Cisco live!

January 29 – February 2, 2018 · Barcelona

BRKSEC-2463

“Why is performance testing of security devices so hard?”

Charlie Stokes

Technical Marketing Engineer

Cisco live!

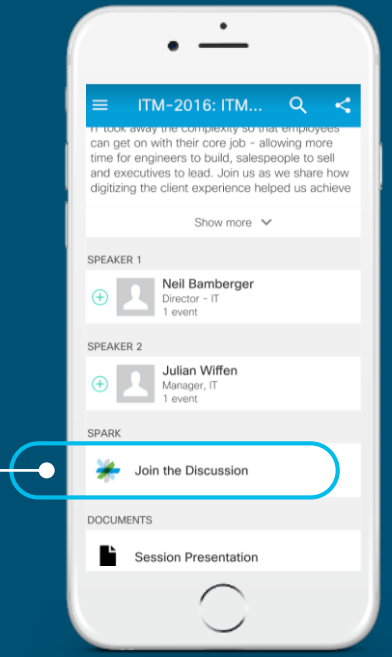
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space



cs.co/ciscolivebot#TECSEC-2463

Agenda

- Introduction
  - What is the performance envelope? What factors influence it? How do choices made in testing influence the results you get?
- Data sheets vs real world performance
- Testing in progress
- Performance Challenges
- Cloud Testing: Private and Public
- Tricks and tips and other types of Testing
- Wrap up

Who am I?

Came to Cisco with the Wheelgroup in 1998 which brought IDS to Cisco.

Spent 2 years in the TAC supporting security products (Go PIX and NetRanger!)

My original badge!

My original picture from so long ago I had hair!

Spent the better part of the next 18 years in Cisco's security business groups as a TME supporting IDS/IPS products and firewalls, and now Firepower products including Firepower Threat Defense.

This included creating testing to compare competitor's products, helping design and create tests for our own datasheets, participating in third party performance testing, and in general understanding how devices perform and how different environments effect the performance of security devices.

Session Guidelines

1. I speak Texan!
   - Tell me to slow down if I start to talk fast, and I probably will!
2. This is “Y’ALL’s” session. *(That means “you all’s” for those who don’t speak the above)*
   - I would like to answer ALL questions
     (within reason, understanding session time constraints and that everybody has their own questions, and also that I may not know the answer!)
3. Lets make sure we all have a rewarding time!
4. If you have a question I can’t or don’t answer, send me an email: cstokes@cisco.com

Introduction

What is performance testing and the “performance envelope”?

PERFORMANCE ENVELOPE

The variation of aircraft performance parameters such as climb rate, acceleration capability, range vary significantly based on aircraft speed and altitude. To correctly determine the optimum operation of the aircraft, the performance measures should be mapped over the full operating range of the aircraft.

from “Aerodynamics for Students”

What is performance testing and the “performance envelope”?

PERFORMANCE ENVELOPE

The variation of aircraft performance parameters such as climb rate, acceleration capability, range vary significantly based on aircraft speed and altitude. To correctly determine the optimum operation of the aircraft, the performance measures should be mapped over the full operating range of the aircraft.

from “Aerodynamics for Students”

What is performance testing and the “performance envelope”?

PERFORMANCE ENVELOPE

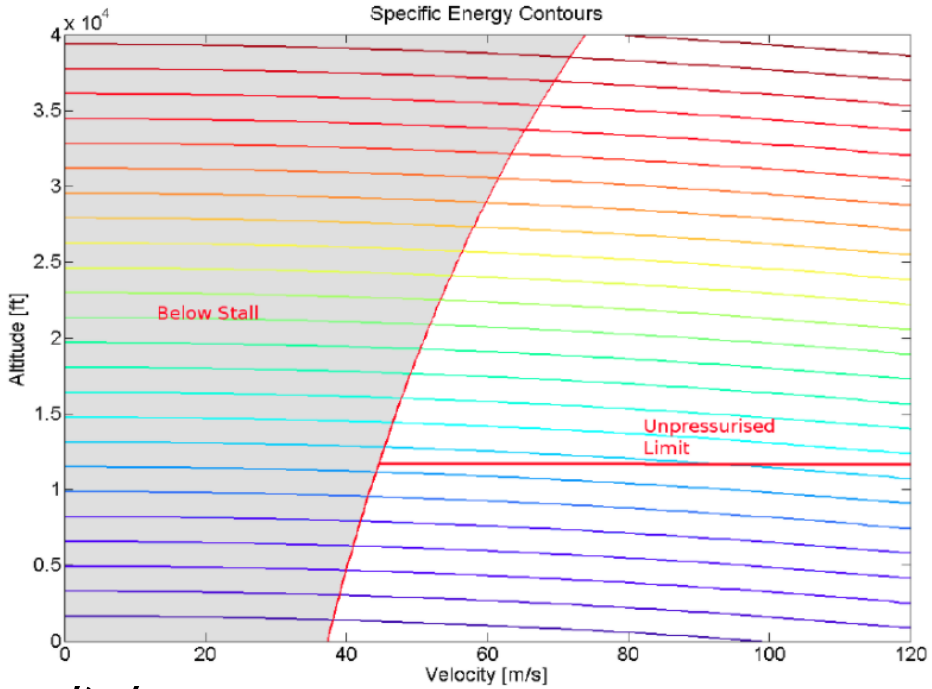
The variation of aircraft performance parameters such as climb rate, acceleration capability, range vary significantly based on aircraft speed and altitude.

“To correctly determine the optimum operation of the aircraft, the performance measures should be mapped over the full operating range of the aircraft.”

from “Aerodynamics for Students”

What is performance testing and the “performance envelope”?

Similarly, an envelope for specific energy can be produced that maps lines along which the aircraft can move with any change of thrust setting and hence with no requirement for excess power. The aircraft can trade potential energy (height) for kinetic energy (speed).

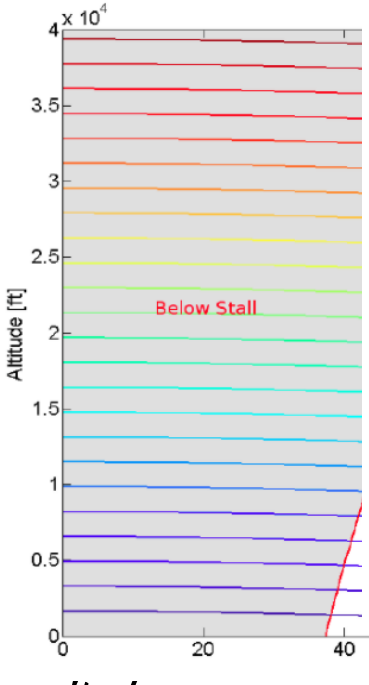


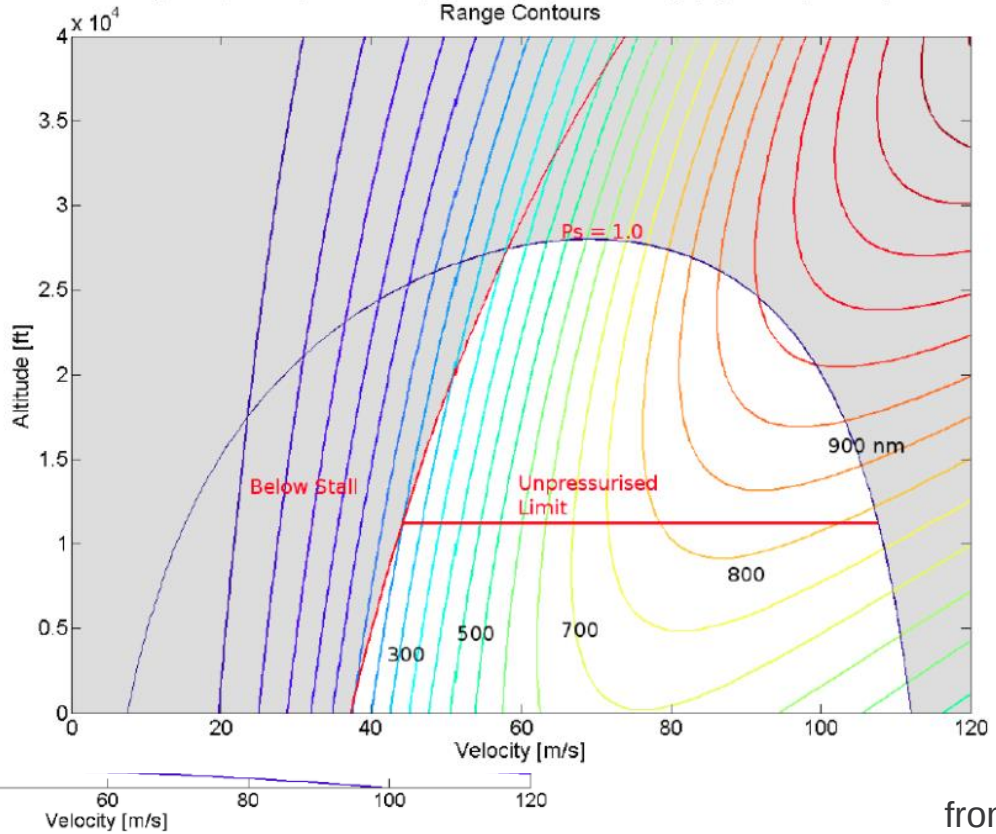
from “Aerodynamics for Students”

What is performance testing and the “performance envelope”?

As well a maximum range envelope can be produced that maps the value of best achievable range (km) over the operational space.

Similarly, an envelope for specific energy can be produc
hence with no requirement for excess power. The aircrat

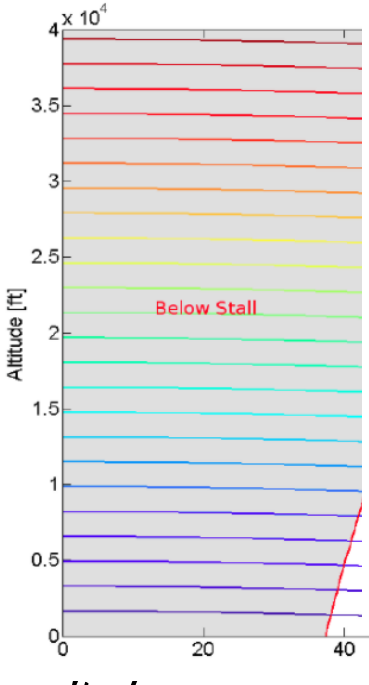




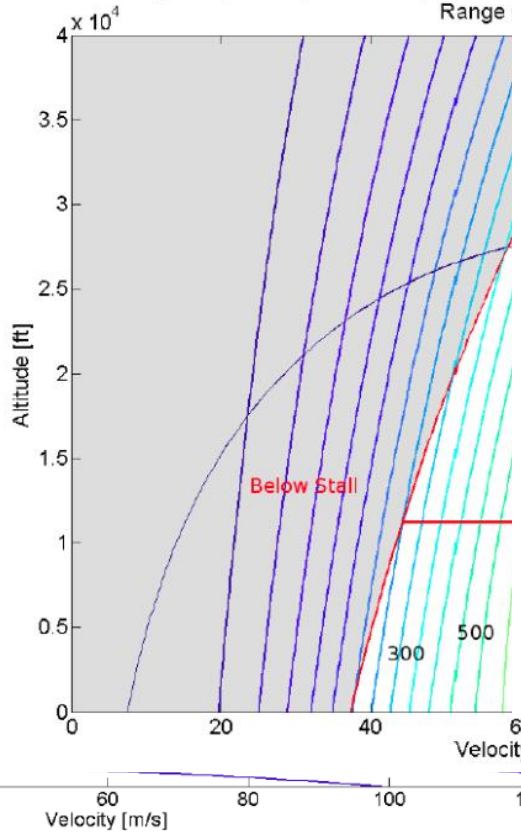
from “Aerodynamics for Students”

What is performance testing and the “performance envelope”?

