Click to verify

High Availability is one of the most crucial requirements for a smooth network operation. In terms of routers or switches, we have a variety of options to choose from such as Switch-Stack, vPC, VSS, HSRP etc.When it comes to firewalls, we only have very limited options because of the stateful nature of the firewall appliances. Most of us would usually go with an Active/Passive firewall design where the Active firewall processes the traffic and the Standby firewall just sits there and waits to take over in an event of a failure. You can also choose an Active/Active design if that suits your environment.In this blog post, we will learn how to configure Active/Passive Failover on the Cisco ASA firewalls.ASA Fail-Over ModesAs I mentioned before, ASA supports two failover modes, Active/Active failover and Active/Standby failover. In Active/Standby failover, one device functions as the Active unit and passes the traffic. The second standby unit does not actively pass traffic. When a failover occurs, the Standby unit assumes the active role and starts passing the traffic. In an Active/Active failover, both ASAs can pass traffic. Please note that Active/Active failover is only available to ASAs in multiple context modes. In Active/Active failover, you divide the security contexts on the ASA into 2 failover groups. A failover group is simply a logical group of one or more security contexts. One group is assigned to be Active on the primary ASA, and the other group is assigned to be active on the Secondary ASA. When a failover occurs, it occurs at the failover group level. Hardware and Software Requirements Both units in a Failover must be the same model and have the same number and types of interfaces. Have the same modules installed and have the same RAM installed. Both units should have the same major (first number) and minor (second number) software version. Have the same AnyConnect images. The two firewalls in a failover configuration do not need to have identical licenses; the licenses combine to make a failover cluster license.As with any other firewall cluster, you need to have some sort of connectivity between the firewalls to exchange information such as heart-beat and state information. With the ASAs, you need two links - the failover link and the optional stateful failover link. Cisco recommends using the same interface between the two firewalls. For example, for a failover link, if you have used Gi0/1 in device 1, use the same interface Gi0/1 in device 2 as well. Failover Link - The two units in a failover pair constantly communicate over the failover link to determine the operating status of each unit. The failover link data includes The unit state (active or standby) Hello messages/keep-alives Link status MAC address exchange Configuration replication and synchronization Stateful Failover Link - To use Stateful Failover, you must configure a Stateful Failover link to exchange 'connection state' information. You can use a dedicated data interface (physical or Port-Channel) as the state link. Cisco recommends the latency for the stateful failover link should be less than 10 milliseconds and no more than 250 milliseconds.Cisco recommends that the failover links and data interfaces use different paths in order to decrease the chance of all interfaces failing at the same time. For example, If the failover link is down, the ASA can use the data interfaces to determine if a failover is necessary. Subsequently, the failover operation is suspended until the health of the failover link is restored.Not recommended - If a single switch or a set of switches is used to connect both failover and data interfaces between two ASAs, then when a switch or inter-switch-link is down, both ASAs become active (split-brain) as shown below. Recommended - Cisco recommends that failover links not use the same switch as the data interfaces. You can use a different switch or connect the failover link directly between the units as shown below. MAC Addresses and IP AddressesStandby IP AddressWhen you configure ASA's interfaces, you can optionally specify a standby IP address alongside the active IP address on the same subnet. When a failover occurs, the new active unit takes over the active IP addresses and MAC addresses. ! Example ! interface Gi0/1 nameif INSIDE security-level 100 ip address 10.10.12.1 255.255.255.0 standby 10.10.12.2IP/Mac address Behaviour During FailoverThe active unit always uses the primary unit's IP and MAC addresses. When a failover occurs, the standby unit assumes the IP addresses and MAC addresses of the failed unit (formerly active) and begins passing traffic.When the failed unit comes back online, it stays in a standby state and takes over the standby IP addresses and MAC addresses.Configuration ExampleI prefer to configure the Standby IP addresses on all the interfaces even though they are optional. interface GigabitEthernet0/0 nameif WAN security-level 0 ip address 201.85.10.1 255.255.255.248 standby 201.85.10.2 ! interface GigabitEthernet0/1 nameif INSIDE security-level 100 ip address 192.168.10.1 255.255.255.0 standby 192.168.10.2 !Failover configuration is very straightforward. The Secondary box doesn't have any configuration except for the failover bits. The only config difference between both units is one line of config failover lan unit failover failover lan unit primary failover lan interface FAILOVER-LINK GigabitEthernet0/5 failover ipsec pre-shared-key cisco123 failover link STATEFUL-LINK GigabitEthernet0/6 failover interface ip FAILOVER-LINK 192.168.100.1 255.255.255.252 standby 192.168.100.2 failover interface ip STATEFUL-LINK 192.168.100.5 255.255.255.252 standby 192.168.100.6Primary ASAfailover failover lan unit secondary failover lan interface FAILOVER-LINK GigabitEthernet0/5 failover ipsec pre-shared-key cisco123 failover link STATEFUL-LINK GigabitEthernet0/6 failover interface ip FAILOVER-LINK 192.168.100.1 255.255.255.252 standby 192.168.100.2 failover interface ip STATEFUL-LINK 192.168.100.5 255.255.255.252 standby 192.168.100.6Secondary ASAMost of the configs are self-explanatory, I've used Gi0/5 and Gi0/6 as failover and state links respectively. Please note that all the information sent over the failover and state links is sent in clear text. There are two ways to secure communication between peers, using IPSec PSK or a failover key, the former is recommended by Cisco. As soon as you finish the failover configuration on both units, the console should display the following message.asa-lab-01# Failover LAN became OK Switchover enabled Configuration has changed, replicate to mate. Beginning configuration replication: Sending to mate. End Configuration Replication to mateVerificationYou can use show failover CLI command to check the current failover status. asa-lab-01# show failover Failover On Failover unit Primary Failover LAN Interface: FAILOVER-LINK GigabitEthernet0/5 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 2 of 61 maximum MAC Address Move Notification Interval not set Version: Ours 9.8(4), Mate 9.8(4) Serial Number: Ours 9A077RPR8KV, Mate 9AS2E40FB75 Last Failover at: 10:01:54 UTC Oct 20 2022 This host: Primary - Active Active time: 409 (sec) slot 0: empty Interface WAN (201.85.10.1): Normal (Monitored) Interface INSIDE (192.168.10.1): Normal (Monitored) Other host: Secondary - Standby Ready Active time: 6 (sec) Interface WAN (201.85.10.2): Normal (Monitored) Interface INSIDE (192.168.10.2): Normal (Monitored)Primary ASAasa-lab-01# show failover Failover On Failover unit Secondary Failover LAN Interface: FAILOVER-LINK GigabitEthernet0/5 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 2 of 61 maximum MAC Address Move Notification Interval not set Version: Ours 9.8(4), Mate 9.8(4) Serial Number: Ours 9AS2E40FB75, Mate 9A077RPR8KV Last Failover at: 16:22:29 UTC Oct 22 2022 This host: Secondary - Standby Ready Active time: 6 (sec) slot 0: empty Interface WAN (201.85.10.2): Normal (Monitored) Interface INSIDE (192.168.10.2): Normal (Monitored) Other host: Primary - Active Active time: 450 (sec) Interface WAN (201.85.10.1): Normal (Monitored) Interface INSIDE (192.168.10.1): Normal (Monitored)Secondary ASATest FailoverLet's power-off the active unit and see what happens. Obviously, we want the secondary unit to take over the role of active and start passing the traffic. Once we powered-off the primary ASA, we can verify the failover status from the secondary unit (now active) as shown below. asa-lab-01# show failover history == From State To State Reason == 10:05:12 UTC Oct 20 2022 Sync Config Sync File System Failover state check 10:05:12 UTC Oct 20 2022 Sync File System Bulk Sync Failover state check 10:05:28 UTC Oct 20 2022 Bulk Sync Standby Ready Failover state check 10:10:37 UTC Oct 20 2022 Standby Ready Just Active HELLO not heard from mate 10:10:37 UTC Oct 20 2022 Just Active Active Drain HELLO not heard from mate 10:10:37 UTC Oct 20 2022 Active Drain Active Applying Config HELLO not heard from mate 10:10:37 UTC Oct 20 2022 Active Applying Config Active Config Applied HELLO not heard from mate 10:10:37 UTC Oct 20 2022 Active Config Applied Active HELLO not heard from mate ==asa-lab-01# show failover Failover On Failover unit Secondary Failover LAN Interface: FAILOVER-LINK GigabitEthernet0/5 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 2 of 61 maximum MAC Address Move Notification Interval not set Version: Ours 9.8(4), Mate 9.8(4) Serial Number: Ours 9AS2E40FB75, Mate 9A077RPR8KV Last Failover at: 10:10:37 UTC Oct 20 2022 This host: Secondary - Active Active time: 91 (sec) slot 0: empty Interface WAN (201.85.10.1): Normal (Waiting) Interface INSIDE (192.168.10.1): Normal (Waiting) Other host: Primary - Failed Active time: 508 (sec) Interface WAN (201.85.10.2): Unknown (Monitored) Interface INSIDE (192.168.10.2): Unknown (Monitored)Secondary ASA (now active)Force FailoverFor whatever reason you want to force the failover, you can use the failover active command. To force the standby unit to become active, run failover active from the standby unit or run no failover active on the active unit. asa-lab-01# no failover active asa-lab-01# Switching to Standbyactive unitFailover Interface MonitoringBy default, monitoring is enabled on all physical interfaces and on any hardware or software modules installed on the ASA, such as the ASA FirePOWER module. So, if one of the monitored links goes down on the active unit, the standby unit will take over the role. To demonstrate interface monitoring, I'm going to shut down one of the links between the active unit and the switch. As you can see below, the console displays a message indicating that the failover occurs due to interface monitoring. You can also use the show failover history command to check the reason behind any failover events. asa-lab-01# Switching to Standby Primary: Switching to Ok for reason Interface check.asa-lab-01# show failover history == From State To State Reason == 10:20:05 UTC Oct 20 2022 Active Config Applied Active Set by the config command 10:20:48 UTC Oct 20 2022 Active Failed Interface check 10:20:51 UTC Oct 20 2022 Failed Standby Ready Interface check 10:20:58 UTC Oct 20 2022 Standby Ready Failed Interface check 10:21:08 UTC Oct 20 2022 Failed Standby Ready Interface check ==Exclude Interfaces from MonitorIf you want to exclude interfaces connected to less critical networks from affecting your failover events, you can use the no monitor-interface command. asa-lab-01# show monitor-interface This host: Primary - Active Interface WAN (201.85.10.1): Normal (Monitored) Interface INSIDE (192.168.10.1): Normal (Monitored) Other host: Secondary - Standby Ready Interface WAN (201.85.10.2): Normal (Monitored) Interface INSIDE (192.168.10.2): Normal (Monitored) asa-lab-01(config)# no monitor-interface INSIDE asa-lab-01# show monitor-interface This host: Primary - Active Interface WAN (201.85.10.1): Normal (Monitored) Other host: Secondary - Standby Ready Interface WAN (201.85.10.2): Normal (Monitored)As you can see above, INSIDE interface is no longer monitored for failover. Failover EXEC mateThis is one of the commands I use frequently, suppose you are logged into the active unit but want to run some commands on the standby unit, you can use failover exec mate command followed by the actual command you want to run. The following shows getting the show failover output from the standby unit but running the command from the active unit. asa-lab-01# failover exec mate show failover | incl This This host: Secondary - Standby Ready Failover Syslog MessagesASA issues a number of syslog messages related to failover. The ranges of message IDs associated with failover are: 101xxx, 102xxx, 103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx, 727xxx. I've included some of the syslog messages below. %ASA-1-104002: (Primary) Switching to STANDBY - Set by the config command %ASA-1-104001: (Primary) Switching to ACTIVE - Set by the config command. %ASA-1-103001: (Secondary) No response from other firewall (reason code = 4). %ASA-1-104001: (Secondary) Switching to ACTIVE - HELLO not heard from mate. %ASA-1-105003: (Primary) Monitoring on interface WAN waiting %ASA-1-105003: (Primary) Monitoring on interface INSIDE waiting %ASA-1-105004: (Primary) Monitoring on interface WAN normal %ASA-1-105004: (Primary) Monitoring on interface INSIDE normal %ASA-1-105003: (Primary) Monitoring on interface INSIDE waiting %ASA-1-105004: (Primary) Monitoring on interface INSIDE normalEven though the configuration and state information are synced across the peers, the files are not. For example, the IOS image and AnyConnect images that you require need to be uploaded into both units individually. Preemption is not supported in Active/Passive failover mode.Closing upConfiguring the failover is very straightforward but understanding how it works is more crucial for troubleshooting. I've tried to cover as much as I can, however, if you would like to learn more about Failover, please check out the official Cisco guide I mentioned under the reference section. References The Cisco ASA failover configuration requires two identical security appliances connected to each other through a dedicated failover link and, optionally, a stateful failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs. In case of Active/Active configuration both Units carry traffic (unlike Active/Standby whereby only the active unit carries traffic). For creating active/active Failover, configuring both ASA devices in Multiple context mode is required. For ASA redundancy scenario the two devices must be the same models, must have the same number and type of interfaces and the same license is required. ASA 5505 and 5510 do not support active/active failover without license upgrade. For active/active configuration, Failover Contexts and Failover groups need to be created. The Failover group is then applied to Primary or Secondary physical ASA unit. After this, the particular Failover group is applied to a Context. For example, primary unit is active ASA of Failover group1, but Secondary unit is Standby ASA of Failover group1. If primary ASA is out of order, Secondary ASA will become Active of Failover group1. For explaining Active/Active Failover configuration in details, let’s do the following LAB. Click on the image above for larger size diagram Configuration Example !Switch both ASA devices to multiple context mode. asa(config)#mode multiple !When ASAs are reloaded, connect them to each other with Ge0/2 and Ge0/3 ports. First start with the Primary Unit configuration. Before starting configuration, all interfaces must be in the up state. !enable LAN Failover. asa(config)#failover lan enable !set this unit as primary. asa(config)#failover lan unit primary Determine Failover and State interfaces. These two interfaces can be the same physical interface if you don’t need to consume one extra port. In our example here we use two separate physical interfaces. In this article, the “failover” (interface name for GigabitEthernet0/2) is used as a failover interface. !Define Failover Interface asa(config)#failover lan interface failover Ge0/2 !assign IP address on Failover Interface. MUST be in same Subnet as the standby on the other unit. asa(config)#failover interface ip failover 192.168.3.1 255.255.255.0 standby 192.168.3.2 In this documentation, the “state” (interface name for GigabitEthernet0/3) is used as a state interface. !Define stateful Failover interface asa(config)#failover link state Ge0/3 !assign IP address on Stateful Failover interface asa(config)#failover interface ip state 192.168.4.1 255.255.255.0 standby 192.168.4.2 !Create Failover groups, where Failover group1 will be the Primary, i.e. active on Primary Unit and Failover group2 will be the Standby on Primary Unit. Configure also HTTP Replication, after which occurs HTTP Connection state replication between active and Standby ASAs. Also determine Preempt Delay. Preempt Delay means in what time to regain role of Active after Fail Recovery. asa(config)#failover group 1 asa(config-fover-group)#primary asa(config-fover-group)#preempt 120 asa(config-fover-group)# replication http MORE READING: Firewall Technologiesasa(config)#failover group 2 asa(config-fover-group)#secondary asa(config-fover-group)#preempt 120 asa(config-fover-group)# replication http Now let’s start creating Contexts and assigning interfaces in each Context. !Configure the admin context asa(config)# admin-context admin asa(config)# context admin asa(config-ctx)# allocate-interface Management0/0 asa(config-ctx)# config-url disk0:/admin.cfg !configure the Sub-interfaces interface GigabitEthernet0/0.10 vlan 10 interface GigabitEthernet0/0.11 vlan 11 interface GigabitEthernet0/1.20 vlan 20 interface GigabitEthernet0/1.21 vlan 21 ! Configure the contexts asa(config)# context c1 asa(config-ctx)# allocate-interface gigabitethernet0/0.10 asa(config-ctx)# allocate-interface gigabitethernet0/1.20 asa(config-ctx)# config-url disk0:/c1.cfg asa(config)# context c2 asa(config-ctx)# allocate-interface gigabitethernet0/0.11 asa(config-ctx)# allocate-interface gigabitethernet0/1.21 asa(config-ctx)# config-url disk0:/c2.cfg !Snap each Context to Failover Groups. If we don’t indicate Contexts to Failover Groups, each context will be in Group1 by default. asa(config)# context c1 asa(config-ctx)# join-failover-group 1 asa(config)# context c2 asa(config-ctx)# join-failover-group 2 !Configure IP addresses on Context1. asa#changeto context c1 asa/c1# show running-config interface ! interface GigabitEthernet0/0.10 nameif outside security-level 0 ip address 192.168.10.1 255.255.255.0 standby 192.168.10.2 ! interface GigabitEthernet0/1.20 nameif inside security-level 100 ip address 192.168.20.1 255.255.255.0 standby 192.168.20.2 !Configure IP addresses on Context2. asa#changeto context c2 asa/c2# show running-config interface ! interface GigabitEthernet0/0.11 nameif outside security-level 0 ip address 192.168.11.1 255.255.255.0 standby 192.168.11.2 ! interface GigabitEthernet0/1.21 nameif inside security-level 100 ip address 192.168.21.1 255.255.255.0 standby 192.168.21.2 ! Now let’s start Secondary Unit configuration. !Define Failover Interface asa(config)#failover lan interface failover Ge0/2 !assign IP address on Failover Interface. MUST be in same Subnet as other unit. asa(config)#failover interface ip failover 192.168.3.1 255.255.255.0 standby 192.168.3.2 !enable LAN Failover. asa(config)#failover lan enable !set this unit as secondary asa(config)#failover lan unit secondary With the above piece of configuration commands everything is completed and now let’s start checking. Verification and Troubleshooting Commands: !verify Primary UNIT asa# show failover Failover On Failover unit Primary Failover LAN Interface: failover GigabitEthernet0/2 (up) Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 8.2(1), Mate 8.2(1) Group 1 last failover at: 05:12:14 tbilisi Dec 7 2010 Group 2 last failover at: 10:13:04 tbilisi Oct 24 2010 Last Updated: [last-modified] (UTC) Context Configuration There are six basic steps to configuring contexts: Enable multi-context mode Configure interfaces in the system context Add a context Configure resource management Assign MAC addresses to context interfaces Configure settings within the context See the configuration in action here: Enable Multicontext mode You can convert an existing ASA to multi-context mode, or you can use a fresh ASA. If