¿Cuál es el algoritmo para la verificación del certificado en el dispositivo de seguridad del correo electrónico de Cisco (ESA)?

Contenido

Introducción

Al usar TLS para entregar el correo electrónico vía un dispositivo de seguridad del correo electrónico de Cisco (ESA) usted puede elegir realizar la verificación del certificado usando o "verifica" o "recibido verifique" las opciones. Esto es una parte de crucial que asegura la salida de los correos electrónicos sobre TLS, y es importante saber se realiza esta verificación.

¿Cuál es el algoritmo para la verificación del certificado en el dispositivo de seguridad del correo electrónico de Cisco (ESA)?

Hay realmente dos algoritmos, uno para "verifica" la opción, y el otro para "recibido verifica" la opción. "Recibidos verifican típicamente" la opción se recomiendan pues son compatibles con una variedad más grande de escenarios.

Antecedentes

- Esta documentación se basa en AsyncOS 8.0.1 y posterior versiones. Las versiones anteriores de AsyncOS pueden tener comportamiento algo diferente.
- Salvo especificación de lo contrario, se soportan las coincidencias del comodín
- Cada algoritmo para después de una correspondencia con éxito y los controles subsiguientes no se evalúan
- El comando CLI **tlsverify las** aplicaciones "verifica el algoritmo"

Definiciones

- CN: Éste es el Common Name, parte del tema del certificado
- SAN: Ésta es la extensión sujeta del nombre alterno al X.509. Cuando están utilizados en este documento, estamos refiriendo específicamente a cualquier nombre DNS incluido en el SAN colocamos.

- Dominio de correo electrónico: Ésta es la porción del dominio de la dirección de correo electrónico del beneficiario. Por ejemplo, cuando la entrega a “user@example.com”, dominio de correo electrónico es “example.com”
- Nombres de host MX: Éstos son los nombres de host de los expedientes MX del dominio del correo electrónico
- Nombre de host PTR: Éste es el nombre de host vuelto por las operaciones de búsqueda PTR DNS de la dirección IP que el ESA está conectando con
- Nombres de host de la ruta S TP: Si una ruta S TP se configura para este destino, éste es el nombre de host usado en la ruta S TP

Recibido verifique el algoritmo

1. Si el certificado contiene los atributos SAN, *sólo* éstos serán utilizados y el CN será ignorado. El CN será utilizado solamente si no hay atributos SAN en el certificado. Esto se ajusta al RFC 6125.
2. El certificado se marca contra dominio de correo electrónico.
3. El certificado se marca contra cualquier nombre de host de la ruta S TP que pueda existir.
4. El certificado se marca contra los hostname MX.
5. Si ningunos de los controles anteriores han tenido éxito, la verificación falla.

Verifique el algoritmo

1. Los atributos SAN se marcan contra dominio de correo electrónico.
2. El CN se marca contra dominio de correo electrónico. **Note**: Las coincidencias del comodín no se soportan.
3. Los atributos SAN se marcan contra el nombre de host PTR.
4. Si ningunos de los controles anteriores han tenido éxito, la verificación falla.