NetScreen-5GT Wireless Reference Guide

ScreenOS 5.0.0-WLAN

P/N 093-1483-000

Rev. B

Copyright Notice

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Preface

This document describes the wireless features available on the Juniper Networks NetScreen-5GT Wireless device. It is organized into the following chapters:

- Chapter 1, "Wireless" describes the wireless feature on the NetScreen device and presents example configurations.
- Chapter 2, "New and Modified CLI Commands" describes ScreenOS CLI commands that are new or changed for wireless support.
- Chapter 3, "New Messages" describes messages that are new for wireless support.

See the *NetScreen-5GT Wireless User's Guide* for information about installing the device and performing basic configuration.

This document is intended to be a supplement to the ScreenOS 5.0.0 documentation set. For more information about ScreenOS features, CLI commands, and messages, refer to the following documents:

- *NetScreen Concepts & Examples ScreenOS Reference Guide*
- *NetScreen CLI Reference Guide*
- *NetScreen Message Log Reference Guide*

CONVENTIONS

This book presents two management methods for configuring a NetScreen device: the Web user interface (WebUI) and the command line interface (CLI). The conventions used for both are introduced below.

WebUI Navigation Conventions

Throughout this book, a single chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links.

Example: Objects > Addresses > List > New

To access the new address configuration dialog box, do the following:

1. Click **Objects** in the menu column.

   The Objects menu option expands to reveal a subset of options for Objects.

2. (Applet menu) Hover the mouse over **Addresses**.

   (DHTML menu) Click **Addresses**.

   The Addresses option expands to reveal a subset of options for Addresses.

3. Click **List**.

   The address book table appears.

4. Click the **New** link in the upper right corner.

   The new address configuration dialog box appears.

CLI Conventions

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means “set the management options for the ethernet1, ethernet2, or ethernet3 interface”.
- Variables appear in *italic.* For example:

  ```
  set admin user name password
  ```

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: “Use the **get system** command to display the serial number of a NetScreen device.”

Note: *When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing* ***set adm u joe j12fmt54*** *is enough to enter the command* ***set admin user joe j12fmt54****. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

NETSCREEN DOCUMENTATION

To obtain technical documentation for any Juniper Networks NetScreen product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs-comments@juniper.net

1

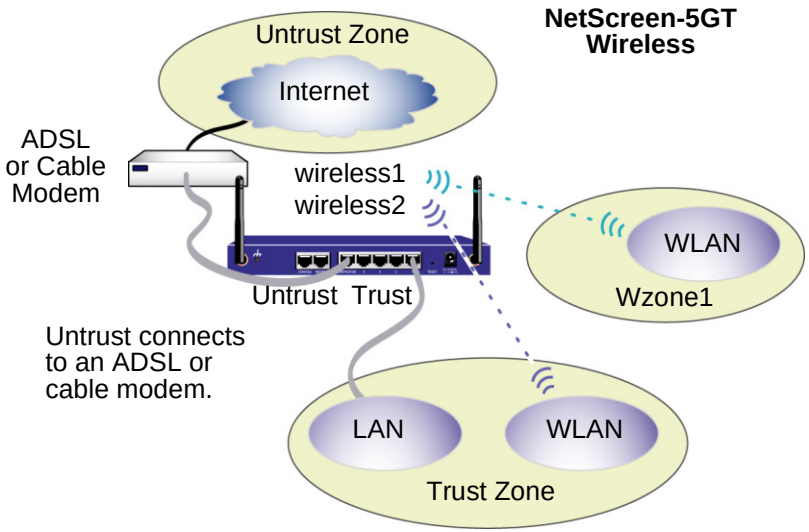
Wireless

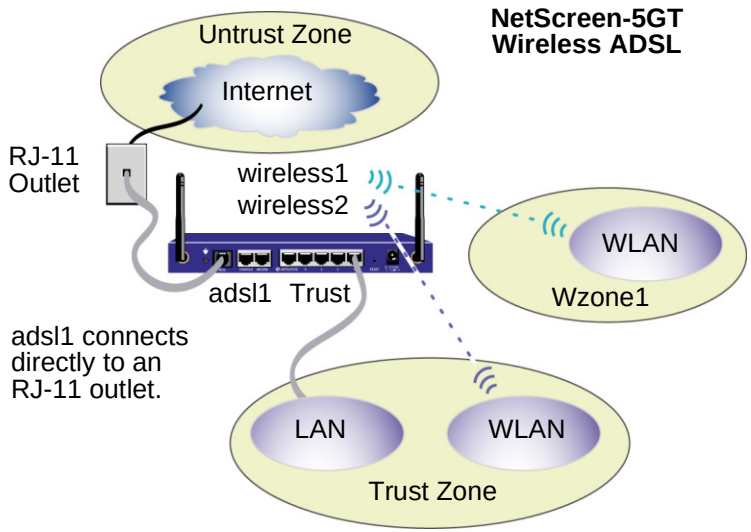
Juniper Networks offers two wireless versions of the NetScreen-5GT security device:

- Juniper Networks NetScreen-5GT Wireless
- Juniper Networks NetScreen-5GT Wireless ADSL

Both devices provide wireless local area network (WLAN) connectivity for resources in their protected security zones. The difference between them is how each device connects to the public network in its Untrust zone:

- The Untrust interface on the NetScreen-5GT Wireless must make an ethernet connection to an external router such as an ADSL or cable modem.
- The NetScreen-5GT Wireless ADSL has ADSL modem functionality. Through its adsl1 interface, this device connects directly to an RJ-11 outlet and can establish and maintain an ADSL connection with an ISP's Digital Subscriber Line Access Multiplexer (DSLAM).





This section describes the major wireless features on the NetScreen device and provides example configurations. The specific topics covered are as follows:

Note: *For information about ScreenOS features, see the NetScreen Concepts & Examples ScreenOS Reference Guide. For information about configuring ADSL features on the NetScreen-5GT Wireless ADSL device, see the NetScreen-5GT ADSL Reference Guide.*

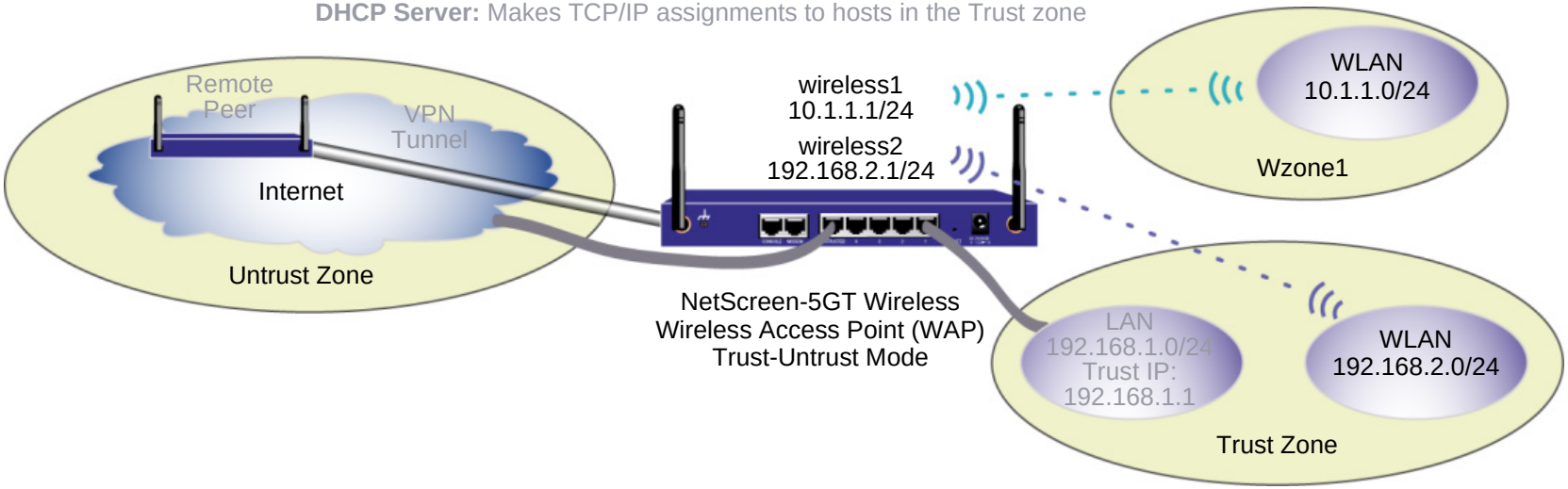
WIRELESS ACCESS POINT

The NetScreen-5GT Wireless (ADSL) device can perform several key functions in a network:

- Firewall
- VPN termination point
- Router
- Network Address Translation (NAT) device
- Dynamic Host Configuration Protocol (DHCP) server
- Wireless access point (WAP)

Network Functions Provided by the NetScreen-5GT Wireless

Firewall: Controls traffic through policy enforcement
VPN: Terminates VPN traffic from remote peer
Router: Routes traffic between interfaces to the next hop
WAP: Connects wireless devices to wired and other wireless networks
NAT: Translates source IP addresses on outbound traffic from private to public addresses
DHCP Server: Makes TCP/IP assignments to hosts in the Trust zone



This section discusses its use as a wireless access point (WAP). For information on its other uses, refer to the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

The basic purpose of a WAP is to connect a wireless network with a wired network. It can also connect multiple wireless networks with each other. To provide this functionality, the NetScreen-5GT Wireless uses ScreenOS 5.0.0-WLAN to manage a distribution system (DS) of one to eight basic service sets (BSSs)[1]. A BSS cannot belong to more than one security zone. By separating each BSS into a different security zone, the NetScreen-5GT can enforce different sets of firewall policies and require different levels of device authentication and encryption. This kind of segmentation allows you to apply appropriate levels of security on a per-zone basis.

