PriveonLabs Research

Cisco Security Agent Series:

Interface Identification and Control with CSA 5.2

Overview

With the release of Cisco Security Agent (CSA) 5.2, Cisco has added the ability to assign end-point security policies based on the network interface type in use. This new feature allows enterprises to secure their end-points via strict policies for systems both connected to the enterprise wireless network and when roaming.

The new "network interface variable" has expanded functionality beyond simple IP address based policies for securing devices. With this new addition, you are now able to set specific firewall policies based on what interface type is in use at any particular time. This new feature also allows you to monitor what wireless network SSID's are in use by your CSA protected systems, require a wireless encryption method for all wireless connections or restrict all wireless traffic when a system is connected to the enterprise network via a wired interface.

The new features:

Local Interface Classification:

By pulling the interface description from Windows systems, CSA is able to determine the network type in use and enforce policy specific for that interface. The CSA administrator can view the interfaces in use on any given system by gathering data now available on the CSA Host Diagnostics page as seen in figure 1.

Figure 1: Interfaces as seen by CSA host Diagnostics

Interface Characteristics:	Virtual\VMware Virtual Ethernet Adapter for VMnet8
Interface Characteristics:	Virtual\VMware Virtual Ethernet Adapter for VMnet1
Interface Characteristics:	Disconnected\Broadcom 440x 10/100 Integrated Controller
Interface Characteristics:	Loopback\Loopback
Interface Characteristics:	Wifi\infra\enc:wep\Loggingyou
Interface Characteristics:	Virtual\Cisco Systems VPN Adapter

Local Interface Variables:

With the ability to identify specific interfaces by type along with IP ranges and DNS suffixes, CSA now provides the "Local Interface Sets" variable (displayed in Figure 2) for use in network policies and system location specification.

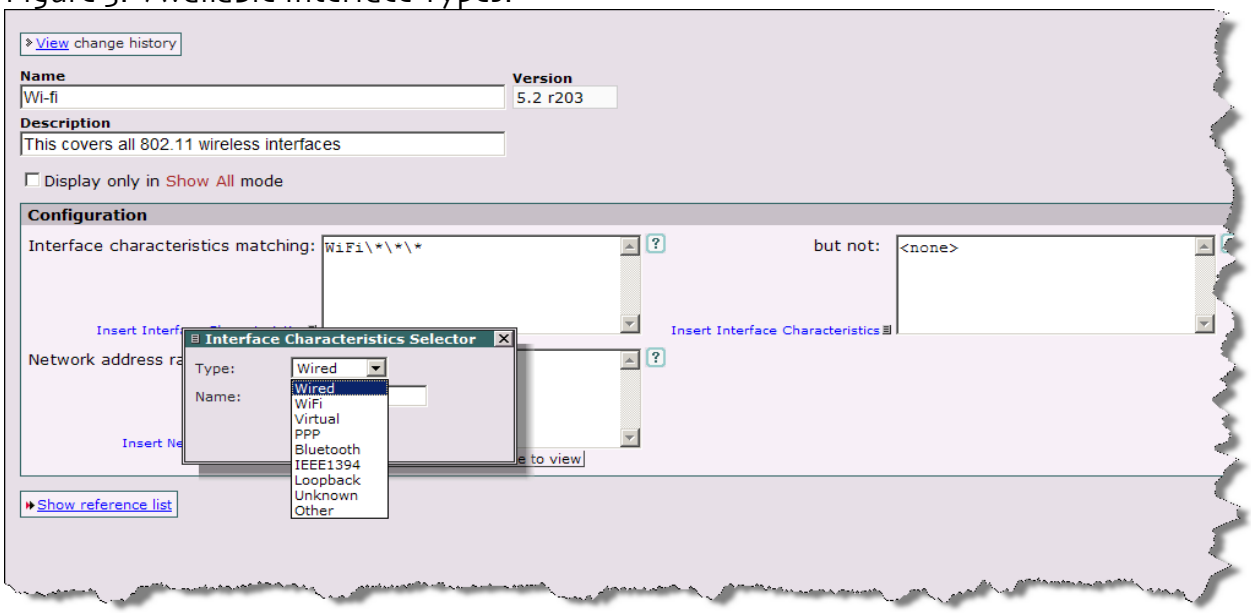
Figure 2: Network Interface Sets:

Name	Filter: <none> OK	Version	<All>	Description	Filter: <none> OK
Wi-fi		5.2 r203		This covers all 802.11 wireless interfaces	
Wi-fi Adhoc		5.2 r203		This covers 802.11 interfaces running in Adhoc mode (i.e. peer to peer)	
Wired		5.2 r203		This covers all ethernet and other wired interfaces	

Using interface characteristics, administrators can be extremely specific to the network interface type in use by end-points. You also have the ability to wildcard the interface characteristics which is an extremely useful function when you are trying to identify all interfaces of a certain type such as WiFi or when defining ranges of acceptable SSIDs.

The available network types are displayed in Figure 3 and listed as:
Wired, WiFi, Virtual, PPP, Bluetooth, IEEE1394, Loopback, Unknown and Other.

Figure 3: Available Interface Types:



Default Installed Policies:

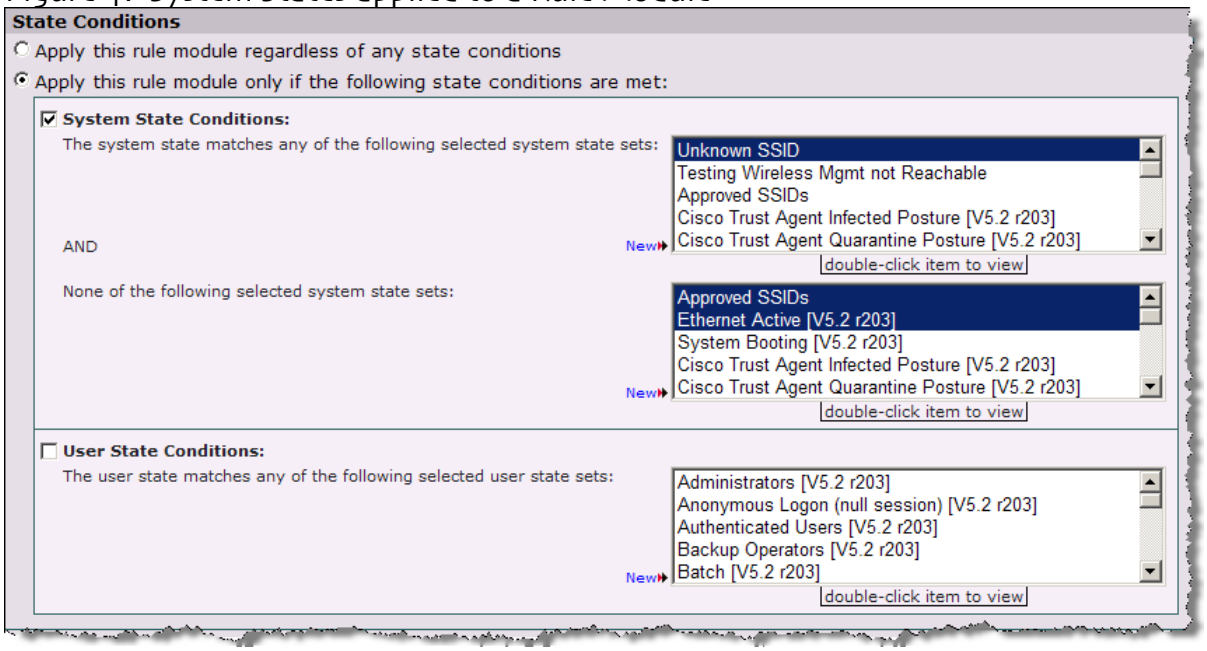
Cisco has added three relevant policies to CSA for the basic security of wireless. These should be used as templates for building policies used in securing wireless networks. None of these interface specific rules are in use by default CSA policies and must be enabled by administrators.

These policies include the denial of all wireless traffic when a system has an active Ethernet (LAN) connection, prevention of all AdHoc wireless networks and the requirement of using a VPN connection when only an active wireless interface is detected.

Usage examples of Securing Wireless with CSA:

Utilizing the System State function in CSA, you can easily enable rules dependant on the network type in use or system location. The matching conditions used for interface type information are applied just as previous System and User States were, on the Rule Module that contains the rules to be applied. This can be seen in Figure 4.

Figure 4: System States applied to a Rule Module



Preventing AdHoc wireless networks:

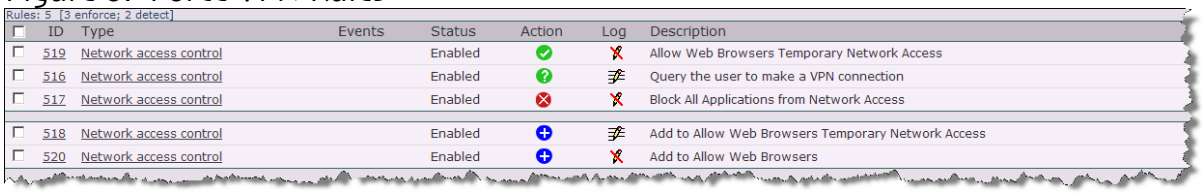
There is a policy provided by Cisco that denies all AdHoc network traffic. Enabling this rule is highly recommended for all systems. The use of AdHoc networks is a large and commonly unmanageable problem for system administrators. In general, this rule should be enabled by default for all managed systems. This is a common attack vector for attackers attempting to gain access to locally stored data on corporate laptops. Denying these connections and helping to solve this common problem for corporate security teams is now as simple as applying this new CSA policy.

Figure 5: AdHoc Rules

Require VPN when non-approved wireless network is in use:

There is also a Cisco provided policy which requires VPN connectivity when only a wireless interface is enabled and in use on the system. This policy requires further configuration prior to use. The policy functions as follows: Upon the initial connection to an unknown SSID, the user will receive a query message informing them that a VPN connection will be required after a short period. This short period allows the user to use a web browser (for 300 seconds) to connect to a hotspot, authenticate, and get a VPN tunnel up and running. The Cisco VPN policy or another custom policy allowing client access via VPN is also required in conjunction with this policy. The rules attached to the Force VPN policy are displayed in figure 6.

Figure 6: Force VPN Rules



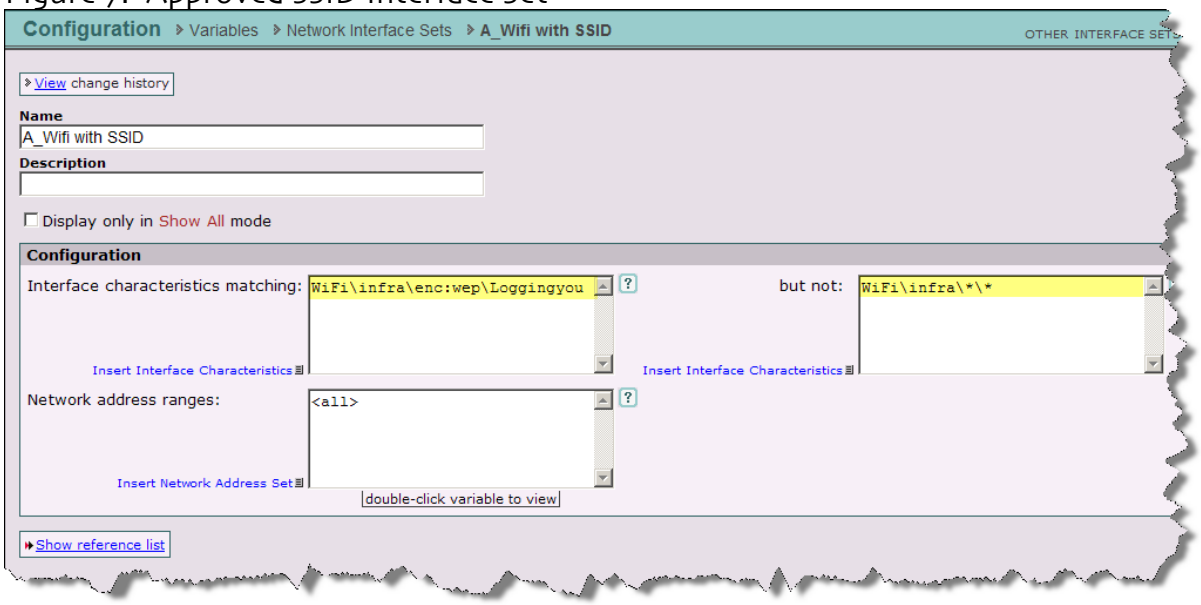
Deny all wireless traffic when Ethernet is active:

This default policy is rather straight forward and simply denies all TCP and UDP traffic to the wireless interface if any Ethernet (LAN) interface is also currently active. By preventing simultaneous wired and wireless access on a system you can help ensure the protected asset does not become a "back door" for illegal entry into the corporate network.

Allowing Traffic to Approved SSID's only while denying all others:

Administrators may want to only allow access to enterprise defined SSID's. This is done by using the network interface characteristics setting in the interface variable. Options for this setting are interface type, network type, encryption method and SSID. The encryption and SSID can also be wild-carded. This interface set can be used to set the system state and apply policies to only those wireless networks that are unknown or not approved. In Figure 7, we define an Interface Set with a specific SSID of "Loggingyou" using WEP encryption.

