range of traffic possible when it is necessary to disable stateful processing.	(configure)**#ip policy-class** <*ipv4 acp name*> (config-policy-class)**#allow list** <*ipv4 acl name*> **stateless**	Stateful processing
7. Apply ACPs to an interface.	(config)**#interface** <*interface*> (config-interface)**#ip access-policy** <*ipv4 acp name*>	No ACPs applied to interfaces

Table A-1. Data Security Recommendations *(Continued)*

Recommendation	Command(s)	Default
8. Use the default event message display priority level.	If levels have been disabled and need to be enabled, use the following command to log all events: (config)**#event-history priority info**	Displays the following levels: 0:Fatal 1:Error 2:Warning 3:Notice 4:Information
9. For units on which the default route goes out the public interface, specify a high administrative distance route that routes to null 0 for any private subnets to which a static route exists.	(config)**#ip route** <*ip address*> <*subnet mask*> **null 0** <*administrative distance*>	No configured routes in the route table
10. Specify a DNS server when IP domain lookup is enabled.	(config)**#domain-lookup** (config)**#name-server** <*primary-server-ip*> **[**<*secondary-server-ip*>**]**	DNS lookup: Enabled No name servers defined
11. Ensure that the DNS proxy is disabled if it is not needed.	(config)**#no domain-proxy**	Disabled

Table A-2. Voice Security Recommendations

Recommendation	Command(s)	Default
1. Use a standard ACL to restrict SIP traffic to allow only trusted user agents.	(config)**#ip sip access-class** <*name*> **in**	No ACLs configured or applied. All traffic reaches the SIP stack.
2. Ensure that the SIP registrar is disabled if SIP voice users are not being used.	(config)**#no ip sip registrar**	Disabled
3. Enable SIP REGISTER and INVITE authentication if SIP voice users are being used.	To enable SIP REGISTER authentication: (config)**#ip sip registrar authenticate** To enable SIP INVITE authentication: (config)**#ip sip authenticate**	SIP REGISTER authentication: Enabled SIP INVITE authentication: Disabled

Table A-2. Voice Security Recommendations *(Continued)*

Recommendation	Command(s)	Default
4. Enable the RTP symmetric filter.	(config)**#ip rtp symmetric-filter**	Varies by product

Table A-3. Management/Access Control Recommendations

Recommendation	Command(s)	Default
Logins and Passwords		
1. Enable password encryption globally.	(config)**#service password-encryption**	Disabled
2. Change the default user name and password on the AOS device.	(config)**#username** <*username*> **password** <*password*> Passwords should contain the following: • Both alphabetic and numeric characters • Both uppercase and lowercase characters • At least one symbol • At least seven characters (longer is better)	User name: **admin** Password: **password**
3. Define local user names and passwords as needed.	To define a user name and password: (config)**#username** <*username*> **password** <*password*> Refer to the password guidelines in Recommendation 2. To remove a user name: (config)**#no username** <*username*>	No additional users configured
4. Change the Enable password.	(config)**#enable password** <*password*> Refer to the password guidelines in Recommendation 2.	Password: **password**

Table A-3. Management/Access Control Recommendations *(Continued)*

Recommendation	Command(s)	Default
5. Create and assign portal lists to restrict user access to services as necessary.	To create a portal list: (config)#**portal-list** <*name*> <*portal1 portal2 portal3...*> The <*name*> parameter specifies the name of the portal list, and the list of portals after the name specifies which of the following portals to allow the the users associated with the portal list to access: **console, ftp, http-admin, ssh,** and **telnet**. To assign a portal list to a user: (config)#**username** <*username*> **portal-list** <*name*> **password** <*password*>	No portal lists created or assigned
Access Control		
1. Disable LLDP on untrusted interfaces.	(config)#**interface** <*interface*> (config-interface)#**no lldp send-and-receive**	Enabled on all interfaces that support LLDP
2. Enable secure services such as SSH and HTTPS as needed.	To enable HTTPS: (config)#**http secure-server** To enable SSH: (config)#**line ssh 0 4** (config-ssh0-4)#**no shutdown**	All services enabled
3. Disable insecure services such as Telnet and HTTP.	To disable Telnet: (config)#**line telnet 0 4** (config-telnet0-4)#**shutdown** To disable HTTP but not HTTPS: (config)#**no http server**	All services enabled
4. Use HTTPS SSLv3 instead of HTTPS SSLv2.	If SSLv2 has been enabled, use the following to enable HTTPS with only SSLv3 enabled: (config)#**http secure-server**	SSLv2: Disabled SSLv3: Enabled
5. Remove the default DHCP server pool.	(config)#**no ip dhcp pool Private**	All units have a default DHCP pool named **Private**.

