Guía de Cisco para endurecer el Firewall de Cisco ASA

Contenido

Introducción

Este documento contiene la información para ayudarle a asegurar los dispositivos de Cisco ASA, que aumenta la seguridad general de su red. Este documento se estructura en 4 secciones

Endurecimiento del plano de administración - Esto aplica a todo el Management/To relacionado ASA el tráfico del cuadro como SNMP, SSH etc.
Asegurando los comandos config a través de quienes podemos parar el poblar de las contraseñas etc para los config corrientes etc
Registro y supervisión - Esto se aplica a cualesquiera configuraciones relacionadas con la apertura de sesión del ASA.
Con el tráfico - Esto se aplica al tráfico que pasa con el ASA.

En este documento las funciones de seguridad se describen en profundidad para que usted pueda configurarlas. Sin embargo, cuando la descripción no es exhaustiva, la función se explica de una manera que le permita evaluar si necesita prestarle más atención a la función. Siempre que sea posible y adecuado, este documento contiene recomendaciones que, de ser implementadas, ayudan a asegurar una red.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA5500-X 9.4(1) y posterior.

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.

Productos Relacionados

Esta configuración se puede también utilizar con la versión de software 9.x del dispositivo de seguridad de las 5500-X Series de Cisco ASA.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Operaciones de Seguridad

Las operaciones de seguridad de la red constituyen un tema primordial. Aunque la mayor parte de este documento se dedique a la configuración segura de un dispositivo de Cisco ASA, las configuraciones solamente no aseguran totalmente una red. Los procedimientos operativos que se utilizan en la red contribuyen tanto a la seguridad como a la configuración de los dispositivos subyacentes.

Estos temas contienen las recomendaciones operativas que se le aconseja implementar. Estos temas resaltan áreas fundamentales específicas de las operaciones de la red y no son exhaustivos.

Monitoreo de Boletines y Respuestas de Seguridad de Cisco

El Equipo de Respuesta a Incidentes de Seguridad en Productos Cisco (PSIRT) crea y mantiene publicaciones, comúnmente conocidas como boletines de PSIRT, para los problemas relacionados con la seguridad en productos Cisco. El método usado para la comunicación de problemas de menor gravedad es Respuesta de Seguridad de Cisco. Los Security Advisory y las respuestas están disponibles en el PSIRT.

Hay información adicional sobre estos medios de comunicación disponible en la Política de Vulnerabilidad de Seguridad de Cisco.

Para mantener una red segura, debe estar al tanto de los boletines y las respuestas de seguridad de Cisco que se han publicado. Debe tener conocimiento de una vulnerabilidad para que se pueda evaluar la amenaza que representa para una red. Consulte Determinación de Prioridad de los Riesgos para los Anuncios de Vulnerabilidad de la Seguridad a fin de obtener ayuda con este proceso de evaluación.

Aprovechamiento de Autenticación, Autorización y Contabilización

El marco del Authentication, Authorization, and Accounting (AAA) es vital asegurar los dispositivos de red. El protocolo AAA proporciona autenticación de las sesiones de administración y puede también limitar a los usuarios a comandos específicos definidos por el administrador y registrar

todos los comandos ingresados por cada usuario. Vea la sección del autenticación, autorización y contabilidad de este documento para más información sobre cómo leverage el AAA.

Centralización de Monitoreo y Colección de Registros

Para ganar el conocimiento sobre la existencia, emergiendo, y los eventos históricos se relacionaron con los incidentes de seguridad, su organización debe tener una estrategia unificada para el registro de evento y la correlación. Esta estrategia debe aprovechar el registro de todos los dispositivos de red y utilizar capacidades de correlación personalizables y previamente diseñadas.

Después de que se implemente el registro centralizado, usted debe desarrollar un método estructurado para registrar el seguimiento de incidentes y análisis. De acuerdo con las necesidades de su organización, este método puede ser una simple revisión minuciosa de datos de registro e, incluso, un análisis avanzado basado en reglas.

Uso de Protocolos de Seguridad Siempre Que Sea Posible

Muchos protocolos se utilizan para transportar datos de administración de red confidenciales Debe utilizar protocolos de seguridad siempre que sea posible. Una elección de protocolo de seguridad incluye el uso del SSH en vez de Telnet para cifrar los datos de autenticación y la información de administración. Además, debe utilizar protocolos de transferencia de archivos seguros al copiar datos de configuración. Un ejemplo es el uso del protocolo Secure Copy Protocol (SCP) en lugar de FTP o de TFTP.

