Troubleshooting Common Firewall Problems

Poonguzhali Sankar

Cisco Support Community - Ask the Expert

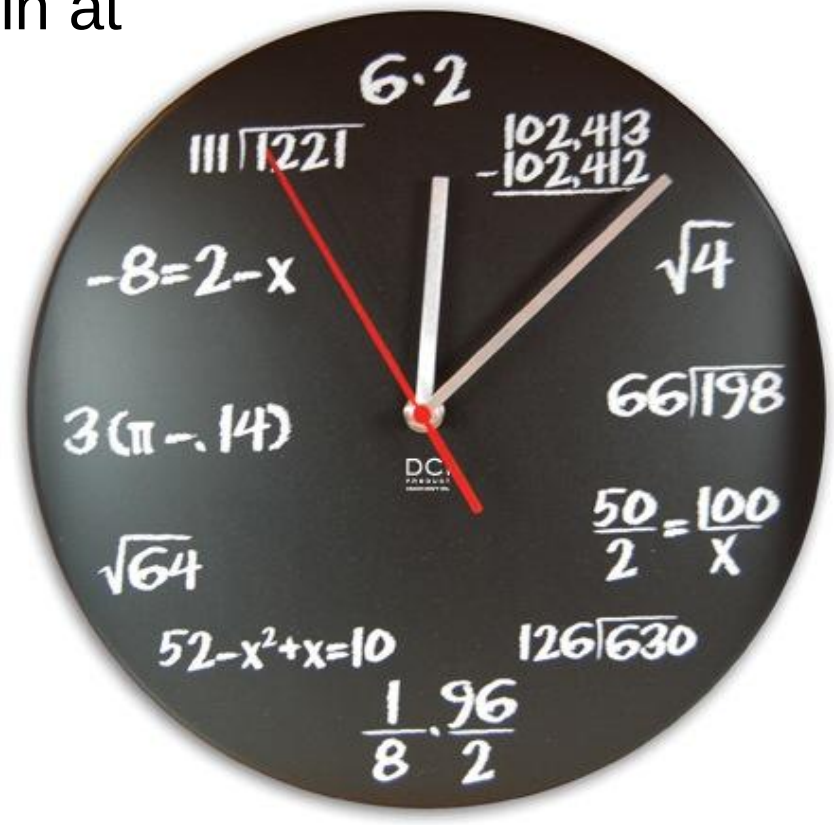
- Today's featured expert is Kureli Sankar
- Ask her questions now about common firewall issues

Kureli Sankar

Firewall Engineer, Cisco

Thank You for Joining Us Today

The Live Ask the Expert Event Will Begin at
10:00 am Pacific Time



Thank You for Joining Us Today

Before We Begin

- To submit a question just type your question below the slides and click submit.
- To see the questions with answers please click on the Refresh Q&A button below the slide window and use F11 to remove toolbars and enable a full screen view.
- If you can hear the music, your Flash player has been installed correctly
- If you cannot hear the music now, please download the latest version of Flash available in the Help section and reload the webcast console
- If you still cannot hear the music, please contact support@ciscolivevirtual.com

Thank You for Joining Us Today

Today’s presentation will include audience polling questions

We encourage you to participate!

Thank You for Joining Us Today

Downloading the Presentation

- If you would like a copy of the presentation slides, click the “Download Presentation” button below the slide window

Please Note

- To submit a question just type your question below the slides and click submit.
- To see the questions with answers please click on the Refresh Q&A button below the slide window and use F11 to remove toolbars and enable a full screen view.
- This event is fully streamed; the audio is heard via your Flash media player
- You can download today's presentation by clicking on the "Download Presentation" button below this slide window
- To take part in the polls, please disable your pop-up blockers during the event so you may see and answer the questions

Troubleshooting Common Firewall Problems

Poonguzhali Sankar

Cisco Support Community - Ask the Expert

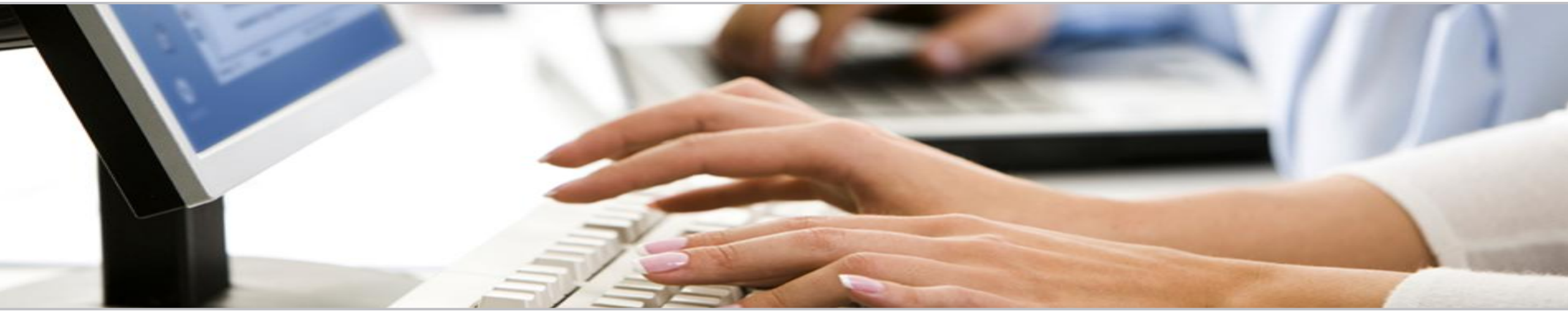
- Today's featured expert is Kureli Sankar
- Ask her questions now about

Kureli Sankar

Firewall Engineer, Cisco

Presentation_ID

Cisco Confidential
Cisco Confidential



Submit Your Questions Now

Use the Submit Text box Below the Slide Window. View Answers by Clicking on the “Refresh” Button

Poll Question

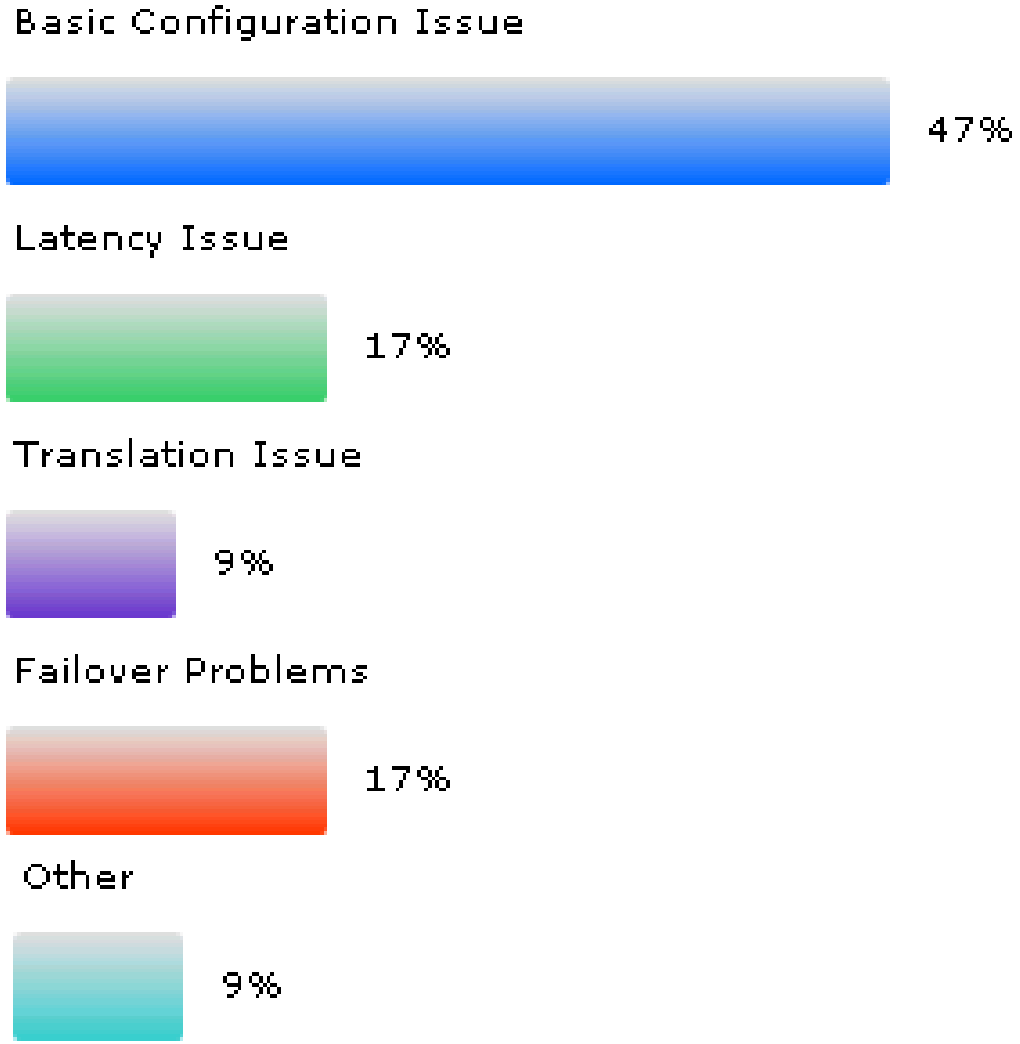
What is the most common firewall issue that you have encountered in the last few months?

- Basic Configuration Issue
- Latency Issue
- Translation Issue
- Failover Problems
- Other

Submit

Poll Response

What is the most common firewall issue that you have encountered in the last few months?



