Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Long Distance Failover - High Availability using Cisco PIX Firewall

The purpose of this document is to provide information security professionals with an understanding of the requirements in implementing long distance failover using Cisco PIX Firewalls. This case study is based on a project that I completed, and covers the major phases of the project including design, implementation and review. The document presents a high level description of the LAN-based Failover design principles and the steps involved in implementing this solution. I have not attempted to present a micro configura...

Copyright SANS Institute

Author Retains Full Rights

AD

Long Distance Failover - High Availability using Cisco PIX Firewall

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 2 - Case Study in Information Security

Author: Chris Ellem
Date: 30 June 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

ABSTRACT **3**

BACKGROUND **3**

DESIGN CONSIDERATIONS **5**

- FAILOVER BASICS 5
- STATEFUL FAILOVER 6
- CONSOLIDATED FAILOVER COMMUNICATIONS 6
- CISCO PIX FIREWALL SOFTWARE UPGRADE 6
- PIX SYSTEM MATCHING 7
- PIX FIREWALL CONFIGURATION 7

IMPLEMENTED SWITCHED SOLUTION **7**

- HUBS VERSUS SWITCHES 8
- PRIVATE VLANS 8
- SWITCH CONFIGURATION 9
- FAILOVER COMMUNICATIONS PATHS 11
- FAILOVER TESTING 13

REVIEW **16**

- FUTURE FAILOVER ENHANCEMENTS 16

LIST OF REFERENCES **18**

© SANS Institute 2003, Author retains full rights

Abstract

The purpose of this document is to provide information security professionals with an understanding of the requirements in implementing long distance failover using Cisco PIX Firewalls. This case study is based on a project that I completed, and covers the major phases of the project including design, implementation and review.

The document presents a high level description of the LAN-based Failover design principles and the steps involved in implementing this solution. I have not attempted to present a micro configuration document or step-by-step training guide.

Background

As part of a risk assessment the requirement for availability of external core business services was highlighted. These core services needed to be available even if the production site was not functioning. Should these services be unavailable the business would not be able to process important client data or provide services to other partners. The impact to the business would include loss of revenue and loss of productivity.

Based on discussions with the client, the project criteria was to design and implement a security infrastructure to provide a framework for redundancy of external core security services. The new security infrastructure was required to be built utilising the Cisco PIX Firewall platform, several of which were already being used by the client to manage several external networks services.

A major factor in the high availability design was the requirement for the Failover or standby equipment to be located in the client Disaster Recovery (DR) site. The DR site in this case was a building located some distance from the main production site. This solution primarily addresses the 'Availability' aspect of the CIA (Confidentiality, Integrity and Availability) security model.

The following diagram shows the Firewall connectivity prior to the implementation of the Firewall Failover solution. Although high availability pre-existed in the system architecture, this extended mainly into the area of production server clustering. The production site and DR site are connected via Fiber links to provide primary and secondary Gigabit access paths to server clusters.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

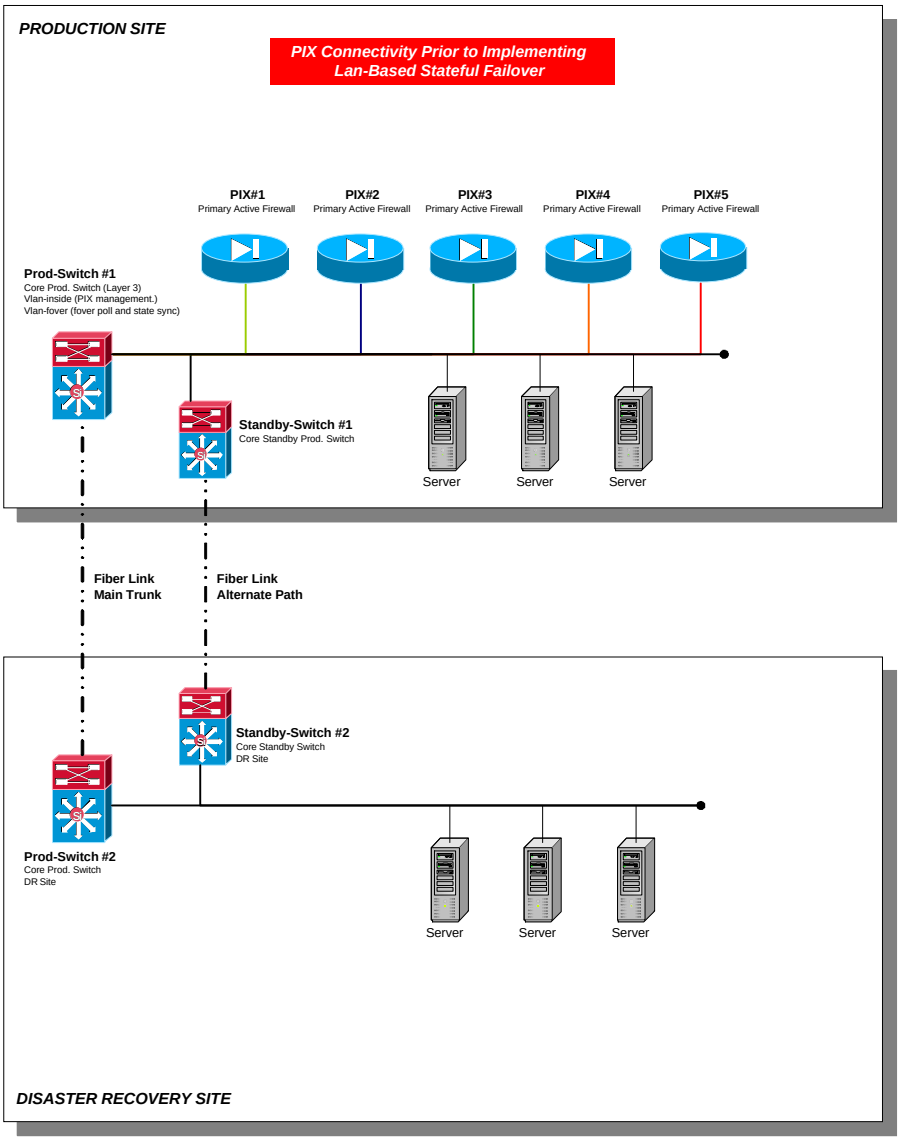

Figure 1: PIX Firewall Connectivity – Prior to implementing LAN-Based Stateful Failover

Redundant services located in the same equipment rack or computer room has limitations. For example, if the production site was made inaccessible or lost power then both production and Failover equipment could be lost. Utilising a specialist remote DR facility would achieve a higher level of redundancy and provide additional physical security and duplication of both hardware and communication services.

The distance between the client production site and DR site was a major obstacle in the past, as the Cisco PIX Firewall did not have a long distance Failover solution until the release of the PIX 6.2(1) code in April 2002. Prior to this the PIX Firewall was limited to a serial cable-based Failover solution that restricted placement of the PIX Firewalls within the confines of the same

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

equipment rack. The serial Failover cable is approximately 1.8 metres in length. Other solutions were considered, including customised line drivers and multiplexers, but this would create unwanted support issues.

Therefore, when the new PIX Firewall code was released the stage was set to demonstrate the capability of the new LAN-based Failover feature. This would provide the client with a supported, secure and manageable long distance solution they required.

Design Considerations[1]

The two major criteria in the design were as follows:

- The new security infrastructure was required to be built utilising the Cisco PIX Firewall platform.
- The Failover or standby equipment was required to be located in the client DR site (provide split split-site redundancy).

The following chapters provide a brief rundown of the baseline requirements within the PIX Firewall LAN-based Failover solution. I also explore some of the various options considered, such as VLANs versus dedicated network switches or hubs.

Failover Basics

PIX Firewall LAN-Based Failover requires the configuration of a pair of identical PIX Firewall units, one PIX being defined as the Primary unit and the other PIX being the Secondary unit. The Primary unit contains the Unrestricted license (UR).

LAN-Based Failover between PIX Firewalls is achieved both automatically and transparently to the user. Initially the Primary unit is setup to control the processing of network connections and is considered to be the Active unit. The Secondary unit waits in the Standby state for any event that causes the Primary unit to fail and then automatically switches to become the Active unit. During this switch in states, the Secondary unit takes ownership of the IP and MAC addresses of the Primary unit and begins processing network traffic. The new standby unit assumes the Failover IP and MAC addresses of the unit that was previously the active unit.
Both the Primary and Secondary PIX Firewalls have a presence on the network with their IP and MAC addresses being dependent upon their state (Active or Standby). All PIX interfaces Failover even if only one interface has had a failover event.

The pair of Failover PIX Firewalls uses encrypted communications to poll each other to monitor each other's status. This Failover communications is known as

[1] Cisco. "How Failover Works on the Cisco Secure PIX Firewall"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the failover poll or heartbeat. The Failover polling feature requires a dedicated PIX Firewall Ethernet interface.

This method of IP switching differs from other hot standby implementation protocol such as Virtual Routing Redundancy Protocol (VRRP)[2] and Hot Standby Router Protocol (HSRP)[3] where devices are configured with both a physical address and a virtual address.

Stateful Failover

Adding the Stateful Failover feature to the LAN-based Failover solution assists in maintaining established end user application connections if a Failover occurs. Without this feature all active connections are dropped during the Failover process requiring the end users to re-establish their sessions.
The Stateful Failover feature requires a dedicated PIX Firewall Ethernet interface. This interface must be 100Mbps or Gigabit Ethernet.

Consolidated Failover Communications

Both units in a LAN-based Failover pair communicate through a dedicated LAN connection. Failover communication requires a dedicated LAN, as does Stateful communication. PIX Firewall Failover was implemented in this solution so that both the Failover communication and stateful communication utilise the same dedicated LAN connection.