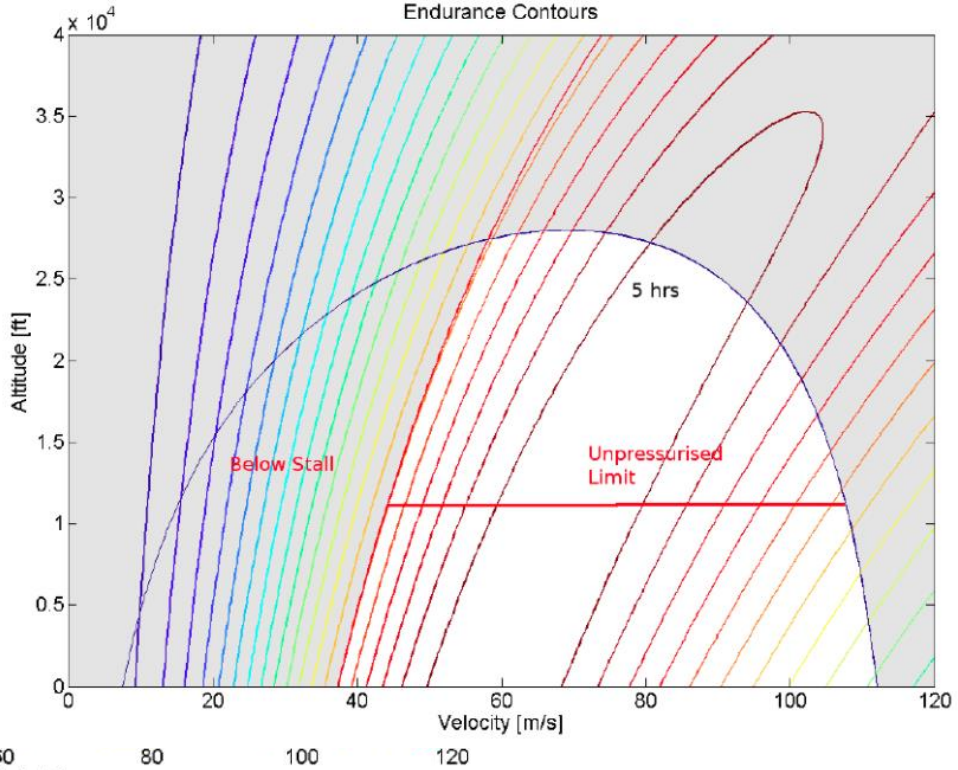
Similarly, an envelope for specific energy can be produc
hence with no requirement for excess power. The aircra



As well a maximum range envelope can be produced that maps the value



And finally an endurance envelope,



from “Aerodynamics for Students”

What is performance testing and the “performance envelope”?

- When you buy a car, how do you compare two different models?
  - Performance: Horsepower, Torque, 0-60, 0-100, quarter mile (402.336 meters!)
  - Efficiency: Miles per gallon (or L / 100 km)
  - Capabilities: Seats, Carrying capacity, Towing Capacity

What would happen if one car gave you their performance results in totally different metrics than another? It might look like a Lamborghini vs a farm truck racing.

What is performance testing and the “performance envelope”?

What is performance testing and the “performance envelope”?

What is performance testing and the “performance envelope”?

Security devices have their own metrics that define their ability to perform a job.

Characteristics on the NGFW “Performance Envelope”:

- Traffic being inspected (what is going through the box)
- Work being performed (what features are enabled)
- Configuration applied (how the box is handling the traffic)

What is performance testing and the “performance envelope”?

Characteristics on the NGFW “Performance Envelope”:

- **Traffic being inspected** (what is going through the box) : 7 or more variables
  - Numbers of connections per second to track (Conns/Sec)
  - Total numbers of flows active at any one time (Max/Conns)
  - Numbers of clients and servers active
  - Type of traffic (what protocols and in what percentages)
  - File Policy: are the files known or unknown, size of files inspected
  - Specifics of each protocol:
    - HTTP connection with one transaction using an 11K object
    - Average packet size 450 byte for the connection
  - Test specific conditions: In L2 Transparent mode, how many MAC addresses are tracked?
- Work being performed (what features are enabled)
- Configuration applied (how the box is handling the traffic)

What is performance testing and the “performance envelope”?

Characteristics on the NGFW “Performance Envelope”:

- Traffic being inspected (what is going through the box)
- **Work being performed** (what features are enabled) : 10 or more features
  - Basic Firewalling features: ACL, NAT
  - Network Discovery: Applications, Users, Hosts in the test traffic
  - IPS: rule applicability to traffic type
  - Application control: looking for the protocol running on the test traffic
  - File Policy: with policy looking for files in the test traffic
  - DNS and URL policy
  - SSL Decryption policy
  - Logging: What events need to be logged and how often does that occur
- Configuration applied (how the box is handling the traffic)

What is performance testing and the “performance envelope”?

Characteristics on the NGFW “Performance Envelope”:

- Traffic being inspected (what is going through the box)
- Work being performed (what features are enabled)
- **Configuration applied** (changing how the box handles the traffic) : 10 or more options
  - Deployment mode: L3 routed vs L2 transparent vs NGIPS vs IDS
  - Basic Firewalling features: large dynamic routing tables or huge ARP tables
  - IPS: Numbers of rules, custom rules, multiple policies
  - Network analysis policy: inspection depth, preprocessor settings
  - File Policy: are the files known or unknown, size of files inspected
  - SSL Decryption policy: Known Key or MITM?
  - Dynamic cut-through: Bypassing inspection for some traffic or at a certain point in the flow

What is performance testing and the “performance envelope”?

