ADTRAN Enterprise SBC

eSBC Firewall Bypass Deployment

Configuration Guide

6AOSSG0032-42A
November 2020

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Table of Contents

1. Overview

This document provides an overview of configuring ADTRAN's Enterprise Session Border Controller (eSBC) firewall bypass application, and it's deployment within existing networks. Included in this guide are a brief overview of the firewall bypass application and the basic command line interface (CLI) configuration required for deployment within SBC or hosted Voice over IP (VoIP) networks.

2. Firewall Bypass Deployment Overview

The firewall bypass application can be used in networks with an existing firewall to which an on-premise Public Branch Exchange (PBX) or hosted VoIP phones will be added. When the firewall bypass configuration is deployed in such networks, voice traffic bypasses the firewall and flows through the Session Initiation Protocol (SIP) proxy in a hosted VoIP scenario, or through the SBC in an on-premise PBX scenario without requiring configuration changes to any existing network elements or having to change the IP address of the firewall. The main configuration requirements for firewall bypass deployments revolve around creating a virtual local area network (VLAN) for the data traffic to flow between the existing firewall and the Internet router and configuring a separate routed interface for the voice traffic, thus using the SIP proxy or SBC functionality on the ADTRAN router for the voice traffic. This deployment requires three usable public IP addresses; one used for Internet routing, one used for firewall traffic, and one used for voice traffic routed to bypass the firewall. *Figure 1* illustrates the network topology in which an SBC device deploys the firewall bypass application for voice traffic, and *Figure 2 on page 5* illustrates the network topology in which the SIP proxy is used for firewall bypass applications in a hosted VoIP environment.