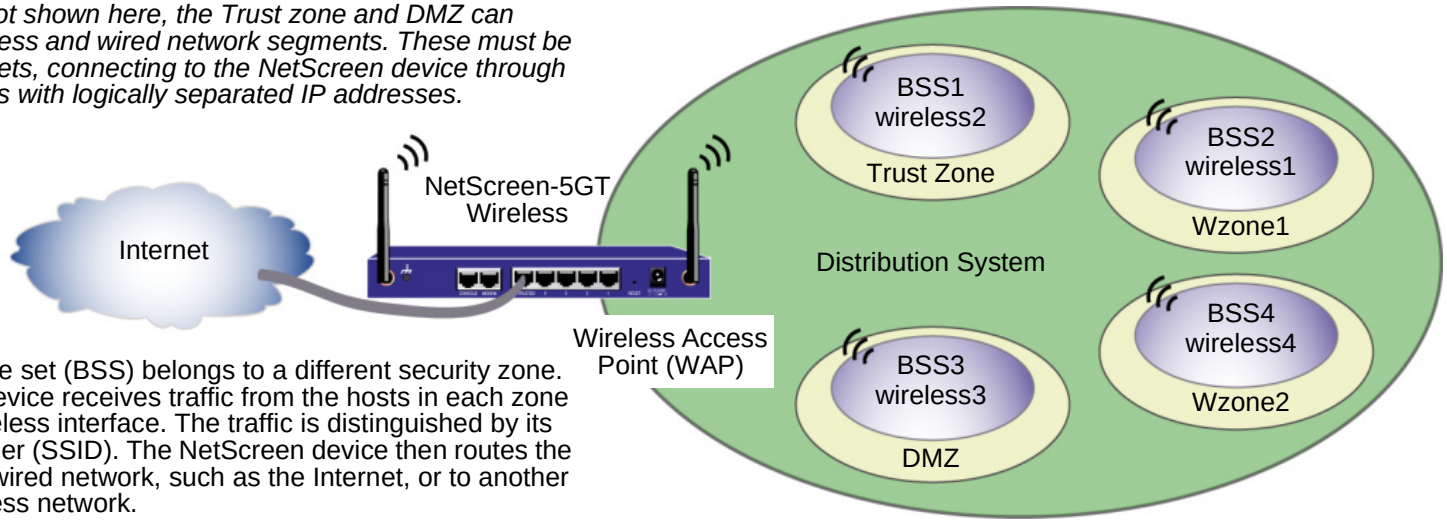
To distinguish one BSS from another, you assign each one a different name. This name is a unique identifier, called a service set identifier (SSID). Each host in a particular BSS must have the same SSID as that configured for that BSS on the NetScreen device.

You can also use the SSID client isolation option to prohibit wireless clients in the same subnet from communicating directly with each other and thereby bypassing the NetScreen firewall. By default, this option is disabled. To prohibit wireless clients from communicating directly with other wireless clients in the same subnet, enable this option.

(WebUI) Wireless > SSID > Edit (for a specific SSID): Select **SSID Client Isolation**, and then click **OK**.

(CLI) set ssid *name_str* client-isolation

Note: *Although not shown here, the Trust zone and DMZ can contain both wireless and wired network segments. These must be on separate subnets, connecting to the NetScreen device through different interfaces with logically separated IP addresses.*



Each basic service set (BSS) belongs to a different security zone. The NetScreen device receives traffic from the hosts in each zone on a different wireless interface. The traffic is distinguished by its service set identifier (SSID). The NetScreen device then routes the traffic either to a wired network, such as the Internet, or to another BSS on the wireless network.

1. You can create up to eight basic service sets, but a maximum of only four can be in use at one time. Having extra service sets defined and ready allows you to activate just the ones that are site-specific or time-specific by binding and unbinding their corresponding SSIDs to interfaces as changing needs warrant.

RADIO

Integrated into the NetScreen-5GT Wireless is a radio transmitter/receiver with a frequency range of 2.4GHz to 2.4835GHz. As such, the NetScreen-5GT Wireless supports the IEEE 802.11b and 802.11g standards.

Antennas

You have a choice of three types of custom-built radio antennas:

- **Diversity antennas** – The pair of diversity antennas provides 2dBi omnidirectional coverage. Diversity antennas provide a fairly uniform level of signal strength within the area of coverage and are suitable for most installations. They ship with the NetScreen-5GT Wireless device.
- **External omnidirectional antenna** – The external antenna also provides 2dBi omnidirectional coverage. Unlike diversity antennas, which function as a pair, an external antenna operates singly to eliminate an echo effect that can sometimes occur from slight delay characteristics in signal reception when two are in use. When using an external antenna, attach it either to the antenna A port (nearest the power connector) or to the antenna B port. By default, both antenna ports are enabled. The term for this setting is “Diversity”. To enable only antenna A or B, do the following:

  (WebUI) Wireless > General Settings: Select **A** or **B** from the Antenna Diversity drop-down list, and then click **Apply**.

  (CLI) set wlan antenna { a | b }

  If you rack mount the NetScreen-5GT Wireless or otherwise put it in a place where its signal is restricted, you can cable the external antenna to the device and relocate it to improve its signal strength.
- **External directional antenna** – The external directional antenna provides 2dBi unidirectional coverage. The directional antenna is well suited for such places as hallways and outer walls (facing inward).

Channels

The regulatory domain for channel assignments is preset in the factory as FCC (USA), TELEC (Japan), or WORLD (all countries)[2]. If the regulatory domain is preset for FCC or TELEC, you cannot select a country. If it is preset for WORLD, then you must select a country, which can also include the USA or Japan.

Note: *Although you can select an "Extended Channel Mode" option when the regulatory domain is WORLD and the selected country code is USA, there are no extended channels in the USA.*

The NetScreen-5GT Wireless (ADSL) device uses the same channel for all basic service sets (BSSs), which share the same overall bandwidth. The NetScreen device distinguishes traffic from different BSSs by the SSID number. The NetScreen device automatically selects the appropriate channel based on the country code that you enter (unless you manually select a specific channel). To enter the country code, do either of the following:

(WebUI) Wireless > General Settings: Select the country from the Country Code drop-down list, and then click **Apply**.

(CLI) set wlan country-code *name_str*

Wireless Clients

The maximum number of wireless clients that can connect to the NetScreen-5GT Wireless (ADSL) device concurrently is 60.

2. The regulatory domain is not user-configurable.

WIRELESS INTERFACES

A wireless interface is a logical interface that is prebound to a security zone. The wireless interface-to-security zone mapping is as follows:

Wireless Interfaces	Security Zones
Wireless1	Wzone1
Wireless2	Trust or Work
Wireless3	DMZ or Home
Wireless4*	Wzone2*

* Wireless4 and Wzone2 are only available on the NetScreen-5GT Wireless (ADSL) after the Extended license key has been installed and you have changed the port mode to Extended.

The security zone to which Wireless2 and Wireless3 are prebound depends on the port mode that is in effect. To see the interface-to-zone mappings for each port mode, refer to “Interface-to-Zone Bindings” on page 8.

Each wireless interface must be in a separate subnet from all other interfaces—both wired and wireless. You can configure a wireless interface very similarly to an ethernet interface. For example, you can configure the following for a wireless interface:

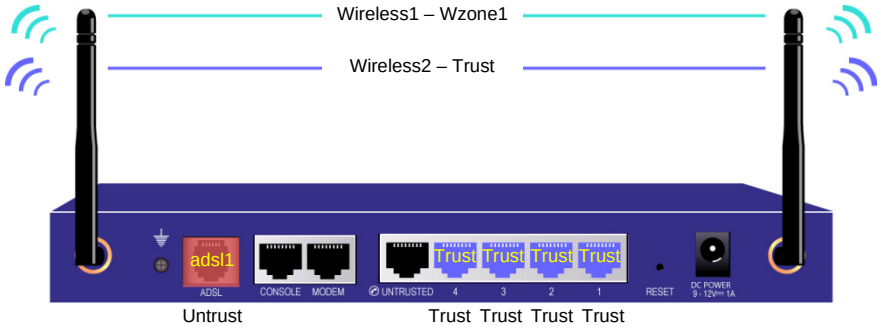
- IP address/netmask and manage IP address
- Management options
- Address translation functionality
- DHCP server functionality

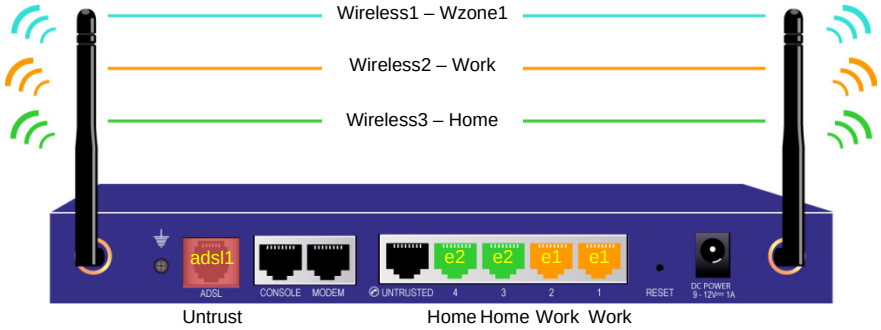
An important difference between a wireless and wired interface is that you must associate a service set identifier (SSID) with a wireless interface. The SSID links its basic service set (BSS) with the interface, which in turn is prebound to a security zone. Because there can be only one BSS per security zone, the policies you apply to that zone also apply to the BSS in that zone.

