

Os endereços IP de Um ou Mais Servidores Cisco ICM NT/domínios/endereços email isentos do ESA saltam a configuração

Índice

[Introdução](#)

[Os endereços IP de Um ou Mais Servidores Cisco ICM NT/domínios/endereços email isentos do ESA saltam a configuração](#)

[Correio de partida](#)

[Correio de entrada](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar de entrada e o correio de partida para isentar endereços IP de Um ou Mais Servidores Cisco ICM NT, domínios, ou endereços email para Cisco envia por correio eletrônico a ferramenta de segurança (ESA).

Os endereços IP de Um ou Mais Servidores Cisco ICM NT/domínios/endereços email isentos do ESA saltam a configuração

Você pode especificar os domínios destinatários em que para desabilitar a verificação do salto quando o ESA entrega 2 aqueles domínios. Você precisará de configurar o correio de partida e de entrada.

Correio de partida

1. Vá às políticas do correio > aos controles do destino.
2. Seletor “adicionar o destino...”.
3. Chame o destino novo “example.com”.
4. Nos ajustes, ajuste do “a verificação salto” a não.
5. Submeta e comprometa mudanças.

Destination Controls	
Destination:	<input type="text" value="example.com"/>
IP Address Preference:	<input type="text" value="Default (IPv6 Preferred)"/>
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <i>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</i>
	Apply limits: Per Destination: <input checked="" type="radio"/> Entire Domain <input type="radio"/> Each Mail Exchanger (MX Record) IP address Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway (recommended if Virtual Gateways are in use)
TLS Support:	<input type="text" value="Default (None)"/> <i>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</i>
Bounce Verification:	Perform address tagging: <input type="radio"/> Default (No) <input checked="" type="radio"/> No <input type="radio"/> Yes <i>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</i>
Bounce Profile:	<input type="text" value="Default"/> <i>Bounce Profile can be configured at Network > Bounce Profiles.</i>

Nota: Para o correio de partida, você pode somente referir o domínio do destino e não um endereço IP de Um ou Mais Servidores Cisco ICM NT ou um endereço email.

Correio de entrada

Security Features	
Spam Detection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Virus Protection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Encryption and Authentication:	TLS: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required <i>A security certificate/key has not been configured and assigned to a listener. (See Network > Certificates.) Enabling TLS will automatically use the "Demo" certificate/key for listeners.</i> <input type="checkbox"/> Verify Client Certificate
	SMTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication
	Domain Key/DMARC Signing: <input type="radio"/> On <input checked="" type="radio"/> Off
	DKIM Verification: <input type="radio"/> On <input checked="" type="radio"/> Off Use DKIM Verification Profile: <input type="text" value="DEFAULT"/>
SPF/SIDF Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Conformance Level: <input type="text" value="SIDF Compatible"/>
	Downgrade PRA verification result if "resent-sender:" or "resent-from:" were used: <input type="radio"/> No <input type="radio"/> Yes
	HELO Test: <input type="radio"/> Off <input type="radio"/> On
DMARC Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Use DMARC Verification Profile: <input type="text" value="DEFAULT"/>
	DMARC Feedback Reports: <input type="checkbox"/> Send aggregate feedback reports <small>* DMARC reporting message must be DMARC compliant. * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls.</small>
Bounce Verification:	Consider Unlagged Bounces to be Valid: <input checked="" type="radio"/> Yes <input type="radio"/> No <small>(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)</small>

Notas: A falha configurar seu correio de entrada pode fazer com que seu ESA deixe cair mensagens de salto válidas para mensagens.

Notas: Para verificar que a verificação do salto está desabilitada para este domínio, você pode permitir o "domínio debuga logs" e ata os logs para verificar.

Informações Relacionadas

- [Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)