

CSC 6.X: Esempio di configurazione della reputazione della posta elettronica

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Impossibile ricevere e-mail da alcuni domini](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene fornito un esempio di configurazione su come configurare la reputazione della posta elettronica nel modulo SSM (Cisco Content Security and Control).

[Prerequisiti](#)

[Requisiti](#)

Per usare questa funzione, devi avere una licenza Security Plus.

[Componenti usati](#)

Le informazioni di questo documento si basano su Cisco Content Security and Control SSM con software versione 6.3.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

[Convenzioni](#)

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

Premesse

La reputazione dell'e-mail è una tecnologia che riduce i messaggi di posta indesiderata. Abilitando questa funzionalità, CSC SSM verifica se l'iniziatore del messaggio di posta elettronica è un indirizzo della lista nera o meno. Mantiene un elenco di database che contiene tutti gli indirizzi IP da cui provengono i messaggi di posta indesiderata. Se un messaggio di posta elettronica presenta un mittente di questo elenco, viene considerato come posta indesiderata e quindi eliminato.

I livelli di servizio offerti da questa tecnologia ERS (Email Reputation Technology) sono fondamentalmente di due tipi. Questi servizi si basano principalmente sul livello di autenticità degli indirizzi IP di origine.

- Standard ERS - Contiene le fonti note di posta indesiderata
- ERS Advanced - Contiene le fonti conosciute e quelle sospette

Quando si aggiunge un indirizzo IP al database ERS Standard, questo viene definito come origine della posta indesiderata ed è raro notare che un indirizzo IP venga rimosso da questo elenco. ERS Standard contiene l'elenco degli indirizzi IP che generano in modo coerente posta indesiderata.

ERS Advanced contiene un elenco di indirizzi IP che devono essere rimossi se trovati per non produrre ulteriormente lo spam. Ad esempio, un server di posta pirata può essere elencato in questo database nel momento in cui viene compromesso. Quando viene ripristinata alla normalità, viene rimossa dal database.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

1. Scegliere **Posta elettronica (SMTP) > Antispam > Reputazione e-mail**. Viene visualizzata una nuova finestra.
2. Per abilitare questa funzionalità di reputazione e-mail, fare clic su **Abilita** nella scheda Target.
3. Scegliere **Avanzate** per Livello di servizio.
4. Nel campo Indirizzi IP approvati specificare l'intervallo di indirizzi IP che si desidera escludere dalla scansione.

TREND MICRO™ InterScan™ for Cisco CSC SSM

SMTP Anti-spam (Email Reputation)

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

Target **Action**

SMTP Anti-spam (Email Reputation): **Disabled**

Email Reputation Services allows you to view global spam information and reports, as well as create or manage Approved and Blocked Sender IP address lists, perform administrative tasks, and configure the service.

[Email Reputation Services Portal](#)

Set Service Level

Standard: Uses the Standard Reputation database to block messages from known spam sources. [Click for more information.](#)

Advanced: Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. [Click for more information.](#)

Approved IP Address(es)

Add approved IP address:

Approved IP address(es):

10.0.0.0/8

5. Nella scheda Azione specificare il tipo di azione in base al criterio di protezione aziendale. Sono disponibili tre azioni: Chiudi connessione con messaggio di errore, Chiudi connessione senza messaggio di errore, Ignora connessione.

TREND MICRO™ InterScan™ for Cisco CSC SSM

SMTP Anti-spam (Email Reputation)

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

Target **Action**

Standard Reputation Database Action

Intelligent action - Permanent denial of connection for Standard Reputation Database matches
SMTP error code: (range 400 - 599; default=550)

Close connection with no error message

Bypass (not recommended)

Dynamic Reputation Database Action

Intelligent action - Temporary denial of connection for Dynamic Reputation Database matches
SMTP error code: (range 400 - 599; default=450)

Close connection with no error message

Bypass (not recommended)

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

[Impossibile ricevere e-mail da alcuni domini](#)

Problema:

Il problema è l'impossibilità di ricevere le e-mail da domini specifici. Sembra che il modulo CSC stia bloccando le e-mail. Quando si ignora il modulo, tutto funziona correttamente. Viene ricevuto questo messaggio di errore: 2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail QIL-NA RejectWithErrorCode-550 NA 0 0 NA NA NA 0 NA

Soluzione:

Per risolvere il problema, configurare correttamente la funzionalità di reputazione della posta elettronica.

[Informazioni correlate](#)

- [Supporto Cisco ASA Content Security and Control \(CSC\) Security Services Module](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)