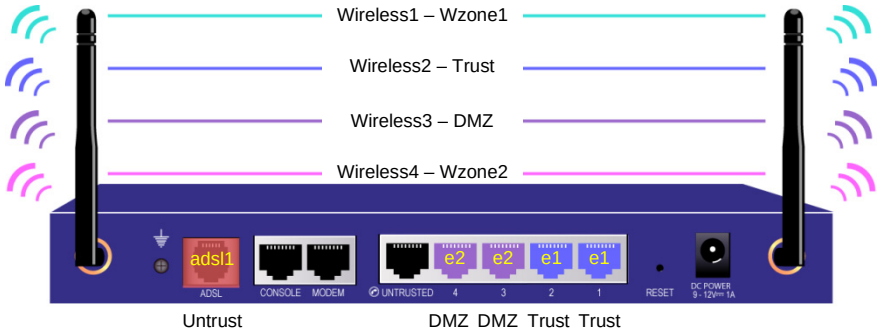
Interface-to-Zone Bindings

The following illustrations and tables present the interface-to-zone bindings for each port mode. Both the NetScreen-5GT Wireless ADSL and the NetScreen-5GT Wireless devices are shown.

NetScreen-5GT Wireless ADSL Port Modes

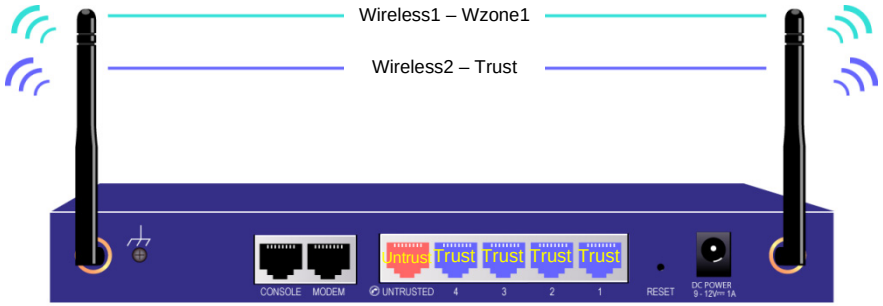




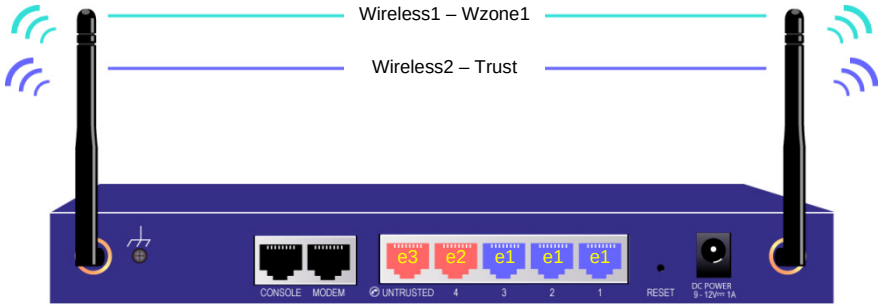


Port Modes	Wireless Interfaces	Security Zones
Trust/Untrust	Wireless1	Wzone1
	Wireless2	Trust
Home/Work	Wireless1	Wzone1
	Wireless2	Work
	Wireless3	Home
Extended	Wireless1	Wzone1
	Wireless2	Trust
	Wireless3	DMZ
	Wireless4	Wzone2

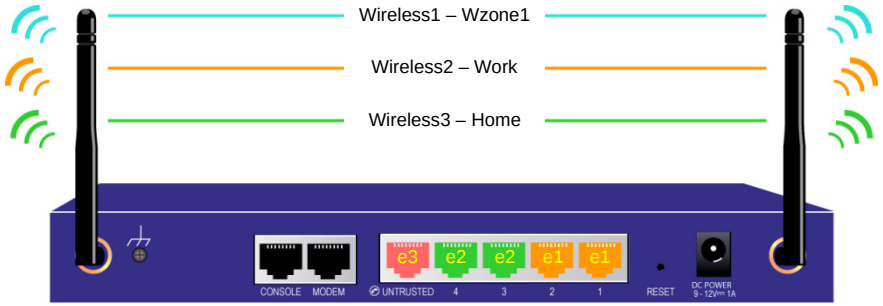
NetScreen-5GT Wireless Port Modes



Untrust Trust Trust Trust Trust



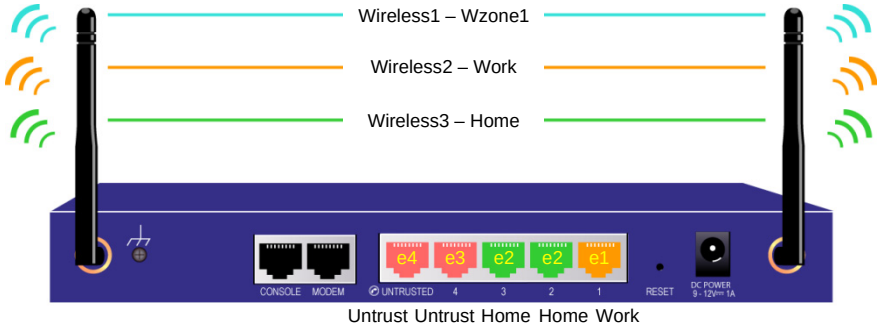
Untrust Untrust Trust Trust Trust

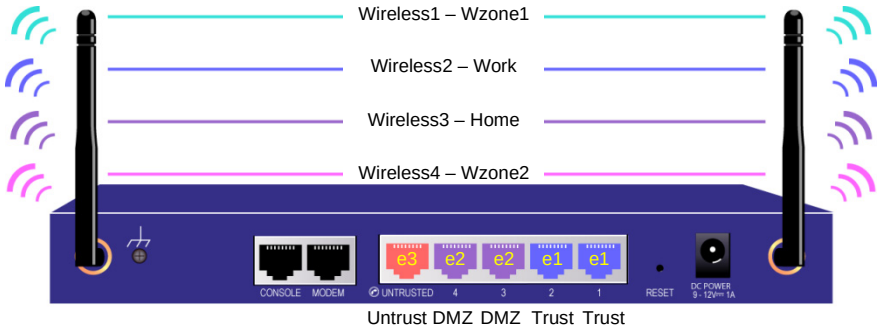


Untrust Home Home Work Work

Port Modes	Wireless Interfaces	Security Zones
Trust/Untrust	Wireless1	Wzone1
	Wireless2	Trust
Dual Untrust	Wireless1	Wzone1
	Wireless2	Trust
Home/Work	Wireless1	Wzone1
	Wireless2	Work
	Wireless3	Home

NetScreen-5GT Wireless Port Modes (Continued)





Port Modes	Wireless Interfaces	Security Zones
Combined	Wireless1	Wzone1
	Wireless2	Work
	Wireless3	Home
Extended	Wireless1	Wzone1
	Wireless2	Trust
	Wireless3	DMZ
	Wireless4	Wzone2

Basic Service Set

A basic service set (BSS) has three major components that you must configure before a wireless client can connect to the NetScreen device through a wireless interface:

- Service set identifier (SSID)
- Wireless interface binding
- Authentication and encryption options

The first two components are relatively simple. For authentication and encryption, Juniper Networks offers a broad set of mechanisms. These options are presented in a following section.

SSID – The SSID is a unique name that you use for the BSS. To create an SSID, do either of the following:

(WebUI) Wireless > SSID > New: Enter a name in the the SSID field, and then click **OK**.

(CLI) set ssid name *name_str*

Note: *(CLI) If the SSID name string contains one or more spaces, enclose it within quotation marks.*

For a slight increase to security, consider not broadcasting the SSID, and making it difficult to guess; that is, use a mix of upper- and lowercase letters, numbers, and symbols. Also, do not give the SSID a meaningful name that an attacker might use, such as the department or location of the WAP[3].

