Red del éxito de Cisco (CSN) en la Seguridad del correo electrónico de Cisco

Contenido

Introducción Beneficios Información recopilada prerrequisitos Requisitos Configuración relacionada del Firewall Componentes Utilizados Configurar CSN y CTR dependencias Configuración CSN usando el UI Configuración CSN usando el CLI Troubleshooting

Introducción

Este documento proporcionó a la información en la función de red del éxito de Cisco que estaría disponible como parte de la versión de AsyncOS 13.5.1 para el dispositivo de seguridad del correo electrónico de Cisco (ESA). La red del éxito de Cisco (CSN) es un servicio usuario-habilitado de la nube. Cuando se habilita CSN, una conexión segura se establece entre el ESA y la nube de Cisco (usando CTR la conexión), para fluir la información de estatus de la característica. Fluir los datos CSN proporciona un mecanismo para seleccionar los datos del interés del ESA y para transmitirlos en un formato estructurado a las estaciones de la administración remota.

Beneficios

- Para informar al cliente con respecto a las características inusitadas disponibles que pueden mejorar la eficacia del producto.
- Para informar al cliente con respecto los Servicios de soporte técnico y a la supervisión adicionales que pudieron estar disponibles para el producto.
- Para ayudar a Cisco para mejorar el producto.

Información recopilada

Éstas son la lista de información de la característica que se recoja como parte de esta característica configurada una vez en el dispositivo ESA:

- Modelo del dispositivo (x90, x95, 000v,100v, 300v, 600v)
- Número de serie del dispositivo (UDI)

- UserAccountID (número de ID VLN o SLPIID)
- Versión de software
- Instale la fecha
- sIVAN (nombre de la cuenta virtual en la autorización de Smart)
- Modo del despliegue
- Anti-Spam de IronPort
- La caja fuerte de Graymail desinscribe
- Sophos
- McAfee
- Reputación del archivo
- Análisis del archivo
- Data Loss Prevention
- Alimentaciones de la amenaza exterior
- Análisis de imagen de Ironport
- Filtros del brote
- Configuraciones de encripción del correo electrónico de Cisco IronPort (cifrado del sobre)
- Cifrado PXE
- Reputación del dominio
- Filtrado de URL
- Arreglo para requisitos particulares de la página del bloque
- Seguimiento de mensajes
- Cuarentenas de la directiva, del virus y del brote
- Cuarentena del Spam

Prerrequisitos

Requisitos

Para configurar esta característica, éstos son algunos de los requisitos que deben ser satisfechos:

• CTR cuenta (de la Respuesta de Cisco ante amenazas)

Configuración relacionada del Firewall

La configuración de escudo de protección necesaria para conseguir CSN funcional es actualmente dependiente en CTR la comunicación y para referir por favor a este documento para más información: <u>ESA de integración con CTR</u>

Componentes Utilizados

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

 Versión 13.5.1.x y posterior de AsyncOS del dispositivo de seguridad del correo electrónico (ESA).

Configurar

Usted puede configurar esta característica usando el ESA UI o el CLI. Los detalles en ambos los pasos se muestran abajo.

CSN y CTR dependencias

La característica CSN depende CTR de la Conectividad de la característica para su funcionamiento exitoso y esta tabla proporciona más información sobre la relación entre estos dos procesos.

Respuesta de la amenaza	CSN	Conecto r de SSE	Proces o CSN
Discapacita do	Discapacit ado	Abajo	Discap acitado
Discapacita do (cancele)	Habilitado	Abajo	Abajo
Discapacita do (registrado)	Habilitado	Encima de	Encima de
Habilitado	Inhabilitad o manualm ente	Encima de	Abajo
Habilitado	Habilitado	Encima de	Encima de

Configuración CSN usando el UI

1) Inicie sesión en el ESA UI.

2) Hojee a las **configuraciones del servicio de la red** >> de la **nube** (asumiré que CTR fue inhabilitado antes de que comenzáramos con la actualización a 13.5.1.x). Antes de que la actualización, si CTR fue habilitado, después CSN también sea habilitada por abandono. Si CTR fue inhabilitado, después CSN también será inhabilitado.

Nota: Asumiremos CTR fuimos inhabilitados antes de que la actualización tan CTR en un despliegue centralizado se suponga ser inhabilitada como se habilita solamente en el S A para enviar la información de la información a CTR.

3) Esto es lo que usted observaría como valor por defecto en el dispositivo ESA: -

Cloud Services	
Threat Response:	Disabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
	Edit Settings
Cloud Services Settings	
Status:	Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.
Cisco Success Network	
Gathering Appliance Details and Feature U	sage
You can enable the Cisco Success Network feature to Cisco.	to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent
Sharing Settings	
Cisco Success Network: 🕐	Disabled
	Edit Settings

4) Ahora registraremos este ESA primero habilitando CTR los servicios en el ESA y "someta" los cambios.

