Conformità alle normative sull'esportazione e restrizioni geografiche per Cisco Secure Access

Sommario

Introduzione

In questo documento viene descritto come esportare la conformità e le restrizioni geografiche per un accesso sicuro Cisco.

Premesse

In conformità con la politica generale di Cisco in materia di conformità delle esportazioni e in risposta alla guerra in Ucraina, Cisco limita l'acquisto, l'installazione e l'accesso sicuro da diversi paesi e regioni, tra cui Russia, Bielorussia, Crimea, Luhansk, Donetsk, Siria, Cuba, Iran e Corea del Nord.

DNS (Domain Name Server)

- Il servizio DNS per le query provenienti da indirizzi IP identificati come provenienti da Russia, Bielorussia, Crimea, Luhansk, Donetsk, Siria, Cuba, Iran, Corea del Nord e altre regioni sanzionate con geobloccaggio non prevedono policy di sicurezza o filtraggio dei contenuti applicate. Anche la creazione di rapporti è disabilitata. Le query DNS ricevono ancora una risposta valida e vengono gestite con lo stesso livello di servizio del traffico proveniente dal resto del mondo.
- Quando viene utilizzato per DNS, il modulo di protezione mobile Secure Client continua a risolvere il traffico DNS.

Sicurezza Web

- I server di sicurezza Web non accettano traffico se l'IP di origine proviene da uno dei paesi o delle aree bloccati.
- La configurazione predefinita del modulo di protezione mobile Secure Client ne determina la

connessione diretta a Internet quando l'accesso sicuro non è disponibile. Alcune configurazioni specifiche del cliente funzionano in modalità "fail-closed", che può causare la perdita dell'accesso a Internet da parte degli utenti.
- Il file predefinito PAC (Secure Access Protected Access Credential) determina la connessione diretta a Internet quando l'accesso protetto non è disponibile. Alcune configurazioni specifiche del cliente (ad esempio, quelle senza un percorso predefinito) possono "non essere chiuse", causando la perdita dell'accesso a Internet da parte degli utenti.
- I tunnel IPSec vengono disconnessi tramite il blocco IP o la revoca delle credenziali IKE (Internet Key Exchange). Il comportamento e l'esperienza dell'utente dipendono dalla configurazione specifica del cliente. In alcune configurazioni viene ripristinata una connessione Internet diretta, in altre viene ripristinata la funzionalità MPLS (Multiprotocol Label Switching), mentre in altre l'accesso a Internet può risultare interrotto.

Accesso al dashboard e agli amministratori

Il dashboard e le API di Accesso sicuro sono bloccati per gli utenti che si connettono da una delle aree elencate.

Wireless LAN Controller serie 9800

1. Cosa succede se gli utenti vengono bloccati ma non si trovano in una delle regioni colpite?
   Contattate il supporto e sono felici di indagare.

2. Quanto sono accurati i vostri dati geobloccanti?
   I servizi di geolocalizzazione leader del settore vengono utilizzati per determinare il paese per un determinato indirizzo IP.

3. Cosa fare se la posizione associata all'indirizzo IP è errata?
   Si consiglia di inviare una richiesta di correzione a questi servizi:

- https://www.maxmind.com/en/geoip-location-correction
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/
- http://www.ipligence.com/

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).