Netflow para Visibilidad del Tráfico

La herramienta Netflow le permite monitorear los flujos de tráfico en la red. Si bien en un principio su objetivo fue exportar la información del tráfico a las aplicaciones de administración de red, la herramienta Netflow también puede ser utilizada para mostrar la información de flujo en un router. Gracias a esta capacidad, usted puede ver el momento en que el tráfico cruza la red en tiempo real. Independientemente de si la información de flujo se exporta a un recolector remoto, se recomienda que configure los dispositivos de red para que admitan Netflow a fin de poder utilizar la herramienta como respuesta si es necesario.

Administración de la Configuración

La administración de la configuración es un proceso mediante el cual se proponen, revisan, aprueban e implementan cambios de configuración. En el contexto de una configuración del dispositivo de Cisco ASA, dos aspectos adicionales de la administración de la configuración son críticos: seguridad y archivo de configuración.

Usted puede utilizar archivos de configuración para restaurar los cambios que se realizan a los dispositivos de red. En un contexto de seguridad, los archivos de configuración también se pueden utilizar para determinar qué cambios se realizaron en la seguridad y cuándo ocurrieron estos cambios. Junto con los datos de registro del protocolo AAA, esta información puede contribuir con la auditoría de seguridad de los dispositivos de red.

La configuración de un dispositivo de Cisco ASA contiene muchos detalles sensibles. Los nombres de usuario, las contraseñas y el contenido de las listas de control de acceso son ejemplos de este tipo de información. El repositorio que usted utiliza para archivar las

configuraciones del dispositivo de Cisco ASA necesita ser asegurado. El acceso inseguro a esta información puede disminuir la seguridad de toda la red.

Plano de Administración

El plano de administración consiste en funciones que permiten alcanzar las metas de administración de la red. Esto incluye a las Sesiones de administración interactivas que utilizan SSH, así como estadística-recolectan con el SNMP o el Netflow. Cuando usted considera la seguridad de un dispositivo de red, es crucial que el plano de administración esté protegido. Si un incidente de seguridad tiene la capacidad de disminuir las funciones del plano de administración, puede resultarle imposible recuperar o estabilizar la red.

Endurecimiento del plano de administración

El plano de administración se utiliza para acceder, configurar y manejar un dispositivo, así como para monitorear sus operaciones y la red en las cual se ha implementado. El plano de administración es el que recibe y envía el tráfico para las operaciones de estas funciones. El plano de administración utiliza esta lista de protocolos:

- Simple Network Management Protocol
- Secure Shell Protocol
- File Transfer Protocol
- Trivial File Transfer Protocol
- Secure Copy Protocol
- TACACS+
- RADIUS
- Netflow
- Network Time Protocol
- Syslog
- ICMP
- SMB

Nota: Habilitar TELNET no se recomienda pues es sólo texto.

Administración de Contraseña

Las contraseñas controlan el acceso a recursos o a dispositivos. Esto se logra con la definición de una contraseña o de un secreto que se utilice para autenticar solicitudes. Cuando se recibe una solicitud para el acceso a un recurso o a un dispositivo, la solicitud exige la verificación de la contraseña y de la identidad, y el acceso se puede conceder, negar o limitar según el resultado de la verificación. Como práctica recomendada de seguridad, las contraseñas se deben administrar con un servidor de autenticación TACACS+ o RADIUS. Sin embargo, observe que una contraseña localmente configurada para el acceso privilegiado todavía está necesitada en caso de error del TACACS+ o de servicios RADIUS. Un dispositivo puede también tener otra información de contraseña presente dentro de su configuración, como un clave NTP, una comunidad SNMP o una clave de Protocolo de Ruteo.

El ASA utiliza la publicación de mensaje 5 (MD5) para el picado de la contraseña. Este algoritmo ha tenido considerable revisión pública y no es reversible. Sin embargo, el algoritmo está sujeto a

ataques de diccionario. En un ataque de diccionario, un atacante prueba todas las palabras de un diccionario o de otra lista de contraseñas candidatas para encontrar una coincidencia. Por lo tanto, los archivos de configuración se deben guardar con seguridad y compartir solamente con individuos de confianza.

