Cisco IOS e IOS-XE con crittografia di nuova generazione

Sommario

Introduzione

In questo documento viene descritto il supporto della crittografia di nuova generazione (NGE) sulle piattaforme Cisco IOS® e Cisco IOS-XE.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco IOS, più versioni come indicato nella tabella
- Cisco IOS-XE, più versioni come indicato nella tabella
- Più piattaforme Cisco come indicato nella tabella

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.

Algoritmi GE

Gli algoritmi che compongono il GNE sono il risultato di oltre 30 anni di progressi globali e di evoluzione nella crittografia. Ogni componente del gruppo ha la propria storia, che descrive la storia variegata degli algoritmi del gruppo e la loro lunga revisione accademica e della comunità. Il

GRE comprende algoritmi creati a livello globale, esaminati a livello globale e disponibili pubblicamente.

Gli algoritmi NGE sono integrati in Internet Engineering Task Force (IETF), IEEE e altri standard internazionali. Di conseguenza, gli algoritmi GRE sono stati applicati ai protocolli più recenti e altamente sicuri che proteggono i dati utente, ad esempio IKEv2 (Internet Key Exchange versione 2).

I tipi di algoritmi crittografici includono:

- Crittografia simmetrica -AES (Advanced Encryption Standard) a 128 o 256 bit in GCM (modalità Galois/Contatore)
- Hash - SHA (Secure Hash Algorithms)-2 (SHA-256, SHA-384 e SHA-512)
- Firme digitali - ECDSA (Elliptic Curve Digital Signature Algorithm)
- Chiave concordata - Diffie-Hellman a curva ellittica (ECDH)

Supporto NGE sulle piattaforme Cisco IOS e Cisco IOS-XE

La tabella riepiloga il supporto NGE sulle piattaforme Cisco IOS e Cisco IOS-XE.

Piattaforme	Tipo di motore di crittografia	Supportato da NGE	Prima versione di Cis IOS/IOS-XE per il supporto di NGE
Tutte le piattaforme con Cisco IOS Classic	Motore di crittografia del software Cisco IOS	Sì	15.1(2)T
7200	VAM/VAM2/VSA	No	N/D
ISR G1	Tutto	No	N/D
ISR G2 2951, 3925, 3945	A bordo[1]	Sì	15.1(3)T
ISR G2 (esclusi 3925E/3945E)	VPN-ISM[1]	Sì	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	A bordo[1]	Sì	15.2(4)M
ISR G2 - CISCO87x	Software/hardware	No	N/D
ISR G2 - CISCO86x/C86x	Software[2]	Sì	15.1(2)T
ISR G2 C812/C819	Software/hardware	Sì	Giorno 1
ISR G2 - CISCO88x/CISCO89x	Software/hardware[3]	Sì	15.1(2)T
ISR G2 C88x	Software/Hardware[4]	Sì	Giorno 1
6500/7600	VPN-SPA	No	N/D
ASR 1000	Onboarding	Sì	Nota[5]
ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X	Onboarding	Sì	Cisco IOX-XE 3.12 (15.4(2)S)
ASR 1001-HX, ASR 1002-HX	Modulo di crittografia opzionale	Sì	Denali-16.3.1
ISR 4451-X	Onboarding	Sì	Cisco IOS-XE 3.9 (15.3(2)S)
ISR 4321, 4331, 4351, 4431	Onboarding	Sì	Cisco IOS-XE 3.13 (15.4(3)S)
ISR 42xx	Onboarding	Sì	Cisco IOS-XE Everes 16.4.1
CSR 1000v	Software	Sì	Cisco IOS-XE 3.12

ISR 1100	Onboarding	Sì	(15.4(2)S) Cisco IOS-XE Everes 16.6.2
Catalyst 8200, 8300, 8500 Edge Platform	Onboarding	Sì	Giorno 1
Catalyst 8000v	Software	Sì	Giorno 1

Nota 1: Sulla piattaforma ISR G2, se ECDH/ECDSA è configurato, queste operazioni di crittografia verrar eseguite nel software indipendentemente dal motore di crittografia. Gli algoritmi di crittografia AES-GCM- AES-GCM-256 sono supportati per la protezione del control plane IKEv2 dalla versione 15.4(2)T.
Nota 2: ISR G2 CISCO86x/C86x non dispone del supporto NGE nel motore di crittografia hardware.
Nota 3: ISR G2 CISCO88x/CISCO89x supporta hardware solo per SHA-256 con versione 15.2(4)M3 o successive.
Nota 4: Le seguenti SKU C88x non dispongono di supporto hardware per NGE: C881SRST-K9, C881SR GN-A-K9, C881SRSTW-GN-E-K9, C881-CUBE-K9, C881-V-K9, C881G-U-K9, C881G-S-K9, C881G-V-K C881G-B-K9, C881G+7-K9, C8 81G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C886VA-CUBE-K C886VAG+7-K9, C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C887VSRSTW-GNA K9, C887VSRSTW-GNE-K9, C887VA-V-K9, C887VA-V-W-E-K9, C887VA-CUBE-K C887VAG-S-K9, C887VAG+7-K9, C887VAMG+7-K9, C888SRSTW-GN-A-K9, C888SRSTW-GN-E-K9, C888SRST-K9, C888ESRST-K9, C888ESRSTW-GNA-K9, C888ESRSTW-GNE-K9, C888-CUBE-K9, C8 CUBE-K9 e C888EG+7-K9.
Nota 5: Il supporto per il piano di controllo di tipo GE (ECDH ed ECDSA) è stato introdotto con la versione XE3.7 (15.2(4)S). Il supporto del control plane iniziale SHA-2 era solo per IKEv2, con il supporto IKEv1 aggiunto nella versione XE3.10 (15.3(3)S). Gli algoritmi di crittografia AES-GCM-128 e AES-GCM-256 so supportati per la protezione del control plane IKEv2 a partire dalla versione XE3.12 (15.4(2)S) e 15.4(2)T. supporto per le corsie dati NGE è stato aggiunto nella versione XE3.8 (15.3(1)S) solo per piattaforme Oct (ASR1006 o ASR1013 con modulo ESP-100 o ESP-200); il supporto di dataplane non è disponibile per a piattaforme ASR1000.

Supporto di altre funzioni GE

Supporto GETVPN per NGE

- Il supporto del software Cisco IOS sulle piattaforme ISR G2 inizia con la versione 15.2(4)M.
- Il supporto per ASR inizia con il software Cisco IOS-XE versione 3.10S (15.3(3)S).

Informazioni correlate

- Crittografia di nuova generazione
- Documentazione e supporto tecnico – Cisco Systems