Edit Cloud Services	
Threat Response:	✓ Enable
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Cancel	Submit

Cancel

5) mostraría que este estatus en CTR la página "el servicio de la nube de Cisco está ocupado. Navegue de nuevo a esta página después de un cierto tiempo para marcar el estatus del dispositivo." Confíe los cambios al dispositivo.

6) Usted entonces se movería a continuación y conseguiría CTR el token y registraría el dispositivo a CTR:

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
	Edit Settings
Cloud Services Settings	
Registration Token: ?	f4bf4ad6b31822c427dce0ee5a91b7e7 Register
Cisco Success Network	
Gathering Appliance Details and Feature U	sage
You can enable the Cisco Success Network feature to Cisco.	to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent
Sharing Settings	
Cisco Success Network: 🕐	Disabled (Register your appliance with Cloud Services to enable the Cisco Success Network.)
	Edit Settings

7) Usted debe ver este estatus una vez que el registro es acertado:

Éxito — Se inicia una petición de registrar su dispositivo con el portal de la Respuesta de Cisco ante amenazas. Navegue de nuevo a esta página después de un cierto tiempo para marcar el estatus del dispositivo.

8) Una vez que usted restaura la página, usted vería CTR haber registrado y el CSN habilitados:

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
	Edit Settings
Cloud Services Settings	
Deregister Appliance:	Deregister
Cisco Success Network	
Gathering Appliance Details and Feature Us	sage
You can enable the Cisco Success Network feature to Cisco.	to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent
Sharing Settings	
Cisco Success Network: ?	Enabled
	Edit Settings

9) Según lo discutido, CTR en este escenario necesita ser inhabilitado como este ESA se centraliza y usted todavía vería CSN habilitado como se esperaba. En caso de que, este ESA no sea manejado por el S A (NON-centralizado), usted puede guardar el CTR habilitado.

Cloud Services	
Threat Response:	Disabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
	Edit Settings
Cloud Services Settings	
Status:	Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.
Cisco Success Network	
Gathering Appliance Details and Feature U	sage
You can enable the Cisco Success Network feature to Cisco.	to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent
Sharing Settings	
Cisco Success Network: 🕐	Enabled
	Edit Settings

Éste debe ser el Estado final de la configuración. Este paso se debe seguir para cada ESA pues esta configuración es nivel de equipo.

Configuración CSN usando el CLI

(Machine esa)> **csnconfig**

You can enable the Cisco Success Network feature to send your appliance details and feature usage to Cisco.

Choose the operation you want to perform: - ENABLE - To enable the Cisco Success Network feature on your appliance. []> enable

The Cisco Success Network feature is currently enabled on your appliance.

Los cambios necesitarían ser confiados como parte de habilitar esto usando el CLI.

Troubleshooting

Para resolver problemas esta característica, hay un registro publicación (/data/pub/csn_logs) disponible que tendría la información sobre esta característica. La muestra abajo es el registro cuando el registro fue completado en el dispositivo:

(Machine ESA) (SERVICE)> tail

PI app aparchive attispam attivirus sarchive atthentication varchive punces i_logs sm_logs ar_logs as acryption as acryption aror_logs aq_logs again logs again logs	API Logs AMP Engine Logs AMP Archive Anti-Spam Logs Anti-Virus Logs Anti-Virus Archive Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download Download Download Download Download Download Download	None None None None None None None None
<pre>mp mparchive attispam attivirus sarchive atthentication varchive ounces i_logs m_logs m_logs m_logs as acryption aror_logs aq_logs agai logs agai logs</pre>	AMP Engine Logs AMP Archive Anti-Spam Logs Anti-Virus Logs Anti-Spam Archive Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs	Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download Download Download Download Download	None None None None None None None None
<pre>mparchive itispam itivirus sarchive ithentication varchive ounces i_logs sm_logs cr_logs cr_logs as acryption cror_logs aq_logs acryption cror_logs acryption cro</pre>	AMP Archive Anti-Spam Logs Anti-Virus Logs Anti-Spam Archive Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download Download Download Download	None None None None None None None None
atispam ativirus sarchive athentication varchive ounces i_logs sm_logs sr_logs as acryption eror_logs uq_logs	Anti-Spam Logs Anti-Virus Logs Anti-Spam Archive Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download Download Download	None None None None None None None None
ativirus sarchive thentication varchive bunces i_logs sm_logs sr_logs sp as acryption eror_logs uq_logs	Anti-Virus Logs Anti-Spam Archive Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download Download	None None None None None None None
archive thentication varchive ounces i_logs m_logs m_logs p tas tr_logs tr_logs tr_logs tror_logs tror_logs	Anti-Spam Archive Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download Download	None None None None None None
Athentication varchive punces i_logs m_logs m_logs m_logs p tas tas taryption tror_logs tq_logs taggui logs	Authentication Logs Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual Manual	Download Download Download Download Download Download	None None None None None
varchive punces i_logs m_logs r_logs p mas moryption mor_logs moryptions moryptions moryptions moryptions moryptions	Anti-Virus Archive Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual Manual	Download Download Download Download Download	None None None None None
nunces i_logs m_logs r_logs .p mas mcryption mror_logs mq_logs	Bounce Logs CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual Manual	Download Download Download Download	None None None None
i_logs m_logs r_logs p as acryption ror_logs aq_logs	CLI Audit Logs CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual	Download Download Download	None None None
m_logs cr_logs p as cryption cror_logs q_logs	CSN Logs CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual Manual	Download Download	None None
r_logs .p las lcryption ror_logs lq_logs	CTR Logs DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual Manual	Download	None
p las lcryption ror_logs lq_logs	DLP Logs Advanced Phishing Protection Logs Encryption Logs	Manual Manual	Download	
as acryption aror_logs aq_logs	Advanced Phishing Protection Logs Encryption Logs	Manual	DOWIITOau	None
acryption gror_logs aq_logs	Encryption Logs		Download	None
ror_logs uq_logs		Manual	Download	None
lq_logs	IronPort Text Mail Logs	Manual	Download	None
agui logs	Spam Quarantine Logs	Manual	Download	None
IYYUT_TOYS	Spam Quarantine GUI Logs	Manual	Download	None
pd_logs	FTP Server Logs	Manual	Download	None
archive	Graymail Archive	Manual	Download	None
raymail	Graymail Engine Logs	Manual	Download	None
ii_logs	HTTP Logs	Manual	Download	None
or_client	IP Reputation Logs	Manual	Download	None
il_logs	IronPort Text Mail Logs	Manual	Download	None
emediation	Remediation Logs	Manual	Download	None
portd_logs	Reporting Logs	Manual	Download	None
portqueryd_logs	Reporting Query Logs	Manual	Download	None
_client	S3 Client Logs	Manual	Download	None
anning	Scanning Logs	Manual	Download	None
lr_client	Sender Domain Reputation Logs	Manual	Download	None
ervice_logs	Service Logs	Manual	Download	None
artlicense	Smartlicense Logs	Manual	Download	None
itpd_logs	NTP logs	Manual	Download	None
atus	Status Logs	Manual	Download	None
rstem_logs	System Logs	Manual	Download	None
reatfeeds	Threat Feeds Logs	Manual	Download	None
ackerd_logs	Tracking Logs	Manual	Download	None
ified-2	Consolidated Event Logs	Manual	Download	None
dater_logs	Updater Logs	Manual	Download	None
grade_logs	Upgrade Logs	Manual	Download	None
l_rep_client	URL Reputation Logs	Manual	Download	None
the number of the	log you wish to tail.			
	anning r_client rvice_logs artlicense tpd_logs atus stem_logs reatfeeds ackerd_logs ified-2 dater_logs grade_logs l_rep_client the number of the	anningScanning Logsr_clientSender Domain Reputation Logsrvice_logsService LogsartlicenseSmartlicense Logstpd_logsNTP logsatusStatus Logsstem_logsSystem LogsreatfeedsThreat Feeds Logsackerd_logsTracking Logsified-2Consolidated Event Logsdater_logsUpdater Logsgrade_logsUpgrade Logsl_rep_clientURL Reputation Logsthe number of the log you wish to tail.	anningScanning LogsManualr_clientSender Domain Reputation LogsManualrvice_logsService LogsManualartlicenseSmartlicense LogsManualtpd_logsNTP logsManualatusStatus LogsManualstem_logsSystem LogsManualreatfeedsThreat Feeds LogsManualackerd_logsTracking LogsManualified-2Consolidated Event LogsManualgrade_logsUpgrade LogsManuall_rep_clientURL Reputation LogsManualthe number of thelog you wish to tail.Manual	anningScanning LogsManual Downloadr_clientSender Domain Reputation LogsManual Downloadrvice_logsService LogsManual DownloadartlicenseSmartlicense LogsManual Downloadtpd_logsNTP logsManual DownloadatusStatus LogsManual Downloadstem_logsSystem LogsManual DownloadreatfeedsThreat Feeds LogsManual Downloadackerd_logsTracking LogsManual Downloadified-2Consolidated Event LogsManual Downloadgrade_logsUpgrade LogsManual Downloadl_rep_clientURL Reputation LogsManual Downloadthe number of thelog you wish to tail.Manual Download

Sun Apr 26 18:16:13 2020 Info: Begin Logfile
Sun Apr 26 18:16:13 2020 Info: Version: 13.5.1-177 SN: 564D2E7007BA223114B8-786BB6AB7179
Sun Apr 26 18:16:13 2020 Info: Time offset from UTC: -18000 seconds
Sun Apr 26 18:16:13 2020 Info: System is coming up.
Sun Apr 26 18:16:13 2020 Info: DAEMON: Watchdog thread started
Sun Apr 26 18:16:16 2020 Info: The appliance is uploading CSN data
Sun Apr 26 18:16:16 2020 Info: The appliance has successfully uploaded CSN data