Wireless Interface Binding – You must associate a BSS with a security zone. To do that, you reference the SSID for that BSS with the wireless interface bound to a zone. To bind a BSS to a wireless interface, do either of the following:

(WebUI) Wireless > SSID > Edit (for the basic service set that you want to bind to an interface): Select an interface from the Wireless Interface Binding drop-down list, and then click **OK**.

or

Network > Interfaces > Edit (for the interface to which you want to bind a basic service set): Select the SSID from the Bind to SSID drop-down list, and then click **OK**.

(CLI) set ssid *name_str* interface *interface*

3. To suppress an SSID broadcast, do either of the following: (WebUI) Wireless > SSID > Edit (for *name_str*): Select **Disable SSID Broadcast**; or (CLI) set ssid *name_str* ssid-suppression. Broadcast suppression offers only a slight increase to security because an attacker can still detect the SSID by sniffing WLAN connection requests. However, it might reduce opportunistic attacks by making the attacker's job that extra bit more difficult.

Authentication and Encryption

The settings for authentication and encryption are specific to each basic service set (BSS). This flexibility allows you to apply differing levels of security as appropriate to the resources in each BSS.

Juniper Networks offers two main authentication and encryption mechanisms: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

WEP

The Wired Equivalent Privacy (WEP) provides confidentiality for wireless communication. It uses the Rivest Cipher 4 (RC4) stream cipher algorithm to encrypt and decrypt data as it travels over the wireless link. You can store WEP keys locally on the NetScreen device or externally on an external authentication server. Wireless network users store one or more of the same keys on their systems and identify them with the same ID numbers.

There are two authentication mechanisms for WEP:

- **Open key authentication:** The wireless client simply supplies the correct SSID for the wireless access point (WAP) to authenticate it.

  This form of authentication is so minimal—especially if you configure the NetScreen device to broadcast the SSID—that it arguably offers no authentication check at all. However, if you enable WEP encryption, an authenticated wireless client still needs the WEP key to encrypt and decrypt communication. Without that key, even after being authenticated, a wireless user cannot communicate with the WAP over the WLAN.

- **Shared key authentication:** Both the WAP and wireless client have the same key. When the client contacts the WAP, it replies with a clear-text challenge text string that the client must then encrypt with the correct WEP key and return to the WAP. When the WAP receives the encrypted string from the client, it decrypts it, and compares it with the original. If they match, authentication is successful. If the client's decrypted string does match the original string, authentication fails. If the client does not reply because there is no key, authentication fails.

  This approach also has a serious security problem. If an attacker intercepts both the clear-text challenge and the same challenge encrypted with a WEP key, he can potentially decipher the WEP key. After gaining the key, the attacker can first use it to authenticate his system, and then use it for encryption and decryption as he communicates with the WAP over the WLAN. In the end, if you decide to use WEP, you must weigh the risks between open authentication or potentially exposing the WEP key by using shared keys.

Juniper Networks supports two WEP key lengths: 40 and 104 bits. Because the keys are concatenated with a 24-bit initialization vector (IV), the resulting lengths are 64 and 128 bits. Some third-party wireless clients include the 24-bit IV when specifying their WEP key lengths. Therefore, if there are any connectivity issues, remember that the same WEP key length described as 40 or 104 bits on the NetScreen-5GT Wireless (ADSL) might actually be the same length as a key described as 64 or 128 bits on a client. The WEP combinations for an individual SSID are as follows:

Authentication	Encryption	Configuration
WEP Shared Key	WEP Shared Key	(WebUI) Wireless > SSID (Edit for *name_str*): Select **WEP Shared Key**. (CLI) set ssid *name_str* authentication shared-key The WEP shared key option requires a WEP key stored locally. To create it: (WebUI) Wireless > SSID (Edit for *name_str*) > WEP Key: Enter the settings, and then click **Add**. (CLI) set ssid *name_str* key-id *number* length *number* method { asciitext | hexadecimal } *string* [default]
Open	None	(WebUI) Wireless > SSID (Edit for *name_str*): Select **Open** and **No Encryption**. (CLI) set ssid *name_str* auth open encrypt none
Open	WEP Key	(WebUI) Wireless > SSID (Edit for *name_str*): Select **Open** and **WEP Encryption**, and choose one of the following: • **Local** if the key is stored on the NetScreen device • **Server** if the key is on an external RADIUS auth server • **Both** if you store some WEP keys locally on the NetScreen device, and a RADIUS server negotiates others (For information about default key ID numbers, see "Multiple WEP Keys" on page 14.) (CLI) set ssid *name_str* authentication open encryption wep key-source { local | server | both } Note that before you can reference a locally stored key, you must first create it: (WebUI) Wireless > SSID (Edit for *name_str*) > WEP Key: Enter the settings, and then click **Add**. (CLI) set ssid *name_str* key-id *number* length *number* method { asciitext | hexadecimal } *string* [default]

ScreenOS provides a mechanism for automatically negotiating with a wireless client whether or not it authenticates itself with a WEP shared key. Using this option can improve compatibility if you want to allow access to wireless devices using various operating systems that support different implementations of WEP. To enable this option, do either of the following:

(WebUI) Wireless > SSID (Edit for *name_str*): Select **Auto**.

(CLI) set ssid *name_str* authentication auto

Note: *Although you can configure WEP for all the basic service sets (BSSs), the NetScreen-5GT Wireless (ADSL) device intentionally restricts its use to only one BSS at a time. Juniper Networks recommends using WPA.*

Multiple WEP Keys

It is possible to define only one WEP key on the NetScreen device for a basic service set (BSS) to use. The NetScreen device, acting as a wireless access point (WAP), uses that key for authenticating wireless clients in that BSS, and for encrypting and decrypting traffic sent between itself and the clients.

You can also define multiple WEP keys on the NetScreen device—up to four keys for a single basic service set (BSS). The NetScreen device uses the WEP key specified as “default” for encryption, and another key (or the default key again) for authentication and decryption. If you do not specify a key as the default, the first key you define becomes the default. Using multiple keys allows you to adjust the level of security for different wireless clients within the same BSS. You can use longer keys to provide greater security for some traffic and smaller keys to reduce processing overhead for other, less critical traffic.

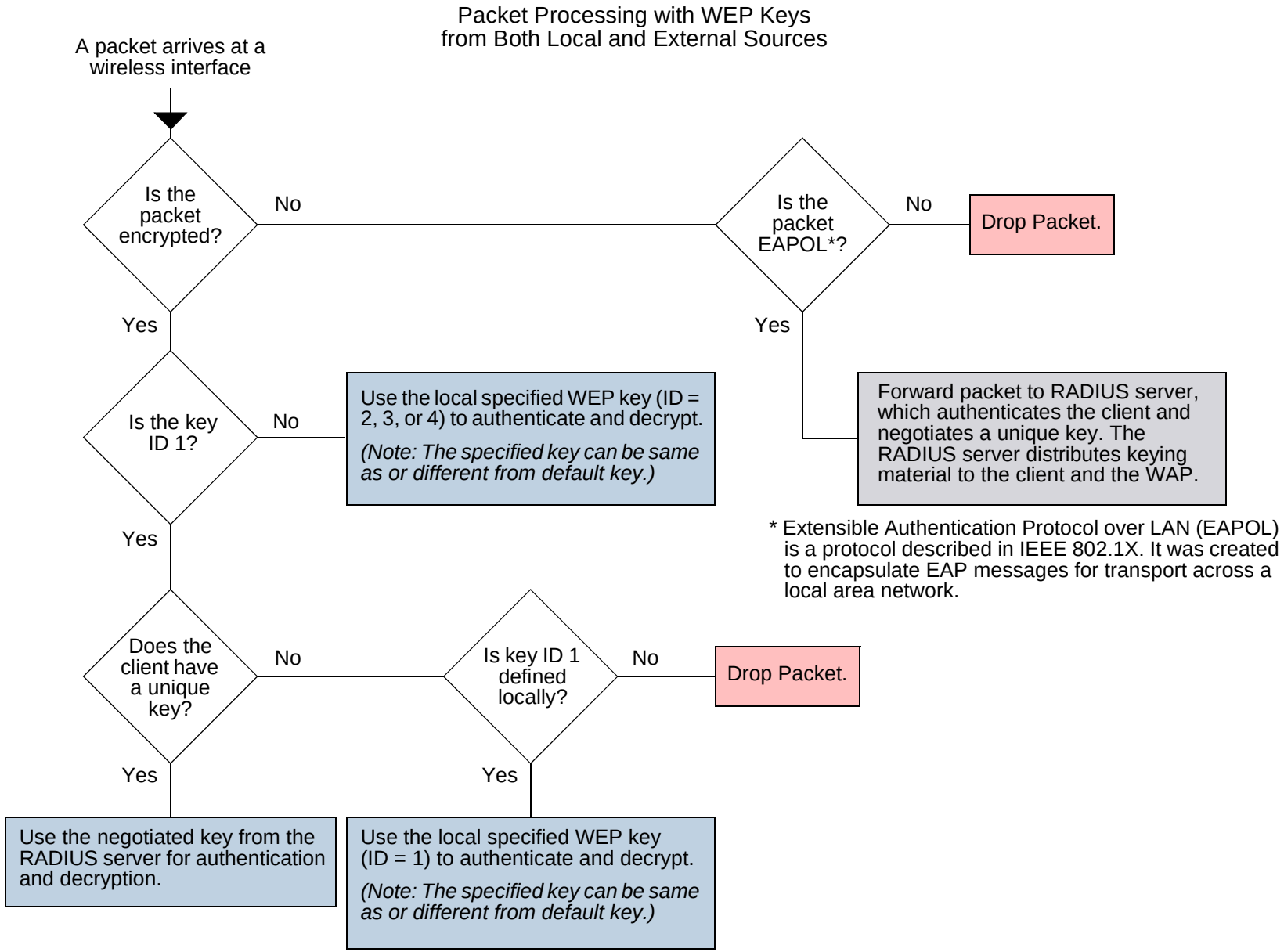
Note the following points about WEP key storage and key ID numbers:

- When clients use a unique, dynamically created WEP key from an external RADIUS server, the WAP uses this unique specific key—which it also receives from the RADIUS server—for bidirectional communication.
- When wireless clients use statically defined WEP keys stored locally on the NetScreen device, the WAP uses the default key to encrypt all wireless traffic that it transmits. The clients must also have this key loaded to be able to decrypt traffic from the WAP.
  - If you store all WEP keys on the NetScreen device, the default key ID can be 1, 2, 3, or 4.
  - If you store some WEP keys on the NetScreen device and use dynamically created WEP keys from an external RADIUS server, the ID for the default WEP key on the NetScreen device cannot be 1 because the RADIUS server uses 1 as the ID for all its keys. The NetScreen device can use a default WEP key with key ID 2, 3, or 4 for encryption, and it can use a statically defined WEP key with ID 1, 2, 3, or 4 for authentication and decryption.
  - If you exclusively use WEP keys from a RADIUS server, the server uses a key ID of 1 for all its keys. RADIUS creates and distributes a different key per session for each client.
- You can specify a different locally stored key for the WAP to use when authenticating and decrypting traffic it receives from wireless clients. The clients must have this key and its ID number loaded to be able to authenticate themselves and encrypt traffic sent to the WAP. (If a client does not supply a key ID, the WAP tries to use the default WEP key to authenticate the client and decrypt its traffic.)

  Note: *If a client uses only one key for encryption, decryption, and authentication, then it must use the default WEP key.*

The flow chart on the following page presents the how the NetScreen device processes a wireless connection request when WEP keys are stored locally and when they come from a RADIUS server. By understanding the flow, together with the key ID details explained above, you can better design your WEP key implementation for each BSS.

Note: *The NetScreen-5GT Wireless (ADSL) device supports 802.1X-compliant RADIUS servers, such as the Funk Odyssey RADIUS server and the Microsoft Internet Authentication Service (IAS) RADIUS server.*


Packet Processing with WEP Keys
from Both Local and External Sources
A packet arrives at a wireless interface
Is the packet encrypted?
No
Is the packet EAPOL*?
No
Drop Packet.
Yes
Yes
Forward packet to RADIUS server, which authenticates the client and negotiates a unique key. The RADIUS server distributes keying material to the client and the WAP.
Is the key ID 1?
No
Use the local specified WEP key (ID = 2, 3, or 4) to authenticate and decrypt.
(Note: The specified key can be same as or different from default key.)
Yes
* Extensible Authentication Protocol over LAN (EAPOL) is a protocol described in IEEE 802.1X. It was created to encapsulate EAP messages for transport across a local area network.
Does the client have a unique key?
No
Is key ID 1 defined locally?
No
Drop Packet.
Yes
Yes
Use the negotiated key from the RADIUS server for authentication and decryption.
Use the local specified WEP key (ID = 1) to authenticate and decrypt.
(Note: The specified key can be same as or different from default key.)

WPA

Wi-Fi Protected Access (WPA) is a more secure solution to the issues of WLAN authentication and encryption and was designed in response to many of the weaknesses in WEP. There are currently two versions: WPA and WPA2.

Note: *In the current ScreenOS release, the NetScreen-5GT Wireless (ADSL) device only supports WPA.*

WPA supports an enterprise mode that uses the Extensible Authentication Protocol (EAP) for authentication through a RADIUS server[4]. When applying WPA in enterprise mode, the NetScreen device forwards authentication requests and replies between the wireless clients and the RADIUS server. After successfully authenticating a client, the RADIUS server sends an encryption key to both the client and to the NetScreen device. From that point on, the NetScreen-5GT Wireless manages the encryption process, including the encryption type—Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES)—and the rekey interval[5].

Note: *The NetScreen-5GT Wireless (ADSL) device supports 802.1X-compliant RADIUS servers, such as the Funk Odyssey RADIUS server and the Microsoft IAS RADIUS server.*

WPA also supports a personal mode that uses preshared keys stored on the WAP (that is, on the NetScreen-5GT Wireless device) and on all the wireless clients.

4. EAP is an encapsulation protocol used for authentication and operates at the Data Link Layer (Layer 2) in the OSI model. For more information, refer to RFC 2284, “PPP Extensible Authentication Protocol (EAP)“.

5. For information about TKIP, see the IEEE standard 802.11. For information about AES, see RFC 3268, “Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)“,

SITE SURVEY

When setting up the NetScreen-5GT Wireless (ADSL) device as a wireless access point (WAP), you can scan the broadcast vicinity to see if there are any other WAPs broadcasting nearby. A site survey detects any WAPs emitting a beacon in its area and records the following details about each detected WAP:

- Service set identifier (SSID)
- MAC address
- Received signal strength indicator (RSSI)

  The RSSI numbers are in decibels (dBs) that indicate the signal-to-noise ratio (SNR) . The SNR is the signal level divided by the noise level, which results in a value representing signal strength.
- Broadcast channel

In addition to performing an initial site survey, you might want to perform surveys occasionally to ensure that no rogue WAPs spring up in the area. To perform a site survey, do either of the following:

(WebUI) WIreless > Statistics > Site Survey

(CLI) exec wlan site-survey

Note: *A site survey takes about 5 – 10 seconds to complete.*

ACCESS CONTROL

You can control which wireless clients have access to the network through an access control list (ACL). The ACL identifies clients by their MAC addresses and specifies whether the NetScreen device allows or denies access for each address. The ACL can operate in one of three access modes:

- **Disabled:** In this mode, the NetScreen device does not filter any MAC addresses. This is the default mode.
- **Enabled:** In this mode, the NetScreen device allows access to all hosts except those marked with a Deny action.
- **Strict:** In this mode, the NetScreen device denies access to all hosts except those marked with an Allow action.

Note: *The ACL settings apply globally to all basic service sets (BSSs).*

To add a MAC address to the ACL, do either of the following:

WebUI

Wireless > MAC Access List: Enter the following, and then click **Add**:

Access Mode: (select one of the three modes from the drop-down list)[6]

Input a new MAC address: (type the *mac_addr* of a wireless client)

Control Status: (select either **Allow** or **Deny**[7])

Note: *In the WebUI, you can also select a MAC address from the* ***Select a learned MAC address*** *drop-down list. Entries appear in this list when a wireless client makes an association with the NetScreen device. The list is an ephemeral, dynamically changing display of all currently associated wireless clients, regardless of the BSS to which they belong.*

6. You can also set the access mode through the MAC Address Access Control drop-down list on the Wireless > General Settings page.
7. You can define up to 64 denied clients and 64 allowed clients.

CLI

```
set wlan acl mode { disable | enable | strict }
set wlan acl mac_addr { deny | allow }
```

WLAN CONFIGURATION ACTIVATION

After making any changes to the wireless local area network (WLAN) configuration, you must reactivate the WLAN subsystem within the NetScreen-5GT Wireless (ADSL) device[8]. Any WLAN-related configuration changes take effect only after you reactivate this subsystem. To reactivate it, do either of the following:

(WebUI) Wireless -> Activate Changes: Click the **Activate Changes** button.

(CLI) exec wlan reactivate

The reactivation process takes several seconds to complete.

Note: *Reactivating the WLAN subsystem severs all wireless connections and clears all wireless sessions from the session table. Wireless clients must then reconnect to reestablish their disrupted sessions. The WAP restarts in about 5 seconds and returns links to an "up" state after another 5 seconds.*

8. In addition to the WLAN and SSID commands, defining the type of an external auth server as 802.1X qualifies as a WLAN-related configuration change.

