Verifica della funzionalità di bypass per la compatibilità con Microsoft 365 Secure Access

Sommario

Problema

Quando si configura Cisco Secure Access con la funzionalità Compatibilità di Microsoft 365 abilitata, non è chiaro se i nomi di dominio completi (FQDN) specifici correlati a Microsoft verranno automaticamente ignorati dall'elaborazione di Secure Web Gateway (SWG) e dalla decrittografia TLS. In particolare, è necessario chiarire il comportamento di bypass per questi domini:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Il problema principale è se questi domini richiedono l'aggiunta manuale all'elenco da non decrittografare o se vengono automaticamente esclusi quando è abilitata la compatibilità con Microsoft 365. Inoltre, c'è confusione sull'interazione tra le bypass a livello SWG e le impostazioni di decrittografia a livello IPS, in particolare per manage.microsoft.com, che appare nella documentazione in cui si suggerisce che la configurazione manuale Non decrittografare l'elenco può ancora essere richiesta.

Ambiente

- Cisco Secure Access
- Funzionalità di compatibilità di Microsoft 365 abilitata
- Ispezione Secure Web Gateway (SWG) e decrittografia TLS configurate
- Criteri di decrittografia IPS in uso
- Servizi di gestione e aggiornamento Microsoft che richiedono connettività

Risoluzione

Il comportamento delle funzionalità di compatibilità con Microsoft 365 è stato verificato tramite test di laboratorio con i seguenti risultati:

Ambito funzionalità compatibilità Microsoft 365

La funzionalità Compatibilità di Microsoft 365 esenta i domini correlati a Microsoft 365 contrassegnati come "Ottimizza" e "Consenti" nelle categorie endpoint di Microsoft dall'ispezione SWG e dall'applicazione delle policy. Ciò consente al traffico verso questi domini di passare inalterato sul layer SWG.

Risultati dei test di laboratorio

I test sono stati condotti in un ambiente lab controllato con compatibilità Microsoft 365 abilitata. Questo comportamento è stato osservato per gli FQDN specificati:

Passaggio 1: Abilita caratteristica di compatibilità di Microsoft 365

La funzionalità Compatibilità Microsoft 365 è stata attivata nella configurazione Secure Access.

Passaggio 2: Test del traffico sugli FQDN di destinazione

Il traffico Web è stato generato per ognuno dei tre FQDN utilizzando un browser Internet standard:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Passaggio 3: Verifica del comportamento di bypass nel dashboard

L'analisi del dashboard di Secure Access ha confermato che l'ispezione e la decrittografia del

traffico Web non sono state eseguite per il traffico verso queste destinazioni specifiche quando è stata abilitata la funzionalità Compatibilità di Microsoft 365.

Passaggio 4: Conferma comportamento di controllo DNS

Il traffico DNS verso queste destinazioni ha continuato a essere indirizzato tramite Secure Access, che è in linea con il comportamento documentato, a meno che non sia configurata una specifica esenzione DNS.

Risultati principali del comportamento

In base ai risultati dei test e all'analisi della documentazione:

- Bypass SWG: I tre FQDN specificati vengono ignorati dall'ispezione del traffico Web quando è abilitata la compatibilità con Microsoft 365.
- Decrittografia TLS: La decrittografia viene ignorata a livello SWG per questi domini.
- Controllo DNS: Le query DNS continuano a essere elaborate tramite l'accesso protetto a meno che non siano esplicitamente esentate.
- Copertura dominio: Mentre "*.microsoft.com" come intero dominio non viene completamente ignorato dalle specifiche, gli URL specifici testati vengono in pratica ignorati.

Considerazioni sui livelli IPS

La funzione di compatibilità di Microsoft 365 opera sul layer SWG. Per il bypass della decrittografia a livello IPS, può essere comunque richiesta la configurazione manuale:

- Se si desidera ignorare la decrittografia IPS anche per questi domini, può essere necessario aggiungere manualmente l'elenco Do Not Decrypt (Non decrittografare).
- L'elenco Non decrittografare influisce principalmente sulla decrittografia IPS invece che sull'elaborazione SWG.
- Per questo motivo, nella documentazione è possibile fare riferimento all'aggiunta di manage.microsoft.com all'elenco da non decrittografare anche quando è abilitata la compatibilità con Microsoft 365.

Causa

La confusione deriva dall'architettura su più livelli di Cisco Secure Access, in cui la compatibilità con Microsoft 365 influisce sull'elaborazione a livello SWG, mentre la decrittografia IPS opera come livello separato con i propri requisiti di configurazione. La funzionalità Compatibilità di Microsoft 365 gestisce automaticamente il bypass SWG per i domini Microsoft qualificati, ma i criteri di decrittografia IPS possono richiedere una configurazione separata tramite l'elenco Non decrittografare.

Contenuto correlato

- Documentazione sulla compatibilità di Cisco Secure Access con Microsoft 365
- Crea elenco indirizzi non decrittografati valido per Cisco Secure Access
- Supporto tecnico Cisco e download

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).