El wIPS adaptante de Cisco aumentó la configuración y el Guía de despliegue del modo local (OLMO)

Contenido

Introducción

La solución inalámbrica adaptante del sistema de prevención de intrusiones de Cisco (wIPS) agrega la característica aumentada del modo local (OLMO), permitiendo que los administradores utilicen su (APS) desplegado de los Puntos de acceso para proporcionar la protección completa sin la necesidad de una red de recubrimiento separada (cuadro 1). Antes del OLMO y en el despliegue adaptante tradicional del wIPS, requieren al modo monitor dedicado (MM) AP proporcionar las necesidades o la protección de la conformidad PCI contra el acceso a la seguridad, la penetración, y los ataques desautorizados (cuadro 2). ELM proporciona con eficacia una oferta comparable que facilita la implementación de la seguridad inalámbrica a la vez que reduce los costes de CapEx y OpEx. Este documento se centra solamente en el OLMO y no modifica ningunas ventajas existentes del despliegue del wIPS con MM AP.

Cuadro 1 - Despliegue aumentado del modo local AP Cuadro 2 - Amenazas superiores de la seguridad de red inalámbrica

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Componentes requeridos del OLMO y versiones del código mínimo

- Regulador del Wireless LAN (WLC) - Versión 7.0.116.xx o posterior
- AP - Versión 7.0.116.xx o posterior
- Sistema de control inalámbrico (WCS) - Versión 7.0.172.xx o posterior
- Motor de los Servicios de movilidad - Versión 7.0.201.xx o posterior

Soportar las Plataformas del WLC

El OLMO se soporta en las Plataformas WLC5508, WLC4400, del WLC 2106,WLC2504, WiSM-1, y WiSM-2WLC.

Soportar los AP

El OLMO se soporta en 11n AP incluyendo 3500, 1250, 1260, 1040, y 1140.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Flujo de la alarma del wIPS del OLMO

Los ataques son solamente relevantes cuando ocurren en la infraestructura de confianza AP. El OLMO AP detectará y comunicará al regulador y correlacionará con el MSE para señalar con la Administración WCS. El cuadro 3 proporciona el flujo de la alarma desde el punto de vista de un administrador:

1. Ataque iniciado contra un dispositivo de infraestructura (“confiaba en” el AP)
2. Detectado en el OLMO AP comunicado con CAPWAP al WLC
3. Pasado transparente a MSE vía NMSP
4. Registrado en la base de datos del wIPS en MSE enviado al WCS vía el SNMP trap
5. Visualizado en el WCS

Cuadro 3 - Detección de la amenaza y flujo de la alarma

Consideraciones sobre la instrumentación para el OLMO

Cisco recomienda que habilitando el OLMO en cada AP en la reunión de la red la mayoría de la

Seguridad del cliente necesita cuando un recubrimiento y/o los costes de la red son consideración de la parte de. La característica primaria del OLMO actúa eficazmente para los ataques del en-canal, sin ningún compromiso al funcionamiento en los datos, los clientes de la Voz y del vídeo, y los servicios.

OLMO contra el MM dedicado

El cuadro 4 proporciona un contraste general entre las implementaciones estándar del wIPS MM AP y el OLMO. En el estudio, el intervalo de cobertura típico para los modos Both sugiere:

- El wIPS dedicado MM AP cubre típicamente 15,000-35,000 pies cuadrados
- la Cliente-porción AP cubrirá típicamente a partir de 3,000-5,000 pies cuadrados

Cuadro 4 - Recubrimiento del MM contra todo el OLMO AP

En el despliegue adaptante tradicional del wIPS, Cisco recomienda una relación de transformación de 1 MM AP a cada 5 modo local AP, que puede también variar basado en el diseño de red y la dirección del experto para la mejor cobertura. Considerando el OLMO, el administrador habilita simplemente la función del software del OLMO para todos los AP existentes, agregando con eficacia las operaciones del wIPS MM al modo local AP de la DATA-porción mientras que mantiene el funcionamiento.

En-canal y funcionamiento del Apagado-canal

UN MM AP utiliza el 100% de la época de la radio para analizar todos los canales, pues no sirve a ninguna clientes WLAN. La característica primaria para el OLMO actúa eficazmente para los ataques del en-canal, sin ningún compromiso al funcionamiento en los datos, Voz y los clientes y los servicios del vídeo. La diferencia principal está en la exploración diversa del apagado-canal del modo local; dependiendo de la actividad, la exploración del apagado-canal proporciona el tiempo de detención mínimo para recopilar bastante información disponible para clasificar y para determinar el ataque. Un ejemplo puede estar con los clientes de la Voz que son asociados y donde los AP RRM que analizan se difieren hasta que desasocien al cliente de la Voz para aseegurarse servicio no son afectados. Para esta consideración, la detección del OLMO durante el apagado-canal se considera mejor esfuerzo. OLMO vecino AP que actúa en todos, país o eficacia de los aumentos de los canales DCA, por lo tanto la recomendación para habilitar el OLMO en cada modo local AP para la cobertura de la protección máxima. Si el requisito está para la exploración dedicada en todos los canales a tiempo completo, la recomendación será desplegar MM AP.

Estas puntas revisan las diferencias del modo local y de MM AP:

- Modo local AP - Los clientes WLAN de los servicios con la exploración del apagado-canal el cortar de tiempo, están atento 50ms en cada canal, y la exploración configurable de las características para los canales todos/country/DCA.
- Modo monitor AP - No sirve a los clientes WLAN, dedicados a analizar solamente, está atento 1.2s en cada canal, y analiza todos los canales.

OLMO a través de los links PÁLIDOS

Cisco ha hecho grandes esfuerzos para optimizar las características en los escenarios

desafiadores, tales como OLMO que desplegaba AP a través de los links de WAN del ancho de banda baja. La característica del OLMO implica el preprocesar en determinar las firmas del ataque en el AP y se optimiza para trabajar sobre los links lentos. Como mejores prácticas, se recomienda para probar y para medir la línea de fondo para validar el funcionamiento con el OLMO sobre WAN.

Integración de CleanAir

La característica del OLMO felicita altamente las operaciones de CleanAir con el funcionamiento similar y las ventajas al despliegue de MM AP con estas ventajas espectro-enteradas existentes de CleanAir:

- Inteligencia dedicada del silicio-nivel RF
- Espectro-enterado, autoregenerable, y uno mismo-optimizando
- Amenaza del canal y detección y mitigación no estándar de interferencia
- No detección del Wi-Fi tal como Bluetooth, microonda, teléfonos inalámbricos, etc.
- Detecte y localice los ataques DOS de la capa RF tales como emisiones RF

Características y beneficio del OLMO

- Exploración adaptante del wIPS en el local de servicio y H-REAP AP de los datos
- Protección sin requerir una red de recubrimiento separada
- Disponible como descarga libre SW para los clientes existentes del wIPS
- Conformidad de los soportes PCI para la Tecnología inalámbrica LAN
- 802.11 y Detección de ataque completos non-802.11
- Agrega las capacidades de la medecina legal y de la información
- Integra con la Administración existente CUWM y de la red inalámbrica (WLAN)
- Flexibilidad para fijar MM integrado o dedicado AP
- El proceso previó en los AP minimiza el regreso de los datos (es decir, trabaja sobre mismo los links de ancho de banda baja)
- Impacto bajo en los datos de la porción

Autorización del OLMO

El wIPS del OLMO agrega una nueva licencia a ordenar:

- AIRE-LM-WIPS-Xx - Licencia del wIPS del OLMO de Cisco
- AIRE-WIPS-AP-xx - Licencia del wIPS de la tecnología inalámbrica de Cisco

Notas adicionales de la autorización del OLMO:

- Si la licencia SKU del wIPS MM AP está instalada ya, esas licencias se pueden también utilizar para el OLMO AP.
- las licencias del wIPS y las licencias del OLMO juntas cuentan hacia los límites de la licencia de la plataforma para el motor del wIPS; 2000 AP en 3310, y 3000 AP en 335x, respectivamente.
- La licencia de evaluación incluirá 10 AP para el wIPS y 10 para el OLMO por un período de hasta 60 días. Antes del OLMO, la licencia de evaluación no prohibió a hasta 20 el wIPS MM

AP. El requerimiento mínimo de las versiones de software que soportan el OLMO debe ser cumplido.

