

CASE STUDY: ROUTING ISSUES IN A CISCO PIX & VPN CONCENTRATOR DEPLOYMENT

Products: Cisco Secure PIX Firewall, Cisco VPN 3000 Concentrator

Overview

This case study describes some routing issues discovered during a deployment of Cisco Secure PIX firewalls and Cisco VPN 3000 series VPN concentrators. Although the PIX firewall offers integrated VPN capabilities, the VPN 3000 series of concentrators were deployed to offer not only LAN-to-LAN VPN tunneling but also to provide robust remote access VPN functionality for mobile users. This case study presents the original design, the limitations of the original design, and the revised design that addressed those limitations.

More Information

The original network design for the combination PIX/VPN concentrator deployment is depicted in Figure 1 below.

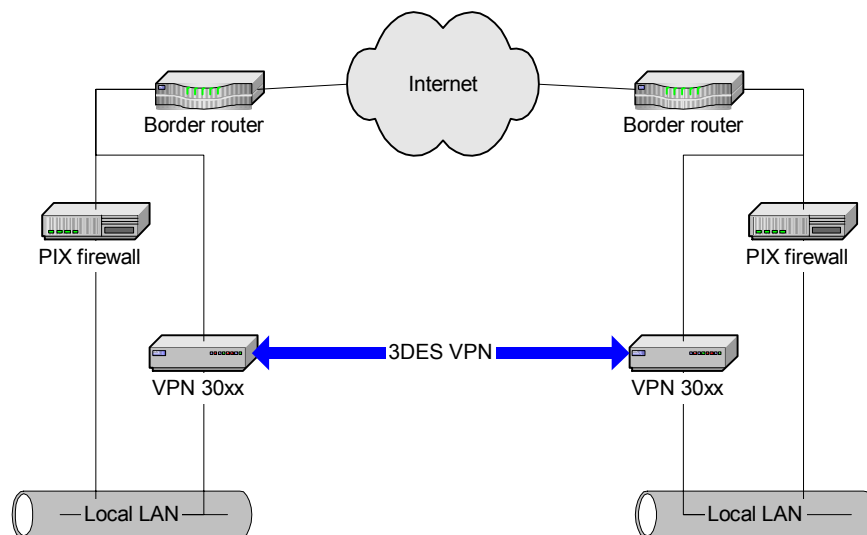


Figure 1. Original design for firewall and VPN deployment

As shown in Figure 1, the PIX firewall and the VPN concentrator would be deployed in parallel, both externally and internally. The external (public) interfaces of the firewall and the VPN concentrator would connect to an external switch or VLAN, and both would receive an external

(public) IP address. Likewise, the internal (private) interfaces of both the PIX firewalls and the VPN concentrators would connect to an internal switch or VLAN and would receive internal (private) IP addresses.

This same architecture had been deployed in previous deployments at other locations for this company, and no problems had been encountered. However, the key difference between the existing deployment and these new deployments was the presence of a multilayer switch. In the existing deployment at the corporate headquarters, a multilayer switch resided in the private network and served as the default gateway for all local LAN clients (transparently redirecting them to the local PIX firewall). This multilayer switch also contained static routes to the other LANs beyond the VPN tunnels.

In these new installations, however, there was no multilayer switch, and local LAN clients were configured to use the internal interface of the PIX firewall as their default gateway. Static routes were added to the PIX firewall to specify that the VPN concentrator was the gateway to the networks beyond the VPN tunnel. The anticipated traffic flow is described in the following five steps.

1. Traffic from the local LAN clients is received by the PIX firewall's internal interface (configured as the default gateway for LAN clients).
2. The PIX firewall looks up the route in the routing table.
3. If external, the PIX firewall forwards the traffic (with network address translation) out the external interface to the router, which then forwards the traffic onto the Internet.
4. If internal, the PIX firewall routes the traffic back onto the local LAN via the internal interface, redirecting the traffic to the IP address of the internal interface on the VPN concentrator.
5. The VPN concentrator puts the traffic into the encrypted VPN tunnel to the other end.

Unfortunately, the Cisco PIX firewall is unable to route traffic between networks on the same interface, so step #4 was impossible. Without the ability for the firewall to act as the sole default gateway, the design would not work. Several potential workarounds were contemplated, including some of the following:

- *Adding static routes to all LAN clients:* This was not feasible because it could not be easily automated, easily modified in the event of network changes, nor was it very scalable.
- *Specifying the VPN concentrator as the default gateway:* The VPN concentrator needed a default gateway anyway (to route the encrypted IPsec packets), so there was no way to instruct the concentrator to forward packets bound for external destinations to the PIX firewall without adversely affecting the concentrator's ability to function correctly.
- *Placing a router on the private LAN:* By mimicking the multilayer switch at headquarters with a simple Ethernet router, the same functionality could be achieved. However, due to time and cost constraints this approach was not feasible.