Servicio del permiso HTTP

Para utilizar el ASDM, usted necesita habilitar al servidor HTTPS, y permite las conexiones HTTPS al ASA. El dispositivo de seguridad permite un máximo de 5 casos simultáneos del ASDM por el contexto, si está disponible, con un máximo de 32 casos del ASDM entre todos los contextos. Para configurar el uso del acceso del ASDM:

```
http server enable <port>
```

Permita solamente el IP que se necesitan en la lista ACL. Permitir un acceso amplio es un incorrecto practica.

```
http 0.0.0.0 0.0.0.0 <interface>
```

Control de acceso del ASDM de la configuración:

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Comenzando con la versión de software ASA 9.1(2),8.4(4.1), El ASA ahora soporta los paquetes efímeros siguientes de la cifra de Diffie Hellman (DHE) SSL.

DHE-AES128-SHA1
DHE-AES256-SHA1

Estas habitaciones de la cifra se especifican en el **RFC 3268**, Advanced Encryption Standard (AES) Ciphersuites para Transport Layer Security (TLS).

Cuando es soportado por el cliente, DHE es la cifra preferida porque proporciona la perfecta reserva hacia adelante. Vea las limitaciones siguientes:

DHE no se soporta en las conexiones del 3.0 SSL, así que aseegurese también habilitar el TLS1.0 para el servidor SSL.

```
// Set server version ASA(config)# ssl server-version tlsv1 sslv3
// Set client version ASA(config) # ssl client-version any
```

Algunas aplicaciones populares no soportan DHE, así que incluya por lo menos otro método de encripción de SSL para asegurarse de que una habitación de la cifra común al cliente SSL y al servidor puede ser utilizada. Algunos clientes pueden no soportar DHE, incluyendo AnyConnect 2.5 y 3.0, Cisco Secure Desktop, y el Internet Explorer 9.0.

El ASA tiene debajo de las cifras habilitadas en la orden como abajo por abandono.

```
ASA(config)#ssl encryption rc4-sha1 dhe-aes128-sha1 dhe-aes256-sha1 aes128-sha1 aes256-sha1
3des-sha1
```

versión del servidor SSL (valor por defecto)

El ASA por abandono utiliza un certificado autofirmado temporal que cambie en cada reinicialización. Si usted está buscando un solo certificado, usted puede seguir el link abajo para generar un certificado autofirmado permanente.

Ahora el startig del TLS versión 1.2 de los soportes ASA de la versión de software 9.3.1for asegura la transmisión de mensajes para el ASDM, el clientless SSVPN, y AnyConnect VPN. Han presentado o modificaron a los siguientes comandos los comandos: **versión de cliente SSL**, **versión del servidor SSL**, **cifra SSL**, confianza-**punta SSL**, DH-**grupo SSL**, **SSL de la demostración**, **cifra SSL de la demostración**, **demostración VPN-sessiondb**

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

Permiso SSH

El ASA permite las conexiones SSH al ASA para los fines de administración. El ASA permite un máximo de 5 conexiones SSH simultáneas por el contexto, si está disponible, con un máximo de 100 conexiones divididas entre todos los contextos.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

El tipo predeterminado del par clave es clave general. El tamaño predeterminado del módulo es 1024. La cantidad de espacio del NVRAM para salvar los pares claves varía dependiendo de la plataforma ASA. Usted puede alcanzar un límite si usted genera más de 30 pares claves. Las claves 4096-bit RSA se soportan solamente en el ASA5580, los 5585, o las Plataformas posteriores.

Para quitar a los pares claves del tipo indicado (rsa o dsa)

```
crypto key zeroize { rsa | dsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

Configuración SSH para el acceso del dispositivo remoto:

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Para restringir la versión de SSH validó por el ASA, utiliza el comando version del ssh en el modo de configuración global. Para restringir el ASA para utilizar solamente la versión 2 puede ser pone wusing debajo del comando.

```
ASA(config)#ssh version 2
```

Para intercambiar las claves usando el método del intercambio de claves del group1 del Diffie-Hellman (DH) o del grupo 14 DH, utilice el comando del intercambio de claves del ssh en el modo

de configuración global. a partir de 9.1(2) el ASA soporta dh-group14-sha1 para SSH

```
ASA(config)#ssh key-exchange dh-group14-sha1
```

Descanso de la configuración para las sesiones de conexión al sistema

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

Administración de Contraseña

Las contraseñas controlan el acceso a recursos o a dispositivos. Esto se logra con la definición de una contraseña o de un secreto que se utilice para autenticar solicitudes. Cuando se recibe una solicitud para el acceso a un recurso o a un dispositivo, la solicitud exige la verificación de la contraseña y de la identidad, y el acceso se puede conceder, negar o limitar según el resultado de la verificación. Como práctica recomendada de seguridad, las contraseñas se deben administrar con un servidor de autenticación TACACS+ o RADIUS. Sin embargo, observe que una contraseña localmente configurada para el acceso privilegiado todavía está necesitada en caso de error del TACACS+ o de servicios RADIUS. Un dispositivo puede también tener otra información de contraseña presente dentro de su configuración, como un clave NTP, una comunidad SNMP o una clave de Protocolo de Ruteo.

Usuario local y contraseña encriptada de la configuración

```
username <local_username> password <local_password> encrypted
```

Contraseña habilitada de la configuración

```
enable password <enable_password> encrypted
```

Autenticación AAA de la configuración para el enable mode

```
ASA(config)#aaa authentication enable console LOCAL
```

Autenticación, autorización y contabilidad

El marco del Authentication, Authorization, and Accounting (AAA) es crítico para asegurar el acceso interactivo a los dispositivos de red. El marco AAA proporciona un entorno altamente configurable que se pueda adaptar basó en las necesidades de la red.

autenticación TACACS+

El TACACS+ es un protocolo de autenticación que el ASA puede utilizar para la autenticación de los usuarios de administración contra un servidor de AAA remoto. Estos usuarios de administración pueden acceder el dispositivo ASA vía SSH, el HTTPS, el telnet, o el HTTP.

La autenticación TACACS+, más comúnmente conocida como autenticación AAA, le da a cada administrador de red la posibilidad de utilizar cuentas de usuarios individuales. Cuando usted no depende de una sola contraseña compartida, la Seguridad de la red se mejora y se consolida su responsabilidad.

El RADIUS es un protocolo similar en el propósito al TACACS+; sin embargo, cifra solamente la contraseña enviada a través de la red. En cambio, el TACACS+ cifra el entero carga útil de TCP,

que incluye ambos el nombre de usuario y contraseña. Por esta razón, se recomienda el uso de TACACS+ en lugar de RADIUS cuando el servidor AAA admite el protocolo TACACS+. Consulte Comparación entre TACACS+ y RADIUS para obtener una comparación más detallada de estos dos protocolos.

Autenticación de TACACS+ puede ser habilitado en un dispositivo de Cisco ASA con una configuración similar a este ejemplo:

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

Firma y verificación de la imagen ASA

A partir de la versión de software 9.3.1 ASA las imágenes ahora se firman usando una firma digital. Se verifica la firma digital después de que se inicie el ASA.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done! Embedded Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e Computed Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e CCO Hash SHA-512:
1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
c99f49f70354715441385e0b96e4bd3e861d18fb30433d52e12b15b501fa790f36d0ea0 Signature Verified
ASA(config)# verify /signature running Requesting verify signature of the running image...
Starting image verification Hash Computation: 100% Done! Computed Hash SHA2:
2fbb0f62b5fbc61b081acfca76bddbb2 26ce7a5fb4b424e5e21636c6c8a7d665
1e688834203dfb7ffa6eaefc7fdf9d3d 1d0a063a20539baba72c2526ca37771c Get key records from key
storage: PrimaryASA, key_store_type: 6 Embedded Hash SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
26ce7a5fb4b424e5e21636c6c8a7d665 1e688834203dfb7ffa6eaefc7fdf9d3d
1d0a063a20539baba72c2526ca37771c Returned. rc: 0, status: 1 The digital signature of the running
image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
Signer Information
Common Name : abraxas
Organization Unit : ASAv
Organization Name : CiscoSystems
Certificate Serial Number : 550DBBD5
Hash Algorithm : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version : A
```

Zona de Hora del reloj de la configuración

```
clock timezone GMT <hours offset>
```

Configuración NTP

El protocolo Network Time Protocol (NTP) no es un servicio particularmente peligroso, pero cualquier servicio innecesario puede representar un vector de ataque. Si se utiliza el protocolo NTP, es importante configurar explícitamente un origen de hora confiable y utilizar la autenticación adecuada. La hora exacta y confiable es necesaria para los fines de syslog, por ejemplo durante las investigaciones forenses de posibles ataques, así como para la conectividad VPN exitosa cuando se depende de certificados para la autenticación de Fase 1.