PIX Firewall models 515 and 520 support a maximum number of six 10/100Mbps Ethernet network interface ports. By combining the Failover polling and stateful communication on one dedicated Ethernet interface the remaining five ports could be allocated for protected networks, such as Demilitarised Zones (DMZ's). The client was not prepared to sacrifice two Ethernet interfaces for Failover.

Cisco PIX Firewall Software Upgrade

As part of the process to implement a PIX Firewall LAN-Based Failover solution, I upgraded all Firewalls to version 6.2(2). This released update supports Stateful Failover over a dedicated Ethernet network and provides the mechanism to connect Firewalls between the client production site and the DR site.

The Firewall PIX Device Manager (PDM) was also upgraded to version 2.1(1) in order to support the new 6.2 Firewall code. The PDM provides secure (https) connection for management of the PIX including administration of the rulebase and address translation table. This means a PIX administrator can connect to the PIX via a browser for Firewall management. In addition to the PDM, management of the PIX Firewalls was still available via SSH.

---

[2] Request for Comments: 2338. "Virtual Router Redundancy Protocol"
[3] Cisco. "Hot Standby Router Protocol Features and Functionality"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

PIX System Matching

PIX Firewall Failover requires that both PIX Firewall units are identical in the following respects:

- Same model number
- Have at least as much RAM
- Have the same Flash memory size
- Be running the same software version
- One of the Failover units must have an Unrestricted license (UR)
- Activation key type (DES or 3DES)

The different models of PIX Firewalls utilised by the client were audited according to the specifications listed above. This required certain Firewalls to be relocated to provide matched hardware within the Failover Firewall pairs.
The client had ten PIX Firewalls involved in this solution. The end result provided five PIX Firewalls installed at the production site and the other five targeted as the long distance Failover pair to be installed in the DR site.

PIX Firewall Configuration[4]

Configurations listings and PIX Failover commands have not been included in this document. The Cisco document "How Failover Works on the Cisco Secure PIX Firewall" provides an excellent reference source for this information including wiring diagram examples and design FAQ's.

Implemented Switched Solution

An integral part of the Firewall Failover design required the implementation of a dedicated switched security network. There were many reasons behind deciding what type of infrastructure to use, including the following:

- Each PIX Firewall interface of the Failover pair, including the Failover interface, is required to be connected into a dedicated network. This is a requirement of LAN-based Failover. Therefore five PIX Firewalls, each with 6 interfaces would require approximately 30 separate networks to be dedicated between themselves and their Failover partners. Providing a Failover solution for five PIX Firewalls, rather than only one Firewall, yields some challenges when deciding network connectivity options.

- Only switch/hub/VLAN connectivity is allowed for Failover. All interfaces of the two units need to be connected between the active and standby units on their own dedicated subnets.

- Ethernet UTP crossover cables are not supported for Firewall Failover connectivity, regardless of their proximity. Disconnecting one end of a UTP cable from a Primary Firewall interface will also drop the link status

[4] Cisco. "How Failover Works on the Cisco Secure PIX Firewall"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of the paired Secondary Firewall interface. This can result in both Primary and Secondary Firewalls dropping an interface and becoming Active at the same time.

- Failover works with all Firewall Ethernet interfaces. However, the Stateful Failover interface must be 100Mbps or Gigabit Ethernet. A 10MBps connection is not supported with Stateful Failover.

- The use of Hubs and low-end switches does not provide a scaleable cost effective solution to implement multiple Firewalls within a Failover scenario. The number of these devices required would create is own management and support issues.

Hubs versus Switches

The implementation of switches within any security network has sparked many a debate about inherent switch design vulnerabilities[5]. The choice of a dedicated switch solution versus multiple hubs/switches really comes down to the level of risk that the organisation is willing to accept. Also a correctly implemented dedicated switch solution, with appropriate safeguards is an effective solution to many situations.

I believe that a trade-off between functionality, risk and cost is required in most solutions. Consider the options:

- 60 Hubs versus two switches
- 30 separate 100Mbps links between two buildings versus 30 VLAN's Trunked on a Gigabit single mode Fiber link

Most of the time the client under the guidance of a security engineer makes the final decision. In many cases clients do not have the luxury of providing a dedicated network switch or hub each external host or router. This results in common or shared DMZ's implemented to accommodate multiple hosts.

Private VLANs[6]

Private VLANs (PVLANs) are supported on specific Cisco Catalyst switches and help by restricting the traffic between hosts in a common segment.
PVLANs are a tool that allows segregating traffic at Layer 2 (L2) turning a broadcast segment into a non-broadcast multi-access-like segment.
The hosts sharing the same DMZ can be isolated to only talk to specific ports such as the PIX Firewall gateway interface and be blocked from seeing other hosts on the same subnet. PVLAN's can help limit attacks should a host in a shared VLAN be compromised. Restricting the visibility of hosts can help limit the spread of exploits.

