CRE FAQ: Como eu uso o TLS para fixar respostas unencrypted CRE?

Índice

Introdução

Este documento descreve como usar o Transport Layer Security (TLS) para fixar respostas do serviço registrado Cisco do envelope (CRE), que permite que um usuário não precise das decifrar, em colaboração com a ferramenta de segurança do email de Cisco (ESA).

Como eu uso o TLS para fixar respostas unencrypted CRE?

Àrevelia, as respostas a um email seguro são cifradas por CRE e enviadas sobre a seu mail gateway. Passam então completamente a seus server do correio cifrados para que o utilizador final abra com suas credenciais CRE.

A fim evitar a necessidade para que o usuário autentique com CRE para abrir a resposta segura, os CRE entregam em um formulário “unencrypted” para enviar os gateways que apoiam o TLS. Na maioria dos casos o mail gateway é o ESA, e este artigo aplica-se.

Contudo, se há um outro mail gateway que se sente na frente do ESA tal como um filtro externo do Spam, lá não está nenhuma necessidade para o certificate/TLS/mail flui configuração em seu ESA. Neste caso, você pode saltar etapas 1 3 na seção de solução deste documento. Para que as respostas unencrypted trabalhem neste ambiente, o filtro externo do Spam (mail gateway) é o dispositivo que precisa de apoiar o TLS. Se apoiam o TLS, você pode mandar CRE confirmar este e obtê-lo estabelecido para respostas “unencrypted” a fim fixar email.

Estrutura de política do remetente

A fim evitar falhas de verificação da estrutura de política do remetente (SPF), você deve adicionar o MX: res.cisco.com, mxnat1.res.cisco.com, e mxnat3.res.csico.com a seu registro SPF.

Onde e como você adiciona CRE a seu registro SPF depende de como o Domain Name System (DNS) é executado em sua topologia de rede. Contacte seu administrador de DNS para mais informação.

Se o DNS não é configurado para incluir CRE, quando seguro compõe e fixe respostas estão gerados e entregado através dos server chaves hospedados, o endereço IP de Um ou Mais Servidores Cisco ICM NT que parte não combinará os endereços IP de Um ou Mais Servidores

Cisco ICM NT listados nos receptores termina, tendo por resultado uma falha de verificação SPF.

Nomes de host e endereços IP de Um ou Mais Servidores Cisco ICM NT

Hostname	IP Address	Tipo de registro
res.cisco.com	184.94.241.74	A
---- ---- ----	---- ---- ----	---- ---- ----
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX
---- ---- ----	---- ---- ----	---- ---- ----
mxnat1.res.cisco.com	208.90.57.32	A
mxnat3.res.cisco.com	184.94.241.96	A

Os nomes de host e os endereços IP de Um ou Mais Servidores Cisco ICM NT são sujeitos mudar baseado no serviço/manutenção de rede e prestar serviços de manutenção/crescimento de rede.

Solução

1. Obtenha e instale um certificado assinado e um certificado do intermediário no ESA. **Note**: É importante você obtém o certificado intermediário de sua autoridade de assinatura como o certificado do programa demonstrativo que vem no dispositivo faz com que o processo de verificação CRE falhe.
2. Crie uma política nova do fluxo de correio: Do GUI, escolha a **política do > Add das políticas do correio > das políticas do fluxo de correio….**Dê entrada com um nome e deixe tudo outro no padrão à exceção dos *recursos de segurança: TLS.* Ajuste isto ao **exigido**.
3. Crie um grupo novo do remetente: Do GUI, escolha o **grupo do remetente do > Add das políticas do correio > da vista geral do CHAPÉU….**Dê entrada com um nome e ajuste o número do ordem a #1. Você pode igualmente incorporar um comentário opcional. Escolha a política que do fluxo de correio você criou na licença de etapa 2. tudo mais placa.O clique **submete e adiciona remetentes >>**.
4. No campo do remetente, entre nestas escalas e em nomes de host IP:
```
.res.cisco.com
.cres.iphmx.com
208.90.57.0/26 (current CRES IP network range)
204.15.81.0/26 (old CRES IP network range)
```
5. Submeta e comprometa as mudanças.
6. Depois que você está seguro o ESA está preparado para o TLS dos server CRE, segue as etapas em como faz o teste I se meu domínio apoia o TLS com CRE? a fim pedir os server CRE para começar usar o TLS.

Informações Relacionadas

- ESA FAQ: Que são os IPs e os nomes de host dos server chaves CRE?
- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems