ESA에서 전달에 대한 TLS 협상 제어

목차

소개

이 문서에서는 ESA(Email Security Appliance)에서 전달 시 TLS(Transport Layer Security) 협상을 제어하는 방법에 대해 설명합니다.

RFC 3207에 정의된 대로 "TLS는 SMTP 서버 및 클라이언트가 전송 계층 보안을 사용하여 인터넷을 통해 인증된 사설 통신을 제공하도록 허용하는 SMTP 서비스의 확장입니다.TLS는 프라이버시 및 인증과 함께 TCP 통신을 향상하기 위해 널리 사용되는 메커니즘입니다."

전송 시 TLS 사용

이 문서에 설명된 방법 중 하나를 사용하여 특정 도메인으로 이메일을 전송하려면 STARTTLS를 요구할 수 있습니다.

- CLI destconfig 명령을 사용합니다.
- GUI에서 **Mail Policies(메일 정책)** > Destination Controls(**대상 제어)를** 선택합니다.

Destination Controls(대상 제어) 페이지 또는 **destconfig** 명령을 사용하면 도메인을 포함할 때 지정된 도메인에 대해 TLS에 대해 5가지 다른 설정을 지정할 수 있습니다.또한 도메인 검증이 필요한지 여부를 지정할 수 있습니다.

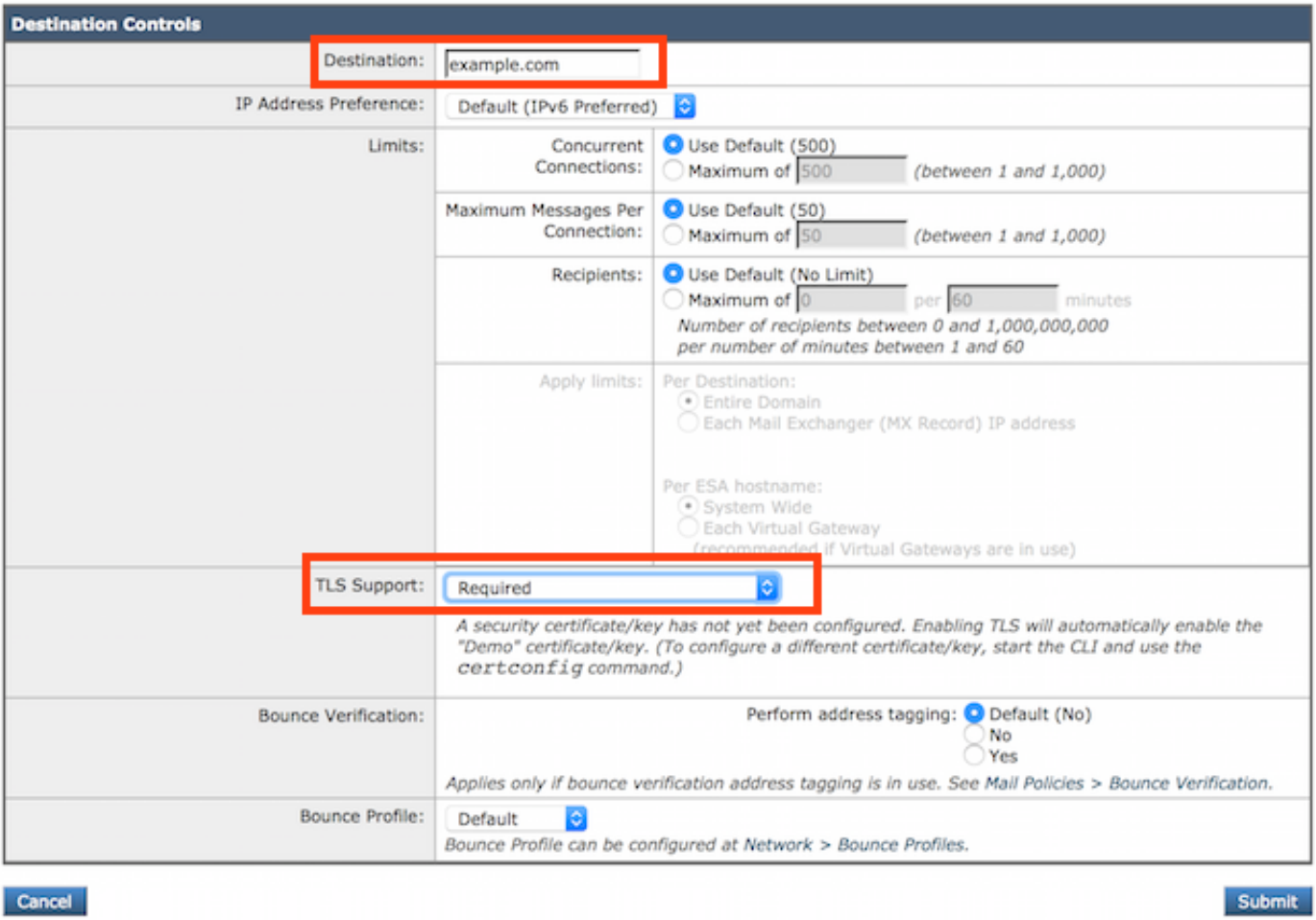
TLS 설정 정의

TLS 설정	의미
기본값	Destination Controls(대상 제어) 페이지 또는 **destconfig -> default** 하위 명령을 사용하여 리스너에서 도메인의 MTA(Message Transfer Agent)로 보내는 연결에 사용되는 기본 TLS 설정입니다.다음 질문에 **no**로 답하면 "Default" 값이 설정됩니다."이 도메인에 대해 특정 TLS 설정을 적용하시겠습니까?"
1. 아니요	TLS는 인터페이스에서 도메인에 대한 MTA로의 발신 연결에 대해 협상되지 않습니다.
2. 선호	TLS는 ESA 인터페이스에서 도메인에 대한 MTA로 협상됩니다.그러나 TLS 협상이 실패할 경우(220개의 응답을 받기 전에) SMTP 트랜잭션은 "암호화되지 않은" 상태로 계속됩니다. 인증서가 신뢰할 수 있는 인증 기관에서 시작되었는지 확인하려고 시도하지 않습니다.220 응답을 받은 후 오류가 발생하면 SMTP 트랜잭션이 일반 텍스트로 되돌아가지 않습니다.
3. 필수	TLS는 ESA 인터페이스에서 도메인에 대한 MTA로 협상됩니다.도메인의 인증서를 확인하려고 시도하지 않습니다.협상이 실패하면 연결을 통해 이메일이 전송되지 않습니다.협상이 성공하면 암호화된 세션을 통해 메일이 전달됩니다.
4. 선호(확인)	TLS는 ESA에서 도메인에 대한 MTA로 협상됩니다.어플라이언스는 도메인의 인증서를 확인하려고 시도합니다.세 가지 결과가 가능합니다. • TLS가 협상되고 인증서가 확인됩니다.메일은 암호화된 세션을 통해 전달됩니다.

	• TLS는 협상되지만 인증서가 확인되지 않습니다.메일은 암호화된 세션을 통해 전달됩니다. • TLS 연결이 만들어지지 않고, 그 후 인증서가 확인되지 않습니다.이메일 메시지는 일반 텍스트로 전달됩니다.
5. 필수(확인)	TLS는 ESA에서 도메인에 대한 MTA로 협상됩니다.도메인 인증서를 확인해야 합니다.다음과 같은 세 가지 결과가 가능합니다. • TLS 연결이 협상되고 인증서가 확인됩니다.이메일 메시지는 암호화된 세션을 통해 전달됩니다. • TLS 연결은 협상되지만 신뢰할 수 있는 CA(인증 기관)에서 인증서를 확인하지 않습니다.메일이 배달되지 않습니다. • TLS 연결이 협상되지 않습니다.메일이 배달되지 않습니다.
6. 필수 - 호스팅된 도메인 확인	TLS Required(**TLS 필요) - Verify(확인)** 및 TLS Required(**TLS 필요) - Verify Hosted Domain(호스팅된 도메인 확인)** 옵션 간의 차이점은 ID 확인 프로세스에서 발생합니다.제공된 ID가 처리되는 방식 및 사용할 수 있는 참조 식별자 유형은 최종 결과에 차이를 만듭니다. 제공된 ID는 dNSName 유형의 subjectAltName 확장자에서 처음 파생됩니다.dNSName과 승인된 참조 ID(REF-ID) 중 하나가 일치하지 않으면 CN이 제목 필드에 존재하더라도 확인이 실패하고 추가 ID 확인을 통과할 수 있습니다.주체 필드에서 파생된 CN은 인증서에 dNSName 유형의 subjectAltName 확장이 없는 경우에만 검증됩니다. 자세한 내용은 Cisco Email Security에 대한 TLS 확인 프로세스를 검토하십시오.

GUI에서 TLS 활성화

1. [모니터] > [**대상 컨트롤]을 선택합니다**.
2. Add **Destination을 클릭합니다**.
3. Destination 필드에 대상 도메인을 추가합니다.
4. TLS Support(TLS 지원) 드롭다운 목록에서 TLS 지원 방법을 선택합니다.
5. Submit(**제출**)을 클릭하여 변경 사항을 제출합니다.



CLI에서 TLS 활성화

이 예에서는 **destconfig** 명령을 사용하여 도메인 example.*com*에 대한 TLS 연결 및 암호화된 대화를 *요청합니다*.이 예에서는 어플라이언스에 사전 설치된 데모 인증서를 사용하는 도메인에 TLS가 필요하다는 것을 보여줍니다.테스트 목적으로 데모 인증서와 함께 TLS를 활성화할 수 있지만, 안전하지 않으며 일반적인 용도로 권장되지 않습니다.

다음 질문에 **no**로 답하면 "Default" 값이 설정됩니다."이 도메인에 대해 특정 TLS 설정을 적용하시겠습니까?" **예**로 응답할 경우 **아니오**, **선호** 또는 **필수**를 **선택합니다**.

```
ESA> destconfig

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
[]> example.com
Choose the operation you want to perform:
```

```
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
[]> example.com

Do you wish to configure a concurrency limit for example.com? [Y]> N

Do you wish to apply a messages-per-connection limit to this domain? [N]> N

Do you wish to apply a recipient limit to this domain? [N]> N

Do you wish to apply a specific TLS setting for this domain? [N]> Y

Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
6. Required - Verify Hosted Domains
[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.

Do you wish to apply a specific bounce verification
address tagging setting for this domain? [N]> N

Do you wish to apply a specific bounce profile to this domain? [N]> N

Do you wish to apply a specific IP sort preference to this domain? [N]> N

There are currently 3 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> list

            Rate                Bounce         Bounce      IP Version
Domain       Limiting  TLS      Verification   Profile     Preference
===========  ========  =======  ============   =========   ============
example.com  Default   On       Default        Default     Default
(Default)    On        Off      Off            (Default)   Prefer IPv6
```