Table A-3. Management/Access Control Recommendations *(Continued)*

Recommendation	Command(s)	Default
6. Set session timeouts for HTTP/HTTPS, console, Telnet, and SSH to 15 minutes or less.	To set the HTTP and HTTPS timeout value: (config)**#http session-timeout** <*value*> The <*value*> parameter specifies the time in seconds and should be **900** or less. To set the console, Telnet, or SSH timeout value: (config)**#line** <*line*> (config-line)**#line-timeout** <*value*> The <*value*> parameter specifies the time in minutes and should be **15** or less. For example, the following sets the SSH session timeout to **5** minutes: (config)**#line ssh 0 4** (config-ssh0-4)**#line-timeout 5**	HTTP/HTTPS: **600** seconds Console: **15** minutes Telnet: **15** minutes SSH: **15** minutes
7. Use ACLs to limit the source IP addresses allowed to access the management interface.	To specify HTTP ACL: (config)**#http ip access-class** <*ipv4 acl name*> **in** To specify HTTPS ACL: (config)**#http ip secure-access-class** <*ipv4 acl name*> **in** To specify Telnet ACL: (config)**#line telnet 0 4** (config-telnet0-4)**#ip access-class** <*ipv4 acl name*> **in** To specify SSH ACL: (config)**#line ssh 0 4** (config-ssh0-4)**#ip access-class** <*ipv4 acl name*> **in**	No ACLs configured or applied

Table A-3. Management/Access Control Recommendations *(Continued)*

Recommendation	Command(s)	Default
Authentication, Authorization, and Accounting (AAA)		
Configure minimum local accounts on devices for emergency use in case of loss of connection to the TACACS+ or RADIUS server.	For information on configuring AAA, refer to *Configuring AAA in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).	N/A
Simple Network Management Protocol (SNMP)		
1. Enable the SNMP agent if needed.	(config)**#snmp agent**	Disabled
2. If SNMP is needed, add SNMPv3 groups and SNMPv3 users using an ACL to restrict allowed hosts.	To add an SNMPv3 group: (config)**#snmp-server group** <*groupname*> **v3 priv ip access-class** <*ipv4 standard acl name*> To add an SNMPv3 user: (config)**#snmp-server user** <*username*> <*groupname*> **v3 auth [md5|sha]** <*authentication password*> **ip access-class** <*ipv4 standard acl name*> The group and user commands should both use the SNMP ACL and the SNMPv3 authentication and privacy authentication options.	No default values
3. Ensure the SNMP trap/inform hosts use SNMPv3 and are pointing only to those devices that are actively managing devices.	(config)**#snmp-server host** <*ip address*> **traps version 3 priv** <*community*> **[bgp | frame-relay | snmp | track | voice]** The user has the option to either specify specific traps to enable (adding the bgp, frame-relay, snmp, track, and/or voice options) or to enable all traps (by pressing Enter without specifying individual traps).	No trap hosts configured
4. Enable all SNMP traps.	(config)**#snmp-server enable traps**	Disabled

Table A-3. Management/Access Control Recommendations *(Continued)*

Recommendation	Command(s)	Default
General		
1. Configure an SNTP or NTP server, time zone, and daylight savings time (DST) mode to ensure a valid time stamp on all system generated logs.	To configure an SNTP server: (config)**#sntp server** <*hostname or ip address*> Alternatively, to configure an NTP server: (config)**#ntp server** <*hostname or ip address*> To set a time zone on the unit: (config)**#clock timezone** <*value*> For a complete list of time zone values, refer to the *AOS Command Reference Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com). To enable DST mode: (config)**#clock auto-correct-DST** To disable DST mode: (config)**#clock no-auto-correct-DST**	SNTP: Not configured NTP: Not configured Time Zone: **-6-Central-Time** DST mode: Enabled
2. Replace the default banner to define your company's policies.	(config)**#banner [exec | login | motd]** <*delimiter*> <*message*> <*delimiter*> Example: (config)**#banner motd #** ********** **ABC Company** **555-555-5555 during Business Hours** **555-555-1234 during Off-Business Hours** **This system is restricted solely to ABC Company.** **Authorized personnel only.** ********** **#**	All products delivered with a default banner
3. Ensure there are no **run tcl** entries in the configuration file.		No Tcl scripts configured to run

Table A-3. Management/Access Control Recommendations *(Continued)*

Recommendation	Command(s)	Default
4. Enable the AOS syslog feature and configure the syslog server IP address to log user login activity.	To enable syslog: (config)**#logging forwarding on** To configure the syslog server IP address: (config)**#logging forwarding receiver-ip** <*ip address*> To capture login events, the priority level must be set to **info**: (config)**#logging forwarding priority-level info**	Syslog: Disabled No syslog server addresses configured Priority-level: **notice**
5. Disable IP directed broadcasts on all interfaces.	(config)**#interface** <*interface*> (config-interface)**#no ip directed-broadcast**	Disabled on all interfaces