- **Huso horario NTP** - Cuando usted configura el NTP, el huso horario necesita ser configurado para poder correlacionar exactamente los grupos fecha/hora. Hay generalmente dos acercamientos para configurar el huso horario para los dispositivos en una red con una presencia global. Un método es configurar todos los dispositivos de red con el Tiempo Universal Coordinado (UTC), previamente conocido como Tiempo Medio de Greenwich (GMT). El otro método es configurar los dispositivos de red con el huso horario local.

```
ntp server ip_address [ key key_id ] [ source interface_name ] [ prefer ]
```

- **Autenticación NTP** - Si usted configura autenticación NTP, ofrece la garantía que los mensajes NTP están intercambiados entre los pares de confianza NTP. Habilite la autenticación usando el comando ntp authenticate, fija la clave de confianza ID para este servidor. Si usted habilita la autenticación, el ASA comunica solamente con un servidor NTP si utiliza la clave de confianza correcta en los paquetes. Para habilitar la autenticación con un servidor NTP, utilice el comando ntp authenticate en el modo de configuración global.

```
ASA(config)#ntp authenticate
```

Servicio del servidor DHCP (si no siendo utilizado)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

Nota: El ASA no soporta el CDP.

Lista de acceso de la controle de plano

Las reglas del control de acceso para el tráfico de administración del a--cuadro (definido por los comandos tales como el HTTP, el ssh, o el telnet) tienen precedencia más alta que una lista de acceso aplicada con la opción de la controle de plano. Por lo tanto, tal tráfico de administración permitido será permitido venir adentro incluso si es negado explícitamente por la lista de acceso del a--cuadro.

```
access-list <name> in interface <Interface_name> control-plane
```

Del ASA

Aquí están los protocolos que se pueden utilizar para copiar/los archivos de la transferencia al ASA.

Texto claro:

- FTP
- HTTP
- TFTP
- SMB

Asegure:

- HTTPS
- SCP (cliente de la Copia segura) a partir de 9.1(5), ASA apoya al cliente de SCP para transferir los archivos a y desde un servidor de SCP.

Para el tráfico directo

Distribución aleatoria del número de secuencia TCP

Cada conexión TCP tiene dos ISN: uno generado por el cliente y uno generado por el servidor. El ASA selecciona al azar el ISN del TCP SYN que pasa en el entrante y las direcciones salientes.

La selección al azar del ISN del host protegido evita que un atacante predecting el ISN siguiente para una nueva conexión y potencialmente secuestre la nueva sesión.

La distribución aleatoria del número de secuencia inicial TCP se puede inhabilitar si procede. Por ejemplo:

- Si otro Firewall en línea también está seleccionando al azar los números de secuencia inicial, no hay necesidad de ambos Firewall de realizar esta acción, aunque esta acción no afecta al tráfico.
- Si usted utiliza el multi-salto del eBGP con el ASA, y los pares del eBGP están utilizando el MD5. La distribución aleatoria rompe la suma de comprobación MD5.
- Si utilizamos un dispositivo WAAS que requiera el ASA no seleccionar al azar los números de secuencia de conexiones.

Decremento de TTL

Por abandono, no decrement TTL en el encabezado IP debido a qué ASA no aparece como salto del router al hacer Traceroute.

dnsguard

Aplica una respuesta de DNS por la interrogación. Puede ser habilitada usando el comando en el modo de configuración global.

```
ASA(config)#dns-guard
```

Controles de la fragmentación del encadenamiento del fragmento de la configuración

Para proporcionar la Administración adicional de la fragmentación de paquetes y mejorar la compatibilidad con el NFS, utilice el comando fragment en el modo de configuración global.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

Configure el examen del protocolo

Los motores del examen se requieren para los servicios que integran la información del IP Addressing en el paquete de datos del usuario o que los canales secundarios abiertos en los puertos dinámicamente asignados. Estos protocolos requieren el ASA hacer una inspección de paquetes profunda en vez de pasar el paquete a través del trayecto rápido. Como consecuencia, los motores del examen pueden afectar al rendimiento de procesamiento general. Refiera por favor la guía de los Config ASA 9.4 para la información detallada en el examen del Application

Layer Protocol.

El examen en el ASA puede ser el usar habilitado debajo de comando

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

Por abandono el ASA tiene **"global_policy"** habilitado global.