Agenda

- Basic Firewall configuration
  - Allowing outbound traffic through the firewall
  - Allowing inbound traffic to web server or e-mail server
- Latency issues while accessing certain websites
- Translation problems
  - Barracuda receives e-mail from the internet destined to the MX record
  - Exchange sends e-mail out (not looking like the MX record)
  - Both of the above should use the same public IP (MX record) address
- Replacing primary unit in a failover pair wipes configuration
- Identifying translation problems—Traffic breaks: Clear local resolves the problem temporarily
- How to identify what is causing high CPU

Basic Firewall Configuration

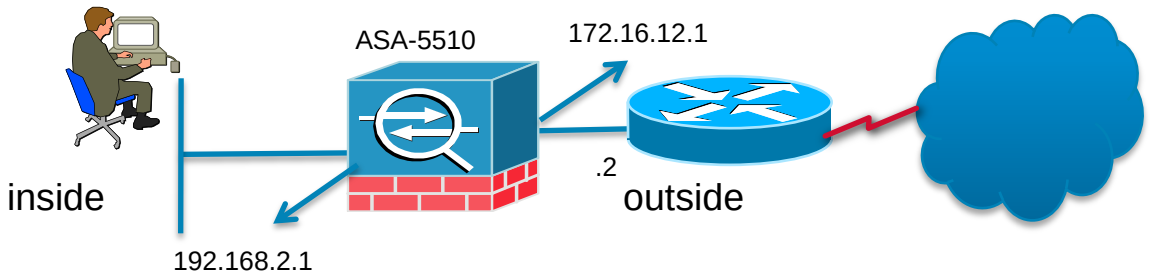
Allowing Outbound Traffic

- Inside interface with nameif, IP address, security level, and no shut

```
ASA(config)#interface E0/0
ASA(config)#nameif inside
ASA(config)#security-level 100
ASA(config)#ip address 192.168.2.1 255.255.255.0
ASA(config)#no shut
```

- Outside interface with nameif, ip address, security level, and no shut

```
ASA(config)#interface E0/1
ASA(config)#nameif outside
ASA(config)#security-level 0
ASA(config)#ip address 172.16.12.1
255.255.255.0
ASA(config)#no shut
```



- Route (default route)

```
ASA(config)#route outside 0.0.0.0  0.0.0.0 172.16.12.2
```

Basic Firewall Configuration

Allowing Outbound Traffic (Cont.)

- Translation

```
ASA(config)#nat (inside) 1 192.168.2.0 255.255.255.0
ASA(config)#global (outside) 1 interface
```

- Permission

  Permission is optional from high to low security; this is true only in case of ASA/PIX. In case of FWSM irrespective of the security level, access-list is required on the interface for traffic to flow through the firewall

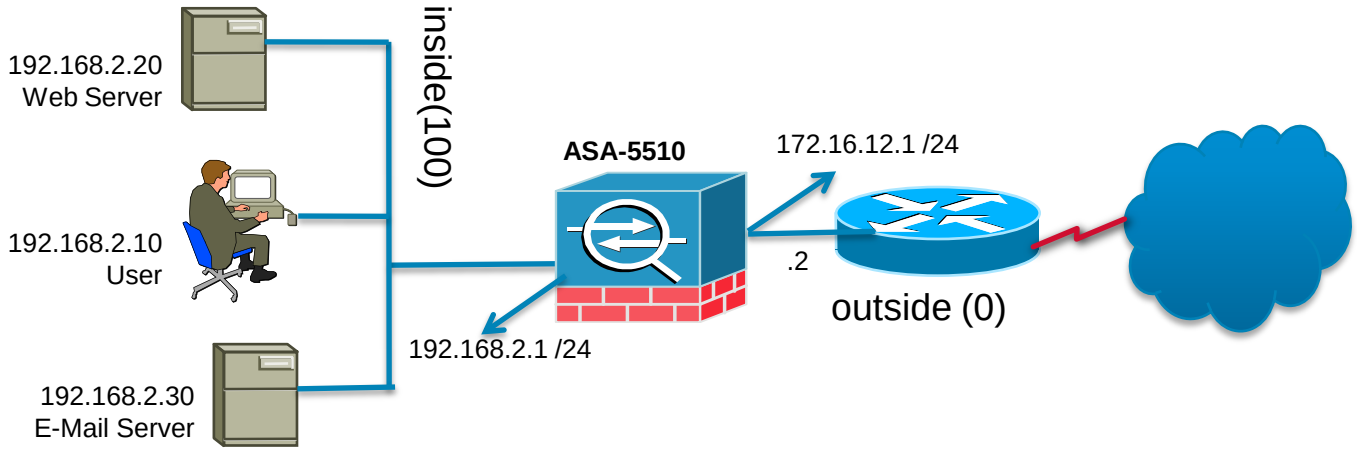
```
ASA(config)#access-list outbound permit tcp any any eq 80
ASA(config)#access-list outbound permit udp any any eq 53
ASA(config)#access-list outbound permit tcp any any eq 443

ASA(config)#access-group outbound in interface inside
```

- Remember—we need RTP for any flow to work through the firewall
- **R**oute **T**ranslation and **P**ermission

Basic Firewall Configuration

Allowing Inbound Traffic



- Configure static 1-1 NAT or static PAT for inbound traffic from low to high security

```
static NAT:
ASA(config)#static (inside,outside) 172.16.12.30 192.168.2.30
ASA(config)#static (inside,outside) 172.16.12.20 192.168.2.20
or
static PAT:
ASA(config)#static (inside,outside) tcp interface 25 192.168.2.30 25
ASA(config)#static (inside,outside) tcp interface 80 192.168.2.20 80
```

Basic Firewall Configuration

Allowing Inbound Traffic (Cont.)

- Allow permission via access-list applied on the outside

static NAT:

```
ASA(config)#access-list inbound permit tcp any host 172.16.12.20 eq 80
ASA(config)#access-list inbound permit tcp any host 172.16.12.30 eq 25

ASA(config)#access-group inbound in interface outside
```

Static PAT:

```
ASA(config)#access-list inbound permit tcp any interface outside eq 80
ASA(config)#access-list inbound permit tcp any interface outside eq 25

ASA(config)#access-group inbound in interface outside
```

Latency Issues While Accessing Certain Websites

PC on the outside of the firewall show the same symptom?

1. http inspection—is it enabled?
2. Policing—is it enabled?
3. Content filtering—is it enabled?
4. Threat Detection—is it enabled?
5. Are the interfaces running clean?
6. Does nat/global fail but static 1–1 work?
7. Translated IP address that your PC looks like on the internet may not be allowed by the remote web server
8. MSS issues
9. Load balancing on the ISP side
10. CNAME and PTR record for the global IP address
11. Translated address listed in http://www.spamhaus.org/?

Latency Issues While Accessing Certain Websites (Cont.)

PC on the outside of the firewall show the same symptom?

1. What IP address is configured on the PC?
2. What DNS is configured on the PC?
3. Is this the same PC that had the trouble when it was on the inside?
4. If this IP address works, then use this same IP address to translate the host on the inside and see if it can load the same page
5. Make sure to clear arp so, the router upstream will learn the changed mac address

Latency Issues While Accessing Certain Websites (Cont.)

http inspection—is it enabled? How do we verify that?

- Ping the website and get the IP address it resolves to
- Issue the following command:

```
ASA#show service-policy flow tcp host 192.168.2.10 host 72.163.4.161 eq 80

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect http
```

Latency Issues While Accessing Certain Websites (Cont.)

- Remove http inspection from the policy-map and try the website again

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)#no ins http

ASA#clear-local 192.168.2.10
```

- Issue “clear local” for the client’s ip address and test loading the website again

Latency Issues While Accessing Certain Websites (Cont.)

Policing—Is it enabled?

```
ASA#show service-policy flow tcp host 192.168.2.10 host 72.163.4.161 eq 80
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect http
Class-map: class-default
      Match: any
      Action:
        Output flow:
Interface outside:
  Service-policy: police-traffic
    Class-map: http-class
      Match: port tcp eq www
      Action:
        Output flow:  police output 250000
    Class-map: class-default
      Match: any
```

Latency Issues While Accessing Certain Websites (Cont.)

- Disable policing and see if the page can be loaded as expected

```
ASA#sh run policy-map
policy-map police-traffic
 class http-class
  police output 250000

ASA(config)# policy-map police-traffic
ASA(config-pmap)# class http-class
ASA(config-pmap-c)#no police output 250000

ASA#clear-local 192.168.2.10
```

- Once clear local is issued for the test host try the same flow again

Latency Issues While Accessing Certain Websites (Cont.)

- Make sure there is no CSC module or any other content scanning device like Websense, N2H2 scanning the http traffic and dropping/resetting the connection and threat detection if they are enabled

Content filtering:

ASA#sh run url-server
ASA#sh run filter

Threat:

ASA#sh run threat

- If the above are enabled disable them one at a time—issue “no” in front of the lines under “Conf t”; test the flow again once clear local is issued for the test host IP address

Latency Issues While Accessing Certain Websites (Cont.)

Are the interfaces running clean?

```
ASA# sh int | i error
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 output errors, 0 collisions, 0 interface resets
```

- If the interfaces do show errors then find out which interface in particular ("show interface" for individual interfaces) and change the port on the switch or replace the ethernet cable

```
105440947 packets input, 2283932667 bytes, 0 no buffer
   Received 1161 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   0 input packets with dribble condition detected
   132064543 packets output, 671431731 bytes, 0 underruns
   27627 output errors, 22353 collisions, 3 interface resets
   0 babbles, 27627 late collision, 66314 deferred
   0 lost carrier, 0 no carrier, 0 PAUSE output
   0 output buffer failures, 0 output buffers swapped out
```

Latency Issues While Accessing Certain Websites (Cont.)

Does nat/global fail but static 1–1 work?

- From the number of connections arriving from a certain IP address the remote web server may appear to be blocking PAT while allowing static (1–1)
- PAT will show many connections arriving from a single IP address while static 1–1 will only show very few connections arriving from a single IP address

Latency Issues While Accessing Certain Websites (Cont.)

Translated address may be denied access

- The remote websites may not allow certain IP addresses to access their website
- If there is another IP address available, then translate the client PC to look like a new IP address and see if the same page would load
- Issue "clear xlate x.x.x.x" where x.x.x.x is the client's inside IP address so, the client can go out looking like the newly translated IP address
- Issue "sh xlate debug | i x.x.x.x" and make sure the client is indeed getting translated properly

Latency Issues While Accessing Certain Websites (Cont.)

MSS issues

- In a normal TCP session, the client sends a SYN packet to the server, with the MSS included within the TCP options of the SYN packet; the server, upon receipt of the SYN packet, should recognize the MSS value sent by the client and then send its own MSS value in the SYN-ACK packet—once both the client and the server are aware of each other's MSS, neither peer should send a packet to the other that is greater than that peer's MSS
- Verify from syslogs that the flow is not failing due to MSS issues
- %ASA-4-419001: Dropping TCP packet from outside:172.18.25.60/443 to inside:10.110.61.153/61312, reason: MSS exceeded, MSS 1380, data 1460
- Please read about it here and apply the fix for it if this is the case

  http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a00804c8b9f.shtml

Latency Issues While Accessing Certain Websites (Cont.)

Load balancing on the ISP side

- ISP may have implemented load balancing based on source and destination IP address
- Depending on the source IP address that the inside client is getting translated to the ISP may carry the flow via a completely different path than another IP address which might work

Latency Issues While Accessing Certain Websites (Cont.)

CNAME and PTR record for the global IP address

- Some websites may verify that the IP address trying to load their page is a legitimate address by trying a reverse lookup on the IP address to make sure it has a name associated with it; make sure the global IP (PAT address) that you are trying to translate the inside client to, has a name CNAME and PRT record created in the DNS zone file for your domain name like http://global.mycompany.com

Latency Issues While Accessing Certain Websites (Cont.)

Translated address listed in http://www.spamhaus.org/?

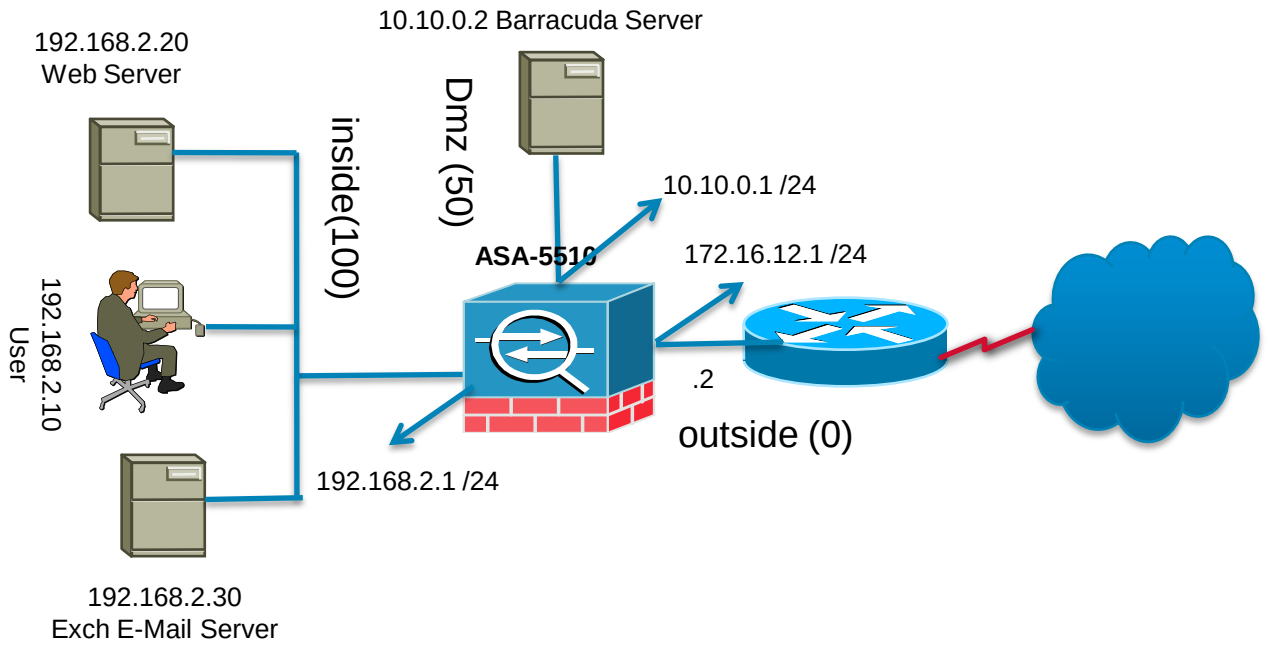
- Last but not least, make sure the translated address is not listed in http://www.spamhaus.org/
- mod_spamhaus is an Apache module that use DNSBL in order to block spam relay via web forms, preventing URL injection, block http DDoS attacks from bots and generally protecting your web service denying access to a known bad IP address

  http://sourceforge.net/projects/mod-spamhaus/

Translation Problems

```
nat (inside) 1 192.168.2.0 255.255.255.0
global (outside) 1 interface

static (dmz,outside) tcp 172.16.12.40 25 10.10.0.2 25
```



- With the above configuration Barracuda server receives e-mail (sent to the MX record) from the internet, cleans it up and sends it to the exchange server on the inside
- Exchange server sends e-mail out directly
- Now, the problem is Exchange server is not looking like the MX record IP address when sending e-mail out; how do we solve this problem?

Translation Problems

Answer

- New translation for Exchange server

```
nat (inside) 2 192.168.2.30 255.255.255.255
global (outside) 2 172.16.12.40
```

- Existing translation for Barracuda server

```
static (dmz,outside) tcp 172.16.12.40 25 10.10.0.2 25
```

- That would do it

Poll Question

Which firewall device(s) do you have installed in your network?

- Cisco PIX 500 Series Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Catalyst 6500 Series Firewall Services Module
- A combination of the above
- Other

Submit

Poll Response

Which firewall device(s) do you have installed in your network?

Cisco PIX 500 Series Security Appliances

6%

Cisco ASA 5500 Series Adaptive Security Appliance

58%

Cisco Catalyst 6500 Series Firewall Services Module

1%

A combination of the above

33%

Other

3%

Replacing Primary Unit in a Failover Pair Wipes Configuration—Sends Blank Config

Typical reason that could end up in this situation

1. Primary unit fails and an RMA is filed
2. Secondary meanwhile takes over as active
3. Upon receiving the primary unit the code is updated to match existing secondary/active unit
4. Copy and paste the failover lines onto the primary
5. Enable failover on the primary
6. At this point due to license mismatch failover gets disabled as expected
7. Later necessary license gets added on to the primary unit
8. Failover enabled on the primary which receives “No response from mate”
9. Then failover is disabled on the primary
10. Failover enabled on the secondary and then on the primary
11. Primary ends up active and sends blank config to secondary

Replacing Primary Unit in a Failover Pair Wipes Configuration—Sends Blank Config (Cont.)

The reason why the above steps failed is because:

1. Failover was enabled on both secondary and primary almost at the same time
2. The rule is: if the primary unit comes up during the negotiation process the primary unit becomes active

    Last Failover at: 03:50:06 UTC Mar 19 2010

    This host: Secondary—Negotiation

        Active time: 0 (sec)

    Other host: Primary—Not Detected

        Active time: 0 (sec)

3. Once the RMA-ed primary unit comes up as active, it sends Blank config to the secondary unit

Replacing Primary Unit in a Failover Pair Wipes Configuration—Sends Blank Config (Cont.)

Steps to replace a failed primary unit

1. Make sure “sh version” looks identical between the two units
2. The above includes: license and code version
3. Make sure the “sh fail” output on the existing sec/act unit shows expected status (this output is from a transparent firewall)

This host: Secondary—Active

Active time: 4 (sec)
slot 0: ASA5550 hw/sw rev (1.0/8.2(2)) status (Up Sys)
Interface inside (10.4.224.7): Normal (Waiting)
Interface Outside (10.4.224.7): Normal (Waiting)
slot 1: ASA-SSM-4GE-INC hw/sw rev (1.0/1.0(0)10) status (Up)

Other host: Primary—Failed

Active time: 0 (sec)
slot 0: empty
Interface inside (10.4.224.8): Unknown (Waiting)
Interface Outside (10.4.224.8): Unknown (Waiting)
slot 1: empty

Replacing Primary Unit in a Failover Pair Wipes Configuration—Sends Blank Config (Cont.)

4. Now, copy and paste the failover lines onto the primary unit

   failover lan unit **primary**
   failover lan interface FAILOVER GigabitEthernet0/3.2624
   failover polltime unit msec 200 holdtime msec 800
   failover polltime interface msec 500 holdtime 5
   failover replication http
   failover link STATE GigabitEthernet0/2.2623
   failover interface ip FAILOVER 10.10.11.37 255.255.255.252 standby 10.10.11.38
   failover interface ip STATE 10.10.11.41 255.255.255.252 standby 10.10.11.42

5. Now enable failover on this new unit with the command "failover"
6. The newly (failover) enabled primary unit will automatically detect the existing sec/act unit and will sync up with it

   ASA(config)# failover
   Detected an **Active mate**
   Beginning configuration replication from mate

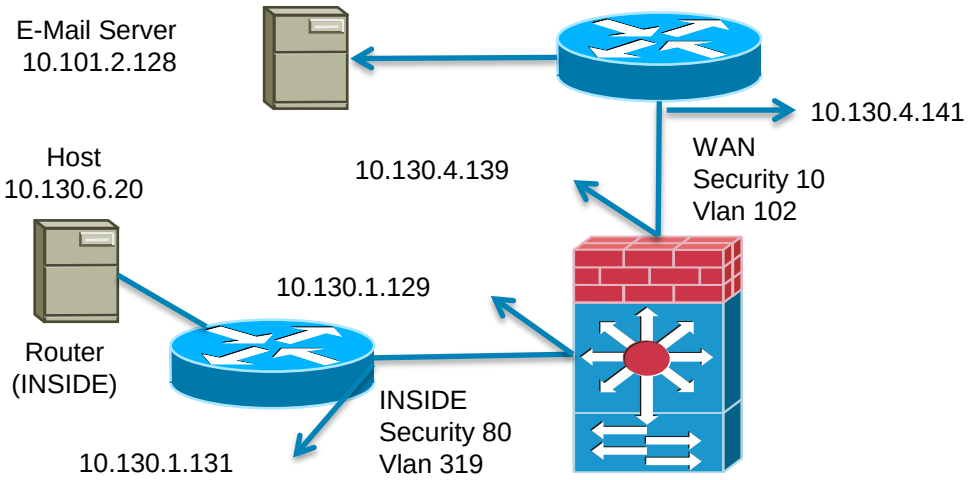
7. "sh fail" status on both units should the secondary unit as active and the primary unit as standby

Replacing Primary Unit in a Failover Pair Wipes Configuration—Sends Blank Config (Cont.)

Take Away

- When ever a unit is replaced whether it is primary or secondary make sure the sitting unit's "sh fail" shows "this unit active" and "other unit failed" before introducing the other unit and enabling failover on it

Identifying Translation Problems—Traffic Breaks: "Clear Local" Resolves the Problem Temporarily



Firewall Services Module

- Relevant config:

  interface Vlan102

  nameif WAN

  security-level 10

  ip address 10.130.4.139 255.255.255.248

  interface Vlan319

  nameif INSIDE

  security-level 80

  ip address 10.130.1.129 255.255.255.248

  no nat-control

  route INSIDE10.130.6.0 255.255.255.0 10.130.1.131 1

  route WAN 10.101.0.0 255.255.0.0 10.130.4.141 1

  host (10.130.6.20)—Router—(80)INSIDE-Vlan319/—FWSM—/Vlan102-WAN(10)—(WAN router)—(10.101.2.128)

- The problem is that the host is unable to ping the e-mail server (10.101.2.128)
- How do we resolve this problem?

Identifying Translation Problems—Traffic Breaks: "Clear Local" Resolves the Problem Temporarily (Cont.)

Remember RTP? We are going to use it…

1. With the sh tech provided, we can quickly come up with a rough sketch
2. Verify that the e-mail server (WAN router) has a route to the host via the FWSM
3. Verify that the host (INSIDE router) has a route to the e-mail server via the FWSM

   Very common conception is that the FWSM is able to ping both the host and the e-mail server so, this flow should work; this is incorrect

   This is like saying I know how to get to the Mall from home… I also know how to get to the Movie theater from home; this does not mean you know how to get to the Mall from the Movie theater—or vice versa

   Assume that we have verified that the routes are in place what next?

Identifying Translation Problems—Traffic Breaks: "Clear Local" Resolves the Problem Temporarily (Cont.)

- Next is translation and no nat-control is configured—this means that the WAN router on the lower security level will be able to establish connection to the host on the higher security level without the need for a static translation; let us verify that

```
FWSM-1# sh xlate debug | i 10.130.6.20
NAT from INSIDE:10.130.6.20 to OUTSIDE:10.130.6.20 flags Ii idle 0:00:42 timeout 3:00:00 connections 4
NAT from INSIDE:10.130.6.20 to WAN:10.130.6.20 flags Ii idle 1:55:26 timeout 3:00:00 connections 0

FWSM-1# sh xlate detail | i 10.101.2.128
NAT from TEST:10.101.2.128 to INSIDE:10.101.2.128 flags Ii
```

- Do you see the problem? The "sh xlate detail shows as if the e-mail server lives off the TEST interface which is incorrect—it should be WAN instead

Identifying Translation Problems—Traffic Breaks: "Clear Local" Resolves the Problem Temporarily (Cont.)

- Now that we have identified the problem what do we need to do solve it so, this doesn't happen again
- There clearly appears to be some routing issue that is causing this; packets from the e-mail server arrive on the TEST interface sometimes which cause incorrect translation to be built—upon clearing the translation it starts to work until packets from the r-mail server start appearing again in the TEST interface
- Enable ip verify reverse path on the interface will stop this problem from happening again; this does not address the routing issue that is present in the network

```
FWSM(config)#ip verify reverse-path interface TEST
```

Identifying Translation Problems—Traffic Breaks: "Clear Local" Resolves the Problem Temporarily (Cont.)

To address the root cause we need to do the following:

- Packet capture on the TEST interface for all packets with the source address of the e-mail server 10.101.2.128
- Once we know the destination, then we can query the router off the TEST as well as the WAN interface and see what the next-hop is supposed to be for that destination when sourced from the e-mail server

How to Identify What Is Causing High CPU

- The difference between the two "**sh proc**" output collected one to two minutes apart would provide some clue as to what the CPU was doing at the time the outputs were taken
- The following usually spikes up the CPU:
  1. Attack due to malicious or infected hosts
  2. Layer 2 loop in the network
  3. Inspections
  4. Syslog server without the syslog services running
  5. Simply hitting the limitation of the unit

How to Identify What Is Causing High CPU (Cont.)

- How to identify infected hosts trying to establish too many tcp, udp or embryonic connections?

```
Firewall#sh local | i host|count/limit
local host: <10.10.57.5>,
    TCP flow count/limit = 16/unlimited
    TCP embryonic count to host = 93404
    UDP flow count/limit = 6/unlimited
local host: <10.10.57.251>,
    TCP flow count/limit = 53/unlimited
    TCP embryonic count to host = 140948
    UDP flow count/limit = 1/unlimited
```

- Embryonic connections are incomplete half-open connections

How to Identify What Is Causing High CPU (Cont.)

- Collect a blanket capture on the interfaces and see what traffic the firewall is seeing at the time of the problem
  - Configure capture:
    - ASA#cap capin interface inside match ip any any
    - ASA#cap capout interface outside match ip any any
  - View captures:
    - ASA#sh cap capin
    - ASA#sh cap capout
  - Save captures:
    - https://firewall_IP/capture/capin/pcap
    - https://firewall_IP/capture/capout/cap
  - Remove captures:
    - ASA#no cap capin
    - ASA#no cap capout

How to Identify What Is Causing High CPU (Cont.)

- Remove inspections to see if that would bring down the CPU
- Prior to doing that collect the output of the following command

  ASA#sh service-policy

- The above command will give an idea about all the inspection being used and the amount of packets each one has processed

How to Identify What Is Causing High CPU (Cont.)

- Let us say that the following is configured on the firewall:

```
logging enable
logging timestamp
logging trap debugging
logging host inside 192.168.2.2
```

- If the syslog service is not running on the host 192.168.2.2, it may send a port unreachable message which may reach the ASA and the ASA may in turn create a syslog for that message and send it back to the syslog server IP address which could cause the amount of syslog messages to grow exponentially causing high CPU

How to Identify What Is Causing High CPU (Cont.)

- If all options discussed have bee addressed and analyzed then it may just be that a hardware upgrade is in order

Poll Question

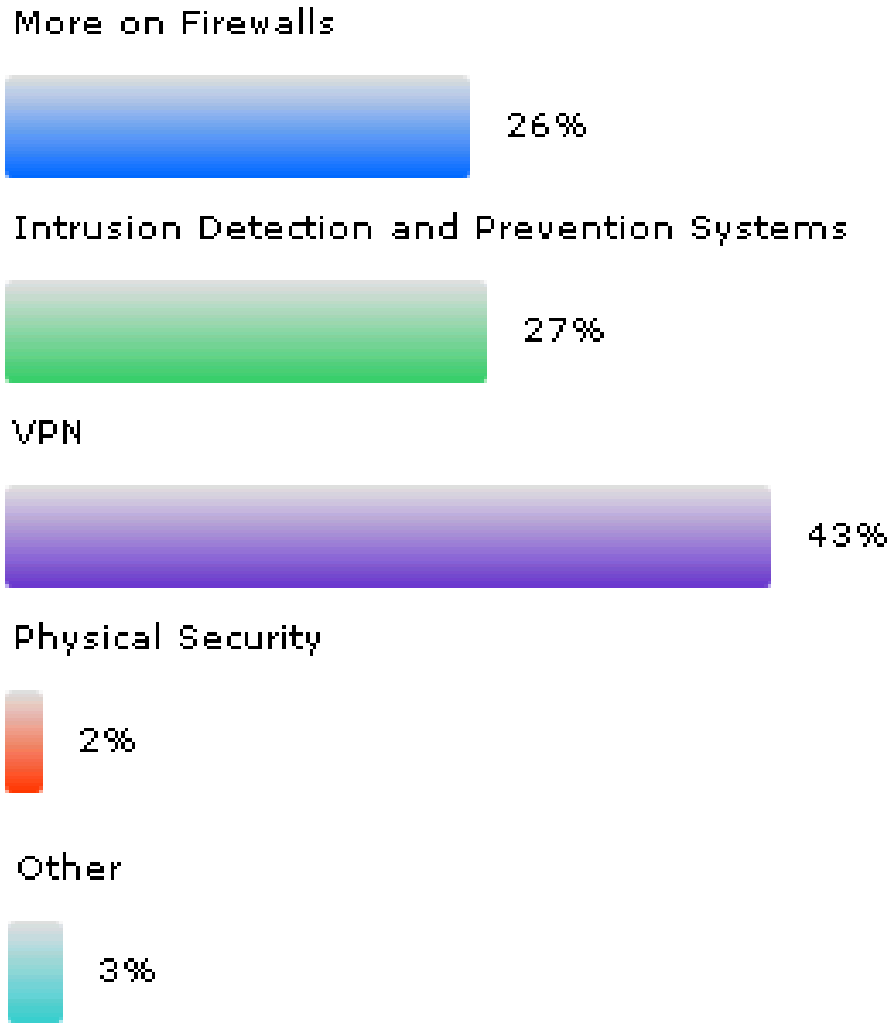
Which security topics would you like to see in a future Webcast?

- ○ More on Firewalls
- ○ Intrusion Detection and Prevention Systems
- ○ VPN
- ○ Physical Security
- ○ Other

Submit

Poll Response

Which security topics would you like to see in a future Webcast?



Submit Your Questions Now

Use the Submit Text Box Below the Slide Window. View Answers by Clicking on the “Refresh” Button

We Appreciate Your Feedback!

The first 10 listeners
who fill out an Evaluation
will receive a free:

$20 USD
Amazon Gift Certificate

To complete the evaluation, please click on Evaluation button under the slides.

Q&A

Some Useful FWSM Links

- FWSM Documentation:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

- ASA/PIX/FWSM—Packet Capture Using CLI and ASDM:

  http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a0080a9edd6.shtml

Some Useful ASA Links

- ASA Release Notes:

  http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html

- ASA Command Reference:

  http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html

- ASA Configuration Guide:

  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

- ASA Syslog Guide:

  http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html

- Bug Tool-Kit:

  http://www.cisco.com/pcgi-bin/Support/Bugtool/home.pl

Post Questions on Our Forum Here:

https://supportforums.cisco.com/community/netpro/security/firewall

Thank You for Your Time

Please Take a Moment to Complete the Evaluation


CISCO