

Освобожденные Адреса/Домены/Адреса электронной почты IP от Конфигурации Сильного удара ESA

Содержание

[Введение](#)

[Освобожденные Адреса/Домены/Адреса электронной почты IP от Конфигурации Сильного удара ESA](#)

[Исходящая почта](#)

[Входящая почта](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить входящую и исходящую почту для освобождения IP-адресов, доменов или адресов электронной почты для Cisco Email Security Appliance (ESA).

Освобожденные Адреса/Домены/Адреса электронной почты IP от Конфигурации Сильного удара ESA

Можно задать домены получателя, на которых можно отключить Проверку Сильного удара, когда ESA доставляет к тем доменам. Необходимо будет настроить и исходящую и входящую почту.

Исходящая почта

1. Перейдите к Почтовой Политике > Целевые Средства управления.
2. Выберите "Add destination...".
3. Вызовите новый целевой "example.com".
4. В параметрах настройки, набор "Проверка Сильного удара" к Нет.
5. Подвергнитесь и изменения Передачи.

Destination Controls	
Destination:	<input type="text" value="example.com"/>
IP Address Preference:	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 <i>(recommended if Virtual Gateways are in use)</i>
TLS Support:	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:	Default <i>Bounce Profile can be configured at Network > Bounce Profiles.</i>

Примечание: Для исходящей почты можно только обратиться к целевому домену и не IP-адресу или адресу электронной почты.

Входящая почта

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: DEFAULT
SPF/SIDF Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Conformance Level: 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 checked="" type="radio"/> On
	Use DMARC Verification Profile: DEFAULT DMARC Feedback Reports: <input checked="" 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 <i>(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)</i>

Примечания: Сбой для настройки входящей почты может заставить ESA отбрасывать допустимые возвращенные сообщения для сообщений.

Примечания: Чтобы проверить, что Проверка Сильного удара отключена для этого домена, можно включить "доменные журналы отладки" и выследить журналы для проверки.

Дополнительные сведения

- [Устройство безопасности электронной почты Cisco - руководства пользователя](#)
- [Cisco Systems – техническая поддержка и документация](#)