using an existing ASA, the original running config is saved as old_running.cfg. The mode multiple command enables multi-context mode. The ASA requires a reboot after running this command. The original running config is converted into a new context. This will also happen whether this is on an existing ASA or a new one. At this point there are two config files. The traditional startup configuration is for the system space. A new file called admin.cfg is created for the first context. Enable Multi-Context Mode CiscoASA(config)# mode multiple WARNING: This command will change the behavior of the device WARNING: This command will initiate a Reboot Proceed with change mode? [confirm] Convert the system configuration? [confirm] The old running configuration file will be written to flash Converting the configuration - this may take several minutes for a large configuration The admin context configuration will be written to flash The new running configuration file was written to flash Security context mode: multiple CiscoASA(config)# CiscoASA# show mode Security context mode: multiple CiscoASA# show context Context Name Class Interfaces Mode URL *admin default Management0/0 Routed disk0:/admin.cfg Total active Security Contexts: 1 NOTE: If you have migrated config to a context, you may not be able to connect with SSH. To resolve this: Connect to the console of the ASA Generate a new RSA key with crypto key generate rsa general-keys modulus 2048 Test logging on over SSH   Restoring Single-Context Mode To restore single context mode, copy the backup file, old_running.cfg, to the startup-config. This overrides the existing system configuration. Next, change the mode back to single. This will restore the config as it was originally backed up. If you’ve made changes to the context since creating the backup, those changes will be lost. Restore Single-Context Mode CiscoASA# copy disk0:/old_running.cfg startup-config Source filename [old_running.cfg]? 3991 bytes copied in 0.40 secs CiscoASA(config)# mode single WARNING: This command will change the behavior of the device WARNING: This command will initiate a Reboot Proceed with change mode? [confirm] Security context mode: single CiscoASA(config)#   Physical interfaces are ‘owned’ by the system. Interfaces are first configured in the system before being allocated to any contexts. This includes configuring port channels and VLANs. This does not include security features such as nameif or security-level. In this example, two interfaces are added to an etherchannel. The etherchannel is then configured as two sub-interfaces, each with a separate VLAN. Although not shown here, remember to configure the connected switch. Configure Physical Interfaces CiscoASA(config)# interface gigabitEthernet 0/0 CiscoASA(config-if)# channel-group 1 mode active CiscoASA(config-if)# no shutdown CiscoASA(config-if)# interface gigabitEthernet 0/1 CiscoASA(config-if)# channel-group 1 mode active CiscoASA(config-if)# no shutdown CiscoASA(config-if)# interface port-channel 1.100 CiscoASA(config-subif)# vlan 100 CiscoASA(config-subif)# interface port-channel 1.200 CiscoASA(config-subif)# vlan 200 Create Contexts Each new context has an individual name, which can be up to 32 characters long, and is case-sensitive. Each context has a config file. Set the config file location with the config-url command. After creating a context, it’s time to assign physical interfaces. The example below uses a mapped-name. This is the name for the interface within the context. Specifying the visible keyword allows the real interface name to be seen in the context. An example of this is when running a show interface command. The same interface may be allocated to more than one routed-mode context. Each transparent-mode context must have it’s own unique interfaces. ! Create a new context for the edge CiscoASA(config)# context edge Creating context 'edge'... Done. (2) CiscoASA(config-ctx)# description Edge Firewall CiscoASA(config-ctx)# allocate-interface port-channel1.100 int100 visible CiscoASA(config-ctx)# config-url disk0:/edge.cfg WARNING: Could not fetch the URL disk0:/edge.cfg INFO: Creating context with default config ! Allocate interfaces to the Admin context CiscoASA(config)# context admin CiscoASA(config-ctx)# allocate-interface port-channel1.200 int200 Use the changeto command to change to a context, and back to system. ! Enter the 'edge' context CiscoASA# changeto context edge CiscoASA/edge# ! See the allocated interface CiscoASA/edge# show interface Interface int100 "", is down, line protocol is down System name Port-channel1.100, VLAN identifier 100 Available but not configured via nameif ! Go back to 'System' CiscoASA/edge# changeto system CiscoASA# Optionally, a different context can be assigned as the admin context. Do this with the admin-context command. This will not create a new context. CiscoASA# show context Context Name Class Interfaces Mode URL *admin default Management0/0,Port- Routed disk0:/admin.cfg channel1.200 edge default Port-channel1.100 Routed disk0:/edge.cfg Total active Security Contexts: 2 CiscoASA(config)# admin-context edge CiscoASA# show context Context Name Class Interfaces Mode URL admin default Management0/0,Port- Routed disk0:/admin.cfg channel1.200 *edge default Port-channel1.100 Routed disk0:/edge.cfg Total active Security Contexts: 2   Classes restrict the amount of resources a context may use. In the example below, two classes are created and assigned to the two contexts. See Cisco’s documentation for a comprehensive list of resources to configure. Configure Resource Classes CiscoASA(config)# class default CiscoASA(config-class)# limit-resource conns 20% CiscoASA(config-class)# limit-resource routes 500 CiscoASA(config-class)# limit-resource vpn other 5 CiscoASA(config-class)# class gold CiscoASA(config-class)# limit-resource conns 80% CiscoASA(config-class)# limit-resource routes 2000 CiscoASA(config-class)# limit-resource vpn other 15 CiscoASA(config-class)# context edge CiscoASA(config-ctx)# member gold CiscoASA(config-ctx)# context admin CiscoASA(config-ctx)# member default   MAC addresses may be auto-assigned or manually assigned. This happens within the context when the using the nameif command on the interface. When using auto configuration, the ASA may generate the entire MAC, or the admin may specify a prefix. If specifying a prefix, the rest is auto generated. If a prefix is not specified, it is generated with the last two bytes of the real interface. CiscoASA# changeto context edge CiscoASA/edge# configure terminal CiscoASA/edge(config)# interface int100 CiscoASA/edge(config-if)# mac-address 1a1a.1a1a.1a1a   Configure Settings Within the Context Context configuration is now complete. The rest of the configuration is within the context, like normal. This includes interface config, ACLs, inspections, and so on. Show context information with show context and show context detail. Run these commands from system execution space. This includes a list of contexts, assigned interfaces, and the URL of the configuration file. CiscoASA# show context Context Name Class Interfaces Mode URL *admin default Management0/0,Port- Routed disk0:/admin.cfg channel1.200 edge gold Port-channel1.100 Routed disk0:/edge.cfg Total active Security Contexts: 2 Specifying the detail keyword shows extra information, such as real and mapped interfaces. This is useful to see if a context has been configured or not, without entering the context. CiscoASA# show context detail Context "system", is a system resource Config URL: startup-config Real Interfaces: Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/2, GigabitEthernet0/3, GigabitEthernet0/4, GigabitEthernet0/5, GigabitEthernet0/6, GigabitEthernet0/7, GigabitEthernet1/0, GigabitEthernet1/1, GigabitEthernet1/2, GigabitEthernet1/3, GigabitEthernet1/4, GigabitEthernet1/5, Internal-Control0/0, Internal-Data0/0, Internal-Data0/1, Internal-Data0/2, Internal-Data0/3, Management0/0, Port-channel1, Port-channel1.100, Port-channel1.200, Port-channel2 Class: default, Flags: 0x00000819, ID: 0 Context "admin", has been created Config URL: disk0:/admin.cfg Real Interfaces: Management0/0, Port-channel1.200 Mapped Interfaces: int200, Management0/0 Real IPS Sensors: Mapped IPS Sensors: Class: default, Flags: 0x00000813, ID: 1 Context "edge", has been created Desc: Edge Firewall Config URL: disk0:/edge.cfg Real Interfaces: Port-channel1.100 Mapped Interfaces: int100 Real IPS Sensors: Mapped IPS Sensors: Class: gold, Flags: 0x00000811, ID: 2 Context "null", is a system resource Config URL: ... null ... Real Interfaces: Mapped Interfaces: Real IPS Sensors: Mapped IPS Sensors: Class: default, Flags: 0x00000809, ID: 507 Check resource allocation to see what resources are configured. CiscoASA# show resource allocation Resource Total % of Avail Conns [rate] unlimited Inspects [rate] unlimited Syslogs [rate] unlimited Conns 1001000 100.18% Hosts unlimited IPSec unlimited Mac-addresses 131072 200.00% ASDM 10 5.00% SSH Client 10 10.00% SSH Server 10 10.00% Storage unlimited Telnet 10 10.00% Xlates unlimited Routes 2500 0.00% Other VPN Sessions 20 0.40% Other VPN Burst 0 AnyConnect 0 AnyConnect Burst 0 IKEv1 in-negotiatio unlimited show resource allocation detail Additionally, actual resource usage can be seen. CiscoASA# show resource usage summary Resource Current Peak Limit Denied Context Routes 0 2 unlimited 0 Summary CiscoASA# show resource usage context admin Resource Current Peak Limit Denied Context Routes 0 2 500 0 admin   Cisco – Multiple Context Mode The failover configuration requires two identical security appliances connected to each other through a dedicated failover link and, optionally, a stateful failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs. The security appliance supports two failover configurations, Active/Active Failover and Active/Standby Failover. Each failover configuration has its own method to determine and perform failover. With Active/Active Failover, both units can pass network traffic. This lets you configure load balancing on your network. Active/Active Failover is only available on units that run in multiple context mode. With Active/Standby Failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby Failover is available on units that run in either single or multiple context mode. Both failover configurations support stateful or stateless (regular) failover. This document focuses on how to configure an Active/Active Failover in Cisco PIX/ASA Security Appliance. Refer to PIX/ASA 7.x Active/Standby Failover Configuration Example in order to learn more information about the Active/Standby Failover configurations. Note: VPN failover is not supported on units that run in multiple context mode as VPN is not supported in multiple context. VPN failover is available only for Active/Standby Failover configurations in single context configurations. This configuration guide provides a sample configuration to include a brief introduction to the PIX/ASA 7.x Active/Active technology. Refer to the Cisco Security Appliance Command Reference, Version 7.2 for a more in-depth sense of the theory based behind this technology. Prerequisites Requirements Hardware Requirement The two units in a failover configuration must have the same hardware configuration. They must be the same model, have the same number and types of interfaces, and the same amount of RAM. Note: The two units do not need to have the same size Flash memory. If you use units with different Flash memory sizes in your failover configuration, make sure the unit with the smaller Flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger Flash memory to the unit with the smaller Flash memory fails. Software Requirement The two units in a failover configuration must be in the operational modes (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version, but you can use different versions of the software within an upgrade process; for example, you can upgrade one unit from Version 7.0(1) to Version 7.0(2) and have failover remain active. Cisco recommends that you upgrade both units to the same version to ensure long-term compatibility. Refer to Performing Zero Downtime Upgrades for Failover Pairs for more information about upgrading the software on a failover pair. License Requirements On the PIX/ASA Security appliance platform, at least one of the units must have an unrestricted (UR) license. The other unit can have a Failover Only Active-Active (FO_AA) license, or another UR license. Units with a Restricted license cannot be used for failover, and two units with FO_AA licenses cannot be used together as a failover pair. Note: You might need to upgrade the licenses on a failover pair in order to obtain additional features and benefits. For more information on upgrade, refer to License Key Upgrade on a Failover Pair Note: The licensed features, such as SSL VPN peers or security contexts, on both security appliances that participate in failover must be identical. Note: The FO license does not support Active/Active Failover. Components Used The information in this document is based on these software and hardware versions: PIX Security Appliance with 7.x version and later The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command. Related Products This configuration can also be used with these hardware and software versions: ASA with 7.x version and later Note: Active/Active failover is not available on the ASA 5505 series adaptive security appliance. Conventions Refer to the Cisco Technical Tips Conventions for more information document conventions. Active/Active Failover This section describes Active/Standby Failover and includes these topics: Active/Active Failover Overview Active/Active failover is only available to security appliances in multiple context mode. In an Active/Active failover configuration, both security appliances can pass network traffic. In Active/Active failover, you divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the security appliance. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default. The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group rather than the unit. When an active failover group fails, it changes to the standby state while the standby failover group becomes active. The interfaces in the failover group that becomes active assume the MAC and IP addresses of the interfaces in the failover group that failed. The interfaces in the failover group that is now in the standby state take over the standby MAC and IP addresses. Note: A failover group failing on a unit does not mean that the unit has failed. The unit may still have another failover group passing traffic on it. Primary/Secondary Status and Active/Standby Status As in Active/Standby failover, one unit in an Active/Active failover pair is designated the primary unit, and the other unit the secondary unit. Unlike Active/Standby failover, this designation does not indicate which unit becomes active when both units start simultaneously. Instead, the primary/secondary designation does two things: Determines which unit provides the running configuration to the pair when they boot simultaneously. Determines on which unit each failover group appears in the active state when the units boot simultaneously. Each failover group in the configuration is configured with a primary or secondary unit preference. You can configure both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, distributing the traffic across the devices. Note: The security appliance does not provide load balancing services. Load balancing must be handled by a router passing traffic to the security appliance. Which unit each failover group becomes active on is determined as shown When a unit boots while the peer unit is not available, both failover groups become active on the unit. When a unit boots while the peer unit is active (with both failover groups in the active state), the failover groups remain in the active state on the active unit regardless of the primary or secondary preference of the failover group until one of the following: A failover occurs. You manually force the failover group to the other unit with the no failover active command You configured the failover group with the preempt command, which causes the failover group to automatically become active on the preferred unit when the unit becomes available. When both units boot at the same time, each failover group becomes active on its preferred unit after the configurations have been synchronized. Device Initialization and Configuration Synchronization Configuration synchronization occurs when one or both units in a failover pair boot. The configurations are synchronized as shown: When a unit boots while the peer unit is active (with both failover groups active on it), the booting unit contacts the active unit to obtain the running configuration regardless of the primary or secondary designation of the booting unit. When both units boot simultaneously, the secondary unit obtains the running configuration from the primary unit. When the replication starts, the security appliance console on the unit sending the configuration displays the message "Beginning configuration replication: Sending to mate," and when it is complete, the security appliance displays the message "End Configuration Replication to mate." During replication, commands entered on the unit sending the configuration may not replicate properly to the peer unit, and commands entered on the unit receiving the configuration may be overwritten by the configuration being received. Avoid entering commands on either unit in the failover pair during the configuration replication process. Depending upon the size of the configuration, replication can take from a few seconds to several minutes. On the unit receiving the configuration, the configuration exists only in running memory. To save the configuration to Flash memory after synchronization enter the write memory all command in the system execution space on the unit that has failover group 1 in the active state. The command is replicated to the peer unit, which proceeds to write its configuration to Flash memory. Using the all keyword with this command causes the system and all context configurations to be saved. Note: Startup configurations saved on external servers are accessible from either unit over the network and do not need to be saved separately for each unit. Alternatively, you can copy the contexts configuration files from the disk on the primary unit to an external server, and then copy them to disk on the secondary unit, where they become available when the unit reloads. Command Replication After both units are running, commands are replicated from one unit to the other as shown: Commands entered within a security context are replicated from the unit on which the security context appears in the active state to the peer unit. Note: context is considered in the active state on a unit if the failover group to which it belongs is in the active state on that unit. Commands entered in the system execution space are replicated from the unit on which failover group 1 is in the active state to the unit on which failover group 1 is in the standby state. Commands entered in the admin context are replicated from the unit on which failover group 1 is in the active state to the unit on which failover group 1 is in the standby state. All configuration and file commands (copy, rename, delete, mkdir, rmdir, and so on) are replicated, with the following exceptions. The show, debug, mode, firewall, and failover lan unit commands are not replicated. Failure to enter the commands on the appropriate unit for command replication to occur causes the configurations to be out of synchronization. Those changes may be lost the next time the initial configuration synchronization occurs. You can use the write standby command to resynchronize configurations that have become out of sync. For Active/Active failover, the write standby command behaves as shown: If you enter the write standby command in the system execution space, the system configuration and the configurations for all of the security contexts on the security appliance is written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state. Note: If there are security contexts in the active state on the peer unit, the write standby command causes active connections through those contexts to be terminated. Use the failover active command on the unit providing the configuration to make sure all contexts are active on that unit before entering the write standby command. If you enter the write standby command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state. Replicated commands are not saved to the Flash memory when replicated to the peer unit. They are added to the running configuration. To save replicated commands to Flash memory on both units, use the write memory or copy running-config startup-config command on the unit that you made the changes on. The command is replicated to the peer unit and cause the configuration to be saved to Flash memory on the peer unit. Failover Triggers In Active/Active failover, failover can be triggered at the unit level if one of the following events occurs: The unit has a hardware failure. The unit has a power failure. The unit has a software failure. The no failover active or the failover active command is entered in the system execution space. Failover is triggered at the failover group level when one of these events occurs: Too many monitored interfaces in the group fail. The no failover active group group_id or failover active group group_id command is entered. Failover Actions In an Active/Active failover configuration, failover occurs on a failover group basis, not a system basis. For example, if you designate both failover groups as active on the primary unit, and failover group 1 fails, then failover group 2 remains active on the primary unit while failover group 1 becomes active on the secondary unit. Note: When configuring Active/Active failover, make sure that the combined traffic for both units is within the capacity of each unit. This table shows the failover action for each failure event. For each failure event, the policy (whether or not failover occurs), actions for the active failover group, and actions for the standby failover group are given. Failure Event Policy Active Group Action Standby Group Action Notes A unit experiences a power or software failure Failover Become standby Mark as failed Become standby. Mark active as failed When a unit in a failover pair fails, any active failover groups on that unit are marked as failed and become active on the peer unit. Interface failure on active failover group above threshold Failover Mark active group as failed Become active None Interface failure on standby failover group above threshold No failover No action Mark standby group as failed When the standby failover group is marked as failed, the active failover group does not attempt to fail over, even if the interface failure threshold is surpassed. Formerly active failover group recovers No failover No action No action Unless configured with the preempt command, the failover groups remain active on their current unit. Failover link failed at startup No failover Become active Become active If the failover link is down at startup, both failover groups on both units become active. Stateful Failover link failed No failover No action No action State information becomes out of date, and sessions are terminated if a failover occurs. Failover link failed during operation No failover n/a n/a Each unit marks the failover interface as failed. You should restore the failover link as soon as possible because the unit cannot fail over to the standby unit while the failover link is down. Regular and Stateful Failover The security appliance supports two types of failover, regular and stateful. This section includes these topics: Regular Failover Stateful Failover Regular Failover When a failover occurs, all active connections are dropped. Clients need to re-establish connections when the new active unit takes over. Stateful Failover When stateful failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session. The state information passed to the standby unit includes these: The NAT translation table The TCP connection states The UDP connection states The ARP table The Layer 2 bridge table (when it runs in the transparent firewall mode) The HTTP connection states (if HTTP replication is enabled) The ISAKMP and IPSec SA table The GTP PDP connection database The information that is not passed to the standby unit when stateful failover is enabled includes these: The HTTP connection table (unless HTTP replication is enabled) The user authentication (uauth) table The routing tables State information for security service modules Note: If failover occurs within an active Cisco IP SoftPhone session, the call remains active because the call session state information is replicated to the standby unit. When the call is terminated, the IP SoftPhone client loses connection with the Call Manager. This occurs because there is no session information for the CTIQBE hang-up message on the standby unit. When the IP SoftPhone client does not receive a response back from the Call Manager within a certain time period, it considers the Call Manager unreachable and unregisters itself. Failover Configuration Limitations You cannot configure failover with these types of IP addresses: IP addresses obtained through DHCP IP addresses obtained through PPPoE IPv6 addresses Additionally, these restrictions apply: Stateful Failover is not supported on the ASA 5505 adaptive security appliance. Active/Active failover is not supported on the ASA 5505 adaptive security appliance. You cannot configure failover when Easy VPN Remote is enabled on the ASA 5505 adaptive security appliance. VPN failover is not supported in multiple context mode. Unsupported Features Multiple context mode does not support these features: Dynamic routing protocols Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode. VPN Multicast Cable-Based Active/Active Failover Configuration Prerequisites Before you begin, verify the following: Both units have the same hardware, software configuration, and proper license. Both units are in the same mode (single or multiple, transparent or routed). Network Diagram This document uses this network setup: Follow these steps in order to configure Active/Active failover using a serial cable as the failover link. The commands in this task are entered on the primary unit in the failover pair. The primary unit is the unit that has the end of the cable labeled "Primary" plugged into it. For devices in multiple context mode, the commands are entered in the system execution space unless otherwise noted. You do not need to bootstrap the secondary unit in the failover pair when you use cable-based failover. Leave the secondary unit powered off until instructed to power it on. Note: Cable-based failover is only available on the PIX 500 series security appliance. Complete these steps in order to configure cable-based, Active/Active failover: Connect the failover cable to the PIX 500 series security appliances. Make sure that you attach the end of the cable marked "Primary" to the unit you use as the primary unit, and that you attach the end of the cable marked "Secondary" to the unit you use as the secondary unit. Power on the primary unit. If you have not done so already, configure the active and standby IP addresses for each data interface (routed mode), for the management IP address (transparent mode), or for the management-only interface. The standby IP address is used on the security appliance that is currently the standby unit. It must be in the same subnet as the active IP address. You must configure the interface addresses from within each context. Use the changeto context command to switch between contexts. The command prompt changes to hostname/context(config-if)#, where context is the name of the current context. You must enter a management IP address for each context in transparent firewall multiple context mode. Note: Do not configure an IP address for the Stateful Failover link if you are going to use a dedicated Stateful Failover interface. You use the failover interface ip command to configure a dedicated Stateful Failover interface in a later step. hostname/context(config-if)#ip address active_addr netmask standby standby_addr In the example, the outside interface for context1 of the primary PIX is configured this way: PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2 For Context2: PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2 In routed firewall mode and for the management-only interface, this command is entered in interface configuration mode for each interface. In transparent firewall mode, the command is entered in global configuration mode. In order to enable Stateful Failover, configure the Stateful Failover link. Specify the interface to be used as Stateful Failover link: hostname(config)#failover link if_name phy_if In this example, the Ethernet2 interface is used to exchange the stateful failover link state information. failover link stateful Ethernet2 The if_name argument assigns a logical name to the interface specified by the phy_if argument. The phy_if argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. This interface should not be used for any other purpose (except, optionally, the failover link). Assign an active and standby IP address to the Stateful Failover link: hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr In this example , 10.0.0.1 is used as an active, and 10.0.0.2 is used as a standby IP address for the stateful failover link. PIX1(config)#failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2 The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby IP address subnet mask. The Stateful Failover link IP address and MAC address do not change at failover except for when Stateful Failover uses a regular data interface. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit. Enable the interface: hostname(config)#interface phy_if hostname(config-if)#no shutdown Configure the failover groups. You can have at most two failover groups. The failover group command creates the specified failover group if it does not exist and enters the failover group configuration mode. For each failover group, you need to specify whether the failover group has primary or secondary preference using the primary or secondary command. You can assign the same preference to both failover groups. For load balancing configurations, you should assign each failover group a different unit preference. The following example assigns failover group 1 a primary preference and failover group 2 a secondary preference: hostname(config)#failover group 1 hostname(config-fover-group)#primary hostname(config-fover-group)#exit hostname(config)#failover group 2 hostname(config-fover-group)#secondary hostname(config-fover-group)#exit Assign each user context to a failover group using the join-failover-group command in context configuration mode. Any unassigned contexts are automatically assigned to failover group 1. The admin context is always a member of failover group 1. Enter these commands to assign each context to a failover group: hostname(config)#context context_name hostname(config-context)#join-failover-group {1 | 2} hostname(config-context)#exit Enable failover: hostname(config)#failover Power on the secondary unit and enable failover on the unit if it is not already enabled: hostname(config)#failover The active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages "Beginning configuration replication: Sending to mate" and "End Configuration Replication to mate" appear on the primary console. Note: Issue the failover command on the primary device first, and then issue it on the secondary device. After you issue the failover command on the secondary device, the secondary device immediately pulls the configuration from the primary device and sets itself as standby. The primary ASA stays up and passes traffic normally and marks itself as the active device. From that point on, whenever a failure occurs on the active device, the standby device comes up as active. Save the configuration to Flash memory on the Primary unit. Because the commands entered on the primary unit are replicated to the secondary unit, the secondary unit also saves its configuration to Flash memory. hostname(config)#copy running-config startup-config If necessary, force any failover group that is active on the primary to the active state on the secondary. To force a failover group to become active on the secondary unit, issue this command in the system execution space on the primary unit: hostname#no failover active group group_id The group_id argument specifies the group you want to become active on the secondary unit. Configurations This document uses these configurations: PIX1 - System Configuration PIX1#show running-config : Saved PIX Version 7.2(2) ! hostname PIX1 enable password 8Ry2YjIyt7RRXU24 encrypted no mac-address auto !--- Enable the physical and logical interfaces in the system execution !--- space by giving "no shutdown" before configuring the same in the contexts ! interface Ethernet0 ! interface Ethernet0.1 vlan 2 ! interface Ethernet0.2 vlan 4 ! interface Ethernet1 ! interface Ethernet1.1 vlan 3 ! interface Ethernet1.2 vlan 5 ! !--- Configure "no shutdown" in the stateful failover interface !--- of both Primary and secondary PIX. interface Ethernet2 description STATE Failover Interface ! interface Ethernet3 shutdown ! interface Ethernet4 shutdown ! interface Ethernet5 shutdown ! class default limit-resource All 0 limit-resource ASDM 5 limit-resource SSH 5 limit-resource Telnet 5 ! ftp mode passive pager lines 24 !--- Command to enable the failover feature failover !--- Command to assign the interface for stateful failover failover link stateful Ethernet2 !--- Command to configure the active and standby IP's for the !--- stateful failover failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2 !--- Configure the group 1 as primary failover group 1 !--- Configure the group 1 as secondary failover group 2 secondary no asdm history enable arp timeout 14400 console timeout 0 admin-context admin context admin config-url flash:/admin.cfg ! !--- Command to create a context called "context1" context context1 !--- Command to allocate the logical interfaces to the contexts allocate-interface Ethernet0.1 inside_context1 allocate-interface Ethernet1.1 outside_context1 config-url flash:/context1.cfg !--- Assign this context to the failover group 1 join-failover-group 1 ! context context2 allocate-interface Ethernet0.2 inside_context2 allocate-interface Ethernet1.2 outside_context2 config-url flash:/context2.cfg join-failover-group 2 ! prompt hostname context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end PIX1 - Context1 Configuration PIX1/context1(config)#show running-config : Saved : PIX Version 7.2(2) ! hostname context1 enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface inside_context1 nameif inside security-level 100 !--- Configure the active and standby IP's for the logical inside !--- interface of the context1. ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2 ! interface outside_context1 nameif outside security-level 0 !--- Configure the active and standby IP's for the logical outside !--- interface of the context1. ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2 ! passwd 2KFQnbNIdI.2KYOU encrypted access-list 100 extended permit tcp any host 172.16.1.1 eq www pager lines 24 mtu inside 1500 mtu outside 1500 monitor-interface inside monitor-interface outside icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 static (inside,outside) 172.16.1.1 192.168.1.5 netmask 255.255.255.255 access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.16.1.3 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no snmp-server location no snmp-server contact telnet timeout 5 ssh timeout 5 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global Cryptochecksum:00000000000000000000000000000000 : end PIX1 - Context2 Configuration PIX1/context2(config)#show running-config : Saved : PIX Version 7.2(2) ! hostname context2 enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface inside_context2 nameif inside security-level 100 !--- Configure the active and standby IP's for the logical inside !--- interface of the context2. ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2 ! interface outside_context2 nameif outside security-level 0 !--- Configure the active and standby IP's for the logical outside !--- interface of the context2. ip address 172.16.2.1 255.255.255.0 standby 172.16.2.2 ! passwd 2KFQnbNIdI.2KYOU encrypted access-list 100 extended permit tcp any host 172.16.2.1 eq www pager lines 24 mtu inside 1500 mtu outside 1500 monitor-interface inside monitor-interface outside icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 static (inside,outside) 172.16.2.1 192.168.2.5 netmask 255.255.255.255 access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.16.2.3 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no snmp-server location no snmp-server contact telnet timeout 5 ssh timeout 5 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global Cryptochecksum:00000000000000000000000000000000 : end LAN-Based Active/Active Failover Configuration Network Diagram This document uses this network setup: This section describes how to configure Active/Active failover using an Ethernet failover link. When configuring LAN-based failover, you must bootstrap the secondary device to recognize the failover link before the secondary device can obtain the running configuration from the primary device. Note: Instead of using a crossover Ethernet cable to directly link the units, Cisco recommends that you use a dedicated switch between the primary and secondary units. This section includes the topics as shown: Primary Unit Configuration Secondary Unit Configuration Primary Unit Configuration Complete these steps in order to configure the primary unit in an Active/Active failover configuration: If you have not done so already, configure the active and standby IP addresses for each data interface (routed mode), for the management IP address (transparent mode), or for the management-only interface. The standby IP address is used on the security appliance that is currently the standby unit. It must be in the same subnet as the active IP address. You must configure the interface addresses from within each context. Use the changeto context command to switch between contexts. The command prompt changes to hostname/context(config-if)#, where context is the name of the current context. In transparent firewall mode, you must enter a management IP address for each context. Note: Do not configure an IP address for the Stateful Failover link if you are going to use a dedicated Stateful Failover interface. You use the failover interface ip command to configure a dedicated Stateful Failover interface in a later step. hostname/context(config-if)#ip address active_addr netmask standby standby_addr In the example, the outside interface for context1 of the primary PIX is configured this way: PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2 For Context2: PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2 In routed firewall mode and for the management-only interface, this command is entered in interface configuration mode for each interface. In transparent firewall mode, the command is entered in global configuration mode. Configure the basic failover parameters in the system execution space. (PIX security appliance only) Enable LAN-based failover: hostname(config)#failover lan enable Designate the unit as the primary unit: hostname(config)#failover lan unit primary Specify the failover link: hostname(config)#failover lan interface if_name phy_if In this example, we use the interface ethernet 3 as LAN based failover interface. PIX1(config)#failover lan interface LANFailover ethernet3 The if_name argument assigns a logical name to the interface specified by the phy_if argument. The phy_if argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. On the ASA 5505 adaptive security appliance, the phy_if specifies a VLAN. This interface should not be used for any other purpose (except, optionally, the Stateful Failover link). Specify the failover link active and standby IP addresses: hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr For this example, we use 10.1.0.1 as active and 10.1.0.2 as standby IP addresses for failover interface. PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2 The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby IP address subnet mask. The failover link IP address and MAC address do not change at failover. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit. To enable Stateful Failover, configure the Stateful Failover link: Specify the interface to be used as Stateful Failover link: hostname(config)#failover link if_name phy_if PIX1(config)#failover link stateful ethernet2 The if_name argument assigns a logical name to the interface specified by the phy_if argument. The phy_if argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. This interface should not be used for any other purpose (except, optionally, the failover link). Note: If the Stateful Failover link uses the failover link or a regular data interface, then you only need to supply the if_name argument. Assign an active and standby IP address to the Stateful Failover link. Note: If the Stateful Failover link uses the failover link or a regular data interface, skip this step. You have already defined the active and standby IP addresses for the interface. hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr PIX1(config)#failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2 The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask. The state link IP address and MAC address do not change at failover. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit. Enable the interface. Note: If the Stateful Failover link uses the failover link or regular data interface, skip this step. You have already enabled the interface. hostname(config)#interface phy_if hostname(config-if)#no shutdown Configure the failover groups. You can have at most two failover groups. The failover group command creates the specified failover group if it does not exist and enters the failover group configuration mode. For each failover group, specify whether the failover group has primary or secondary preference using the primary or secondary command. You can assign the same preference to both failover groups. For load balancing configurations, you should assign each failover group a different unit preference. The following example assigns failover group 1 a primary preference and failover group 2 a secondary preference: hostname(config)#failover group 1 hostname(config-fover-group)#primary hostname(config-fover-group)#exit hostname(config)#failover group 2 hostname(config-fover-group)#secondary hostname(config-fover-group)#exit Assign each user context to a failover group using the join-failover-group command in context configuration mode. Any unassigned contexts are automatically assigned to failover group 1. The admin context is always a member of failover group 1. Enter these commands to assign each context to a failover group: hostname(config)#context context_name hostname(config-context)#join-failover-group {1 | 2} hostname(config-context)#exit Enable failover. hostname(config)#failover Secondary Unit Configuration When configuring LAN-based Active/Active failover, you need to bootstrap the secondary unit to recognize the failover link. This allows the secondary unit to communicate with and receive the running configuration from the primary unit. Complete these steps in order to bootstrap the secondary unit in an Active/Active failover configuration: (PIX security appliance only) Enable LAN-based failover.

hostname(config)#failover lan enable Define the failover interface. Use the same settings as you used for the primary unit: Specify the interface to be used as the failover interface. hostname(config)#failover lan interface if_name phy_if PIX1(config)#failover lan interface LANFailover ethernet3 The if_name argument assigns a logical name to the interface specified by the phy_if argument. The phy_if argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. On the ASA 5505 adaptive security appliance, the phy_if specifies a VLAN. Assign the active and standby IP address to the failover link: hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2 Note: Enter this command exactly as you entered it on the primary unit when you configured the failover interface. The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask. Enable the interface. hostname(config)#interface phy_if hostname(config-if)#no shutdown Designate this unit as the secondary unit: hostname(config)#failover lan unit secondary Note: This step is optional because by default units are designated as secondary unless previously configured otherwise. Enable failover. hostname(config)#failover After you enable failover, the active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages Beginning configuration replication: Sending to mate and End Configuration Replication to mate appear on the active unit console. Note: Issue the failover command on the primary device first, and then issue it on the secondary device. After you issue the failover command on the secondary device, the secondary device immediately pulls the configuration from the primary device and sets itself as standby. The primary ASA stays up and passes traffic normally and marks itself as the active device. From that point on, whenever a failure occurs on the active device, the standby device comes up as active. After the running configuration has completed replication, enter this command to save the configuration to Flash memory: hostname(config)#copy running-config startup-config If necessary, force any failover group that is active on the primary to the active state on the secondary unit. To force a failover group to become active on the secondary unit, enter this command in the system execution space on the primary unit: hostname#no failover active group group_id The group_id argument specifies the group you want to become active on the secondary unit. Configurations This document uses these configurations: Primary PIX PIX1(config)#show running-config : Saved : PIX Version 7.2(2) ! hostname PIX1 enable password 8Ry2YjIyt7RRXU24 encrypted no mac-address auto ! interface Ethernet0 ! interface Ethernet0.1 vlan 2 ! interface Ethernet0.2 vlan 4 ! interface Ethernet1 ! interface Ethernet1.1 vlan 3 ! interface Ethernet1.2 vlan 5 ! !--- Configure "no shutdown" in the stateful failover interface as well as !--- LAN Failover interface of both Primary and secondary PIX/ASA. interface Ethernet2 description STATE Failover Interface ! interface Ethernet3 description LAN Failover Interface ! interface Ethernet4 shutdown ! interface Ethernet5 shutdown ! class default limit-resource All 0 limit-resource ASDM 5 limit-resource SSH 5 limit-resource Telnet 5 ! ftp mode passive pager lines 24 failover failover lan unit primary !--- Command to assign the interface for LAN based failover failover lan interface LANFailover Ethernet3 !--- Command to enable the LAN based failover failover lan enable !--- Configure the Authentication/Encryption key failover key ***** failover link stateful Ethernet2 !--- Configure the active and standby IP's for the LAN based failover failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2 failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2 failover group 1 failover group 2 secondary no asdm history enable arp timeout 14400 console timeout 0 admin-context admin context admin config-url flash:/admin.cfg ! context context1 allocate-interface Ethernet0.1 inside_context1 allocate-interface Ethernet1.1 outside_context1 config-url flash:/context1.cfg join-failover-group 1 ! context context2 allocate-interface Ethernet0.2 inside_context2 allocate-interface Ethernet1.2 outside_context2 config-url flash:/context2.cfg join-failover-group 2 ! prompt hostname context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end Note: Refer the Cable based Failover Configuration section, PIX1 - Context1 Configuration and PIX1 - Context2 Configuration for context configuration in LAN based failover scenario. Secondary PIX PIX2#show running-config failover failover lan unit secondary failover lan interface LANFailover Ethernet3 failover lan enable failover key ***** failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2 Verify Use of the show failover Command This section describes the show failover command output. On each unit, you can verify the failover status with the show failover command. Primary PIX PIX1(config-subif)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover unit Primary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15 seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(2), Mate 7.2(2) Group 1 last failover at: 06:12:45 UTC Apr 16 2007 Group 2 last failover at: 06:12:43 UTC Apr 16 2007 This host: Primary Group 1 State: Active Active time: 359610 (sec) Group 2 State: Standby Ready Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal context1 Interface outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2 Interface outside (172.16.2.2): Normal Other host: Secondary Group 1 State: Standby Ready Active time: 0 (sec) Group 2 State: Active Active time: 3900 (sec) context1 Interface inside (192.168.1.2): Normal context1 Interface outside (172.16.1.2): Normal context2 Interface inside (192.168.2.1): Normal context2 Interface outside (172.16.2.1): Normal Stateful Failover Logical Update Statistics Link : stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 48044 0 48040 1 sys cmd 48042 0 48040 1 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0 0 0 0 ARP tbl 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 72081 Xmit Q: 0 1 48044 Secondary PIX PIX1(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover unit Secondary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15 seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(2), Mate 7.2(2) Group 1 last failover at: 06:12:46 UTC Apr 16 2007 Group 2 last failover at: 06:12:41 UTC Apr 16 2007 This host: Secondary Group 1 State: Standby Ready Active time: 0 (sec) Group 2 State: Active Active time: 3975 (sec) context1 Interface inside (192.168.1.2): Normal context1 Interface outside (172.16.1.2): Normal context2 Interface inside (192.168.2.1): Normal context2 Interface outside (172.16.2.1): Normal Other host: Primary Group 1 State: Active Active time: 359685 (sec) Group 2 State: Standby Ready Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal context1 Interface outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2 Interface outside (172.16.2.2): Normal Stateful Failover Logical