ForeScout

Technical Documentation

Detecting MAC Spoofing Using ForeScout CounterACT®

Professional Services Library

Introduction

MAC address spoofing is used to impersonate legitimate devices, circumvent existing security mechanisms and to hide malicious intent. It can be an effective attack on defensive strategies where user and device identity provide a basis for access control policies.

In a typical MAC spoofing sequence, the attacker:

1. Identifies the MAC address of a device with authorized access to the network.
2. Connects a computer to the network, changing its MAC address to match (impersonate) that of the authorized device.
3. Exploits security controls based on static MAC addresses to access network segments, applications and sensitive information.

This document describes how an IT operator can protect against MAC address spoofing using ForeScout CounterACT®.

Mapping the Scope of MAC Spoofing

The vulnerability of a device to a MAC spoofing attack depends on the following variables:

- **Network type**: Wired or wireless?
- **Endpoint type**: Is it a human-operated device running an operating system that supports authentication (a Windows device, for instance), or a "dumb" Internet of Things (IoT) device such as a printer?
- **Switch port**: Is the attacker's device connected to the same port as the spoofed device, or somewhere else in the network?
- **Authentication methodology**: 802.1X or post-connect?

The following table summarizes the scope of the issue:

Network	Endpoint	Switch port	NAC	Vulnerable	Notes
Wired	Operated	Anywhere	802.1X	No	
Wired	Operated	Same port	802.1X	Yes	At least until next re-auth (1 hour) (note 1)
Wired	Dumb	Anywhere	802.1X	Yes	Due to MAB. Limited exposure (note 2)
Wired	Dumb	Same port	802.1X	Yes	Due to MAB. Limited exposure (note 2)
Wireless	Operated	Anywhere	802.1X	No	
Wireless	Operated	Same AP	802.1X	No	Due to encryption between the endpoint and the AP
Wireless	Dumb	*	*	N/A	
Wired	Operated	Anywhere	Post	No*	Can be detected shortly after (notes 3, 4)
Wired	Operated	Same port	Post	No*	Can be detected shortly after (notes 3, 4, 6)
Wired	Dumb	Anywhere	Post	No*	Can be detected shortly after. Limited exposure (notes 2, 3, 5)
Wired	Dumb	Same port	Post	No*	Can be detected shortly after. Limited exposure (notes 2, 3, 5)
Wireless	Operated	Anywhere	Post	No*	Can be detected shortly after (notes 3, 4)
Wireless	Operated	Same AP	Post	No*	Can be detected shortly after (notes 3, 4)

Note 1: We assume the attacker connects the malicious device via a hub/unmanaged switch, thus avoiding immediate 802.1X authentication. There are commercially available tools that bypass 802.1X indefinitely (e.g. Pwnie Express).

Note 2: Exposure can be limited by associating a restricting access profile per MAC address.

Note 3: The asterisk on the "No" is due to the time (however short) it takes until discovery of the intrusion.

Note 4: A "sign-in" policy needs to be in place.

Note 5: Assuming devices can be passively profiled (e.g. using traffic monitoring or DHCP classification).

Note 6: We assume that only the spoofing device is on the port. If both spoofed and spoofing devices are on the port (e.g. using a hub), then the vulnerability depends on whether or not the spoofed device is running a firewall.

ForeScout performs multiple security functions and contributes to a multilayered defense. It restricts the network access of foreign or guest devices, manages the security posture of corporate devices by enforcing policy compliance, and limits the time an attacking device can remain undetected on the corporate network.

The Solution

This solution relies on CounterACT's inherent ability to monitor a host's switch interface and track changes in properties such as switch ID, interface number and port ID. Such changes may be legitimate (for example, an endpoint moving between physical networks), but should be closely monitored to detect abnormal behavior. CounterACT can identify malicious activity in real time and automatically initiate policy-based control interventions, including device quarantine and remediation actions.

The solution offers another layer of protection using CounterACT's ability to impose network access restrictions on non-corporate or guest users. A CounterACT policy grants a host network access only if its user was successfully authenticated, while enforcing limited access on hosts that have not been authenticated.

The following sections describe the two policies that implement the solution as described above, while addressing two distinct scenarios:

- **Tracking switch port changes** – Provides a solution when the malicious and genuine hosts are on the network at the same time.
- **Imposing network access restrictions on guest users** – Provides a solution when only the malicious host is on the network.