Unicast Reverse Path Forwarding de la configuración

```
ip verify reverse-path interface <interface_name>
```

Cuando el tráfico consigue caída debido a revisión de "RPF", el "descenso abajo de la demostración ASP" contrario en el ASA incrementa.

```
ASA(config)# show asp drop

Frame drop:
 Invalid TCP Length (invalid-tcp-hdr-length)                  21
   Reverse-path verify failed (rpf-violated)                    90

// Check Reverse path statistics

ASA(config)# sh ip verify statistics
 interface inside: 11 unicast rpf drops
interface outside: 79 unicast rpf drops
```

Detección de la amenaza

La detección de la amenaza proporciona a los administradores del Firewall con las herramientas necesarias para identificar, para entender, y para parar los ataques antes de que alcancen la infraestructura de red interna. Para hacer así pues, la característica confía en varios diversos activadores y estadísticas, que se describe en el detalle adicional en estas secciones.

Refiera por favor las funciones y la configuración de la detección de la amenaza ASA para la explicación de detalle en la detección de la amenaza en el ASA.

Filtro de Botnet

Las peticiones y las respuestas del Domain Name Server de los monitores del filtro de tráfico de BotNet (DNS) entre los clientes de los DN internos y los servidores DNS externos. Cuando se procesa una respuesta de DNS, el dominio asociado a la respuesta se marca contra la base de datos de los dominios malévolos sabidos. Si hay una coincidencia, cualquier tráfico más otro a la dirección IP presente en la respuesta de DNS se bloquea.

Malware es el software malévolo que está instalado en un host inconsciente. Malware que intenta la actividad de la red tal como envío de los datos privados (contraseñas, números de placa de crédito, movimientos dominantes, o datos propietarios) se puede detectar por el filtro de tráfico de Botnet cuando el malware comienza una conexión a una mala dirección IP sabida. El filtro de tráfico de Botnet marca entrante y las conexiones salientes contra una base de datos dinámica de los malos Domain Name sabidos y de los IP Addresses (la *lista negra*), y entonces los registros o

bloquea cualquier actividad sospechosa.

Usted puede también complementar la base de datos dinámica de Cisco con los direccionamientos puestos de su elegir agregandolos a una lista negra estática; si se pone la base de datos dinámica incluye los direccionamientos puestos que usted piensa si, usted puede ingresarlos manualmente en un *whitelist* estático. Los direccionamientos de Whitelisted todavía generan los mensajes de Syslog, pero porque usted está apuntando solamente los mensajes de Syslog de la lista negra, son informativos. Refiérase por favor configurando el filtro de tráfico de Botnet para la información detallada.

Adiciones de memoria caché ARP para las subredes NON-conectadas

Por abandono el ASA no responde al ARP para los IP Addresses de la subred conectada NON-directo. Si usted tiene un IP NAT en el ASA que no pertenece al IP de la misma subred de la interfaz ASA, tendremos que habilitar el “permiso-nonconnected arp” en el ASA al Proxy-arp para el IP de NATted.

```
arp permit-nonconnected
```

Se recomienda siempre para tener la encaminamiento correcta en los dispositivos en sentido ascendente y descendentes para que el NAT trabaje sin habilitar el comando antedicho.

Registro y supervisión

Configurar el SNMP

Esta sección resalta varios métodos que se puedan utilizar para asegurar el despliegue del SNMP dentro de los dispositivos ASA. Es crítico que el SNMP esté asegurado correctamente para proteger la confidencialidad, la integridad, y la Disponibilidad de los datos de red y de los dispositivos de red con los cuales estos datos transitan. SNMP le brinda una gran cantidad de información sobre el estado de los dispositivos de red. Esta información se debe proteger contra los usuarios malintencionados que quieren leverage estos datos para realizar los ataques contra la red.

Identificaciones de comunidad SNMP

Las cadenas de comunidad son las contraseñas que se aplican a un dispositivo ASA para restringir el acceso, solo lectura y el acceso de lectura/escritura, a los datos SNMP en el dispositivo. Al igual que con todas las contraseñas, estas comunidades se deben elegir cuidadosamente para asegurarse de que no sean triviales. Se recomienda cambiar las comunidades regularmente y de acuerdo con las políticas de seguridad de la red. Por ejemplo, las comunidades se deben modificar cuando un administrador de red cambia los roles o deja la compañía.

Acceso de lectura del permiso SNMP:

```
snmp-server host <interface_name> <remote_ip_address>
```

SNMP traps del permiso

```
snmp-server enable traps all
```

Configurar el Syslog

Ha aconsejado para enviar la información de ingreso al sistema a un servidor del syslog remoto. Esto permite correlacionar y Auditar red y los eventos de seguridad a través de los dispositivos de red más con eficacia. Tenga en cuenta que los mensajes syslog son transmitidos de manera poco fiable por el protocolo UDP y en texto sin formato. Por este motivo, cualquier protección que una red permita al tráfico de administración (por ejemplo, cifrado o acceso fuera de banda) debe ser extendida para incluir el tráfico del Syslog. Los registros se pueden cofnigured para ser enviado al destino siguiente del ASA:

- ASDM
- Buffer
- Flash
- Correo electrónico
- Servidor FTP
- Servidor SNMP como desvíos
- Servidor de los Syslog

Nivel de gravedad del registro de la consola de la configuración

```
logging console critical
```

El Syslog basado TCP está también disponible. Todos los Syslog se pueden enviar al servidor de Syslog en el texto simple o adentro cifrar en caso del TCP.

Texto simple

syslog_ip del interface_name del host de registro [puerto tcp/

Cifrado

syslog_ip del interface_name del **host de registro** [**tcp/** *puerto* / [secure]

Si una conexión TCP no se puede establecer con el servidor de los Syslog, todas las nuevas conexiones serán negadas. Usted puede cambiar este comportamiento predeterminado ingresando el comando del “**permiso-hostdown de registración”**.

Grupos fecha/hora de la configuración en los mensajes del registro

La configuración de fechados de registro lo ayuda a correlacionar los eventos en los dispositivos de red. Es importante implementar una configuración correcta y constante de los fechados de registro para asegurarse de que pueda correlacionar los datos de registro.

```
logging timestamp
```

Para relacionado con la información adicional al Syslog refiera por favor el ejemplo de la configuración de syslog ASA.

Configurar el Netflow

A veces, usted puede necesitar identificar y determinar rápidamente el origen del tráfico de la red, especialmente durante una respuesta a un incidente o un rendimiento deficiente de la red. Netflow permite ver todo el tráfico en la red. Además, Netflow se puede implementar con colectores que pueden proporcionar tendencia a largo plazo y análisis automatizado.

Cisco ASA soporta los servicios de la versión 9 del Netflow. Las implementaciones ASA y ASASM de NSEL proporcionan un stateful, el método de seguimiento del flujo IP que exporta solamente esos expedientes que indiquen los eventos importantes en un flujo. En el flujo stateful que sigue, los flujos seguidos pasan con una serie de cambios de estado. Los eventos NSEL se utilizan para exportar los datos sobre el estatus del flujo y son accionados por el evento que causó el cambio de estado.

Refiera por favor el guía de instrumentación del Netflow de Cisco ASA para más información del Netflow en el ASA:

Sujeción de los config

Verificación de la imagen en el ASA

A partir de 9.1(2) y 8.4(4.1), el soporte para marcar de la integridad de imagen del SHA-512 fue agregado. Para verificar la suma de comprobación de un archivo, utilice el comando verify en el modo EXEC privilegiado.

Calcula y visualiza el valor MD5 para la imagen del software especificada. Compare este valor con el valor disponible en el cisco.com para esta imagen.

```
verify [ /md5 path ] [ md5-value ]
```

Contraseñas en los config

Se cifran o se ofuscan todas las contraseñas y las claves. El “ejecutar-config de la demostración” no revela las contraseñas reales.

Tal respaldo no se puede utilizar para el respaldo/el restore en el ASA. El respaldo que se toma para el restore purposes el whould se realice usando el comando “más sistema: ejecutar-config”. Las contraseñas de los config ASA se pueden cifrar usando una palabra clave principal. Refiera por favor la encripción de contraseña para la información detallada.

Mantenga la recuperación de contraseña

Inhabilitando esto inhabilitará el mecanismo de la recuperación de contraseña y inhabilitará el acceso al ROMMON. Los únicos medios de la recuperación de perdido o de las contraseñas olvidadas estarán para que el ROMMON borre todos los sistemas de archivos incluyendo los archivos de configuración y las imágenes. Usted debe hacer un respaldo de su configuración y tener un mecanismo para restablecer las imágenes de la línea de comando rommon.

Troubleshooting

No hay sección de Troubleshooting para este documento.