“To correctly determine the optimum operation of the aircraft, the performance measures should be mapped over the full operating range of the aircraft.”

To correctly determine the optimum operation of a security device, the performance measures should be mapped over the full operating range of the device.

Due to the complexity of more than 26 variables, options and features, and the time and cost impacts resulting from all those permutations (67 million if every variable was binary!), nobody can test every performance variation.

And changing just a few of any of these can change the test results drastically!

IPS Throughput [1] (HTTP / Enterprise Mix)	82 / 32 Gbps

IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

What does this mean for a consumer?

Changing the traffic profile from HTTP to an Enterprise Mix and running it through the IPS engine:

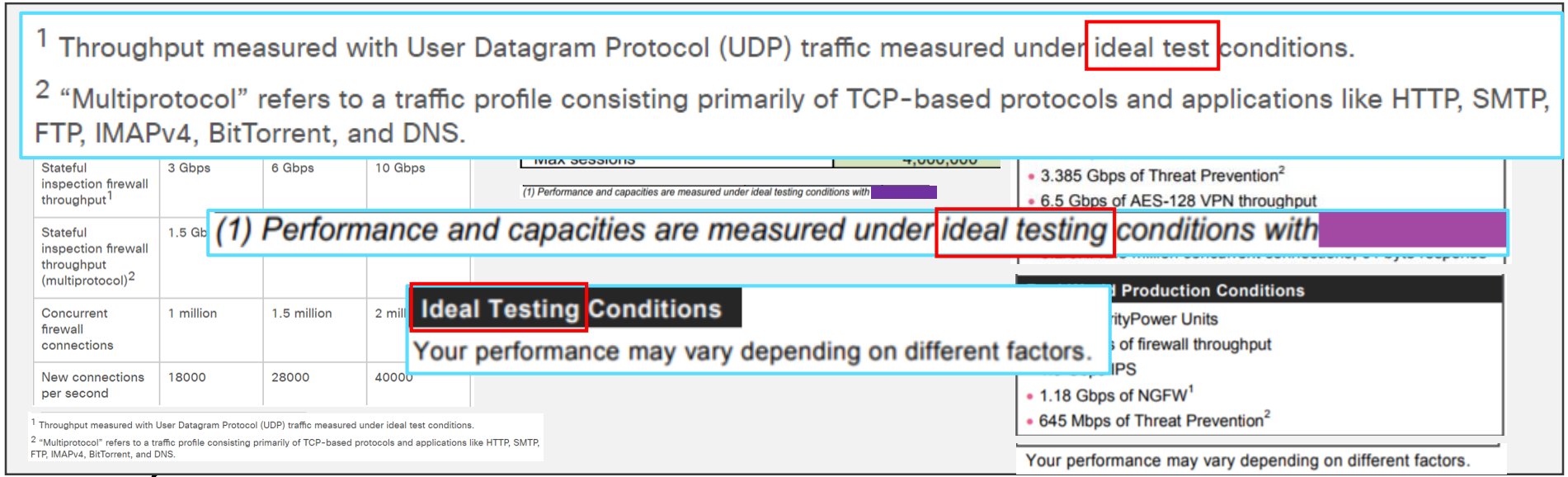
What other difference is contributing to the change in measured performance?

Data Sheets
What are they good for?

Data Sheets: What are they good for?

Or more precisely, what are they used for?

Example portions of 3 Security Product Datasheets



So what can you use a datasheet for?

(or what not to use them for!)

IDEAL
or
Perfect

≠ Real World

What makes an ideal test condition?

Depends on the test, but changing traffic, features, and configuration is a start.

- Throughput get maximized when other work get minimized:
  - UDP is easier than TCP: Less state to track
  - Largest possible packet size (Jumbo frames generally)
    - Fewer connections to pass the same amount of data
    - Fewer packet headers to parse
- Max connections:
  - Open lots of connections
  - Pass little to no data
  - Don’t close the connections
- Max new connections per second:
  - Use lots of very small connections
  - Pass little to no data
  - Close the connections as fast as possible

Is there such a thing as ‘Real World’ performance tests?

- Describe the goals of a test to simulate real world conditions
  - Force the device to pass traffic through it’s entire chain of inspection (exercise the CPU’s)
  - Don’t allow the device to bypass inspection
    - Use traffic that the device has rules to inspect for or detect
    - Enable the features that will be used in production
    - Make sure the configuration matches the required security policy (inspecting HTTP return traffic)
  - The test should be reasonably easy to describe. Complex tests are generally harder to diagnose issues and troubleshoot problems, and much harder to replicate.
  - Standards based tests can help if they are well documented and easy to replicate. But if not, they can just obfuscate and confuse.

