Tech Note

# ForeScout CounterACT™: Network Address Translation (NAT) Detection

## Introduction

With the increase in the usage of smartphones, tablets and personal devices in a corporate network, the problem of rogue wireless access points and other rogue Network Address Translation (NAT) devices is on the rise. The detection of such devices is important against unauthorized access to the network.

This document explains how ForeScout CounterACT™ detects NAT devices using its patented algorithm

## Why NAT Detection is Important

The ability to detect a NAT device on your network is important because NAT devices are usually unauthorized and may pose a security threat to the network on which they are installed. Rogue NAT devices, especially wireless access points, can serve as unauthorized entry points into the network. Unlike managed wireless access points, which typically are included within the scope of IT security, including authentication and compliance checking for the endpoints that connect to them, rogue wireless access points are outside the scope of traditional IT security and provide an unmanaged door into the network.

The problem of rogue wireless access points has increased in recent years with the increased popularity of smartphones and tablets. Most of these devices support two main methods of communication: Broadband (3G, 4G) and Wi-Fi. To reduce data usage fees and increase speed, users are more tempted than ever to connect their handheld devices to the enterprise network via Wi-Fi while they are at work. If their employer does not readily provide a Wi-Fi connection, users may try to solve the problem themselves by bringing their own Wi-Fi access point into the office and connecting it to the corporate network.

ForeScout customers have reported increased concern over this problem. Not only are they concerned over the entrance of unauthorized personal devices (smartphones and tablets) onto the network, but they are also concerned over the possibility that the handheld devices can bridge their native broadband connection into the Wi-Fi connection that has been introduced onto the corporate network. Once the network is bridged to the broadband, the wireless access point can theoretically allow anyone on the Internet to access the corporate network.

## ForeScout's NAT Detection Solution

ForeScout CounterACT is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with ForeScout ControlFabric™ Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools.

As mentioned in the introduction, CounterACT includes a ForeScout patented NAT detection algorithm In brief, here is how the algorithm works:

- CounterACT retransmits a packet to the network after setting its TTL (Time To Live) to routing distance between CounterACT and the endpoint.
- If an endpoint is connected through a NAT device, the NAT device will reply with an Internet Control Message Protocol (ICMP) TTL-Exceeded packet that has the source IP of the tested system.
- If the endpoint is not connected through a NAT device, no ICMP TTL-Exceeded packet will be sent from the IP address of the tested IP.

More details of how ForeScout's NAT detection algorithm works are contained in the following sections.

## Algorithm Details

ForeScout CounterACT uses its built-in packet engine for NAT detection, leveraging both passive traffic monitoring and the ability to send responses. The first step is passive traffic monitoring. CounterACT connects to a mirror port on a switch and passively listens to network traffic. CounterACT identifies traffic coming from an endpoint to a network server. To detect if the endpoint is connected via a NAT device, CounterACT calculates the routing distance (the number of router hops) between the mirroring port that CounterACT is connected to and the NAT device. CounterACT then retransmits a server side packet (packet from the server to the client) with one change: it will set the TTL so that when the packet arrives to the end system, the TTL would reach 1. For example, if the calculated routing distance from the endpoint is 2 hops (namely, 1 router and then the endpoint) then CounterACT will send a packet with TTL=2. Because of potential asymmetric traffic, or because the response interface may not be connected to the same broadcast domain as the mirroring port, CounterACT also sends a packet with TTL+1 and TTL–1. Therefore, if the calculated routing distance is 2, there are actually 3 packets sent, with TTL={1,2,3}.

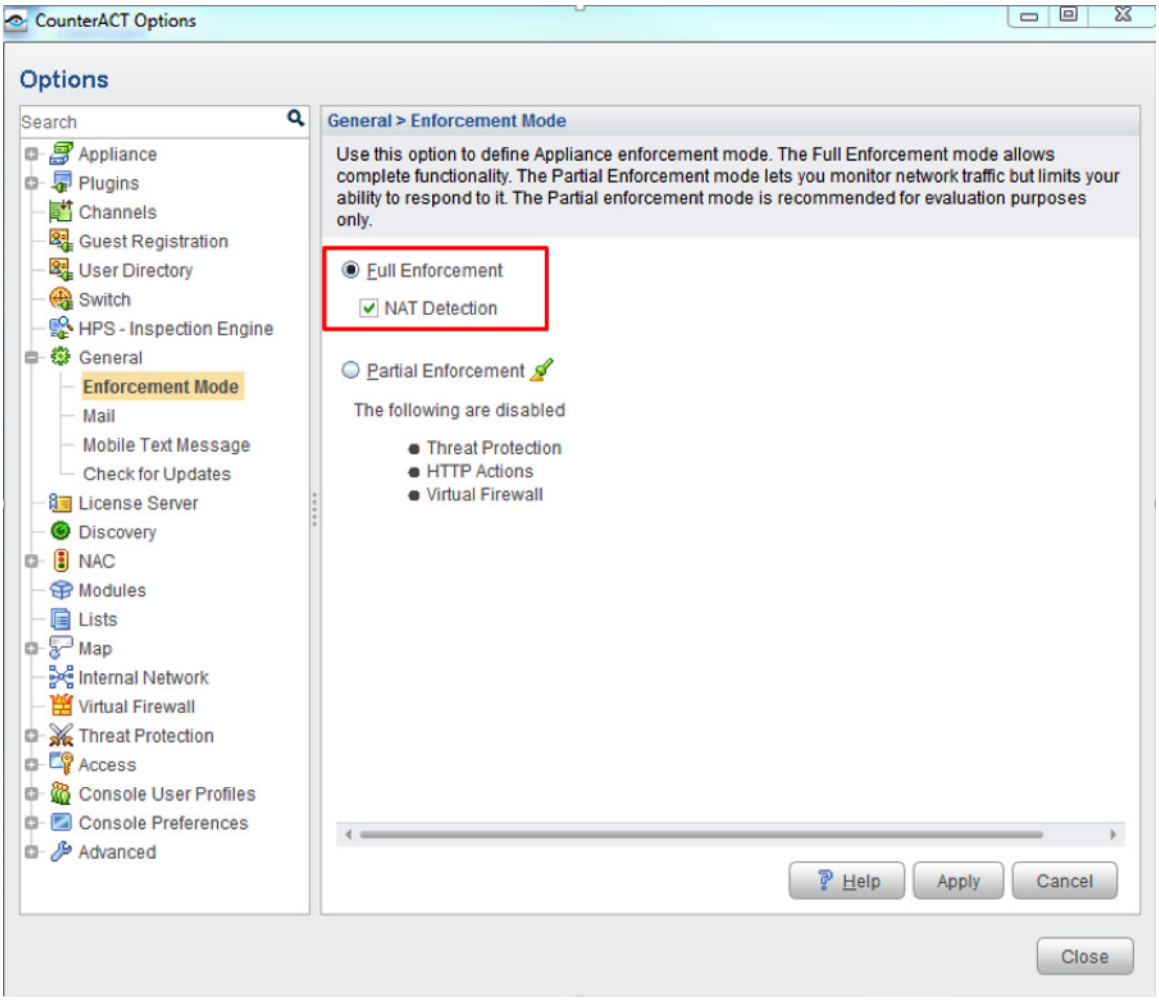
A packet with TTL=1 may reach one of 3 types of devices:

1. **Endpoint:** If the packet reaches an endpoint, the endpoint's IP-stack would handle it regardless of its TTL. Since the packet is a retransmission, the endpoint will normally not respond to the packet. For example, if it is a TCP (Transmission Control Protocol) packet, then the receiving endpoint would consider this a retransmission of something it had already received and will either ignore it or reply with an ACK. (acknowledgement).
2. **Router:** If the packet reaches a router, the router will decrease the TTL by 1, reach 0, drop the packet and send a TTL-Exceeded packet. The source IP of the TTL-Exceeded packet will be one of the router's addresses and not the address of the tested endpoint.
3. **NAT device:** If the packet reaches a NAT device, the NAT device will behave like a router, decrease the TTL to 0, drop the packet and send a TTL-Exceeded packet. The difference between a router and the NAT device is that the NAT device will send the TTL-Exceeded packet with a source IP identical to the tested endpoint address. Such a packet is sent in the scenario of a NAT device; therefore this algorithm can identify if the device is a NAT device.

## Configuration Details

By default, ForeScout CounterACT's NAT detection algorithm is enabled and tries to properly classify each endpoint once every 4 hours. The algorithm will send 8 retransmissions of each packet and will send 3 packets—with TTL equal to the calculated routing distance, with –1 and with +1. These parameters are configurable.

To enable/disable the NAT detection, the following configuration screen can be used:



The following table shows the names of the other configurable parameters responsible for the NAT detection algorithm:

| | Parameter Name | Default Value | Description |
|---|---|---|---|
| **1** | DetectNATPeriod | 14400 | Time period between testing if a specific IP is a NAT device (In Seconds). Default is 4 hours (14,400 seconds). |
| **2** | DetectNATTimes | 8 | Number of retransmissions of each packet used for NAT detection. |
| **3** | DetectNATTTLWindow | 1 | Sets the TTL above and below the calculated routing distance that will be used in the detection. Default value is 1, meaning 3 detection packets are sent, with TTL = {x–1, x , x+1} (Where x is the calculated routing distance). If set to 0, only one packet will be used, with TTL= {x}. If set to 2, 5 packets will be used, with TTL= {x-2, x–1, x, x+1, x+2}, etc. |
| **4** | DetectNATClientFilter | -1 | Tells CounterACT if packets from the client side to the server side should be used for NAT<br>detection: –1 = Disable NAT detection, 1 = Use only 80/tcp |
| **5** | DetectNATFromServerFilter | 1 | Tells CounterACT if packets from the server side to the client side should be used for NAT<br>detection: –1 = Disable NAT detection, 1 = Use only 80/tcp |

These parameters are configurable from command-line. To change these parameters, connect to the appliance directly or via SSH and run the following command:

*fstool set_property <Parameter Name> <Parameter Value>*

*fstool service restart*

After the second command, the system will restart with the new parameter configuration. (If you want to change more than one parameter, you can apply changes with the 'fstool set_property' command and perform the restarts after the changes are applied).

## Detection Results

Based on ForeScout's experience with this NAT detection algorithm, receiving a TTL-exceeded packet from the destination IP is typically a positive identification that this device is performing NAT. While we haven't seen this algorithm produce any false-positives (where CounterACT classified a regular device as a NAT device), we have seen some false-negatives in the following scenarios:

- Some NAT devices have a firewall that blocks the ICMP packet. (In some cases it was configurable.)
- Some NAT devices don't decrease the TTL, specifically some VM hypervisors that run in NAT mode.

## Additional Detection Heuristics

To overcome some of the scenarios described above where CounterACT's primary NAT detection algorithm fails to detect a NAT device, ForeScout has developed some additional policy-based heuristics. The following table describes these policies and how each one works:

| | Policy | Description |
|---|---|---|
| **1** | NIC vendor of WAP and OS type of PC, phone, or tablet. | Detect IPs where the NIC vendor is a network device (such as D-Link®, Cisco®/ Linksys™, NETGEAR®, etc.) and the detect OS type based on passive fingerprinting is of a PC (Windows®, Linux, Mac) or a phone/tablet (iOS, Android, Blackberry®, etc.) |
| **2** | iPhone/iPad that don't have 62078/tcp open | Detect IPs where the OS passive fingerprinting indicates that the device is an iPhone/ iPad but port 62078/tcp is not open. This port is open on such devices and if it is not accessible then it is likely to be because the device is NAT'ed.<br>*Note: This method may fail if the device connects via VPN that filters the port. Another limitation is that it is applicable only if an iOS based device is trying to* |
| **3** | Handheld device that has switch information | Most phones and tablets do not have LAN interface and can only be connected by a separate IP to the network via Wi-Fi (iOS, Android, Blackberry, etc.). Therefore, when such device has switch information it is likely to indicate that the device is connected through a Wi-Fi device performing NAT. |

Learn more at
**www.ForeScout.com**

### About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of October 2015, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

**Toll-Free (US)** 1.866.377.8771
**Tel (Intl)** 1.408.213.3191
**Support** 1.708.237.6591
**Fax** 1.408.371.2284

Copyright © 2015. All rights reserved. Privacy policy. ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ControlFabric, CounterACT Edge, ActiveResponse and CounterACT are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners. **Version 11_15**