Que é o algoritmo para a verificação de certificado na ferramenta de segurança do email de Cisco (ESA)?

Índice

Introdução

Ao usar o TLS para entregar o email através de uma ferramenta de segurança do email de Cisco (ESA) você pode escolher executar a utilização da verificação de certificado “verifica que” ou “hospedado verifique” opções. Este é um crucial parte de fixando a entrega dos email sobre o TLS, e é importante saber esta verificação é executada.

Que é o algoritmo para a verificação de certificado na ferramenta de segurança do email de Cisco (ESA)?

Há realmente dois algoritmos, um para “verifica” a opção, e o outro para “hospedado verifica” a opção. Tipicamente “hospedados verificam que” a opção está recomendada porque é compatível com uma variedade maior de encenações.

Informações de Apoio

- Esta documentação é baseada em AsyncOS 8.0.1 e em umas versões mais atrasadas. As versões anterior de AsyncOS podem ter o comportamento um tanto diferente.
- Salvo disposição em contrário, os fósforos do convite são apoiados
- Cada algoritmo para após uma compatibilidade bem sucedida e as verificações subsequentes não são avaliadas
- O comando CLI **tlsverify os** usos “verifica o algoritmo”

Definições

- CN: Este é o Common Name, parte do assunto do certificado
- SAN: Esta é a extensão sujeita do nome alternativo ao X.509. Quando usados neste documento, nós estamos referindo especificamente todos os nomes de DNS incluídos no campo SAN.

- Domínio de e-mail: Esta é a parcela do domínio do endereço email do receptor. Por exemplo, ao entregar a “user@example.com”, o domínio de e-mail é “example.com”
- Nomes de host MX: Estes são os nomes de host dos registros MX do domínio de e-mail
- Hostname PTR: Este é o hostname retornado por uma consulta PTR DNS do endereço IP de Um ou Mais Servidores Cisco ICM NT que o ESA está conectando a
- Nomes de host da rota S TP: Se uma rota S TP é configurada para este destino, este é o hostname usado na rota S TP

Hospedado verifique o algoritmo

1. Se o certificado contém atributos SAN, *simplesmente* estes estarão usados e o CN será ignorado. O CN será usado somente se não há nenhum atributo SAN no certificado. Isto conforma-se ao RFC 6125.
2. O certificado é verificado contra o domínio de e-mail.
3. O certificado é verificado contra todos os nomes de host da rota S TP que puderem existir.
4. O certificado é verificado contra os hostname MX.
5. Se nenhumas das verificações precedentes sucederam, a verificação falha.

Verifique o algoritmo

1. Os atributos SAN são verificados contra o domínio de e-mail.
2. O CN é verificado contra o domínio de e-mail. Nota: Os fósforos do convite não são apoiados.
3. Os atributos SAN são verificados contra o hostname PTR.
4. Se nenhumas das verificações precedentes sucederam, a verificação falha.