EOTSS Defined Standards

Secure WiFi Standards

Document History

Version	Author/Editor	Reason for Change	Date
1.0	Jessica Powers	Initial Document	September 2020

Overview

EOTSS Secure Wireless defined

The EOTSS Secure Wireless refers to dedicated Commonwealth wireless local area network access at various Commonwealth agency locations. The service is built in a manner to ensure that only authorized devices can access Commonwealth resources. The term "Secure Wireless" at mass.gov and agency locations have the below security measures in place in for unauthorized access to the secure SSIDs and capturing user data over the air.

WPA1 and WPA2 data encryption

Data Transmitted over the air between the wireless devices (Laptop / Smart Phone) is encrypted based on industry standards. WPA2 is the standard designed and enforced by the WIFI Alliance standards boards and the IEEE 802.1i standard. All devices capable of WPA2 should dynamically use WPA2 encryption or have the wireless configuration be forced to WPA2 by the EOTSS Service Desk. In the event an older legacy device is only capable of WPA1 an exception would be required for that device to be granted access to the WIFI network.

802.1x Radius Authentication

No wireless network users are allowed onto any secure wireless network until the Windows Domain Username and password has been authenticated against the central Windows Active Directory domain controllers. This is done by tunneling the initial logon request in Ethernet frame level encapsulation to our Cisco Identity Services Engine (ISE) Radius servers. ISE then sends a request to the Windows Active Directory domain controllers on behalf of the user device requesting to logon. If the Laptop belongs to a Mass Gov Windows Domain and the User logon account is in the proper Windows Domain Active Directory container, then ISE authenticates the login attempt, a network TCP/IP address is assigned to the device and the user is granted access to the network. If the Laptop Object is not found in an approved Windows Active Directory container then the login request/attempt is denied, and no valid network TCP/IP address is assigned to the wireless device.

DHCP required for WIFI Connection

If a device has a hard coded or self-assigned TCP/IP address it is not allowed on the secure wireless network. This is further assurance that wireless device on the secure network must have passed the 802.1x authentication detailed above and received its IP address from our internal Infoblox Dynamic Address servers in order to be allowed on the secure network. This also protects against an intruder joining a rogue device to the WIFI and capturing encrypted requests between end user devices and ISE.

Internal Wired Devices, Server Data and Network Appliance protection from devices connecting on Secure SSIDs

Layer 1 Physical separation of data

The standard wireless design includes a separate physical backbone in building or campus where EOTSS wireless is deployed, meaning that a second set of switches and cabling are installed throughout the location. Wireless APs use a separate physical path to transfer the data so it is neither physically nor logically possible for wireless network transmissions to impede wired data by flooding the network path. Similarly, trouble such as Broadcast storms cannot affect wired data.

Access to wired Resources:

End user workstations, application, file and print servers, network switches, routers and firewalls are policed and protected in the same way that these wired resources are protected from other wired resources. Once a wireless device has been authenticated and given access to the secure wireless network, it is treated the same as a wired end user device and all the protection in place is the same as wired devices.

The same protections that EOTSS has in place for internal wired devices also applies to secure wireless devices.

The attached Basic Secure WIFI Data Transmission Diagram shows the flow of data from the wireless devices through the APs and Cisco Wireless Controller to the wired network.

WIFI device to/from WIFI device

All wireless data from end user devices passes through the wireless controller prior to any other destination, including other wireless user devices on the same secure SSID or other SSIDs (illustrated by the Basic Secure WIFI Data Transmission Diagram below).

Wi-Fi Direct - Disabled (Not Permitted)

WIFI direct is an updated form of Ad-Hoc wireless networking. The user WIFI device acts like a wireless access point and provides access to other Wi-Fi devices through its authenticated connection on secure wireless. The Cisco controller checks if connected WIFI devices have gained access VIA a WIFI Direct connection and, if so, logs the instance and disconnects the device.

P2P Network Sharing (Not Permitted)

BitTorrent and similar P2P sharing applications data packets on the network are detected by the Cisco controller and are discarded from the network. This eliminates the P2P traffic and disables the P2P application, allowing the WIFI device to remain on secure wireless and continue to use legitimate network resources and applications.

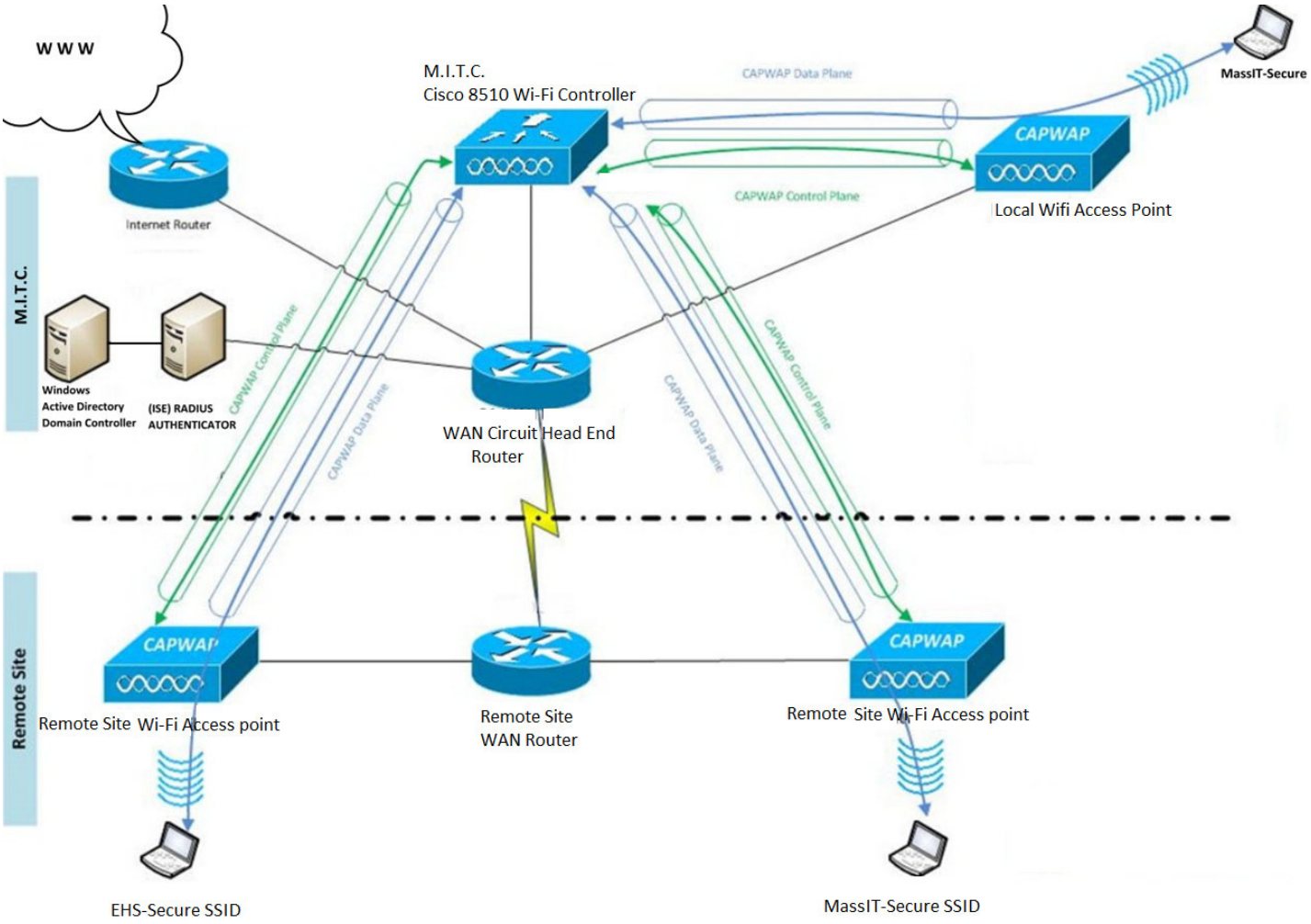
Wireless devices can connect and exchange data with other wireless devices on the secure network but <u>only</u> within the limits allowed by Windows Access Control and firewall rules implemented on the EOTSS laptop itself.

EOTSS does not use ACLs between wireless devices; doing so would require a sized full-time staff in order to maintain.

Data access across the Secure SSIDs can occur as mentioned above; however flooding and other network-based performance issues are mitigated by logical VLAN separation of the two networks and must be forwarded by a network router and its ACLs to do so.

Basic Secure WIFI Data Transmission Diagram

NOTE: Actual Topology has N+1 Redundancy with the Springfield Data Center, not shown here to reduce complexity of this diagram.


W W W
M.I.T.C.
Cisco 8510 Wi-Fi Controller
CAPWAP Data Plane
CAPWAP Control Plane
MassIT-Secure
CAPWAP
Local Wifi Access Point
Internet Router
M.I.T.C.
Windows
Active Directory
Domain Controller
(ISE) RADIUS
AUTHENTICATOR
WAN Circuit Head End
Router
Remote Site
CAPWAP
Remote Site Wi-Fi Access point
Remote Site
WAN Router
CAPWAP
Remote Site Wi-Fi Access point
EHS-Secure SSID
MassIT-Secure SSID