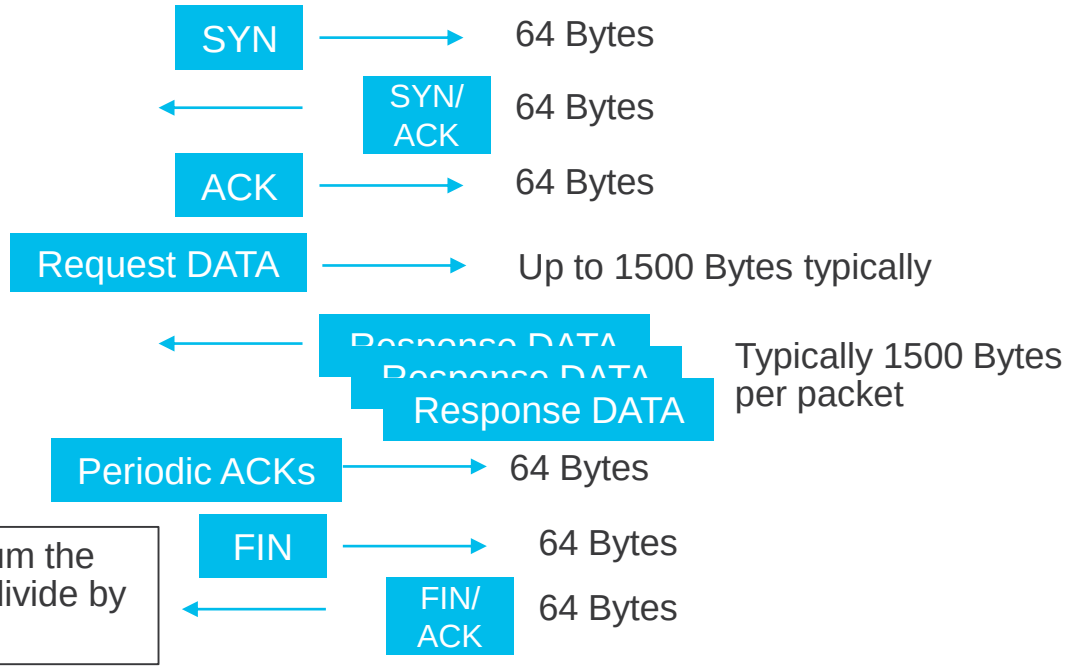
Why is simple HTTP a good baseline “real world” test?

IPS industry vs Firewall industry testing

What is a 450 byte average packet size HTTP test?

(Hint: it is not the size of each packet!)

Typical TCP/HTTP flow:



Average packet size = Sum the size of each packet and divide by the number of packets

Why is Multiprotocol difficult to use for testing and comparing?

Do you know the specifics of each test?

- Is a test called HTTP an easy test or a hard test for security devices? Can you tell?
- What if I said 450 byte average packets size HTTP or 1024 byte average packet size HTTP? Which one is easier?

Using that, tell me if this test is easy or hard?

- HTTP 44%, Bittorrent 22%, IMAP v4 16%, FTP 9%, SMTP 9%

This is Cisco's generic Multiprotocol test and is very similar to all the Internet multiprotocol standards.

- For you as the datasheet reader, is that an easy or hard test?

Table 3. ASA Performance and Capabilities on Firepower Appliances

Features	Cisco Firepower Appliance Model		
	2110	2120	2130
Stateful inspection firewall throughput[1]	3 Gbps	6 Gbps	10 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	1.5 Gbps	3 Gbps	5 Gbps
Concurrent firewall connections	1 million	1.5 million	2 million
New connections per second	18000	28000	40000

[1] Throughput measured with User Datagram Protocol (UDP) traffic measured under ideal test conditions.

[2] "Multiprotocol" refers to a traffic profile consisting primarily of TCP-based protocols and applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

Data Sheet Numbers: So what are they good for?

- They are used to provide comparison to other vendors data sheets: Orange to Orange comparisons.
- Make sure you are comparing similar numbers: Ideal numbers to ideal numbers or “real world” to “real world”.

- This Cisco FTD datasheet is not referencing “ideal test conditions” and instead calls out the features enabled and the specific test being run, in this case 1024 byte average packet size HTTP.

Table 2. Performance Specifications and Feature Highlights for Physical and Virtual Appliances with the Cisco Firepower Threat Defense Image

Features	Cisco Firepower Model
	4150
Throughput: FW + AVC	30 Gbps
Throughput: AVC + IPS	24 Gbps
Maximum concurrent sessions, with AVC	30 million
Maximum new connections per second, with AVC	200,000

Note: Throughput assumes HTTP sessions with an average packet size of 1024 bytes.

https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html

Testing


CAUTION
TESTING
IN PROGRESS
DO NOT DISTURB
CUIDADO
EXAMENES
EN PROGRESO
NO MOLESTAR

So you decided to go down the path of testing yourself?

What were you thinking? No, I'm not kidding…….

What factors go into choosing the best test (or most applicable) tool?

- Cost will always be an overriding factor. Commercial test tools are expensive!
- What is available to your organization? Is there already an existing test tool available?
- Performance: It doesn't do much good to decide to test multigigabit security devices with a test tool that can only do 1 gbps.
- Features: Are you testing performance only? Is SSL included? Are you testing security coverage?
- Operations: Is the tool GUI only or is their an API or scriptable interface to allow automation?

Test Tools

- Ixia Breaking Point: Got its start on the security coverage side of the house. As such we have seen it used more for that component of testing. It does have a full selection of performance tests including many different protocols. Not used as much for SSL testing that I have seen internally.
- Spirent Avalanche: This tool got its start as a pure HTTP performance test tool, Web Avalanche, and as such it is used more for traffic generation side of performance testing. It has added in security testing as well. Have seen this used internally for SSL testing in some groups.
- Tera VM: A newer test tool. Have seen this used for SSL testing internally.

Test Tools

Free tools

- I have seen numerous cases of some free test tools like Speedtest being used as performance testing tools. Ugghhh, single flow test tool. I guess it has some value. Just not anywhere outside of the niche of security testing single flow performance.
- In general, you get what you pay for. So while you can save money by using free tools or open source, its generally up to you to deal with having to design and orchestrate each test run. Assuming the tool can even do what you want or need it to do.

Typical Tests

Describing the 1024 Byte HTTP Test

Average packet size = Sum the size of each packet and divide by the number of packets

What is the 1024 byte average packet size HTTP test?