Figure 7: Approved SSID Interface Set



Denying Bluetooth Network Access:

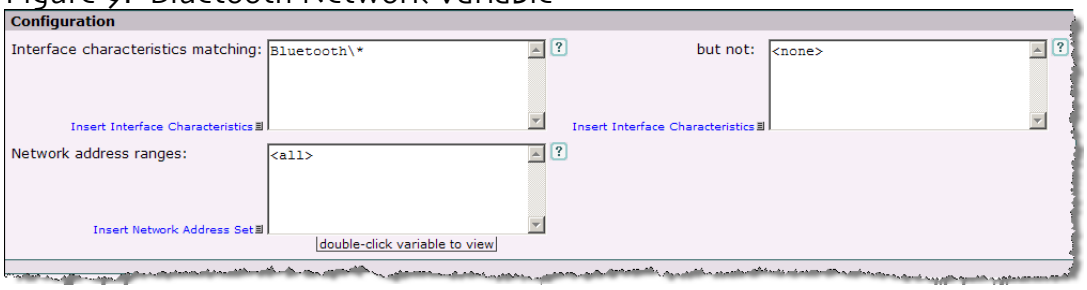
In addition to securing WiFi access, you also now have the ability to secure practically anything that creates a network interface in Windows - whether it is a virtual interface for a VPN adapter or a Bluetooth personal network. An example of a Bluetooth interface as seen by CSA is displayed in figure 8.

Figure 8: Bluetooth Interface

```
Interface Characteristics:  Virtual\VMware Virtual Ethernet Adapter for VMnet8
Interface Characteristics:  Virtual\VMware Virtual Ethernet Adapter for VMnet1
Interface Characteristics:  Wired\Broadcom 440x 10/100 Integrated Controller
Interface Characteristics:  Disconnected\Intel(R) PRO/Wireless 2915ABG Network Connection
Interface Characteristics:  Loopback\Loopback
Interface Characteristics:  Bluetooth\Bluetooth Personal Area Network from TOSHIBA
Interface Characteristics:  Virtual\Cisco Systems SSL VPN Adapter
```

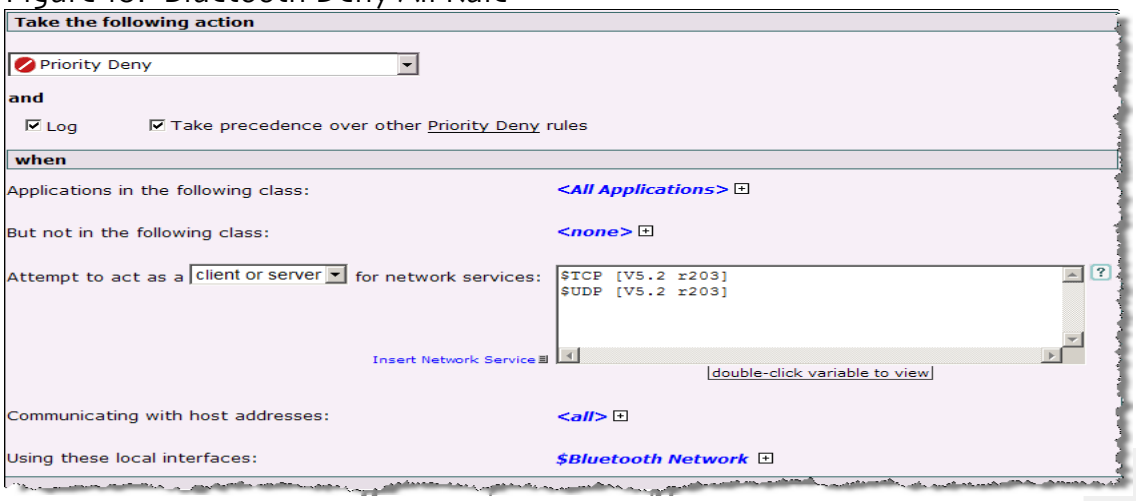
Using the Bluetooth interface variable, as seen in Figure 9, administrators can add this to a rule denying all traffic to and from the particular interface. This will eliminate the need to manually disable Bluetooth networking and can be centrally managed through CSA.

Figure 9: Bluetooth Network Variable



Adding the rule (seen in Figure 10) to the default policies will block all Bluetooth networking. Administrators using the system state can be very granular on when Bluetooth networking can be used and what it may be used for.

Figure 10: Bluetooth Deny All Rule



Summary

The ability to leverage the new network interface type through CSA is a powerful tool. Administrators now have the ability to enforce enterprise security policies for roaming systems based on the network type in use. The flexibility through the existing CSA architecture allows for granular control of not only wireless but all network interfaces on a host system from a centrally managed security solution.

Where to Go for More Information:

Custom Research Documents
Exploit Reverse Engineering/Forensics
Security Implementation
Real-World Training
Managed Services

Available @ www.Priveon.com