Table A-4. Wi-Fi Security Recommendation

Recommendation	Command(s)	Default
Use the WPA2 security mode. If using preshared keys, use a long and relatively unguessable key.	To specify using WPA2 with preshared keys (PSK), enter the following: (config)**#interface dot11ap 1/1.1** (config-dot11ap 1/1.1-bg)**#security mode wpa aes-ccmp psk** <*key*> The <*key*> parameter specifies a security key. The security key must be 8 to 63 ASCII or 16 to 126 hexadecimal characters. To specify using WPA2 with a RADIUS server, enter the following: (config)**#interface dot11ap 1/1.1** (config-dot11ap 1/1.1-bg)**#security mode wpa aes-ccmp eap**	No security mode defined

Table A-5. Auto-Link Recommendation

Recommendation	Command(s)	Default
Use HTTPS for auto-link communication.	If auto-link has been changed to use HTTP instead of HTTPS, use the following to change back to the default: (config)**#auto-link https**	HTTPS

Table A-6. Saving and Verification Recommendations

Recommendation	Command(s)	Default
1. Save changes made in the running configuration to the startup configuration file.	**#write**	N/A
2. Use the security audit tool to identify possible security issues.	To run the security audit tool and save the log to flash memory: **#run audit security log** The audit results save to a file named **securityAudit_**<*timestamp*>. The file name has the timestamp attached in the format yyyymmddhhmmss. To find the exact name of your file by listing all files currently stored in flash memory: **#show flash** To view the file: **#show file flash** <*filename*> To view the file if your unit only has a flash file system: **#show file** <*filename*>	N/A

Appendix B. Attack Log Messages

This appendix provides a list of all the possible attack log messages that can appear on an AOS unit. Threats can possibly be attacks, but not necessarily as they could also be caused by misconfigurations or peculiarities in the network. Threats have been categorized and been assigned a weight based on their possible severity. Threats with a higher severity have the potential to be more disruptive to hosts behind the firewall than threats with a lower severity.

Keep in mind that the IPv4 firewall in your AOS device provides protection against all of these potential threats.

Each attack log message indicates that an event has occurred, which has the potential to pose a threat to host(s) behind the IPv4 firewall. In all cases outlined in *Table B-1. Attack Log Messages on page 48*, the message indicates that the firewall has detected the threat and has protected the hosts behind the firewall from the attack. Each threat listed includes the actual message seen in the event history, a description of the event and its cause (or possible causes), and the action AOS takes in response to the threat. It also includes the ID, short definition, category, and weight of the threat. Except for the category (which is visible from neither the GUI nor the CLI) and the message itself (which appears in the event history) all of this information can be viewed in the GUI's Security Dashboard. The only items that are visible from the CLI are the ID, short definition, and weight.

For more information on accessing and using the Security Dashboard feature, refer to the configuration guide *Configuring the Security Dashboard in AOS* available from the ADTRAN Support Community (https://supportforums.adtran.com).

The IPv4 firewall can bypass certain attack checks if the initial packet in the flow matches a stateless IPv4 ACP entry. This bypass can be helpful in cases where it is known that certain traffic will trigger an attack condition in the firewall, but the condition is actually a false positive and the traffic is known not to be a threat.

Refer to *Table B-1. Attack Log Messages on page 48* for a complete list of the messages along with threat description, category, and weight. In addition, a notation is added next to the threats for which attack checking can be bypassed using a stateless IPv4 ACP entry.

Table B-1. Attack Log Messages

ID	Message and Description	Category and Weight
1	**TCP connection request received is invalid (expected SYN), dropping packet; flags=<*flags*>**	
	Short Definition: TCP: expected SYN **Description:** Indicates that the first packet in a TCP flow did not have the SYN flag set. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. The first packet of a TCP flow should have the SYN flag (and no other flags) set to indicate the beginning of the three-way handshake to transition from the LISTEN state to the SYN RCVD and SYN SENT states. This threat can be observed for valid traffic when the policy session is deleted or times out, but the TCP session is still established. Check your TCP policy timeout settings and verify that the timeout accounts for the longest interval between observing packets. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 6 **Check can be bypassed by using a stateless IPv4 ACP entry**
2	**TCP connection request received is invalid (expecting SYN only), dropping packet; flags=<*flags*>**	
	Short Definition: TCP: expected SYN only **Description:** Indicates that the first packet in a TCP flow had other flags set in addition to the SYN flag. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. The first packet of a TCP flow should have the SYN flag (and no other flags) set to indicate the beginning of the three-way handshake to transition from the LISTEN state to the SYN RCVD and SYN SENT states. This threat can be observed for valid traffic when the policy session is deleted or times out, but the TCP session is still established. Check your TCP policy timeout settings and verify that the timeout accounts for the longest interval between observing packets. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 7 **Check can be bypassed by using a stateless IPv4 ACP entry**
3	**TCP connection request received is invalid (expected SYN, got ACK), dropping packet; flags=<*flags*>**	
	Short Definition: TCP: expected SYN, got ACK **Description:** Indicates that the first packet in a TCP flow had the ACK flag set in addition to the SYN flag. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. The first packet of a TCP flow should have the SYN flag (and no other flags) set to indicate the beginning of the three-way handshake to transition from the LISTEN state to the SYN RCVD and SYN SENT states. This threat can be observed for valid traffic when the policy session is deleted or times out, but the TCP session is still established. Check your TCP policy timeout settings and verify that the timeout accounts for the longest interval between observing packets. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 6 **Check can be bypassed by using a stateless IPv4 ACP entry**

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
4	**TCP connection request received is invalid (expected SYN, got RST), dropping packet; flags=<*flags*>**	
	Short Definition: TCP: expected SYN, got RST **Description:** Indicates that the first packet in a TCP flow had the RST flag set in addition to the SYN flag. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. The first packet of a TCP flow should have the SYN flag (and no other flags) set to indicate the beginning of the three-way handshake to transition from the LISTEN state to the SYN RCVD and SYN SENT states. This threat can be observed for valid traffic when the policy session is deleted or times out, but the TCP session is still established. Check your TCP policy timeout settings and verify that the timeout accounts for the longest interval between observing packets. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 6 **Check can be bypassed by using a stateless IPv4 ACP entry**
5	**Received ACK from initiator but did not receive SYN/ACK from responder**	
	Short Definition: TCP: ACK before SYN/ACK **Description:** Indicates that a packet with only the ACK flag set was received from the initiator of the TCP flow even though a packet with both the SYN and ACK flags set has not yet been received from the responder. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. After a packet that only has the SYN flag set initiates the TCP flow, the next packet in the flow should be a SYN/ACK packet sent from the responder back to the initiator. It is only after the SYN/ACK packet has been received by the initiator that the initiator should send an ACK packet back to the responder. At this point the three-way handshake is complete and the TCP connection is fully established. Therefore, if an initiator sends out an ACK packet before it receives a SYN/ACK packet, this indicates either incorrect implementation of TCP in the initiator or that the initiator is an attacker. An attacker might, for example, be attempting a DoS attack, the intent being to establish many different TCP connections through the firewall by repeatedly sending SYN packets immediately followed by ACK packets (in the hope that the firewall does not simply drop the ACK packets) so that there is no room for other TCP connections to be established. If the network is configured for asymmetric routing, there is also a possibility that the initiator did receive a SYN/ACK packet before sending out the ACK packet, but that the firewall only saw the ACK packet because the SYN/ACK packet traveled a different path through the network. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 6 **Check can be bypassed by using a stateless IPv4 ACP entry**

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
6	**Post connection SYN attack detected**	
	Short Definition: Post connection SYN attack **Description:** Indicates that a packet with the SYN flag set was received for an established TCP connection. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. The SYN flag should not be received for an established TCP connection, indicating a possible attack. For example, an attacker could send a spoofed packet with the SYN flag set in order to have the legitimate client receive an RST packet, thus disrupting the connection. This threat can also be caused by an incorrect implementation of TCP in a client. For example, if a client does not change source ports between sessions and attempts to initiate a new session within the TIME WAIT timeout, this threat will be observed. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 7 **Check can be bypassed by using a stateless IPv4 ACP entry**
7	**Data packet received after reset, dropping packet**	
	Short Definition: RX data after TCP RST **Description:** Indicates the receipt of data on a TCP connection after a RST has already been received on that connection. The firewall maintains a state for each TCP flow and inspects the TCP flags to ensure that they are valid for the current state of the flow. This attack check prevents an attacker from sending data on a TCP connection that has already been closed. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 4 **Check can be bypassed by using a stateless IPv4 ACP entry**
9	**Invalid sequence number received with RST, dropping packet, seq=<*seq*>, high=<*high*>**	
	Short Definition: Invalid seq # with RST **Description:** Indicates the receipt of a TCP packet with the RST flag set whose sequence number is outside the valid range of sequence numbers. The firewall maintains a state for each TCP flow and inspects the sequence number to ensure that it is valid for the current state of the flow. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 6 **Check can be bypassed by using a stateless IPv4 ACP entry**
10	**Invalid ack value received for connection, dropping packet**	
	Short Definition: Invalid TCP ACK value **Description:** Indicates the receipt of a TCP packet with the ACK flag set whose acknowledgement number is invalid for the current state of the flow. The firewall maintains a state for each TCP flow and inspects the acknowledgement number to ensure that it is valid for the current state of the flow. **Action:** The firewall drops the offending packet.	**Category:** TCP Statefulness **Weight:** 7 **Check can be bypassed by using a stateless IPv4 ACP entry**