CONFIGURATION EXAMPLES

This section contains configurations for the following examples:

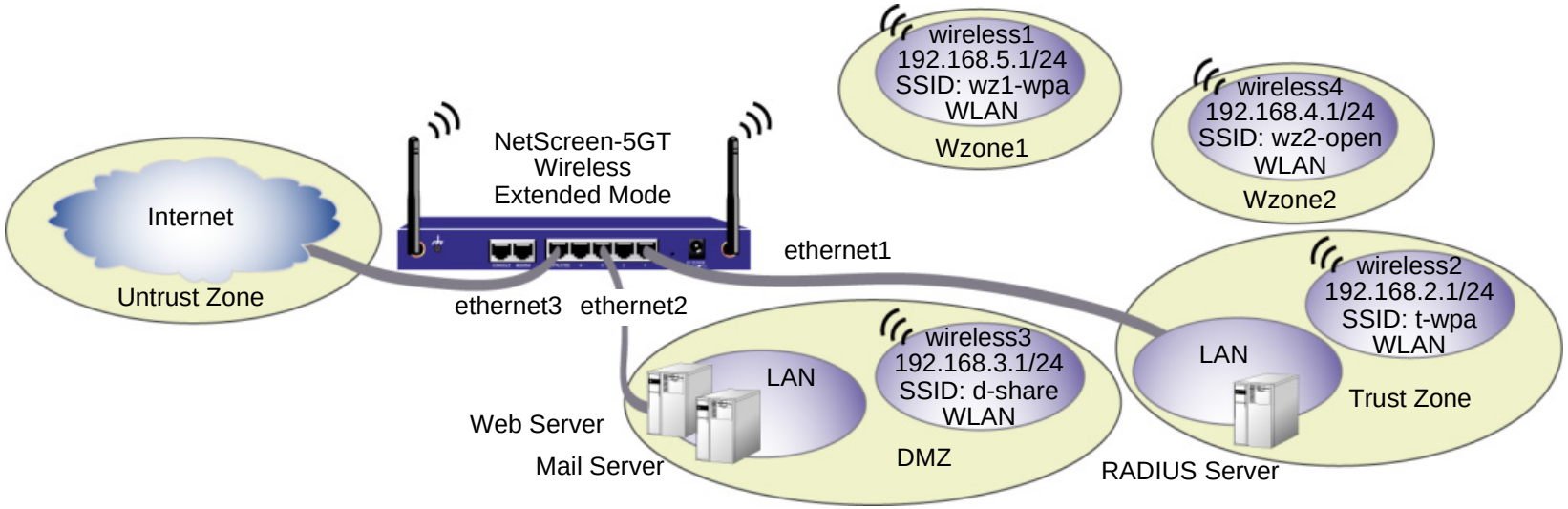
Example 1: Multiple and Differentiated Profiles

In this example, you set up four basic service sets (BSSs), each with a different authentication and encryption scheme, for a NetScreen device in Extended port mode. This mode provides the following port, interface, and zone bindings (the BSSs that you create are also included in the table):

Interfaces	Security Zones	
ethernet1 (ports 1 and 2)	Trust	
ethernet2 (ports 3 and 4)	DMZ	
ethernet3 (Untrust port)	Untrust	
		Basic Service Sets
Wireless1	Wzone1	SSID: wz1-wpa; WPA preshared key
Wireless2	Trust	SSID: t-wpa; WPA using RADIUS server
Wireless3	DMZ	SSID: d-share; WEP shared key
Wireless4	Wzone2	SSID: wz2-open; WEP open/no encryption

You configure the four wireless interfaces and define a different BSS for each interface. You set up each wireless interface to act as a DHCP server to assign addresses dynamically to the wireless clients in each BSS/security zone. You enable management on the wireless1 interface. This interface is in Wzone1, a trusted zone from which you want administrators to be able connect to the NetScreen device. You also configure the NetScreen device to use a RADIUS server for WPA encryption. Finally, you create a policy set, and activate the WLAN configuration.

Note: *Except for setting the ethernet3 interface to act as a DHCP client, this example only includes the configuration for wireless network elements.*



WebUI

1. Basic Service Sets

Wireless > SSID > New: Enter the following, and then click **OK**:

SSID: wz1-wpa

WPA Based Authentication Methods

WPA Pre-shared Key: (select)

Key by Password: (select), 12345678

Confirm Key by Password: 12345678

Encryption Type: Auto

Wireless Interface Binding: wireless1

Wireless > SSID > New: Enter the following, and then click **OK**:

SSID: t-wpa

WPA Based Authentication Methods

WPA: (select)

Encryption Type: Auto

Wireless Interface Binding: wireless2

Wireless > SSID > New: Enter the following, and then click **OK**:

SSID: d-share

> WEP Key: Enter the following, and then click **Back to SSID Edit**:

Key ID: 1

Key Length: 40

Key String

ASCII: (select), abcde

Add: (select)

WEP Based Authentication and Encryption Methods

WEP Shared Key: (select)

Wireless Interface Binding: wireless3

Wireless > SSID > New: Enter the following, and then click **OK**:

SSID: wz2-open

WEP Based Authentication and Encryption Methods

Open: (select)

No Encryption: (select)

Wireless Interface Binding: wireless4

2. Interfaces

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**.

Obtain IP using DHCP: (select)

Automatic update DHCP server parameters: (select)

Network > Interfaces > Edit (for wireless1): Enter the following, and then click **OK**:

IP Address/Netmask: 192.168.5.1/24

Management Options

Management Services: WebUI, Telnet, SSH, SNMP, SSL

Other Services: Ping

Network > DHCP > Edit (for wireless1) > DHCP Server: Enter the following, and then click **OK**:

DHCP Server: (select)

DHCP Server Mode: Enable

Lease: Unlimited

> Addresses > New: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 192.168.5.2

IP Address End: 192.168.5.22

Note: *You use the default IP address for wireless2: 192.168.2.1/24. By default, management is enabled for wireless2.*

Network > DHCP > Edit (for wireless2) > DHCP Server: Enter the following, and then click **OK**:

DHCP Server: (select)

DHCP Server Mode: Enable

Lease: Unlimited

> Addresses > New: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 192.168.2.2

IP Address End: 192.168.2.22

Network > Interfaces > Edit (for wireless3): Enter **192.168.3.1/24** in the IP Address/Netmask fields, and then click **OK**.

Network > DHCP > Edit (for wireless3) > DHCP Server: Enter the following, and then click **OK**:

DHCP Server: (select)

DHCP Server Mode: Enable

Lease: Unlimited

> Addresses > New: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 192.168.3.2

IP Address End: 192.168.3.22

Network > Interfaces > Edit (for wireless4): Enter **192.168.4.1/24** in the IP Address/Netmask fields, and then click **OK**.

Network > DHCP > Edit (for wireless4) > DHCP Server: Enter the following, and then click **OK**:

DHCP Server: (select)

DHCP Server Mode: Enable

Lease: Unlimited

> Addresses > New: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 192.168.4.2

IP Address End: 192.168.4.22

3. RADIUS Auth Server

Configuration > Auth > Servers > New: Enter the following, and then click **OK**:

Name: radius1

IP/Domain Name: 192.168.1.50

Backup1: 192.168.1.60

Backup2: 192.168.1.61

Timeout: 30

Account Type: 802.1x

RADIUS: (select)

Shared Secret: A56htYY97kl

4. Policies

Policies > (From: Wzone1, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Any

Service: ANY

Action: Permit

Policies > (From: Wzone1, To: DMZ) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Any

Service: ANY

Action: Permit

Policies > (From: Wzone2, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Any

Service: ANY

Action: Permit

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Any

Service: HTTP

Action: Permit

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Any

Service: MAIL

Action: Permit

Note: *A default policy permits any type of traffic from the Trust zone to the Untrust zone.*

5. WLAN Configuration Activation

Wireless > Activate Changes: Click **Activate Changes**.

CLI

1. Basic Service Sets

```
set ssid name wz1-wpa
set ssid wz1-wpa authentication wpa-psk passphrase 12345678 encryption auto
set ssid wz1-wpa interface wireless1

set ssid name t-wpa
set ssid t-wpa authentication wpa encryption auto
set ssid t-wpa interface wireless2

set ssid name d-share
set ssid d-share key-id 1 length 40 method ascii abcde
set ssid d-share authentication shared-key
set ssid d-share interface wireless3

set ssid name wz2-open
set ssid wz2-open authentication open encryption none
set ssid wz2-open interface wireless4
```

2. Interfaces

```
set interface ethernet3 dhcp client settings update-dhcpserver
set interface ethernet3 dhcp client

set interface wireless1 ip 192.168.5.1/24
set interface wireless1 manage
set interface wireless1 dhcp server ip 192.168.5.2 to 192.168.5.22
```

Note: *You use the default IP address for wireless2: 192.168.2.1/24. By default, management is enabled for wireless2.*

```
set interface wireless2 dhcp server ip 192.168.2.2 to 192.168.2.22
```

```
set interface wireless3 ip 192.168.3.1/24
set interface wireless3 dhcp server ip 192.168.3.2 to 192.168.3.22

set interface wireless4 ip 192.168.4.1/24
set interface wireless4 dhcp server ip 192.168.4.2 to 192.168.4.22
```

3. RADIUS Auth Server

```
set auth-server radius1 server-name 192.168.1.50
set auth-server radius1 type radius
set auth-server radius1 account-type 802.1x
set auth-server radius1 backup1 192.168.1.60
set auth-server radius1 backup2 192.168.1.61
set auth-server radius1 timeout 30
set auth-server radius1 radius secret A56htYY97kl
```

4. Policies

```
set policy from wzone1 to untrust any any any permit
set policy from wzone1 to dmz any any any permit
set policy from wzone2 to untrust any any any permit
set policy from untrust to dmz any any http permit
set policy from untrust to dmz any any mail permit
save
```

Note: *A default policy permits any type of traffic from the Trust zone to the Untrust zone.*

5. WLAN Configuration Activation

```
exec wlan reactivate
```

Example 2: Open Authentication and WEP Encryption

In this example, you assign an SSID named openwep to the wireless2 interface, which is bound to the Trust security zone. This configuration sets the WEP key-id to 1 with an input ASCII string of 40-bits. It allows anyone to authenticate but encrypts communication using the WEP key.