Each of these options addressed the root problem, and each had its own advantages and disadvantages. The final resolution involved a fourth option, described in the following section.

Resolution

The final decision was to add another interface to the PIX firewalls, allowing them to route traffic between networks on separate interfaces. This resolution required only slight modifications to the network design. The revised network design is depicted visually in Figure 2, below. By allowing the PIX firewalls to route traffic between interfaces, the limitation of routing on the same interface was removed.

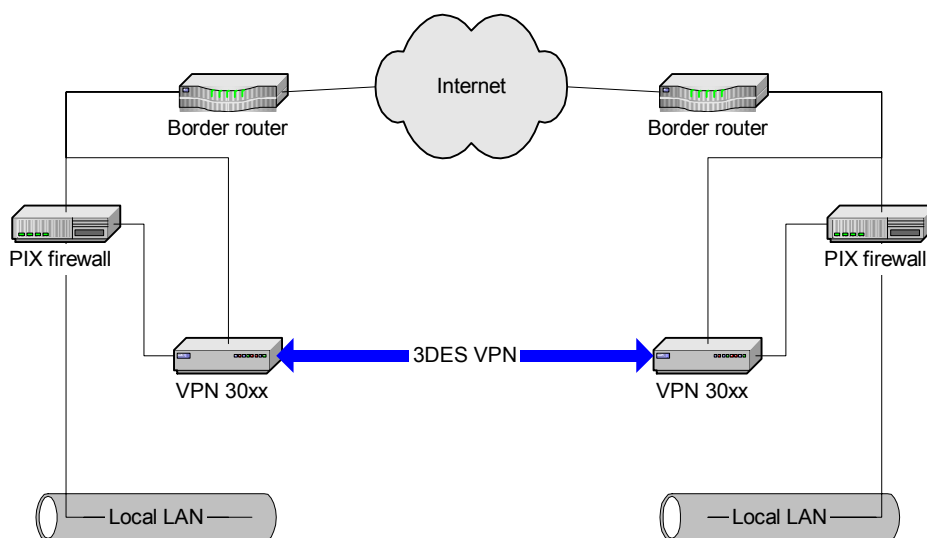


Figure 2. Revised design for firewall and VPN deployment

As shown in the figure, this design provided local LAN clients with a single egress point (the internal interface on the PIX firewall), which would serve as their default gateway. The VPN concentrators retained their external connection directly to an external switch or VLAN. In that regard, the concentrators remained parallel to the firewalls. On the inside, however, the VPN concentrators were plugged into an additional interface in the PIX firewall. This interface, termed the VPN interface, provided the PIX firewall with the ability to route between networks on separate interfaces. Static routes were added to the PIX firewalls to indicate that VPN-connected remote networks could be accessed via the concentrator on the PIX's VPN interface.

While this design eliminated many of the routing issues surrounding the original design, it was not without its challenges. Some of these challenges are described below.

- Access lists:** Again, since all traffic passed through the firewalls, even when it was bound for another private network, the PIX firewalls' access lists had to be created such that private-to-private traffic was not impeded, but public-to-private traffic was carefully controlled. The final access list applied to the VPN interface looked similar to the example below. As in the previous example, the first few commands define the access list, and the final command links that access list to a specific interface on the firewall.

```
access-list acl_vpn permit icmp any any
access-list acl_vpn permit ip 1.0.0.0 255.0.0.0 1.0.0.0 255.0.0.0
access-list acl_vpn permit ip 1.0.0.0 255.0.0.0 2.0.0.0 255.0.0.0
access-list acl_vpn permit ip 2.0.0.0 255.0.0.0 1.0.0.0 255.0.0.0
...
access-group acl_vpn in interface vpn
```

- *Network address translation (NAT) configuration:* The NAT configuration on the PIX firewalls was significantly more complex. This was due to the fact that all traffic, private or public, moved through the firewall, but only traffic bound for public destinations should be translated. Traffic bound for private destinations should not be translated. The final PIX configurations included numerous access lists to define which traffic flows were and were not affected by NAT; those access lists were then tied to a NAT statement in the PIX configuration that disabled NAT for those packets matching the access list. Some of the commands required in this configuration are listed below. The first three commands create the list of matching addresses, and the last statement ties those to a NAT statement that instructs the PIX not to perform NAT on addresses matching the specified access-list.

```
access-list 101 permit ip 1.0.0.0 255.0.0.0 1.0.0.0 255.0.0.0
access-list 101 permit ip 1.0.0.0 255.0.0.0 2.0.0.0 255.0.0.0
access-list 101 permit ip 2.0.0.0 255.0.0.0 1.0.0.0 255.0.0.0
...
nat (inside) 0 access-list 101
```

Other Notes

None

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.