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
52	**ICMP error message received for uninitiated connection**	
	Short Definition: No session for ICMP error **Description:** Indicates the receipt of an ICMP error message for which no corresponding flow exists. The firewall determines the original flow corresponding to the ICMP error message, and if none exists, drops the offending packet. This threat could be observed for valid traffic if the policy session for the original flow times out or is deleted, or if the original flow has not been observed by the firewall due to asymmetric routing. **Action:** The firewall drops the offending packet.	**Category:** ICMP Statefulness **Weight:** 6 **Check can be bypassed by using a stateless IPv4 ACP entry**
100	**Zero length IP option detected**	
	Short Definition: Zero length IP option **Description:** Indicates the receipt of an IPv4 packet with an IP option length of zero. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** IP Options **Weight:** 7
101	**Source routing option set in IP packet**	
	Short Definition: Source routing option set **Description:** Indicates the receipt of an IPv4 packet with the source routing IP option set. The source routing IP option can be used maliciously in order to route packets through devices under the control of the attacker. **Action:** The firewall drops the offending packet.	**Category:** IP Options **Weight:** 4
150	**Zero bytes transferred for connection**	
	Short Definition: Connection with no data **Description:** Indicates that a policy session has been created and has timed out without any data being observed for that connection. This threat can be caused by a port scan. An attacker could send a TCP SYN message to many ports in order to determine whether there are any services listening on those ports with the intention of exploiting those services. Port scans can be prevented or limited in several ways: • Configure an IPv4 ACP to control port access. • Configure a limit to the number of sessions that can be opened by any one host. This can be configured on a per IPv4 ACP basis using the command **ip policy-class** *<ipv4 acp name>* **max-host-sessions** *<number>*. • Enable the stealth setting using the command **ip firewall stealth**. Refer to the *AOS Command Reference Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).	**Category:** Timeout **Weight:** 2 **Check can be bypassed by using a stateless IPv4 ACP entry**

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
151	**Data connection not established from remote**	
	Short Definition: No connection from remote **Description:** Indicates that a pending policy session has timed out without being used. Pending policy sessions are typically created by ALGs to anticipate the reception of returning traffic. If a malicious user is purposely using an application to create openings through the firewall for malicious purposes, this could be an attack. In some cases, this is a valid message to receive. For example, the SIP ALG will create a pending policy session anticipating RTCP traffic. If the user agent never sends RTCP, then this policy session will never become active, resulting in one occurrence of this threat.	**Category:** Timeout **Weight:** 2
200	**Fragment of size less than configured minimum fragment size detected**	
	Short Definition: Fragment size < minimum **Description:** Indicates the receipt of a fragment smaller than the minimum allowed fragment size. This threat is detected during IP reassembly. It can indicate a corrupted or malformed packet, or it could indicate a possible attack. **Action:** The reassembly engine drops the offending fragment.	**Category:** Reassembly **Weight:** 7
201	**Tiny or overlapping fragment attack detected**	
	Short Definition: Tiny fragment attack **Description:** Indicates the receipt of an unusually small TCP fragment. An attacker could be attempting to bypass firewall rules by forcing a portion of the TCP header into subsequent fragments. Additionally, an attacker could be attempting to consume processing time on a server by sending it many very small packets to reassemble. **Action:** The reassembly engine drops the offending tiny fragment.	**Category:** Reassembly **Weight:** 10
202	**IpReasmbly datagram size exceeds max limit**	
	Short Definition: Datagram exceeds max size **Description:** Indicates the receipt of an IP datagram larger than the maximum allowable size of 65535 bytes. Some systems cannot handle datagrams of this type correctly. Because of this, an attacker could craft a datagram of this type in order to crash vulnerable systems. **Action:** The reassembly engine drops the offending datagram.	**Category:** Reassembly **Weight:** 7
203	**IpReasmbly last fragment length changed**	
	Short Definition: Last fragment len changed **Description:** Indicates an error in IP fragment reassembly. **Action:** The reassembly engine drops the offending fragment.	**Category:** Reassembly **Weight:** 6

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
204	**IpReasmbly Fragment count exceeds max limit**	
	Short Definition: Exceeded max fragments **Description:** Indicates the receipt of more than the maximum number of allowable fragments prior to reassembly. An attacker could have attempted to consume all of the resources in the reassembly engine of a server or other network device. **Action:** The reassembly engine drops the offending fragments.	**Category:** Reassembly **Weight:** 6
205	**IpReasmbly time out**	
	Short Definition: Reassembly timeout **Description:** Indicates that the fragments necessary to complete reassembly have not arrived in a timely manner. An attacker could have attempted to consume all of the resources in the reassembly engine of a server or other network device. **Action:** The reassembly engine drops the offending fragments and frees the resource.	**Category:** Reassembly **Weight:** 1
250	**Source IP is a broadcast address, dropping packet**	
	Short Definition: Source IP is broadcast **Description:** Indicates the receipt of an IPv4 packet whose source address is broadcast. An attacker could be attempting to initiate or propagate a DoS attack, possibly to an unknown host, by causing a vulnerable system to reply to the broadcast address. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 10
251	**TCP connection request received has invalid TCP header length, dropping packet**	
	Short Definition: Invalid TCP hdr length **Description:** Indicates the receipt of a TCP packet whose TCP header length is invalid. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7
252	**IP header length is less than the minimum length**	
	Short Definition: IP hdr length too small **Description:** Indicates the receipt of an IPv4 packet whose IP header length is smaller than the smallest allowable IP header. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
253	**Packet without any data received**	
	Short Definition: Pkt w/o data received **Description:** Indicates the receipt of an IPv4 packet containing an IP header and no data. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash vulnerable systems **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7
254	**Packet with Short TCP Header length detected, packet dropped**	
	Short Definition: Short TCP hdr length **Description:** Indicates the receipt of a TCP packet whose TCP header length is smaller than the smallest allowable TCP header. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight: 7**
255	**Dropping packet due to length problem in TCP**	
	Short Definition: Len in TCP hdr > pkt size **Description:** Indicates the receipt of a TCP packet whose TCP header length is larger than the actual packet. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7
256	**Packet with short UDP header length detected, packet dropped**	
	Short Definition: Short UDP hdr length **Description:** Indicates the receipt of a UDP packet whose UDP header length is smaller than the smallest allowable UDP header. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7
257	**Dropping packet because of invalid length in UDP**	
	Short Definition: Len in UDP hdr > pkt size **Description:** Indicates the receipt of a UDP packet whose UDP header length is larger than the actual packet. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
258	**Packet with Short ICMP length detected, packet dropped**	
	Short Definition: Short ICMP hdr length **Description:** Indicates the receipt of an ICMP packet whose ICMP header length is smaller than the smallest allowable ICMP header. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 7
259	**ICMP error message contains less data than expected (Possible attack)**	
	Short Definition: ICMP error data too small **Description:** Indicates the receipt of an ICMP error message with less data than expected. An ICMP error message is accompanied by information regarding the errored packet that caused it to be sent. This threat indicates that such information is missing or truncated. Some systems cannot handle ICMP error messages of this type correctly. Because of this, an attacker could craft an ICMP error message of this type in order to crash or execute malicious code within vulnerable systems. **Action:** The firewall drops the offending packet.	**Category:** Against Specifications **Weight:** 6
260	**HTTP Method exceeded max, dropping pkt src=<*ip address*>**	
	Short Definition: HTTP method > max size **Description:** Indicates the receipt of an HTTP packet whose method field exceeds the maximum allowable length. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. This threat is only observed when URL filtering is being used. **Action:** The firewall drops the offending packet and sends TCP RST packets to both the client and the server to close the connection.	**Category:** Against Specifications **Weight:** 5
261	**HTTP URI exceeded max, dropping pkt src=<*ip address*>**	
	Short Definition: HTTP URI > max size **Description:** Indicates the receipt of an HTTP packet whose Uniform Resource Identifier (URI) field exceeds the maximum allowable length. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. This threat is only observed when URL filtering is being used. **Action:** The firewall drops the offending packet and sends TCP RST packets to both the client and the server to close the connection.	**Category:** Against Specifications **Weight:** 5

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
262	**HTTP version exceeded max, dropping pkt src=<*ip address*>**	
	Short Definition: HTTP version > max size **Description:** Indicates the receipt of an HTTP packet whose version field exceeds the maximum allowable length. Some systems cannot handle packets of this type correctly. Because of this, an attacker could craft a packet of this type in order to crash or execute malicious code within vulnerable systems. This threat is only observed when URL filtering is being used. **Action:** The firewall drops the offending packet and sends TCP RST packets to both the client and the server to close the connection.	**Category:** Against Specifications **Weight:** 5
350	**Unable to determine route to destination, dropping packet**	
	Short Definition: No route found for dest **Description:** Indicates that no route was found for the destination of the first packet in a flow. The firewall performs a route lookup on all first packets in order to determine the destination ACP for the flow. This destination ACP is needed so that return traffic can also match the flow. Additionally, some ACP entries match against a destination ACP in order to enforce certain rules. This is commonly used in load sharing. Inspect your routing configuration to determine that correct routes exist for all valid traffic. **Action:** The firewall drops the offending packet.	**Category:** Route Table Issue **Weight:** 1
351	**Unable to find route for source, dropping packet**	
	Short Definition: No route found for source **Description:** Indicates that no route was found for the source of a packet. The firewall performs a route lookup on the source of a packet in order to ensure that the packet arrived on the correct ACP, which helps prevent traffic spoofing. Inspect your routing configuration to determine that correct routes exist for all valid traffic. **Action:** The firewall drops the offending packet.	**Category:** Route Table Issue **Weight:** 5
352	**Unable to guess source interface for ICMP error packet contents**	
	Short Definition: Bad src iface for ICMP **Description:** Indicates that upon a route lookup, no source interface was found for the errored packet provided with an ICMP error message. The firewall performs a route lookup on the errored packet corresponding to the received ICMP error message. This is used to ensure that the ICMP error message matches an existing flow, helping to prevent an attacker from sending a malicious uninitiated ICMP error message. This threat could indicate a problem with the routing configuration or an uninitiated ICMP error message. Inspect your routing configuration to determine that correct routes exist for all valid traffic. **Action:** The firewall drops the offending ICMP error message.	**Category:** Route Table Issue **Weight:** 4