[5] SecurityFocus. "Cisco Catalyst 2900 VLAN Vulnerability"
[6] Cisco. "Securing Networks with Private VLANs and VLAN Access Control Lists"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

PVLANs can be extended across multiple Ethernet switches by trunking these VLANs to other switches that support private VLANs. This feature provides clients with the option to extend the level of security within each DMZ. However implementing this does complicate the configurations and management of the security switches. This needs to be considered during maintenance and troubleshooting of the security environment.

Switch configuration[7]

Implementation of the security switches required special preparation and configuration to ensure all levels of security were addressed. This began with the choice of software for the switches being a CatOS encryption image with support for SSH. Both the security switches were hardened to provide an external security layer against unauthorised access. The hardening included the following steps:

- Disabling all unneeded services including Telnet, SNMP, VTP mode off, CDP disable, Channel mode off, Trunk mode off (except for Gigabit port trunk)
- Create a login banner to notify users of Unauthorised access
- TACACS+ Authentication login/enable via console and SSH
- Limiting management access to SSH via restricted internal hosts (network permit list)
- Disable unused ports
- Port speed and duplex were fixed on both the switch and host to ensure there were no port negotiation mismatches
- VLAN 1 not used as native VLAN for management or for hosts
- Spantree global-default portfast enabled (to ensure quick Failover)

I implemented dedicated Cisco Catalyst 4006 series Switches (Layer-2) to be used specifically for connections within the client security network and its external services. Two switches were installed as part of the Firewall Failover solution, one at the production site and the other located at the DR site.
Dedicating a Switch to this purpose provides several advantages, as follows:

- A Switch dedicated to the security network will provide a higher level of security if it does not share VLANs with Internal production hosts.

- Support for Private VLANs (PVLANs) help by restricting the traffic between hosts in a common segment. This is a feature available in only certain models of Cisco switches.

- A single high-end Switch, rather than multiple smaller low-end switches, will consolidate rack space and provide more features such as redundant (dual) switch power supplies.

[7] Cisco. "Best Practices for Catalyst 4000, 5000, and 6000 Series Switch Configuration and Management"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- The Cisco Catalyst 4006 series Switch provides Gigabit VLAN Trunking (IEEE 802.1Q) and Spanning on multiple VLANs for monitoring purposes. This is important for both management and Intrusion Detection Network Engines that listen into specified network traffic.

- The two 48 port 10/100BaseTX line modules provide (96) Ethernet interface ports to be utilised for security networks, router connections and host server connections. Approximately 80 ports are required to support the security infrastructure and provide a Trunked VLAN Failover solution.

One of the primary benefits in the Trunked switch solution is implementing split site redundancy. If a dedicated switch were required for each network, this solution would require multiple switches and multiple fiber runs between the production and DR sites for each network, proving expensive.

The following diagram illustrates the Failover design connectivity between the production and DR sites:

© SANS Institute 2003, Author retains full rights

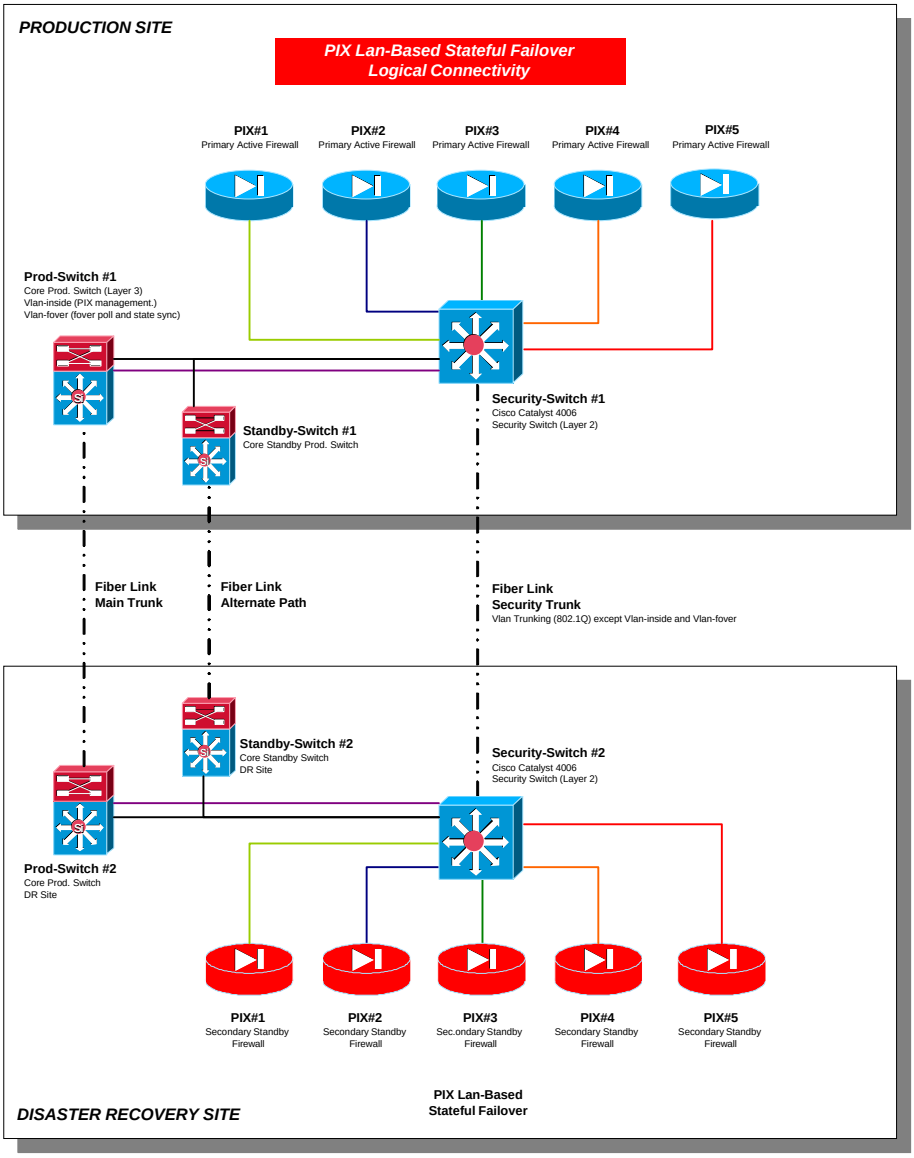

Figure 2: PIX Firewall LAN -Based Stateful Failover – High Level Connectivity

Failover Communications Paths

During the Proof-of-Concept Lab Testing a basic version of the design was setup to demonstrate the overall mechanics of PIX LAN-based Failover.

One major limitation I found during testing was the result of the PIX Firewall Failover pair being separated by a single communication path. This path was to represent a Fiber link between two buildings.
Should the single communication path fail the Failover units would lose visibility of each other and each PIX would switch to the Active state. To overcome this, two communication paths were provided (a separate path for the Failover

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

polling and a separate path for the Trunked PIX DMZ's) so that the PIX Firewalls had two discrete paths to automatically and transparently monitor each other's status. If the Failover polling heartbeat times-out then the PIX Firewalls can automatically test the interface status of its partner through other methods, such as ARP tests, Broadcast Ping tests and network activity tests.

This scenario ensures that the Failover units do not lose visibility of each other should one of the fiber links between the production site and the DR site fail.
This was designed specifically to avoid the "Mexican standoff" scenario where both Primary and Secondary Firewalls cannot see each other, and as a result both become Active at the same time. This would result in duplication of IP addresses on the network.

It is important to note that the Failover polling heartbeat was set to the minimum time (3 seconds) to ensure that both the Failover process and the state synchronisation would work quickly enough to maintain active connections. If this poll time is configured too high then other factors such as application time-outs may cause connections to be dropped during the Failover process. I found that the default Failover poll of 15 seconds was less effective than the 3 second timeout.

To ensure that external services would not be terminated directly onto the client internal network, the core production switches were not used for the primary security network inter-connections. However, in order to provide alternate path visibility between the PIX Firewall Failover pairs at the production site and the DR site, I used a separate VLAN-fover (layer 2 with no IP addressing) to pass the encrypted Failover polling heartbeat and traverse through the production switches. All other connectivity to the security network passes through the dedicated security switches.

Each PIX Firewall interface, including the Failover interface, is connected into a dedicated network (VLAN port of the switch). All hosts or routers associated with a dedicated security network or sharing a security network are also connected into the same VLAN as the PIX. All VLAN's (except the Failover VLAN and the Firewall management VLAN) are then Trunked between the two security switches located at the production and DR sites.

The following diagram illustrates the Failover communications paths between the production and DR sites:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

