

BE-SPA-SSL: داهش ىلع فرعتلا ةلكشم SPA112

دحمل ا خيراتلا

م 2017، ريانى 30

لحل ا خيرات

رفوم ريغ

ةرثأتملا تاجت نمل

1.4.2	SPA112

ةلكشملا فصول

نايبل SNI معد نودب (SNI) مداخل مسا ةراش SPA نم هيقلت مت يذلا بلطلال معددي ال مداخل مسا تامولعم ىلع Client Hello ويوتحي ال ،لقنلا ةقبط نام ةلحرم ىلع مسالا

مت يتل TLS ليمعب ةصاخلا Hello ةلاسرل ةشاش ةطق لكيدل ،ةيلاتلا روصلا يف ام دنع مداخل ةطساوب اهياقلت

1. SPA نم بلطلال يقلت مت (SNI معد متي ال)

Handshake Protocol Client Hello يف server_name قحلم دجوي ال ،ةلحال هذه يف :ةظحالم

Time	Source	Destination	Protocol	Length	Info
07.771605	172.16.39.4	172.16.36.29	TCP	74	36611 -> 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4294958457 TSecr=0 WS=2
07.771641	172.16.36.29	172.16.39.4	TCP	74	443 -> 36611 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=61223503 TSecr=4294958457 WS=128
07.772489	172.16.39.4	172.16.36.29	TCP	66	36611 -> 443 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=4294958458 TSecr=61223503
07.775655	172.16.39.4	172.16.36.29	TLSv1.2	285	Client Hello
07.775672	172.16.36.29	172.16.39.4	TCP	66	443 -> 36611 [ACK] Seq=1 Ack=220 Win=15616 Len=0 TSval=61223504 TSecr=4294958458

Frame 7: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)

- Ethernet II, Src: CiscoInc_f1:74:b4 (50:67:ae:f1:74:b4), Dst: 02:c5:4f:4f:8a:8e (02:c5:4f:4f:8a:8e)
- Internet Protocol Version 4, Src: 172.16.39.4, Dst: 172.16.36.29
- Transmission Control Protocol, Src Port: 36611 (36611), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 219
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 214
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 210
 - Version: TLS 1.2 (0x0303)
 - Random
 - Session ID Length: 0
 - Cipher Suites Length: 60
 - Cipher Suites (30 suites)
 - Compression Methods Length: 1
 - Compression Methods (1 method)
 - Extensions Length: 109
 - Extension: ec_point_formats
 - Extension: elliptic_curves
 - Extension: SessionTicket TLS
 - Extension: signature_algorithms
 - Extension: Heartbeat

2. ضرعت سمل ربع بلطلال مي دقت مت (SNI معد متي)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة و مچم مادختساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچي فني م دخت سمل معد و ت م مدي دقتل لة يرش بل او
امك ة قيق د نوك ت نل لة آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا م ل ا ح ل ا و ه
ى ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رفوتم طبارل) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل