

# Mercurion Systems, Inc.

**Information Technology Consulting and Support Services**

Phone: 919.266.5957

Fax: 919.217.5769

## CASE STUDY: EXCHANGE 2000 SMTP AND CISCO PIX FIREWALLS

*Products: Cisco Secure PIX Firewall, Exchange 2000 Server*

### Overview

This case study discusses the interaction between Cisco PIX firewalls and SMTP connectivity between Microsoft Exchange 2000 routing groups. In a recent Exchange 2000 deployment, it was discovered that the Cisco PIX's MailGuard functionality was interfering with the ESMTTP (Extended SMTP) commands required by Exchange 2000 to successfully pass messages between routing groups. To resolve this issue, MailGuard had to be disabled before messages would flow correctly between the routing groups.

### More Information

A simplified visual depiction of the basic network architecture is shown below in Figure 1. Note the differences in how the VPN 30xx concentrators were wired each routing group. In Routing Group A, the VPN 30xx concentrator terminated directly on the internal LAN. In Routing Group B, the VPN 30xx terminated into a third interface in the PIX firewall.

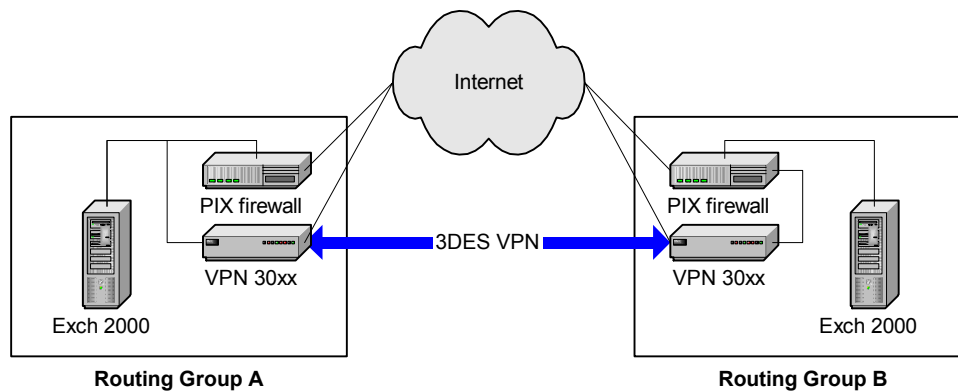


Figure 1. Simplified overview of network and routing group architecture

When messages were sent from Routing Group A to Routing Group B, the messages went out the VPN 30xx concentrator in Routing Group A and across the IPsec tunnel to the VPN 30xx concentrator in Routing Group B. Note that Routing Group A's PIX firewall was not involved in the data transfer. In Routing Group B, the traffic passed from the VPN 30xx concentrator into the PIX firewall, then into the internal LAN and the mail server found there.

Because this traffic was considered inbound traffic (headed from an interface with a lower security level to an interface with a higher security level), MailGuard's functionality kicked in to restrict the information provided during an SMTP session.

This is illustrated in the following excerpts. A typical Exchange 2000 SMTP session looks something like the following:

```
220 mail.domainname.com Microsoft ESMTP MAIL Service, Version:
5.0.2195.2966 ready at Sat, 29 Sep 2001 13:09:18 -0400
ehlo remote-domain.com
250-mail.domainname.com Hello [10.53.7.203]
250-TURN
250-ATRN
250-SIZE
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250-X-EXPS GSSAPI NTLM LOGIN
250-X-EXPS=LOGIN
250-AUTH GSSAPI NTLM LOGIN
250-AUTH=LOGIN
250-X-LINK2STATE
250-XEXCH50
250 OK
```

An Exchange 2000 SMTP session when the server is behind a Cisco PIX firewall with MailGuard enabled looks like this:

```
220
*****0*****2*****2*****2
*****200***2*****0*00
ehlo remote-domain.com
500 5.5.1 Command unrecognized: "XXXX remote-domain.com"
helo remote-domain.com
250 mail.domainname.com Hello [10.53.7.203]
```

As illustrated above, the MailGuard functionality severely limits 1) the amount and type of information returned during the SMTP session; and 2) the commands that are supported during an SMTP session. Because MailGuard allows only the "standard" SMTP commands (see the next paragraph), ESMTP commands required by Exchange 2000 for the successful routing of messages between routing groups are blocked.

According to the Cisco PIX documentation, the commands allowed by MailGuard are as follows: HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. All other commands are intercepted by the PIX and are never sent to the mail server behind the PIX.

No Microsoft documentation was available to fully list the ESMTP commands required by Exchange 2000 when passing messages between routing groups. It is well-documented that Exchange 2000 uses the X-LINK2STATE command verb when creating and maintaining the

Exchange link-state routing table, and that the CHUNKING and PIPELINING command verbs are supported to enhance the performance of SMTP transfer, but it is not documented that these command verbs are required for successful message transfer between routing groups. It is conceivable that if the X-LINK2STATE commands are never transferred between the routing groups, then the link state routing table is never built properly and traffic between routing groups would fail.

## Resolution

In this case, the resolution to the problem was to disable the PIX's MailGuard feature using the **no fixup protocol smtp 25** command in the PIX configuration in Routing Group B. This turned off MailGuard and allowed the Exchange 2000 Server in Routing Group B to fully utilize all of the necessary ESMTP commands needed to transfer messages between the two routing groups.

## Other Notes

While the information in this case study describes only the effects of the Cisco PIX MailGuard functionality, note that other firewalls or application proxies could cause this situation as well. For example, the WatchGuard Firebox series of firewall appliances have built-in SMTP proxies that can limit the SMTP commands and extensions supported. If those restrictions were enabled, the same results could be expected as described above with the PIX MailGuard functionality.

## Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification, in its entirety, and with this disclaimer and proof of authorship.