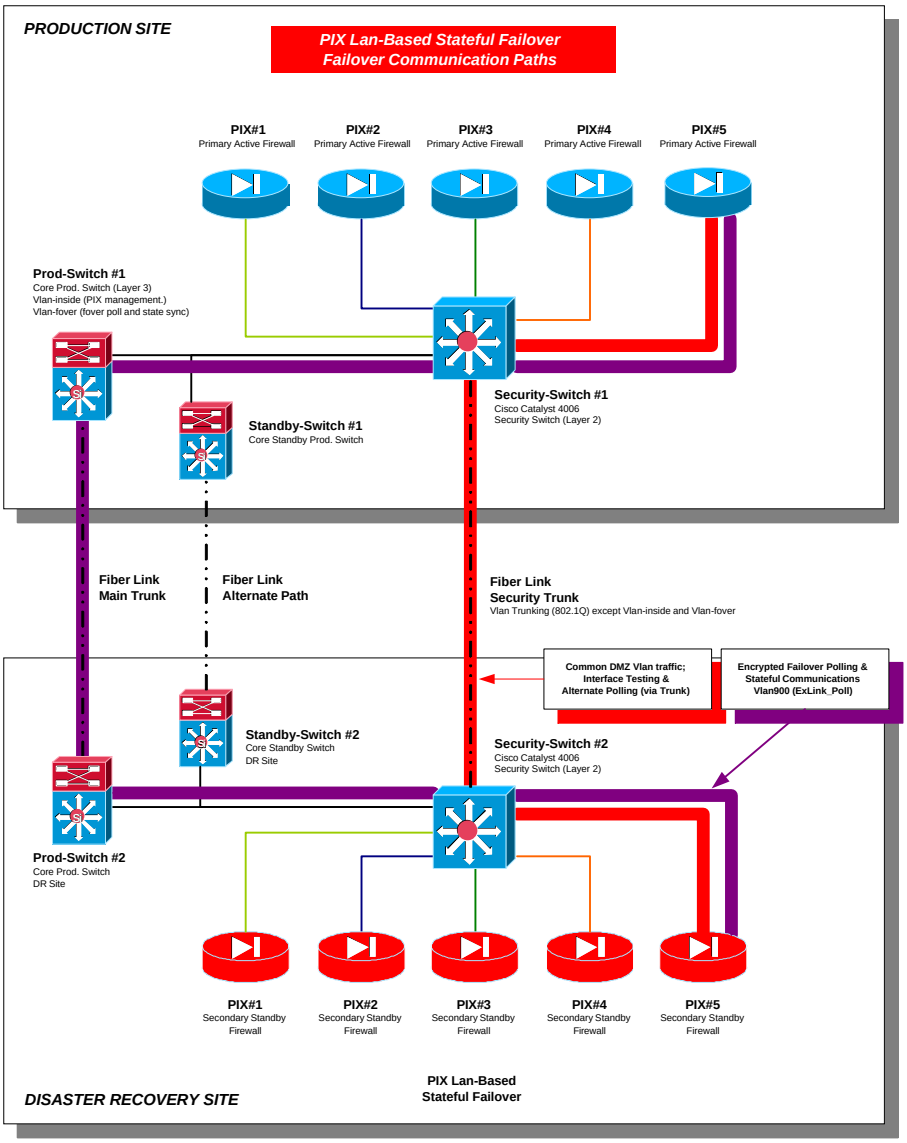

Figure 3: PIX Firewall LAN -Based Stateful Failover – Failover Communication Paths

Failover Testing

Once the PIX Firewalls change Failover states between Active and Standby following an event, they will remain in this new state until another event occurs or an administrator issues a manual Failover command. The Primary PIX Firewall (now in Standby mode) does not automatically resume Active state after the fault condition is cleared. This helps prevent flapping of states.
Notification of Failover events is available through PIX Syslog messages. This is critical information that administrators should be alerted to with regards to management of Failover Firewalls.

The following diagram illustrates the PIX Firewalls switching states during Failover:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