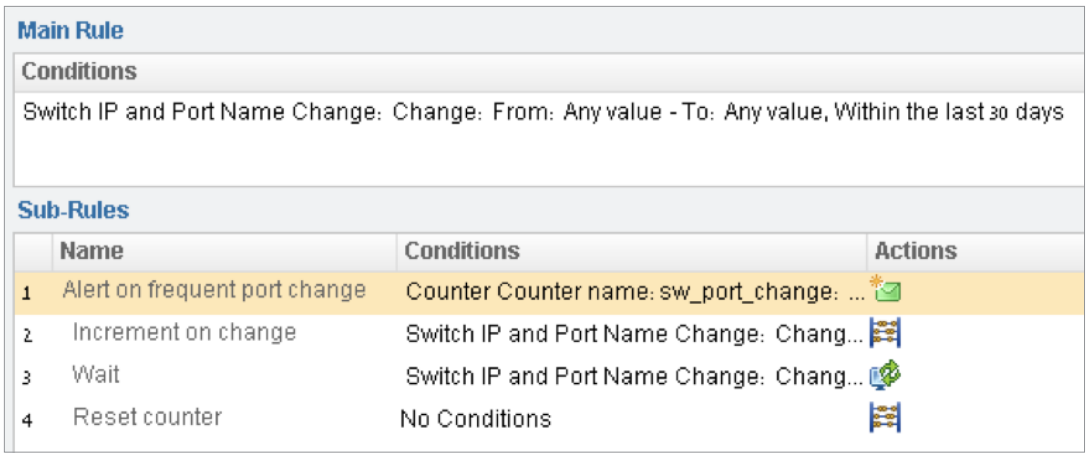
These two policies detect and block most MAC spoofing attacks and are effective in both pre-connect and post-connect CounterACT deployments. As with other access control policies, pre-connect execution provides a higher level of security with a slightly greater impact on user productivity and convenience. Post-connect execution reduces user impacts in exchange for a slight delay in detecting and containing unauthorized users and non-compliant devices.

Unlike other MAC spoofing defenses, this CounterACT solution can detect and stop 802.1X bypass attacks. Its ability to identify and block malicious behavior in the network supports and complements CounterACT's Thread Protection capabilities.

Tracking switch port changes

This policy monitors changes in switch connection address (IP and port). A scenario of frequent switch connection address changes may indicate that this specific MAC address was spoofed.

The suggested policy (see the attached policy **Frequent port change**) detects endpoints that experience four changes of IP address or port in four-minute intervals.



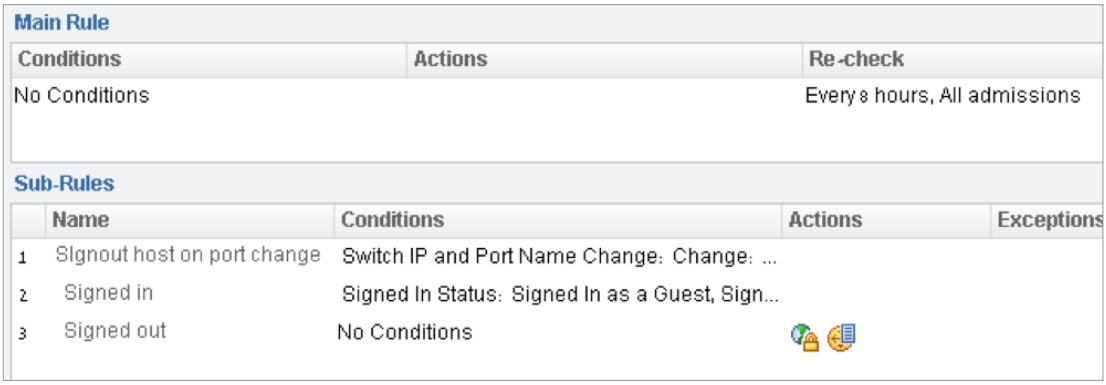
Policy rules walkthrough:

1. **Main rule**: Switch IP and Port name change – Initial detection of network address change initiates monitoring on suspicious host.
2. **Sub-rule one**: If four or more changes in switch IP or port are detected in a four-minute interval, then send an alert notification email.
3. **Sub-rule two**: If a change in switch IP or port is detected, then initiate the counter.
4. **Sub-rule three**: Set time intervals of four minutes.
5. **Sub-rule four**: If no change in switch IP or port occurs in a four-minute interval, then reset the counter.

Imposing network access restrictions on unauthenticated users

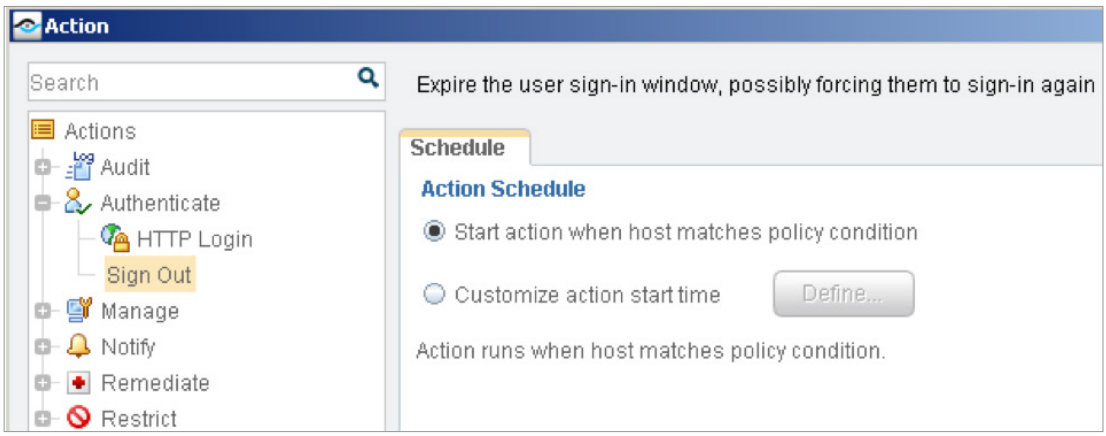
This policy enforces authentication to identify legitimate users and enforces network access restrictions on unauthenticated hosts. It complements the change tracking policy to cover a scenario where the spoofed host is no longer online.

To prevent the spoofing of devices whose owners have left the network without signing off, switch address change events are treated as suspicious, and are used to force a guest authentication process using the CounterACT HTTP Login action. Corporate users who authenticate successfully are then granted authorized network access. Guest users (and unsuccessful spoofers) are restricted to the guest network.

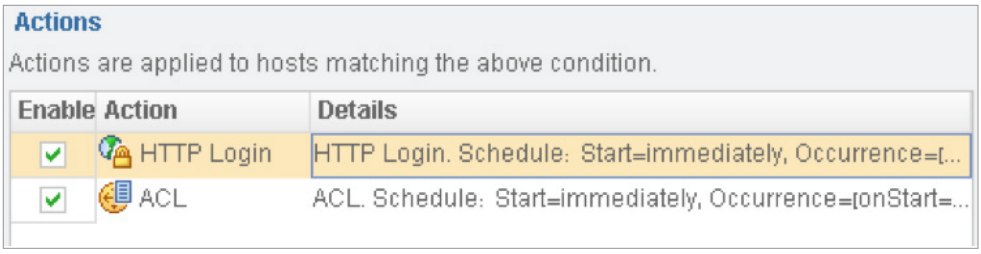


Policy Rules Walkthrough:

1. **Sub-rule one**: If a switch IP or port change is detected (a potential MAC spoofing event), then sign-out the user. The following shows the 'sign-out' action (which is introduced in User Directory Plugin version 6.0.4.1).



2. **Sub-rule two**: Signed-in hosts are granted access.
3. **Sub-rule three**: If the host is detected as signed-out, then execute two actions:
   - Force the user to authenticate using the HTTP Login action to redirect them to an authentication interaction
   - Impose network access restriction using the Access Port ACL action



Note that it may take up to 10 minutes for CounterACT to identify a signed-out user. It is possible to decrease this interval to 1 minute by running the following commands on the CounterACT appliance:

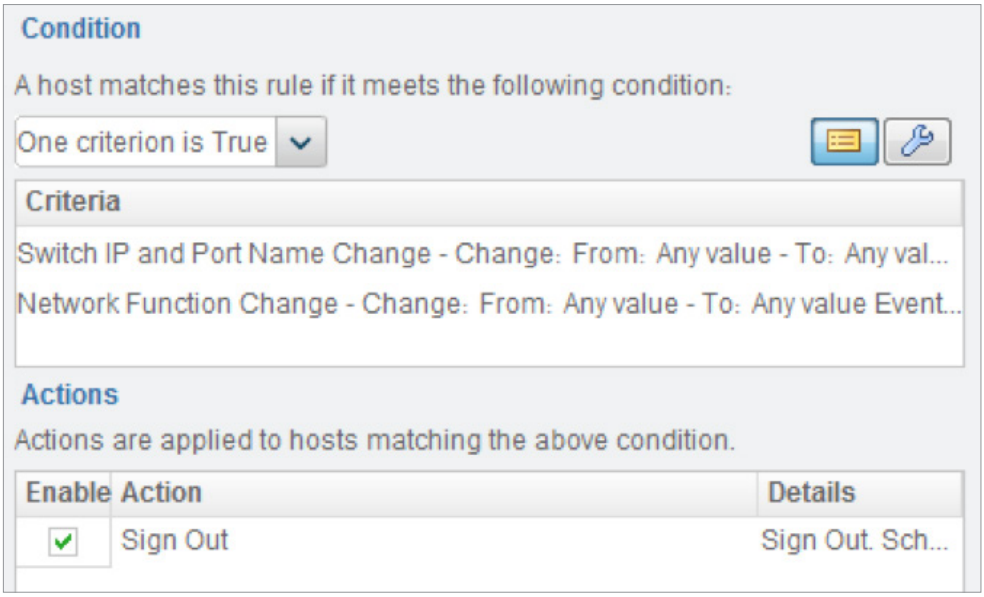
- fstool ad set_property signin.ka.ttl 60
- fstool ad set_property signin.ka.period 30
- fstool ad restart

Improving detection with stored host information

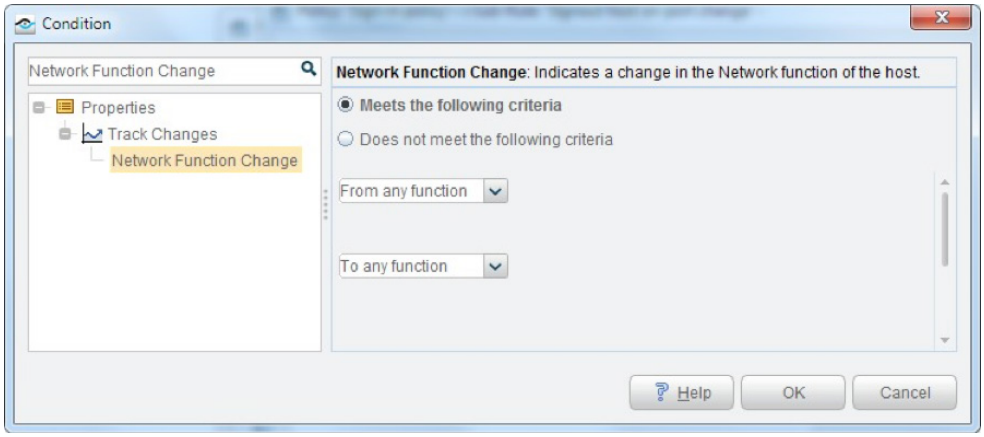
Information about a host may aid in determining which device is legitimate and which is malicious. For this purpose, stored host information (this MAC address was a Windows device) can be compared to new information (this MAC address is now a Linux machine).

This condition can also be easily used in this policy, as follows:

1. Add a condition to sub-rule one to detect changes in OS identification using the Network Function Change:



2. Set the Network Function Change as follows:



Best Practice Recommendations

For best results with the MAC spoofing detection policies described in this document, we recommend the following CounterACT configuration practices:

- Set the switch MAC query interval to 30 seconds
- Enable the packet engine to obtain passive monitoring
- In addition to MAC address notification, enable switch SNMP traps so that CounterACT is immediately made aware of new connections. When this isn't possible, set the switch MAC query interval to 30 seconds.
- Enable Expedite IP Discovery, allowing on-demand ARP table reads to accelerate IP address discovery

One potential limitation of this solution should be noted. If both the spoofed device and the imposter are connected to the same switch port, CounterACT will see no property changes and will not trigger the MAC spoofing policies. This can only occur if both devices are connected to the switch port through a hub or equivalent port-sharing device, and it can be overcome by using CounterACT's Number-of-Hosts-on-Port property.

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591