OLMO de la configuración con el WCS

Cuadro 5 - Usando el WCS para configurar el OLMO

1. Del WCS, inhabilite 802.11b/g y las radios del 802.11a del AP antes de habilitar el “motor aumentado del wIPS.”**Note**: Todos los clientes asociados serán disconnected, y no se unirán a hasta que se habiliten las radios.
2. Configure un AP, o utilice una plantilla de configuración WCS para el peso ligero múltiple AP. Véase el cuadro 6.**Cuadro 6 - Habilite el modo aumentado del submarino del motor del wIPS (OLMO)**
3. Elija el **motor aumentado del wIPS**, y haga clic la **salvaguardia**.Habilitar el motor aumentado del wIPS no hará el AP reiniciar.Se soporta H-REAP; habilite la misma manera que para el modo local AP.**Note**: Si cualquiera de las radios de este AP se habilita, el WCS ignorará la configuración y lanzará el error en el cuadro 7.**Cuadro 7 - Recordatorio WCS para inhabilitar las radios AP antes de habilitar el OLMO**
4. El éxito de la configuración puede ser verificado observando el cambio adentro modo AP del “Local o de H-REAP” al **Local/al wIPS** o a **H-REAP/wIPS**. Véase el cuadro 8.**Cuadro 8 - WCS que visualiza modo AP para incluir el wIPS con el Local y/o H-REAP**
5. Habilite las radios que donde inhabilitado en el paso 1.
6. Cree el perfil del wIPS y avancelo al regulador para que la configuración complete.**Note**: Para la información de la configuración completa en el wIPS, refiera al Guía de despliegue adaptante del wIPS de Cisco.

Configuración del WLC

Cuadro 9 - OLMO de la configuración con el WLC

1. Elija un AP de la lengueta **inalámbrica**.**Cuadro 10 - WLC que cambia el modo sub AP para incluir el OLMO del wIPS**
2. Del menú desplegable del modo del submarino AP, elija el **wIPS** (cuadro 10).
3. Aplique, y después salve la configuración.

Note: Para que las funciones del OLMO trabajen, MSE y el WCS se requieren con la autorización del wIPS. El cambio del modo del submarino AP del WLC solamente no habilitará el OLMO.

Ataques detectados en el OLMO

Cuadro 1 - matriz de soporte de las firmas del wIPS

Ataques detectados	OLMO	MM
Ataque DOS contra el AP		
Inundación de la asociación	S	S
Desbordamiento de la tabla de asociación	S	S
Inundación de la autenticación	S	S
Ataque del EAPOL-principio	S	S

Inundación de la PS-encuesta	S	S
Inundación de la petición de la sonda	N	S
Asociación del unauthenticated	S	S
Ataque DOS contra la infraestructura		
Inundación CTS	N	S
Exploit de la Universidad Tecnológica de Queensland	N	S
Atasco RF	S	S
Inundación RTS	N	S
Ataque virtual del portador	N	S
Ataque DOS contra la estación		
Ataque de la falla de autenticación	S	S
Inundación del bloque ACK	N	S
Inundación del broadcast del De-auth	S	S
Inundación del De-auth	S	S
Inundación del broadcast del dis-Assoc	S	S
Inundación del dis-Assoc	S	S
Ataque del EAPOL-cierre de sesión	S	S
Herramienta de FATA-Jack	S	S
EAP-error prematuro	S	S
EAP-éxito prematuro	S	S
Ataques de la penetración de la Seguridad		
Herramienta ASLEAP detectada	S	S
Ataque de Airsnarf	N	S
Ataque de ChopChop	S	S
Ataque del día-Cero por la anomalía de la Seguridad de WLAN	N	S
Ataque del día-Cero por la anomalía de la seguridad del dispositivo	N	S
Dispositivo que sonda para los AP	S	S
Establecimiento de diccionario en los métodos EAP	S	S
Ataque EAP contra la autenticación del 802.1x	S	S
Falsificación AP detectada	S	S
Servidor DHCP falso detectado	N	S
Herramienta RÁPIDA de la grieta WEP detectada	S	S
Ataque de fragmentación	S	S
Honeypot AP detectado	S	S
Herramienta de Hotspotter detectada	N	S
Tramas de broadcast incorrectas	N	S
Paquetes malformados del 802.11 detectados	S	S