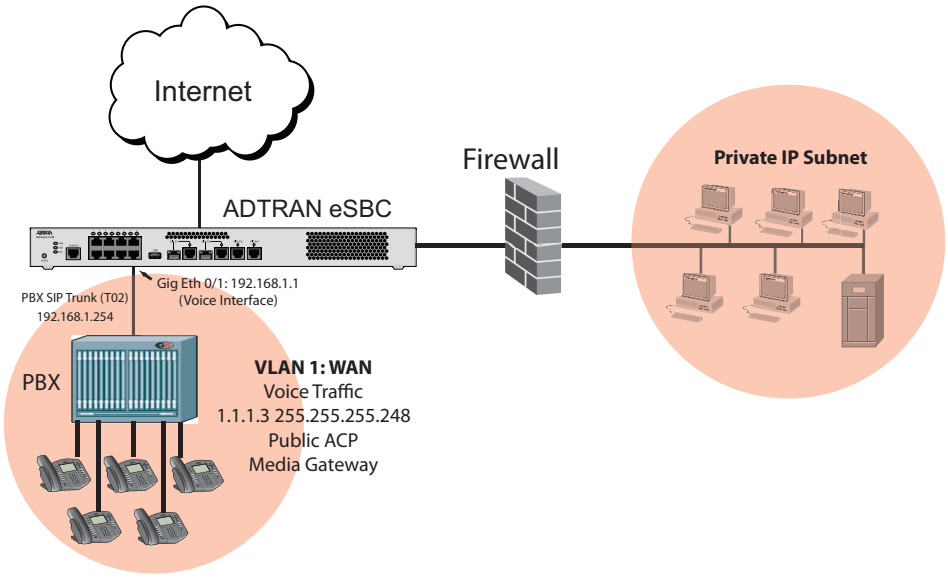

Figure 1. Firewall Bypass Deployment Using an SBC with an On-Premise PBX

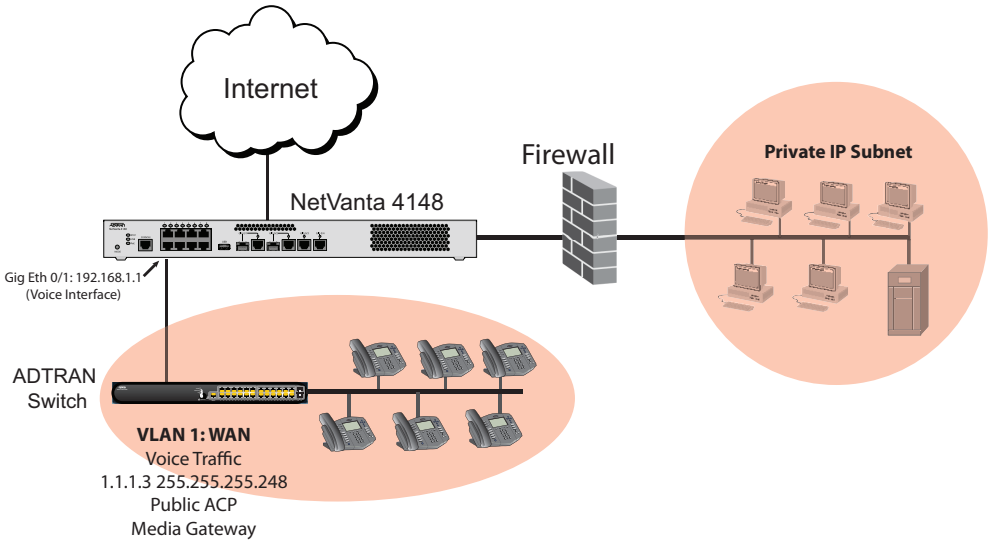

Figure 2. Firewall Bypass Deployment Using the SIP Proxy in Hosted VoIP Networks

3. Hardware and Software Requirements and Limitations

Firewall bypass deployments are supported on ADTRAN routers with switchports, specifically the NetVanta 3148/4148 Series products and the NetVanta 3448 SBC.

Configuration descriptions assume a familiarity with AOS commands and AOS CLI. For more information about specific commands, refer to the *AOS Command Reference Guide*, available in the ADTRAN Support Community.

4. Configuring the Firewall Bypass

Firewall bypass configuration consists of creating a VLAN for the data traffic to flow between the existing firewall and the Internet router and configuring a separate routed interface for the voice traffic, thus using the SIP proxy or SBC functionality on the ADTRAN router for the voice traffic. Both configuration scenarios require the following:

- A VLAN used for WAN traffic (includes a public access policy and IP address, and is enabled as a media gateway)
- A configured voice interface (includes IP address, appropriate access policy type, and an enabled media gateway)
- Two configured switchport interfaces: one for routed traffic, and one for firewall traffic
- Two configured access control policies (one for private VLAN voice traffic, and one for all public traffic)

The differences in configuration are detailed in the following sections.

Separate Voice VLAN SBC Configuration

The specific configuration needed on an SBC device to support the firewall bypass application includes the following:

- Specifying that voice features are handled by the network (using the **voice feature-mode network** command)

- Specifying that voice forwarding and transferring is handled by the local device (using the **voice forward-mode local** and **voice transfer-mode local** commands)
- Enabling the filtering of received nonsymmetric Realtime Transport Protocol (RTP) packets (using the **ip rtp symmetric-filter** command)
- Enabling media anchoring (using the **ip rtp media-anchoring** command)
- Configuring one voice trunk as the provider SIP trunk and another voice trunk as the PBX SIP trunk
- Configuring a PSTN trunk group and a PBX trunk group (using the **voice grouped-trunk PTSN** and **voice grouped-trunk PBX** commands)

Separate Voice VLAN SIP Proxy Configuration

The specific configuration needed to support the firewall bypass application when using SIP proxy includes the following:

- A Dynamic Host Control Protocol (DHCP) server pool configured for voice traffic (includes the network IP address, Dynamic Naming Server (DNS) address, and an IP address for the voice interface)
- Enabling SIP proxy and SIP transparent proxy (using the **sip proxy** and **sip proxy transparent** commands)
- Specifying that voice features and the voice forwarding are handled by the network (using the **voice feature-mode network** and **voice forward-mode network** commands)

5. Firewall Bypass Configuration Examples

The following section provides sample configuration for deploying the firewall bypass application in both an SBC device and a device using SIP proxy. In each configuration, voice VLANs are used to pass voice traffic from the public-facing WAN, through the AOS device, bypassing a configured firewall.

NOTE

The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. You should make the necessary adjustments to these configurations before adding them to your configuration to ensure they will function properly in your network.