WebUI

Wireless > SSID > New: Enter the following, and then click **OK**:

SSID: openwep

> WEP Key: Enter the following, and then click **Back to SSID Edit**:

Key ID: 1

Key Length: 40

Key String

ASCII: (select), abcde

Add: (select)

WEP Based Authentication and Encryption Methods

Open: (select)

WEP Encryption: (select); Key Source: Local

Wireless Interface Binding: wireless2

Wireless > Activate Changes: Click **Activate Changes**.

CLI

```
set ssid name openwep
set ssid openwep key-id 1 length 40 method ascii abcde
set ssid openwep authentication open encryption wep
set ssid openwep interface wireless2
save
exec wlan reactivate
```

Example 3: WPA Preshared Key Authentication

In this example, you create basic service set (BSS) with SSID “wpapsk”. It uses Wi-Fi Protected Access (WPA) authentication with a preshared key and automatic encryption.

You then bind it to the wireless2 interface, which is bound to the Trust security zone. Wireless clients who want to connect to the wireless2 interface to access the network must use the WPA passphrase “i7BB92-5o23iJ” when establishing a wireless connection.

WebUI

Wireless > SSID > New: Enter the following, and then click **OK**:

SSID: wpapsk

WPA Based Authentication Methods

WPA Pre-shared Key: (select)

Key by Password: (select), i7BB92-5o23iJ

Confirm Key by Password: i7BB92-5o23iJ

Encryption Type: Auto

Wireless Interface Binding: wireless2

Wireless > Activate Changes: Click **Activate Changes**.

CLI

```
set ssid name wpapsk
set ssid wpapsk authentication wpa-psk passphrase i7BB92-5o23iJ encryption auto
set ssid wpapsk interface wireless2
save
exec wlan reactivate
```

2

New and Modified CLI Commands

This chapter introduces the following new commands:

- **ssid**
- **wlan**

In addition, it presents changes to the following commands:

- **auth-server**
- **interface**

New command elements in the Syntax sections appear in red. For example, in the following command, **account-type 802.1X** is new in this release:

```
set auth-server name_str account_type 802.1X
```

The following command descriptions focus only on the new elements added in this release. For more information about other command elements, refer to the *NetScreen CLI Reference Guide* for ScreenOS 5.0.0.

ssid

Description: Use the **ssid** commands to configure the wireless SSID (Service Set Identifier). You must create an SSID instance before you can configure its parameters.

Syntax

get

```
get ssid [ name_str ]
```

set (SSID Instance)

```
set ssid name name_str
```

set (SSID Authentication)

```
set ssid name_str authentication
    {
    auto |
    open encryption { none | wep [ key-source { local | server | both } ] } |
    shared-key |
    wpa [ rekey-interval { disable | number } ] encryption { aes | auto | tkip } |
    wpa-psk
        {
        passphrase string |
        psk key_str
        }
        [ rekey-interval { disable | number } ]
        encryption { aes | auto | tkip }
    }
```

set (SSID Client Isolation)

```
set ssid name_str client-isolation
```

set (SSID Interface)

```
set ssid name_str interface { wireless1 | wireless2 | wireless3 | wireless4 }
```

set (SSID WEP Key Configuration)

```
set ssid name_str key-id { 1 | 2 | 3 | 4
   length { 104 | 40 | 128 }
   [ method { asciitext string | hexadecimal string [ default ] }
```

set (SSID Broadcast)

```
set ssid name_str ssid-suppression
```

unset (SSID Parameters)

```
unset ssid name_str { client-isolation | interface | key-id { 1 | 2 | 3 | 4 } |
ssid-suppression }
```

unset (SSID Instance)

```
unset ssid { name | name_str }
```

Keywords and Variables

Variable Parameter

```
get ssid name_str
set ssid name name_str { ... }
unset ssid name name_str
```

name Assigns a name to the SSID. The *name_str* can be a maximum of 32 characters. If the name includes a space, then the name needs to be enclosed by quotation marks.

authentication

```
set ssid name_str authentication {...}
```

authentication Allows you to set authentication and encryption options for a specific SSID.

- **auto**: Specifies that the device accepts both open encryption with Wired Equivalent Privacy (WEP) or shared-key authentication.
- **open encryption**: Specifies that either no encryption is performed or WEP encryption is to be used. In either case, no authentication is performed. You can specify the following options:
  - **none**: Specifies that no encryption is performed.
  - **wep**: Specifies that WEP encryption is to be used. **key-source** allows you to select where the WEP key is to be read from: **local** (from the NetScreen device), **server** (Radius auth server), or **both**. If you do not specify a key-source, local (the NetScreen device) is the default. If the key-source is local or both, you must select a default key. If the key source is server, the key does not need to exist on the NetScreen device.
- **shared-key**: Enables shared-key for both authentication and encryption. When this option is specified, the encryption method can only be WEP and you must select a default key.

- **wpa**: Enables Wi-Fi Protected Access (WPA) authentication when a Radius auth server is used and sets an optional rekey-interval. If you enable WPA authentication, you also need to configure the Radius server.
  - **rekey-interval**: Sets the group key update interval, which can range from 30-42949672 seconds. The default value is 1800 seconds. You can also specify **disable** to if you are not using key updates.
  - **encryption**: Specifies the encryption used between the NetScreen device and wireless clients in the subnetwork. You can specify the following options:
    - **aes**: Specifies American Encryption Standard (AES), used by WPA 2 devices.
    - **tkip**: Specifies temporal key integrity protocol (TKIP), used by WPA 1 devices.
    - **auto**: Specifies either AES or TKIP encryption.
- **wpa-psk**: Allows you to configure the WPA pre-shared key on the NetScreen device.
  - **passphrase**: Sets a passphrase to access the SSID. The string should contain 8-63 ASCII characters.
  - **psk:** Sets a pre-shared key to access the SSID. The key must be a 256-bit (64 characters) hexadecimal value.
  - **encryption**: Specifies the encryption used between the NetScreen device and wireless clients in the subnetwork. You can specify the following options:
    - **aes**: Specifies American Encryption Standard (AES), used by WPA 2 devices.
    - **tkip**: Specifies temporal key integrity protocol (TKIP), used by WPA 1 devices.
    - **auto**: Specifies either AES or TKIP encryption.

Example: The following commands set different types of authentication and encryption methods for the SSID named example1.

```
set ssid example1 authentication auto
set ssid example1 authentication open encryption wep
```

client-isolation

```
set ssid name_str client-isolation
unset ssid name_str client-isolation
```

client-isolation Prevents wireless clients on the same subnetwork (SSID) from accessing each other. Note that intra-zone blocking, which you can configure with the **set zone** command, blocks traffic between an SSID and a wired or wireless subnetwork.

interface

```
set ssid name_str interface { wireless1 | wireless2 | wireless3 | wireless4 }
unset ssid name_str interface
```

interface Activates a wireless interface. The number of wireless interfaces you can configure depends on the port mode of the device.

key-id

```
set ssid name_str key-id { 1 | 2 | 3 | 4 } ...
unset ssid name_str key-id { 1 | 2 | 3 | 4 }
```

key-id Enables WEP key configuration and sets the WEP identification value. The key-id value ranges from 1 to 4.

length Specifies the length of the encryption key, in bits:

- **40-bit**: Enter 10 hexadecimal digits or 5 ASCII characters.
- **104-bit**: Enter 26 hexadecimal digits or 13 ASCII characters.

method Sets the string type: **asciitext** *string* or **hexadecimal** *string*. The default method is hexadecimal. Use the **default** keyword to specify the default key; if you do not specify a default key, the key that is entered first is the default.

Example: This example sets the SSID example with a key-id of 1, key length of 40 bits and ASCII password abcde.

```
set ssid example key-id 1 length 40 method asciitext abcde
```

ssid-suppression

set ssid *name_str* **ssid-suppression**
unset ssid *name_str* **ssid-suppression**

ssid-suppression Disables display of the SSID *name_str* in broadcasts.

wlan

Description: Use the **wlan** commands to configure WLAN features.

Syntax

exec

```
exec wlan { find-channel | reactivate | site-survey }
```

get

```
get wlan [ acl ]
```

set

```
set wlan
     {
     acl { mac_addr { allow | deny } | mode { enable | strict } } |
     advanced
          { aging-interval { disable | number } |
          beacon-interval { number } |
          burst-threshold { number } |
          cts-mode { auto | off | on } |
          cts-rate { 1 | 11 | 2 | 5.5 } |
          cts-type { cts-only | cts-rts } |
          dtim-period { number } |
          fragment-threshold { number } |
          long-preamble |
          rts-threshold { number } |
          slot-time long } |
     antenna { a | b | diversity } |
```

```
    channel { auto | number } |
    country-code { name_str } |
    mode { 11b | 11g [ 11g-only ] } |
    transmit { power { eighth | full | half | minimum | quarter } |
               rate { 1 | 11 | 12 | 18 | 2 | 24 | 36 | 48 | 5.5 | 54 | 6 | 9 | auto
                    }
             }
  }
```

unset

```
unset wlan
     {
     acl { mac_addr | mode } |
     advanced
        { aging-interval |
        beacon-interval |
        burst-threshold |
        cts-mode |
        cts-rate |
        cts-type |
        dtim-period |
        fragment-threshold |
        long-preamble |
        rts-threshold |
        slot-time } |
     antenna |
     channel |
     country-code |
     mode |
     transmit { power | rate }
    }
```

Keywords and Variables

acl

set wlan acl { *mac_addr* { **allow** | **deny** } | **mode** { **disable** | **enable** | **strict** } }
get wlan acl

acl	Allows or denies access for the specified MAC address (*mac_addr)*. You can specify a maximum of 128 MAC addresses.
ES	Sets the wireless client restriction. • **disable**: The device does not check for restricted clients. • **enable**: Wireless clients that match the deny list are not allowed; all other clients are allowed.. • **strict**: Only wireless clients that match the allow list are allowed; all other clients are denied.

Example: This example sets the WLAN to only allow the wireless client with MAC address 000bdfd781f9 to access the NetScreen device.

set wlan acl 000bdfd781f9 allow mode strict

advanced

```
set wlan advanced
        { aging-interval { disable | number } |
        beacon-interval { number } |
        burst-threshold { number } |
        cts-mode { auto | off | on } |
        cts-rate { 1 | 11 | 2 | 5.5 } |
        cts-type { cts-only | cts-rts } |
        dtim-period { number } |
        fragment-threshold { number } |
        long-preamble |
        rts-threshold { number } |
        slot-time long
        }
```

advanced Allows you to configure the following advanced radio settings:

- **aging-interval:** Sets the aging value for wireless clients and bridge entities. Value range is 60 to 1,000,000 seconds. The default value is 300 seconds. A zero value disables aging in the WebUI. To disable aging in the CLI, use the **aging-interval disable** command.
- **beacon-interval**: Sets the beacon interval. The range is 20 to 1,000 time units (1 time unit equals 1024 µs). The default value is 100 time units.
- **burst-threshold**: Sets the frame burst threshold. The range is 2 to 255 frames. The default value is 3 frames.

- **cts-mode**: Sets the Clear to Send (CTS) control frame protection. Does not work in 802.11b wireless mode. The default value is **auto**.
  - **on**: Always use protection.
  - **off**: Never use protection
  - **auto**: Automatically detects the CTS mode.
- **cts-rate**: Sets the rate at which CTS frames are sent, in Mbps. Does not work in 802.11b wireless mode. The default is 11 Mbps.
- **cts-type**: Sets the CTS protection type. Does not work in 802.11b wireless mode. The default is **cts-only**.
  - **cts-only**: Single, self-directed frame.
  - **cts-rts**: Two-frame exchange occurs prior to the actual network transmission.
- **dtim-period**: Sets the beacon intervals between data beacon rates, referred to as DTIM. Range is 1 to 255. The default value is 1 beacon interval.
- **fragment-threshold**: Sets the fragmentation threshold. Range is even numbers between 256 and 2346. The default value is 2346.
- **long-preamble**: Allows long preambles (802.11b wireless mode only). Default is short.
- **rts-threshold**: Set the threshold for Request to Send (RTS) packets. The range is 256 to 2346.
- **slot-time long**: Disables the use of short slots. Does not work in 802.11b wireless mode. Default is short.

antenna

`set wlan antenna` { **`a`** | **`b`** | **`diversity`** }

antenna	Selects a specific antenna or enables antenna diversity. Default is diversity. Antenna a is located closest to the power connection.

channel

set wlan channel

channel	Sets the channel for the wireless interface radio. The channel range is from 1 - 11, which is dependent on the country code and extended channel selections. Channels 12 and 13 are reserved for non-U.S. frequency regulations. Default is automatic channel selection.

country-code

set wlan country-code [*string*]

string	(This keyword is not available in the United States or Japan.) Selects a country code for which a wireless interface is configured. This setting affects the range of selectable channels and the transmit power level. If your region code is FCC or TELEC, you cannot set the country code.

find-channel

exec wlan find-channel

find-channel	Finds the best radio channel for the device to use for transmission.

mode

set wlan mode { **11b** | **11g** | [**11g-only**] }

mode	Sets the operation mode for the wireless interface. • **11b**: Allows 802.11b wireless clients to connect to the NetScreen device. • **11g**: Allows 802.11b and 802.11g wireless clients to connect to the NetScreen device. The **11g-only** mode allows only 802.11g wireless clients to connect to the NetScreen device.

reactivate

exec wlan reactivate

reactivate	Reboots the wireless interfaces in order for the new configurations to take effect. This command should be issued after all wireless configurations are complete.

site-survey

exec wlan site-survey

site-survey	The NetScreen device scans all channels and reports all operating wireless interfaces on the device.

transmit

set wlan transmit { **power** {...} | **rate** {...} }

transmit	Adjusts the transmission power and rate for the wireless interface. • **power**: Sets the power transmission and adjusts the radio range when using more than one wireless interface in the same location and frequency. You can set the power level to an eighth, full, half, minimum, or quarter. The default is full power. • **rate**: Sets the wireless interface data transmission rate for sending frames. If you select auto, the wireless interface uses the best rate first, and then automatically falls back to the next rate if transmission fails. You can set 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, or auto as the rate setting. Default is auto.

Example: The following examples set the WLAN to transmit an eighth of the power of the device to clients and set the frame transmit rate to auto.

```
set wlan transmit power eighth
set wlan transmit rate auto
```

auth-server

Description: Use the **auth-server** commands to configure the NetScreen device for user authentication with a specified authentication server. Admins, policies, VPN tunnel specifications, and XAuth configurations use these server specifications to gain access to the appropriate resources.

Syntax

set

```
set auth-server name_str account-type { [ 802.1X ] ... }
```

unset

```
unset auth-server name_string [ account-type { [ 802.1X ]... }
```

Keywords and Variables

account-type

```
set auth-server name_str account-type
     { [ 802.1X ] | [ admin ] | [ auth ] | [ l2tp ] | [ xauth ] }
```

account-type Specifies the types of users authenticated by the server (*name_str*).

- **802.1X** specifies 802.1X users.
- **admin** specifies admin users.
- **auth** specifies authentication users.
- **l2tp** specifies Layer 2 Tunneling Protocol (L2TP) users.

- **xauth** specifies XAuth users.

You can define a user as a single user type—an admin user, an authentication user, an L2TP user, or an XAuth user. You can combine auth, L2TP, and XAuth user types to create an auth-L2TP user, an auth-XAuth user, an L2TP-XAuth user, or an auth-L2TP-XAuth user. You cannot combine an admin user with another user type.

Example: The following example set the auth-server account type to 802.1X users.

```
set auth-server example account-type 802.1X
```

interface

Description: Use the **interface** commands to disable a wireless interface.

Syntax

get (Wireless)

set interface *interface* **association** [*mac_addr*]

set (Wireless)

set interface *interface* **shutdown**

Keywords and Variables

Variable Parameters

set interface *interface* [...]

interface	Specifies the wireless interface: **wireless1**, **wireless2**, **wireless3** or **wireless4**. The wireless interfaces you can specify are dependent on the port mode you have configured on your NetScreen device.

association

set interface *interface* **association** [*mac_addr*]

association	Displays association information for the specified wireless interface. You can optionally specify the MAC address to display information about a specific wireless client.

shutdown

set interface *interface* **shutdown**

shutdown	Disables the specified wireless interface. The wireless interfaces are dependent on the port mode you have configured on your NetScreen device.

3

New Messages

This chapter introduces the new NetScreen messages for this release. Each message is presented, its meaning explained, and— where appropriate—an administrative action recommended. The messages are grouped by message type, and then within that type by severity level, from the most severe to the least.

For a complete list of NetScreen log messages, refer to the *NetScreen Message Log Reference Guide* for ScreenOS 5.0.0.

AP

These messages relate to the wireless interface, refered to in the messages as AP, on the NetScreen device.

Notification

Message Wireless AP in <mode> mode.

Meaning Displays the status of the wireless interface.

Action No recommended action.

Message Wireless AP fatal error: <error>.

Meaning A fatal error occured on the wireless interface.

Action Run the **exec wlan reactivate** command to reset the wireless interface.

Message Wireless CLI updated: <command>

Meaning Recorded the CLI commands entered for the wireless configuration.

Action No recommended action.

Message Wireless AP re-activated with error: <CLIs sequence>Error index: <index>Error code: <code>

Meaning An incorrect command was configured before reactivating the wireless interface.

Action Check the incorrect command from error index.

Message Wireless station event:<event>

Meaning Displays the station association information.

Action No recommended action.

Message Wireless RADIUS event:<event-string>

Meaning Displays information about the station that is using 802.1X authentication.

Action No recommended action.