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
353	**Unable to find source interface for incoming packet!**	
	Short Definition: Bad src iface for pkt **Description:** Indicates that upon a route lookup, no source interface was found for the packet. The firewall performs a route lookup on the source of a packet in order to ensure that the packet arrived on the correct ACP, which helps prevent traffic spoofing. Inspect your routing configuration to determine that correct routes exist for all valid traffic. **Action:** The firewall drops the offending packet.	**Category:** Route Table Issue **Weight:** 4
400	**Ceiling for per-host associations reached; dropping packet**	
	Short Definition: Max per-host sessions **Description:** Indicates that the maximum number of connections have been established from a given host. Each ACP can be configured to enforce a maximum number of connections that can be established from any given host. This can be configured using the command **ip policy-class** <*ipv4 acp name*> **max-host-sessions** <*number*>. (By default, no limits are enforced on the number of sessions established from a given host.) If this limit is reached, it can indicate a possible port scan, or it can indicate that an attacker is initiating or propagating a DoS attack with the intention of consuming all of the available network resources. You can view the current host sessions using the CLI by issuing the command **show ip policy-class** [<*ipv4 acp name*>] **host-sessions**. **Action:** Any traffic exceeding the limit is dropped until the number of connections drops below the configured limit.	**Category:** Configuration-related **Weight:** 9
401	**Security policy configured but plain pkt received, dropping packet**	
	Short Definition: Plain pkt on secure iface **Description:** Indicates that an unencrypted packet was received on a connection marked for encrypted traffic. If a connection is to be used for VPN, the connection is associated with the appropriate IPSec SA to enforce that only encrypted traffic will arrive from a flow associated with a VPN tunnel. This prevents unauthorized traffic from being injected into a secure network. Verify that the remote endpoint of the VPN tunnel is properly encrypting the traffic before sending it. **Action:** The firewall drops the unencrypted packet.	**Category:** Configuration-related **Weight:** 6
450	**General attack detected, dropping packet**	
	Short Definition: General attack detected **Description:** No detailed information is available regarding this threat. **Action:** The firewall drops the offending packet.	**Category:** Miscellaneous **Weight:** 8

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
451	**Packet with unsupported IP protocol received, dropping packet**	
	Short Definition: Unsupported IP protocol **Description:** Indicates the receipt of a packet with an unsupported IP protocol. In order to properly inspect the statefulness of traffic flows, the firewall drops any IP protocols that are not well known. If NAT is not required, an unsupported IP protocol can be allowed through the firewall statelessly using a stateless allow in the ACP. Supported IP protocols include: • AH • ESP • GRE • ICMP • IGMP • OSPF • PIM • TCP • UDP • VRRP **Action:** The firewall drops the offending packet.	**Category:** Miscellaneous **Weight:** 3 **Check can be bypassed by using a stateless IPv4 ACP entry**
452	**Dropping ICMP packet of type <*type*>**	
	Short Definition: Unsupported ICMP type **Description:** Indicates the receipt of an ICMP packet with an unsupported type. In order to properly inspect the statefulness of ICMP traffic flows, the firewall drops any ICMP types that are not well known. If NAT is not required, an unsupported ICMP type can be allowed through the firewall statelessly using a stateless allow in the ACP. Supported ICMP types include the following: • Echo • Timestamp • Destination unreachable • Source quench • Time-to-live (TTL) exceeded **Action:** The firewall drops the offending packet.	**Category:** Miscellaneous **Weight:** 4 **Check can be bypassed by using a stateless IPv4 ACP entry**

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
550	**Spoofing detected, dropping packet**	
	Short Definition: Spoofing detected **Description:** Indicates the receipt of a packet on a different ACP than determined by a route lookup on the source of the packet. The firewall performs a route lookup on the source of packets to determine whether they have arrived on the correct ACP. A packet arriving on a different ACP than indicated by a route lookup may be spoofed. In certain routing configurations (for example, when policy-based routing (PBR) can act on certain packets of the flow), you might want to allow traffic to arrive on an ACP that differs from the results of the route lookup. If this is desired, use the command **no ip policy-class** *<ipv4 acp name>* **rpf-check** to disable the reverse path forwarding check for packets arriving at that ACP. **Action:** The firewall drops the offending packet.	**Category:** Spoofing **Weight:** 8
551	**Blind Spoofing attack detected**	
	Short Definition: Blind spoofing attack **Description:** Indicates the receipt of a TCP packet with the FIN flag set without the ACK flag. **Action:** The firewall drops the offending packet.	**Category:** Spoofing **Weight:** 8
552	**Echo response for uninitiated echo request (possible smurf attack), dropping packet**	
	Short Definition: Possible ICMP smurf attack **Description:** Indicates the receipt of an ICMP echo response for which no ICMP echo request was observed by the firewall. The firewall maintains the state of an ICMP connection and will attempt to match a response to its original request. If no corresponding request is found, the response is dropped. An uninitiated response can indicate a possible smurf attack, in which an attacker spoofs an ICMP echo request, typically to a broadcast address. The source of the request is spoofed to be the address of a legitimate server or other network resource, causing all of the hosts in the broadcast domain to flood the legitimate resource with responses. **Action:** The firewall drops the offending packet.	**Category:** Smurf Attack **Weight:** 9 **Check can be bypassed by using a stateless IPv4 ACP entry**
553	**UDP echo response received for uninitiated echo request (possible smurf attack), dropping packet**	
	Short Definition: Possible UDP smurf attack **Description:** Indicates the receipt of a UDP echo response for which no UDP echo request was observed by the firewall. The firewall maintains the state of a UDP connection and will attempt to match a response to its original request. If no corresponding request is found, the response is dropped. An uninitiated response can indicate a possible smurf attack, in which an attacker spoofs a UDP echo request, typically to a broadcast address. The source of the request is spoofed to be the address of a legitimate server or other network resource, causing all of the hosts in the broadcast domain to flood the legitimate resource with responses. **Action:** The firewall drops the offending packet.	**Category:** Smurf Attack **Weight:** 9 **Check can be bypassed by using a stateless IPv4 ACP entry**