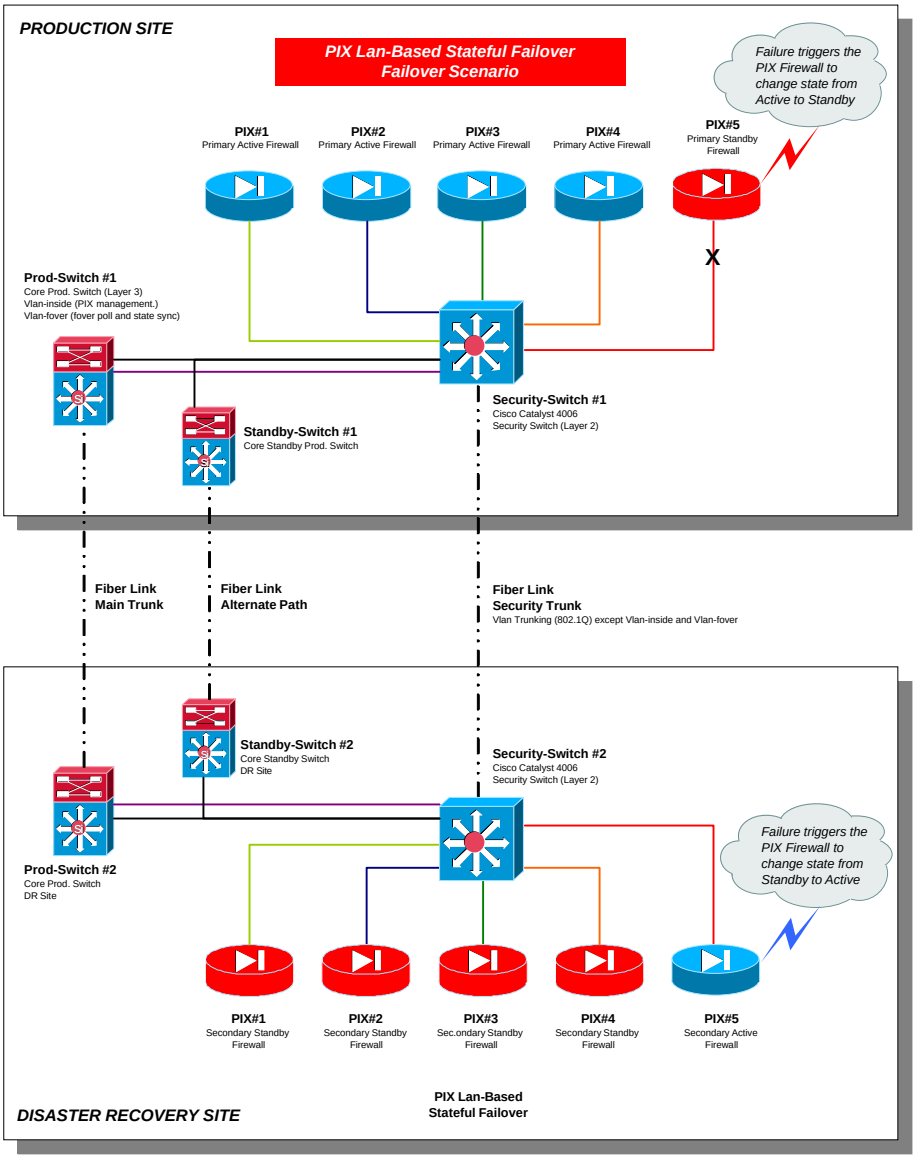

Figure 4: PIX Firewall LAN -Based Stateful Failover – Failover Scenario

During Failover the Active IP and MAC addresses of all interfaces (not just the inside interface) shift to the Secondary PIX Firewall. The Primary PIX assumes the Standby IP and MAC addresses.

To a network host access to the gateway has remained unchanged. Any connections currently established are momentarily paused during the Failover and then resumed. The following tables show a example of Failover state switching occurring as a result of disconnecting the Internal (inside) interface of the Primary PIX Firewall:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
pix01# sh Failover
Failover On
Serial Failover Cable status: My side not connected
Reconnect timeout 0:00:00
Poll frequency 3 seconds
        This host: Primary - Active                          This host: Primary - Standby
            Active time: 521718 (sec)                            Active time: 521742 (sec)
            Interface dmz5 (192.168.5.1): Normal                 Interface dmz5 (192.168.5.2): Normal
            Interface dmz4 (192.168.4.1): Normal                 Interface dmz4 (192.168.4.2): Normal
            Interface dmz3 (192.168.3.1): Normal                 Interface dmz3 (192.168.3.2): Normal
            Interface outside (192.168.2.1): Normal              Interface outside (192.168.2.2): Normal
            Interface inside (192.168.1.1): Normal               Interface inside (192.168.1.2): Link Down (Waiting)
        Other host: Secondary - Standby                      Other host: Secondary - Active
            Active time: 111 (sec)                               Active time: 132 (sec)
            Interface dmz5 (192.168.5.2): Normal                 Interface dmz5 (192.168.5.1): Normal
            Interface dmz4 (192.168.4.2): Normal                 Interface dmz4 (192.168.4.1): Normal
            Interface dmz3 (192.168.3.2): Normal                 Interface dmz3 (192.168.3.1): Normal
            Interface outside (192.168.2.2): Normal              Interface outside (192.168.2.1): Normal
            Interface inside (192.168.1.2): Normal               Interface inside (192.168.1.1): Normal (Waiting)

Stateful Failover Logical Update Statistics
        Link : fover
        Stateful Obj     xmit       xerr       rcv        rerr
        General          69436      0          69412      0
        sys cmd          69408      0          69410      0
        up time          12         0          2          0
        xlate            1          0          0          0
        tcp conn         15         0          0          0
        udp conn         0          0          0          0
        ARP tbl          0          0          0          0
        RIP Tbl          0          0          0          0
        Logical Update Queue Information
                         Cur     Max     Total
        Recv Q:          0       1       69412
        Xmit Q:          0       1       69430

LAN-based Failover is Active
        interface fover (192.168.6.1): Normal, peer (192.168.6.2): Normal
```

Figure 5: Primary PIX Firewall – Switching From Active to Standby Example

```
pix01# sh Failover
Failover On
Serial Failover Cable status: My side not connected
Reconnect timeout 0:00:00
Poll frequency 3 seconds
        This host: Secondary - Standby                       This host: Secondary - Active
          Active time: 162 (sec)                               Active time: 183 (sec)
          Interface dmz5 (192.168.5.2): Normal                 Interface dmz5 (192.168.5.1): Normal
          Interface dmz4 (192.168.4.2): Normal                 Interface dmz4 (192.168.4.1): Normal
          Interface dmz3 (192.168.3.2): Normal                 Interface dmz3 (192.168.3.1): Normal
          Interface outside (192.168.2.2): Normal              Interface outside (192.168.2.1): Normal
          Interface inside (192.168.1.2): Normal               Interface inside (192.168.1.1): Normal (Waiting)
        Other host: Primary - Active                         Other host: Primary - Standby
          Active time: 521970 (sec)                            Active time: 521988 (sec)
          Interface dmz5 (192.168.5.1): Normal                 Interface dmz5 (192.168.5.2): Normal
          Interface dmz4 (192.168.4.1): Normal                 Interface dmz4 (192.168.4.2): Normal
          Interface dmz3 (192.168.3.1): Normal                 Interface dmz3 (192.168.3.2): Normal
          Interface outside (192.168.2.1): Normal              Interface outside (192.168.2.2): Normal
          Interface inside (192.168.1.1): Normal               Interface inside (192.168.1.2): Link Down (Waiting)