Firewall Bypass Configuration in an SBC Device

The following configuration example creates a separate VLAN used for voice traffic in SBC devices to bypass the firewall in existing networks, as well as two SIP trunks to use for the PBX and voice traffic, and configures switchports for routed Internet and firewall data traffic. *Figure 1 on page 4* describes the network topology for this example.

```
hostname "NV4148"
enable password password
!
clock timezone -6-Central-Time
!
ip subnet-zero
ip classless
ip routing
ipv6 unicast-routing
!
```

```
domain-proxy
name-server 4.2.2.2
!
auto-config
!
event-history on
no logging forwarding
no logging email
!
no service password-encryption
!
username "admin" password "password"
!
ip firewall
no ip firewall alg msn
no ip firewall alg mszone
no ip firewall alg h323
!
vlan 1
  name "WAN"
!
interface gigabit-eth 0/1
  description voice interface
  ip address 192.168.1.1
  ip access-policy Private
  media-gateway ip primary
  no shutdown
!
interface gigabit-eth 0/2
  no ip address
  shutdown
!
interface gigabit-eth 0/3
  no ip address
  shutdown
!
interface gigabit-eth 0/4
  no ip address
  shutdown
!
interface gigabit-switchport 0/1
  description Internet Router
  no shutdown
!
interface gigabit-switchport 0/2
  description Firewall
  no shutdown
!
interface gigabit-switchport 0/3
  no shutdown
!
interface gigabit-switchport 0/4
  no shutdown
!
```

```
interface gigabit-switchport 0/5
  no shutdown
!
interface gigabit-switchport 0/6
  no shutdown
!
interface gigabit-switchport 0/7
  no shutdown
!
interface gigabit-switchport 0/8
  no shutdown
!
interface vlan 1
  ip address  1.1.1.3 255.255.255.248
  ip access-policy Public
  media-gateway ip primary
  no shutdown
!
ip access-list extended matchall
  permit ip any  any
!
ip policy-class Private
  allow list matchall self
  nat source list matchall interface vlan 1 overload
!
ip policy-class Public
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
!
no tftp server
no tftp server overwrite
http server
http secure-server
snmp agent
ip ftp server
no ip scp server
ip sntp server
!
sip
sip udp 5060
no sip tcp
no sip tls
!
voice feature-mode network
voice forward-mode local
voice transfer-mode local
!
ip rtp symmetric-filter
ip rtp media-anchoring
!
voice trunk T01 type sip
  description "Provider SIP Trunk"
  sip-server primary sip.provider.com
!
```

```
voice trunk T02 type sip
  description "PBX SIP Trunk"
  sip-server primary 192.168.1.254
  transfer-mode network
  grammar from host local
!
voice grouped-trunk PSTN
accept NXX-NXX-XXXX
!
voice grouped-trunk PBX
accept NXXX
!
line con 0
  no login
!
line telnet 0 4
  login
  password password
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
end
```

Firewall Bypass Configuration Using SIP Proxy

The following configuration example creates a separate VLAN used for voice traffic in a hosted VoIP environment using the SIP proxy, and configures separate switchports for routed Internet and firewall data traffic. *Figure 2 on page 5* describes the network topology for this example.

```
hostname "NV4148"
enable password password
!
clock timezone -6-Central-Time
!
ip subnet-zero
ip classless
ip routing
ipv6 unicast-routing
!
domain-proxy
name-server 4.2.2.2
!
auto-config
!
event-history on
no logging forwarding
no logging email
!
no service password-encryption
!
username "admin" password "password"
!
```

```
ip firewall
no ip firewall alg msn
no ip firewall alg mszone
no ip firewall alg h323
!
ip dhcp pool "Voice"
  network 192.168.1.0 255.255.255.0
  dns-server 192.168.1.1
  default-router 192.168.1.1
!
vlan 1
  name "WAN"
!
interface gigabit-eth 0/1
  description voice interface
  ip address 192.168.1.1
  ip access-policy Private
  media-gateway ip primary
  no shutdown
!
interface gigabit-eth 0/2
  no ip address
  shutdown
!
interface gigabit-eth 0/3
  no ip address
  shutdown
!
interface gigabit-eth 0/4
  no ip address
  shutdown
!
interface gigabit-switchport 0/1
  description Internet Router
  no shutdown
!
interface gigabit-switchport 0/2
  description Firewall
  no shutdown
!
interface gigabit-switchport 0/3
  no shutdown
!
interface gigabit-switchport 0/4
  no shutdown
!
interface gigabit-switchport 0/5
  no shutdown
!
interface gigabit-switchport 0/6
  no shutdown
!
interface gigabit-switchport 0/7
  no shutdown
```

```
!
interface gigabit-switchport 0/8
  no shutdown
!
interface vlan 1
  ip address  1.1.1.3 255.255.255.248
  ip access-policy Public
  media-gateway ip primary
  no shutdown
!
ip access-list extended matchall
  permit ip any  any
!
ip policy-class Private
  allow list matchall self
  nat source list matchall interface vlan 1 overload
!
ip policy-class Public
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
!
no tftp server
no tftp server overwrite
http server
http secure-server
snmp agent
ip ftp server
no ip scp server
ip sntp server
!
sip
sip udp 5060
no sip tcp
no sip tls
!
sip proxy
sip proxy transparent
!
voice feature-mode network
voice forward-mode network
!
line con 0
  no login
!
line telnet 0 4
  login
  password password
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
end
```

6. Warranty and Contact Information

Warranty

Warranty information can be found at: www.adtran.com/warranty.

Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. **Technical Support:** • Web: **Training:** • Email: • Web:	1-888-4ADTRAN (1-888-423-8726) + 1 (256) 963-8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1-800-827-0807