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
554	**TCP Null Scan attack detected**	
	Short Definition: TCP Null scan attack **Description:** Indicates the receipt of a TCP packet with no flags set and a sequence number of zero. Since this packet provides no state information or data, its sole purpose is the anticipation of a response. This type of packet is used in a port scan to determine what TCP ports are open and whether services are listening on those ports. An attacker could use this information to later exploit a resource at that port. **Action:** The firewall drops the offending packet.	**Category:** TCP Null Scan Attack **Weight:** 8
555	**Crossed 80% of associations allocated. Possible TCP SYN flooding.**	
	Short Definition: Possible TCP SYN flood **Description:** Indicates that 80 percent of the maximum configured connections for an ACP are in use. **Action:** The firewall performs SYN flooding prevention using SYN cookies until the number of connections drops below 70 percent.	**Category:** TCP Syn Flood Attack **Weight:** 8
556	**Possible Land attack detected, dropping packet**	
	Short Definition: Possible Land attack **Description:** Indicates the receipt of a packet whose source and destination information is identical. An attacker could craft a packet of this type in order to exploit vulnerabilities in systems that do not handle these packets correctly. The packet is crafted so that the source and destination of the packet are an open port on a network resource. This will cause the vulnerable system to reply to itself continuously. **Action:** The firewall drops the offending packet.	**Category:** Land Attack **Weight:** 10
557	**Length in IP Header > Data length. Possible JOLT attack**	
	Short Definition: Possible JOLT attack **Description:** Indicates the receipt of fragments for which the total length reported in the IPv4 header is longer than the actual length of the reassembled packet, indicating a possible JOLT attack. Some systems cannot handle fragments of this type correctly. Because of this, an attacker could craft a fragment of this type in order to crash vulnerable systems or make them unresponsive. **Action:** The reassembly engine drops the offending fragments.	**Category:** JOLT Attack **Weight:** 10

Table B-1. Attack Log Messages *(Continued)*

ID	Message and Description	Category and Weight
558	**Ping of Death attack detected**	
	Short Definition: Ping of Death attack **Description:** Indicates the receipt of fragments whose total reassembled length exceeds 65535 bytes, the maximum length for an IPv4 packet. Because older operating systems often permitted a user to send ICMP echo requests with this characteristic, this attack is known as the ping of death. Some systems cannot handle fragments of this type correctly. Because of this, an attacker could craft fragments of this type in order to crash vulnerable systems or make them unresponsive. **Action:** The reassembly engine drops the offending fragments.	**Category:** Ping of Death **Weight:** 10
559	**Possible TARGA3 attack: UDP length > IP length - IP header length.**	
	Short Definition: Possible TARGA3 attack **Description:** Indicates the receipt of a packet or fragment matching the characteristics of a TARGA3 attack. The TARGA3 attack encompasses a wide variety of protocols, header options, offsets, invalid fragmentation, etc., expecting that systems could be vulnerable to at least some of the packets in the suite. **Action:** The reassembly engine drops the offending fragments.	**Category:** TARGA3 Attack **Weight:** 10
560	**Terminating connection as WinNuke Attack detected, OOB packet**	
	Short Definition: WinNuke attack **Description:** Indicates the receipt of a TCP packet with the urgent (URG) flag set. Sometimes such traffic is referred to as OOB traffic. Certain systems could be vulnerable to this attack because they cannot process the URG flag correctly. An attacker could craft a packet with this flag set in order to exploit this vulnerability. **Action:** The firewall drops the offending packet.	**Category:** WinNuke Attack **Weight:** 9
562	**FTP PORT misdirection attack**	
	Short Definition: FTP PORT misdirection **Description:** Indicates the receipt of an FTP PORT command that specifies a port below 1024. This threat is similar to an FTP bounce attack. An attacker can use the FTP PORT command to obtain access to low numbered ports on the same network resource as the FTP server. These will often be ports to which the attacker would not ordinarily have access, and the attacker could possibly access other services listening at those ports. Note that if the FTP ALG is disabled, this threat will not be detected. **Action:** The firewall drops the offending packet.	**Category:** FTP Port Misdirection **Weight:** 8

