

Systems Engineering
“How to” Guide
Spoof Protection with
IronPort Email Security Appliance



Tom Foucha, CCSP, CISSP
Consulting Systems Engineer
tofoucha@cisco.com

July 23, 2012

INTRODUCTION	3
Configure Mail Flow Policy	3
Configure HAT	4
Configure Exception Table	5

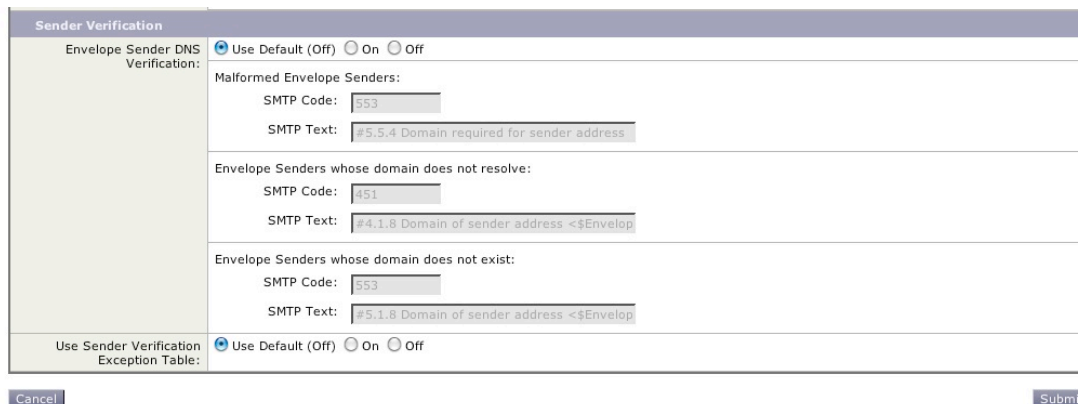
INTRODUCTION

By default the IronPort Email Security Appliance does not prevent the inbound delivery of messages that are addressed “from” the same domain going to the same domain. This allows messages to be “spoofed” by outside companies that do legitimate business with the customer. Many companies rely on 3rd party organization to send email on behalf of the company such as Health Care, Travel Agencies etc.

This paper documents how to enable Spoof Protection and still allow those outside authorized vendors to represent (spoof) email to the same domain.

Configure Mail Flow Policy

Create a new Mail Flow Policy using a name that is relevant like **SpoofAllow** and at the very end of the section in **Sender Verification** change from the **Use Sender Verification Exception Table**: Default to the **OFF** position.



Sender Verification	
Envelope Sender DNS Verification:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> On <input type="radio"/> Off
Malformed Envelope Senders:	
SMTP Code:	553
SMTP Text:	#5.5.4 Domain required for sender address
Envelope Senders whose domain does not resolve:	
SMTP Code:	451
SMTP Text:	#4.1.8 Domain of sender address <\$Envelop
Envelope Senders whose domain does not exist:	
SMTP Code:	553
SMTP Text:	#5.1.8 Domain of sender address <\$Envelop
Use Sender Verification Exception Table:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> On <input type="radio"/> Off
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	


Next in the Default Policy Parameters of Mail Flow Policies set Use Sender Verification Exception Table to **On**

If you are using a single listener validate that this is turned **off** for your **Relay Policy** so internal servers are not subject to Verification hitting the Relaylist HAT Group.

Configure HAT

Create a HAT entry above Whitelist and Blacklists named **ALLOWSPOOF** and assign the **SPOOFALLOW** mail flow policy to this Sender Group. Add those domains, external parties that you want to **allow** to spoof the internal domain.


HAT Overview













Mode — Cluster: **Hosted_Cluster** 

› Centralized Management Options

Find Senders

Find Senders that Contain this Text:

Sender Groups (Listener: IncomingMail )

Order	Sender Group	SenderBase™ Reputation Score 											Mail Flow Policy	Delete		
		-10	-8	-6	-4	-2	0	2	4	6	8	+10				
1	SMA														RELAYED	
2	RELAYLIST														RELAYED	
3	CiscoMonitoring														ACCEPTED	
4	ALLOWSPOOF														SPOOFALLOW	
5	WHITELIST														TRUSTED	
6	BLACKLIST												BLOCKED			
7	SUSPECTLIST												THROTTLED			
8	UNKNOWNLIST												ACCEPTED			
	ALL														ACCEPTED	

Key:

Configure Exception Table

Add the local domain to the Sender Verification Exception Table and set the Behavior to **Reject**

Add Sender Verification Exception

Mode —Cluster: **Hosted_Cluster**

▸ Centralized Management Options

Sender Verification Exception	
Exception:	<input type="text" value="enter local domain"/> <small>(e.g.: user@example.com, user@, @example.com, @.example.com, @[1.2.3.4])</small>
Order:	<input type="text" value="1"/> (of 1)
Behavior:	<input type="radio"/> Allow <input checked="" type="radio"/> Reject SMTP Code: <input type="text" value="553"/> SMTP Text: <input type="text" value="Envelope sender <\$EnvelopeSender> rejected"/>

Copyright © 2003-2011 Cisco Systems, Inc. All rights reserved.

At this point mail coming from yourdomain to yourdomain will be rejected unless the sender is listed in the Sender Group **ALLOWSPOOF** as it is tied to a mail flow policy that does not Use Sender Verification Exception Table.

Finished configuration