Update Statistics Link : stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 940 0 942 2 sys cmd 940 0 940 2 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0 0 0 0 ARP tbl 0 0 2 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 1419 Xmit Q: 0 1 940 Use the show failover state command to verify the state. Primary PIX PIX1(config)#show failover state State Last Failure Reason Date/Time This host - Primary Group 1 Active None Group 2 Standby Ready None Other host - Secondary Group 1 Standby Ready None Group 2 Active None ====Configuration State=== Sync Done ====Communication State=== Mac set Secondary unit PIX1(config)#show failover state State Last Failure Reason Date/Time This host - Secondary Group 1 Standby Ready None Group 2 Active None Other host - Primary Group 1 Active None Group 2 Standby Ready None ====Configuration State=== Sync Done - STANDBY ====Communication State=== Mac set In order to verify the IP addresses of the failover unit, use the show failover interfacecommand. Primary unit PIX1(config)#show failover interface interface stateful Ethernet2 System IP Address: 10.0.0.1 255.255.255.0 My IP Address : 10.0.0.1 Other IP Address : 10.0.0.2 interface LANFailover Ethernet3 System IP Address: 10.1.0.1 255.255.255.0 My IP Address : 10.1.0.1 Other IP Address : 10.1.0.2 Secondary unit PIX1(config)#show failover interface interface LANFailover Ethernet3 System IP Address: 10.1.0.1 255.255.255.0 My IP Address : 10.1.0.2 Other IP Address : 10.1.0.1 interface stateful Ethernet2 System IP Address: 10.0.0.1 255.255.255.0 My IP Address : 10.0.0.2 Other IP Address : 10.0.0.1 View of Monitored Interfaces In order to view the status of monitored interfaces: In single context mode, enter the show monitor-interface command in global configuration mode. In multiple context mode, enter the show monitor-interface within a context. Note: In order to enable health monitoring on a specific interface, use the monitor-interface command in global configuration mode: monitor-interface Primary PIX PIX1/context1(config)#show monitor-interface This host: Secondary - Active Interface inside (192.168.1.1): Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby Ready Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal Secondary PIX PIX1/context1(config)#show monitor-interface This host: Secondary - Standby Ready Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Secondary - Active Interface inside (192.168.1.1): Normal Interface outside (172.16.1.1): Normal Note: If you do not enter a failover IP address, the show failover command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remains in a "waiting" state. You must set a failover IP address for failover to work. For more information about different states for failover, refer to show failover. By default, monitoring of physical interfaces is enabled, and monitoring of subinterfaces is disabled. Display of the Failover Commands in the Running Configuration In order to view the failover commands in the running configuration, enter this command: hostname(config)#show running-config failover All of the failover commands are displayed. On units that run in multiple context mode, enter the show running-config failover command in the system execution space. Enter the show running-config all failover command to display the failover commands in the running configuration and include commands for which you have not changed the default value. Failover Functionality Tests In order to test failover functionality, perform these steps: Test that your active unit or failover group passes traffic as expected with FTP (for example) to send a file between hosts on different interfaces. Force a failover to the standby unit with this command: For Active/Active failover, enter the following command on the unit where the failover group containing the interface connecting your hosts is active: hostname(config)#no failover active group group_id Use FTP to send another file between the same two hosts. If the test was not successful, enter the show failover command to check the failover status. When you are finished, you can restore the unit or failover group to active status with this command: For Active/Active failover, enter the following command on the unit where the failover group containing the interface connecting your hosts is active: hostname(config)#failover active group group_id Forced Failover In order to force the standby unit to become active, enter one of these commands: Enter this command in the system execution space of the unit where the failover group is in the standby state: hostname#failover active group group_id Or, enter this command in the system execution space of the unit where the failover group is in the active state: hostname#no failover active group group_id Entering this command in the system execution space causes all failover groups to become active: hostname#failover active Disabled Failover In order to disable failover, enter this command: hostname(config)#no failover If you disable failover on an Active/Standby pair, it causes the active and standby state of each unit to be maintained until you restart. For example, the standby unit remains in standby mode so that both units do not start to pass traffic. In order to make the standby unit active (even with failover disabled), see the Forced Failover section. If you disable failover on an Active/Active pair, it causes the failover groups to remain in the active state on whichever unit they are currently active on, no matter which unit they are configured to prefer. The no failover command can be entered in the system execution space. Restoration of a Failed Unit In order to restore a failed Active/Active failover group to an unfailed state, enter this command: hostname(config)#failover reset group group_id If you restore a failed unit to an unfailed state, it does not automatically make it active; restored units or groups remain in the standby state until made active by failover (forced or natural). An exception is a failover group configured with the preempt command. If previously active, a failover group becomes active if it is configured with the preempt command and if the unit on which it failed is its preferred unit. Replace the Failed Unit with a New Unit Complete these steps in order to replace a failed unit with a new unit: Run the no failover command on the primary unit. The status of the secondary unit shows standby unit as not detected. Unplug the primary unit, and connect the replacement primary unit. Verify that the replacement unit runs the same software and ASDM version as the secondary unit. Run these commands on the replacement unit: ASA(config)#failover lan unit primary ASA(config)#failover lan interface failover Ethernet3 ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2 ASA(config)#interface Ethernet3 ASA(config-if)#no shut ASA(config-if)#exit Plug the replacement primary unit to the network, and run this command: ASA(config)#failover Troubleshoot When a failover occurs, both security appliances send out system messages. This section includes these topics: Failover System Messages Debug Messages SNMP Failover System Messages The security appliance issues a number of system messages related to failover at priority level 2, which indicates a critical condition. In order to view these messages, refer to the Cisco Security Appliance Logging Configuration and System Log Messages to enable logging and to see descriptions of the system messages. Note: Within switchover, failover logically shuts down and then brings up interfaces, which generates syslog 411001 and 411002 messages. This is normal activity. Primary Lost Failover communications with mate on interface interface_name This failover message is displayed if one unit of the failover pair can no longer communicate with the other unit of the pair. Primary can also be listed as Secondary for the secondary unit. (Primary) Lost Failover communications with mate on interface interface_name Verify that the network that is connected to the specified interface is functioning correctly. Debug Messages In order to see debug messages, enter the debug fover command. Refer to the Cisco Security Appliance Command Reference, Version 7.2 for more information. Note: Because debugging output is assigned high priority in the CPU process, it can drastically affect system performance. For this reason, use the debug fover commands only to troubleshoot specific problems or within troubleshooting sessions with Cisco technical support staff. SNMP In order to receive SNMP syslog traps for failover, configure the SNMP agent to send SNMP traps to SNMP management stations, define a syslog host, and compile the Cisco syslog MIB into your SNMP management station. Refer to the snmp-server and logging commands in the Cisco Security Appliance Command Reference, Version 7.2 for more information. Failover Polltime In order to specify the failover unit poll and hold times, issue the failover polltime command in global configuration mode. The failover polltime unit msec [time] represents the time interval to check the existence of the standby unit by polling hello messages. Similarly, the failover holdtime unit msec [time] represents the time period during which a unit must receive a hello message on the failover link, after which the peer unit is declared to have failed. Refer to failover polltime for more information. WARNING: Failover message decryption failure. Error message: Failover message decryption failure. Please make sure both units have the same failover shared key and crypto license or system is not out of memory This problem occurs due to failover key configuration. In order to resolve this issue, remove the failover key, and configure the new shared key. Related Information hi, you just need a minimum config on the new/secondary ASA 5545-X. the config will be replicated from the primary FW afterwards. note the default ASA security context is 2, so you have 1x 'admin' context by default and 2 customer contexts. 1) upgrade secondary FW to the same ASA and ASDM image 2) enable 'multiple mode' 3) unshut the 'failover' interface 4) configure the failover config. see config sample below: configure terminalmode multiple