Hombre en el ataque medio	S	S
Netstumbler detectó	S	S
Víctima de Netstumbler detectada	S	S
Infracción PSPF detectada	S	S
AP suave o host AP detectado	S	S
Dirección MAC del spoofed detectada	S	S
Sospechoso después del tráfico de las horas detectado	S	S
Asociación desautorizada por la lista del vendedor	N	S
Asociación desautorizada detectada	S	S
Wellenreiter detectó	S	S

Note: Agregar CleanAir también habilitará la detección de los ataques non-802.11.

Cuadro 11 - Opinión del perfil del wIPS WCS

En el cuadro 11, configure el perfil del wIPS del WCS, el icono indica que el ataque será detectado solamente cuando el AP está en el MM, mientras que solamente mejor esfuerzo cuando en el OLMO.

Resuelva problemas el OLMO

Marque estos elementos:

- Aseegurese el NTP se configura.
- Aseegurese la configuración horaria MSE está en el UTC.
- Si el grupo de dispositivos no está trabajando, utilice el perfil SSID del recubrimiento con ningunos. Reinicie el AP.
- Se configura la autorización Make sure (el OLMO AP está utilizando actualmente las licencias KAM)
- Si los perfiles del wIPS se cambian demasiado a menudo, sincronice el MSE-regulador otra vez. Aseegurese el perfil es activo en el WLC.
- Aseegurese el WLC es la parte de MSE usando MSE CLI:SSH o telnet a su MSE.Ejecute **/opt/mse/wips/bin/wips_cli** - Esta consola se puede utilizar para acceder a los siguientes comandos de recopilar la información con respecto al estado del sistema adaptante del wIPS.**muestre el wlc todo** – Publique dentro de la consola del wIPS. Se utiliza este comando de verificar a los reguladores que están comunicando activamente con el servicio del wIPS en el MSE. Véase el cuadro 12.**Cuadro 12 - MSE CLI que verifica el Active del WLC con los servicios del wIPS MSE**

```
wIPS>show wlc all

WLC MAC              Profile            Profile
Status                  IP
Onx Status Status
-----------------------------------------------
-----------------------------------------------
----
00:21:55:06:F2:80    WCS-Default        Policy
active on controller     172.20.226.197
```

```
Active
```

- Aseegurese las alarmas están consiguiendo detectó en MSE usando MSE CLI.**muestre la lista de la alarma** - Publique dentro de la consola del wIPS. Se utiliza este comando de enumerar las alarmas contenidas actualmente dentro de la base de datos del servicio del wIPS. El campo clave es la clave única del hash asignada a la alarma específica. El campo del tipo es el tipo de alarma. Esta carta en el cuadro 13 muestra una lista de la alarma ID y de descripciones:**Cuadro 13 - Comando list de la alarma de la demostración MSE CLI**

```
wIPS>show alarm list

Key        Type  Src MAC
LastTime              Active          First Time
-------------------------------------------------
-----------------------------------------
89         89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631      95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183    99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

  La primera vez que y los campos de la última vez significan los grupos fecha/hora en que la alarma fue detectada; éstos se salvan en la hora UTC. Los resaltados del campo activo si la alarma se detecta actualmente.
- Borre la base de datos MSE.Si usted se ejecuta en una situación donde está corrupta la base de datos MSE, o ningún otros métodos de Troubleshooting trabaja, puede ser el mejor borrar la base de datos y comenzar encima.**Cuadro 14 - MSE mantiene el comando**

```
wIPS>show alarm list

Key        Type  Src MAC
LastTime              Active          First Time
-------------------------------------------------
-----------------------------------------
89         89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631      95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183    99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

Información Relacionada

- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0
- Guía de configuración del Cisco Wireless Control System, versión 7.0.172.0
- Soporte Técnico y Documentación - Cisco Systems