Stateful Failover Logical Update Statistics
        Link : fover
        Stateful Obj     xmit       xerr       rcv        rerr
        General          401        0          394        0
        sys cmd          401        0          392        0
        up time          0          0          2          0
        xlate            0          0          0          0
        tcp conn         0          0          0          0
        udp conn         0          0          0          0
        ARP tbl          0          0          0          0
        RIP Tbl          0          0          0          0
        Logical Update Queue Information
                         Cur     Max     Total
        Recv Q:          0       1       394
        Xmit Q:          0       1       401

LAN-based Failover is Active
        interface fover (192.168.6.2): Normal, peer (192.168.6.1): Normal
```

Figure 6: Secondary PIX Firewall – Switching From Standby to Active Example

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Review

The implementation of the security infrastructure described in this document achieved the client goal of establishing a secure framework to a remote DR site. The new framework currently provides a manageable high availability solution for multiple production PIX Firewalls and is scaleable for future requirements.

The Firewall Failover testing produced predictable results that were acceptable to the client. The Failover timeout was between 1-6 seconds depending on how the error event was generated and created minimal impact to the end-user. Stateful LAN-Based Failover between PIX Firewalls was achieved both automatically and transparently to the user.

Although the security solution utilises switches, albeit high-speed layer-2 with hardened configuration, the client understands the trade-off between the risks and functionality required. Additional security measures such as administration authentication, disabling un-needed services and ability to implement PVLAN's all help reduce the risks and vulnerabilities within this environment. For example the "Cisco Catalyst CatOS Authentication Bypass Vulnerability"[8] was avoided due to these security measures being in place.

The overall solution has helped consolidate many external services within the security infrastructure. Several services that had historically been connected into the production network were migrated onto the new security infrastructure.

The following summarises the tasks that were required to complete the LAN-based Failover solution:

- Proof-of-Concept Lab testing
- PIX Firewall software upgrade
- PIX Firewall system matching
- Commissioning of Fiber link between the production site and DR site
- Switch preparation (pre-stage security switches)
- Installation of security switches
- Testing of security switches across Fiber Link
- Configure production switches for Failover VLAN
- Patch PIX Firewalls and DMZ hosts into security switches
- Configure PIX Firewalls for LAN-based Failover
- Testing

Future Failover Enhancements

The PIX Firewall Failover design can be further enhanced for future development. This can be achieved by extending the Failover functionality to the router and server hardware utilised within the security infrastructure. Communication links, routers and hosts are potentially all single points of failure within any service.

[8] SecurityFocus. "Cisco Catalyst CatOS Authentication B ypass Vulnerability"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Many of the external services are connected via Cisco routers. These routers could be duplicated at the DR site and upgraded to implement Hot Standby Routing Protocol (HSRP). HSRP is a Cisco proprietary protocol that provides a redundancy mechanism when more than one router is connected to the same segment/subnet of an Ethernet/FDDI/Token Ring network.

Once the routers are duplicated at the DR site and configured for HSRP, the communications link could then be switched should the active router fail. The switching of the communication services would be dependent on the type of service e.g. Frame-Relay, ISDN. It is possible for the Telco to switch a Frame-Relay PVC circuit between different sites based on the router WAN interface status for the Frame-Relay connection.

Providing high service availability without relying on the availability of any single server provides a greater challenge. This is due to some security services being specifically developed within strict application guidelines. Customising these applications for a clustered arrangement or Failover solution could be greatly restricted. Server and application redundancy would need to be investigated for each external service. The ability to implement host redundancy (router or server) is greatly dependant on device ownership. Configuration changes or application customisation options may not be available if the host is owned or managed by a third party.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

List of References

Cisco. "How Failover Works on the Cisco Secure PIX Firewall" May 22, 2003. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094ea7.shtml

Cisco. "Best Practices for Catalyst 4000, 5000, and 6000 Series Switch Configuration and Management" June 10, 2003. URL: http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml

Cisco. "Securing Networks with Private VLANs and VLAN Access Control Lists" April 01,2003. URL: http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008013565f.shtml

SecurityFocus. "Cisco Catalyst 2900 VLAN Vulnerability". September 02, 1999. URL: http://www.securityfocus.com/bid/615

SecurityFocus. "Cisco Catalyst CatOS Authentication Bypass Vulnerability" April 24, 2003. URL: http://www.securityfocus.com/bid/7424

Network Working Group - Request for Comments: 2338
Virtual Router Redundancy Protocol. URL: http://www.faqs.org/rfcs/rfc2338.html

Cisco. "Hot Standby Router Protocol Features and Functionality" Feb 13, 2003. URL: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a91.shtml

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced