Configurazione delle mappe crittografiche basate su DN per il controllo dell'accesso ai dispositivi VPN

Sommario

Introduzione

In questo documento viene descritto come configurare le mappe crittografiche basate su nome distinto (DN) per fornire il controllo dell'accesso in modo che un dispositivo VPN possa stabilire tunnel VPN con un router Cisco IOS®. Nell'esempio, la firma di Rivest, Shamir e Adelman (RSA) è il metodo per l'autenticazione IKE. Oltre alla convalida dei certificati standard, le mappe crittografiche basate su DN cercano di far corrispondere l'identità ISAKMP del peer con determinati campi nei certificati, ad esempio il nome distinto X.500 o il nome di dominio completo (FQDN).

Prerequisiti

Requisiti

Questa funzione è stata introdotta per la prima volta nel software Cisco IOS versione 12.2(4)T. Per questa configurazione, è necessario usare questa release o versioni successive.

Èstato anche testato il software Cisco IOS versione 12.3(5). Tuttavia, le mappe crittografiche basate su DN non sono riuscite a causa dell'ID bug Cisco CSCed45783 (solo utenti registrati).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 7200 router
- Software Cisco IOS release 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

In precedenza, durante l'autenticazione IKE con il metodo di firma RSA e dopo la convalida della certificazione e la verifica dell'elenco di revoche di certificati (CRL) opzionale, Cisco IOS ha continuato la negoziazione in modalità rapida IKE. Non è stato fornito un metodo per impedire ai dispositivi VPN remoti di comunicare con interfacce crittografate, ad eccezione delle restrizioni sull'indirizzo IP del peer.

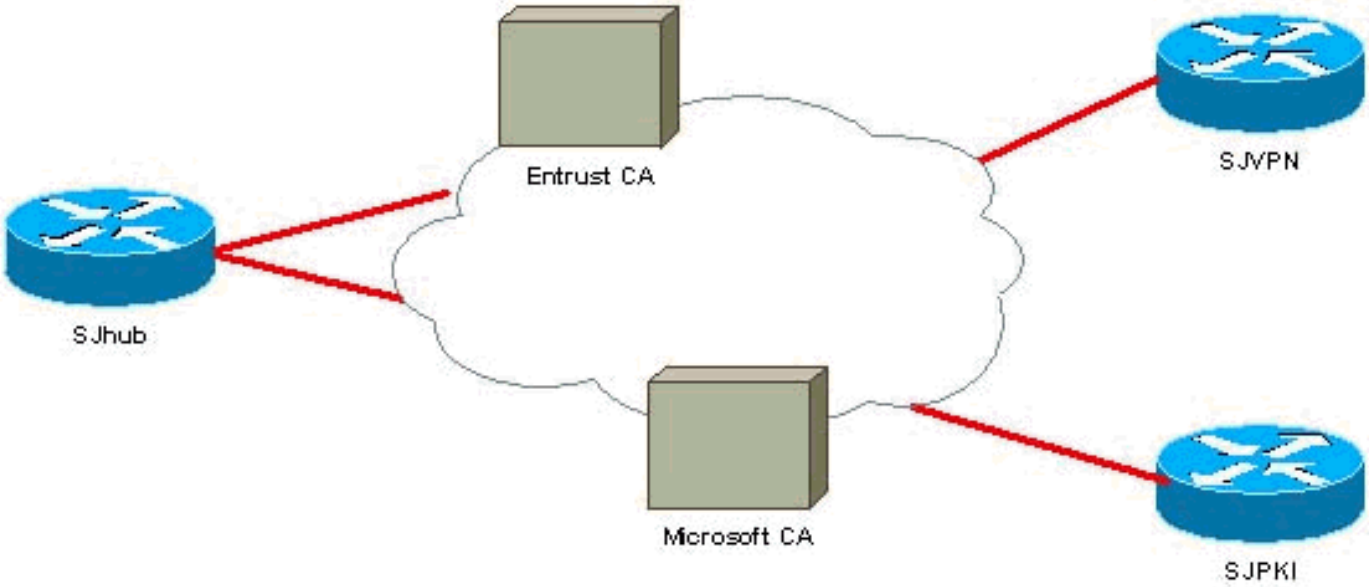
Ora con la mappa crittografica basata su DN, Cisco IOS può limitare i peer VPN remoti all'accesso solo alle interfacce selezionate con certificati specifici. In particolare, i certificati con determinati DN o FQDN.

Configurazione

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

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

Nell'esempio, per illustrare la funzione viene utilizzata una semplice configurazione di rete. Il router SJhub dispone di due certificati di identità, uno di Entrust Certificate Authority (CA) e l'altro di Microsoft CA. Vedere le informazioni correlate