MSS (Max Segment Size) = 1460

HTTP Response = 250Kbyte

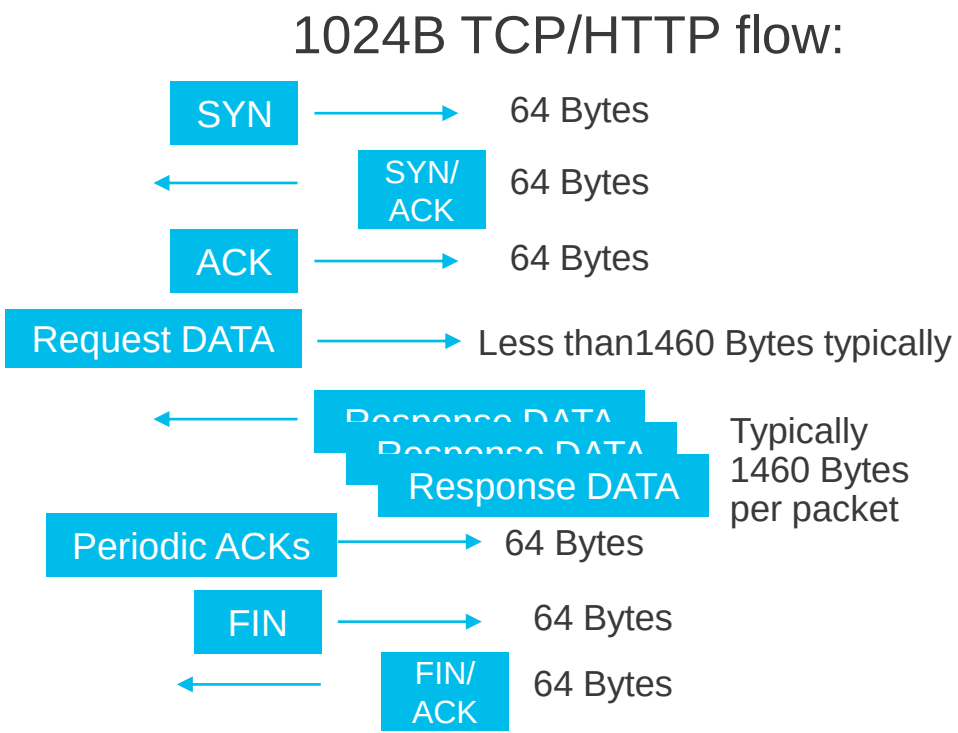
# of Gets = 1

Delayed Ack = Enabled

Features Enabled

IPS: Balanced Sec over Conn

AVC: Application Discovery Enabled



Demo

1024Byte HTTP
AVC: Network Discovery Apps
IPS: Balanced
NAP: Balanced

Describing the 450 Byte HTTP Test

Average packet size = Sum the size of each packet and divide by the number of packets

What is the 450 byte average packet size HTTP test?

MSS (Max Segment Size) = 1100

HTTP Response = 11000 Byte

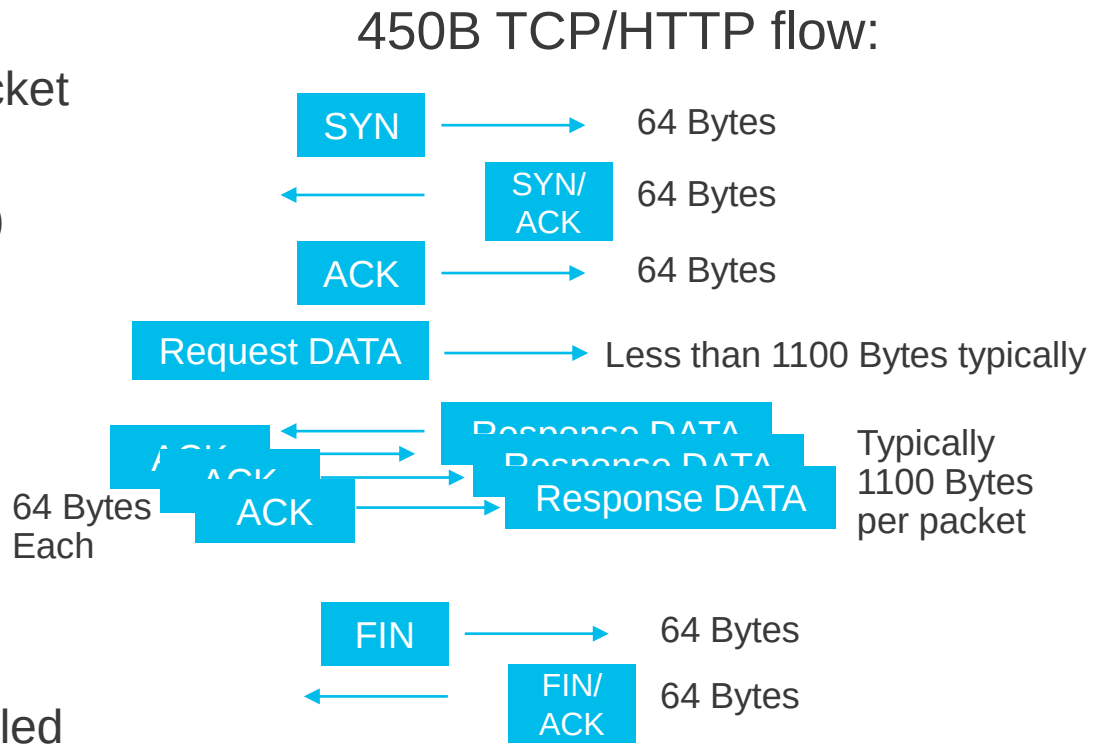
# of Gets = 1

Delayed Ack = Disabled

Features Enabled

IPS: Balanced Sec over Conn

AVC: Application Discovery Enabled



Other Standard Datasheet Tests

Max Connections: HTTP

- MSS: 516
- HTTP response: 8 bytes
- # of Gets: 10
- SFR Policy: IPS Balanced, AVC Network Discovery Apps

New Connections per second: HTTP

- MSS: 516
- HTTP response: 1 kbyte
- # of Gets: 1
- SFR Policy: IPS Balanced, AVC Network Discovery Apps

Demo

450 Byte HTTP
AVC: Network Discovery Apps
IPS: Balanced
NAP: Balanced

Testing Failure

When is a test considered failed?

Or when is it passed?

- Ways to check in a specific test tool
  - Failed Connections in tool test summary
- Ways to check on the device itself
  - Full Queues
  - Dropped packets
  - CPU Load
- Ways to check on the network
  - Missed packets
  - Latency

Performance Changes due to Configuration

Demo Test to Failure

1024Byte HTTP
AVC: Network Discovery Apps
IPS: Balanced
NAP: Change Balanced to Security over Connectivity

Failed Test

Test Tool

- Test tools will all come with various ways to detect when they can’t complete a test or are having problems completing a test.
- Each test tool will have different ways to do this so you will need to learn the tool to know the best way.

Failed Test

Device level

This is entirely device specific.

- On Cisco's Firepower Threat Defense there are a variety of commands that can be used during testing to help determine when a test is succeeding or failing:
  - show asp drop : any ongoing drops here indicate oversubscription and a failed test
  - show cpu : as cpu gets up above 95% the chance of oversubscription gets higher
  - show cpu core
  - show memory
  - show resource usage
  - show interface
  - show traffic

Failed Test

Network

- Depending on the test setup, its possible a device upstream or downstream can be used to test latency through the device.
- Something as simple as a ping can help indicate changes in latency through a device as it starts to become overloaded.
- Other network analysis tools can also help detect dropped packets or latency.

Customer Use Case Challenge

Testing in Public Cloud

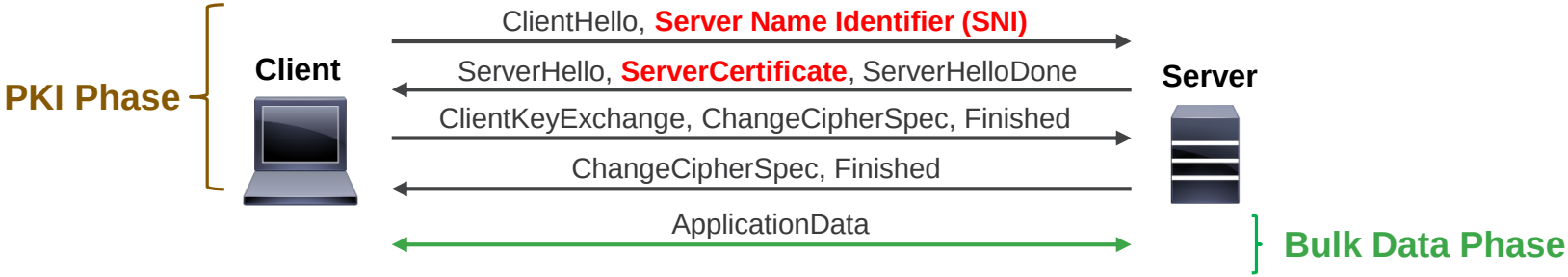
```
user@db:~$ ping 10.1.40.102
PING 10.1.40.102 (10.1.40.102) 56(84) bytes of data.
64 bytes from 10.1.40.102: icmp_req=1 ttl=64 time=16.0 ms
64 bytes from 10.1.40.102: icmp_req=2 ttl=64 time=9.54 ms
64 bytes from 10.1.40.102: icmp_req=3 ttl=64 time=11.3 ms
64 bytes from 10.1.40.102: icmp_req=4 ttl=64 time=18.2 ms
64 bytes from 10.1.40.102: icmp_req=5 ttl=64 time=23.4 ms
64 bytes from 10.1.40.102: icmp_req=6 ttl=64 time=22.0 ms
64 bytes from 10.1.40.102: icmp_req=7 ttl=64 time=11.8 ms
64 bytes from 10.1.40.102: icmp_req=8 ttl=64 time=22.3 ms
64 bytes from 10.1.40.102: icmp_req=9 ttl=64 time=13.1 ms
64 bytes from 10.1.40.102: icmp_req=10 ttl=64 time=21.6 ms
64 bytes from 10.1.40.102: icmp_req=11 ttl=64 time=15.3 ms
64 bytes from 10.1.40.102: icmp_req=12 ttl=64 time=31.6 ms
64 bytes from 10.1.40.102: icmp_req=13 ttl=64 time=1.02 ms  <<<<<<< start load traffic
64 bytes from 10.1.40.102: icmp_req=14 ttl=64 time=0.891 ms
64 bytes from 10.1.40.102: icmp_req=15 ttl=64 time=0.888 ms
64 bytes from 10.1.40.102: icmp_req=16 ttl=64 time=0.770 ms
64 bytes from 10.1.40.102: icmp_req=17 ttl=64 time=14.0 ms  <<<<<<< stop traffic
64 bytes from 10.1.40.102: icmp_req=18 ttl=64 time=31.8 ms
64 bytes from 10.1.40.102: icmp_req=19 ttl=64 time=6.97 ms
64 bytes from 10.1.40.102: icmp_req=20 ttl=64 time=21.8 ms
64 bytes from 10.1.40.102: icmp_req=21 ttl=64 time=21.8 ms
64 bytes from 10.1.40.102: icmp_req=22 ttl=64 time=29.3 ms
```

- A customer was doing very basic latency testing of the virtual product, NGFWv in the public cloud and they were seeing >20 ms latency on a basic ping test.
- After checking with engineering, this was because the pings were the only traffic being seen by the sensor. Once they increased the load, latency went down to normal.

Performance Challenges: SSL Traffic

Transport Layer Security Introduction

- Secure Sockets Layer (SSL) is broken, obsolete and no longer in use
- Transport Layer Security (TLS) is the current generic protocol layer

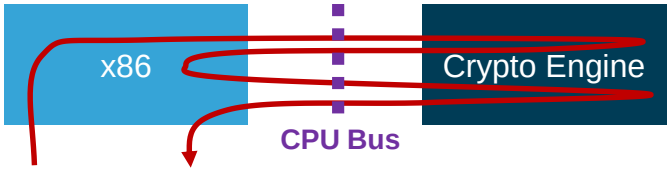


- Some detectors do not need decryption without Diffie-Hellman (DH)
  - Cleartext SNI extension indicates where client may be going – spoofable
  - ServerCertificate contains server identity – legitimate if CA is trusted
- Man-in-the-Middle (MITM) inspection is inevitable with TLS 1.3

Transport Layer Security

- MITM TLS inspection is two separate sessions with client and server

- **Resign** mode breaks with Public Key Pinning, **not** Certificate Pinning
  - Client certificate authentication or custom encryption **always** break MITM
- Hardware acceleration of PKI and Bulk Data phases still leans on x86 (*coming in LA in FTD 6.2.3*)



Challenges of SSL Testing

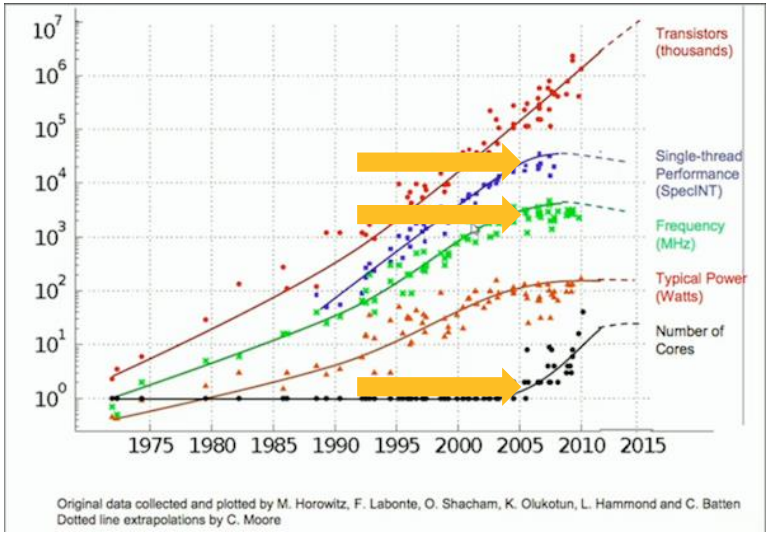
- Setting up the test is not easy with any test product. Care must be taken to make sure certificates are all created and imported carefully and that policies are created correctly.
- When testing, start with a small workload and very open security policies to ensure base decryption is occurring correctly. Ramp up after you have proven that the base decryption is occurring correctly and the sensor is identifying they underlying traffic correctly.
- Performance wise, understand that its not always a linear slope for decryption and that just changing one part of the configuration can have a fairly drastic effect on the performance envelope, ie moving from known key to resign, changing a cipher suite or key size.
- Also, be sure to test the testing gear out without a device in the middle to ensure it can handle the expected load. SSL testing is notoriously strenuous on both test gear and security gear.
- I have seen primarily either Spirent or Tera VM for SSL testing used internally. Other test tools have experienced some challenges but every vendor is working hard to improve their performance and features as this becomes the normal testing, not the exception.

Performance Challenges: Single Flow Performance

Single-Flow Performance Considerations

- A single stateful flow must be processed by one CPU core at a time
  - Trying to share a complex data structure leads to race conditions
  - Stateless parallel processing leads to out-of-order packets or missed events
- No magic trick to single-flow throughput
  - Deploy more powerful CPU cores
  - Reduce the amount of security inspection
- Pay performance price for real security

  … or deploy a router or a switch instead



Jumbo Flows

What is a jumbo flow and why do they cause problems?

- Flows that last a long time (generally minutes) with lots of max sized packets and generally they are fast, >1 gbps speed.
- Because they get processed by a single CPU, any flow that gets hashed to the same core ends up sharing the core with the jumbo flow and in many cases are impacted if the jumbo flow exceeds the capabilities of the core.

In Cisco FTD:

- Roughly calculated as overall throughput divided by Snort cores
  - 53 Gbps of 1024-byte AVC+IPS on SM44 / 48 Snort cores = ~**1.1Gbps**
  - Similar on most high-end ASA, FirePOWER, and Firepower platforms
  - Reducing impact on all flows from few superflows is more important

Jumbo Flows

What to do about jumbo flows?

- *What does your security policy tell you to do?"*
  - NGFW performance capacity should not dictate your security policy
    - Flow Offload (or similar, deterministic) **is** the right way
    - Dynamic Bypass (non deterministic) **isn't** generally
- Exposing a product that implicitly offloads is easy
  - Transfer multiple benign and malicious files over a single SMB session
  - Use HTTP pipelining to service multiple requests over one TCP connection

If they cut the flow through because its difficult then they will not fire on all possible events.

Bypassing specific known flows isn't the problem (high speed database backup between 2 servers in the DC).

Letting your security device bypass random flows because it's overwhelmed is a problem.

Customer Use Case: Single Flow Testing Challenge

Customer needed to pass large video files in a single flow while still inspecting to block .exe files

- As a base test, a prefilter policy to Fastpath the flow resulted in almost 1 gbps of throughput. (This is not flow-offload in hardware which can move TCP at almost >1 Gbps)
- With default setup, AMP, AVC and Security Over Connectivity IPS policy applied, the speed to send this file over FTP was limited to 340 mbps.
- Changing the IPS policy, including NAP, to Connectivity over Security raised the single flow speed to 650 mbps.
- With a very highly tuned configuration (unlikely to be usable outside of this specific test environment), running AVC, AMP, and a specific FTP-only, highly tuned IPS and NAP policy, the single flow speed was raised to 800 mbps.

Cloud Environments and Challenges

Private Cloud

Virtual Workloads in your Datacenter

This environment, esxi and KVM, isn't that much different from the physical environment.

In general, there will be some specific setup differences on the hypervisor, and in the troubleshooting of issues.

Test on the same host hardware as you will deploy for best results.

Test setup will also be similar to test setup for physical hardware:

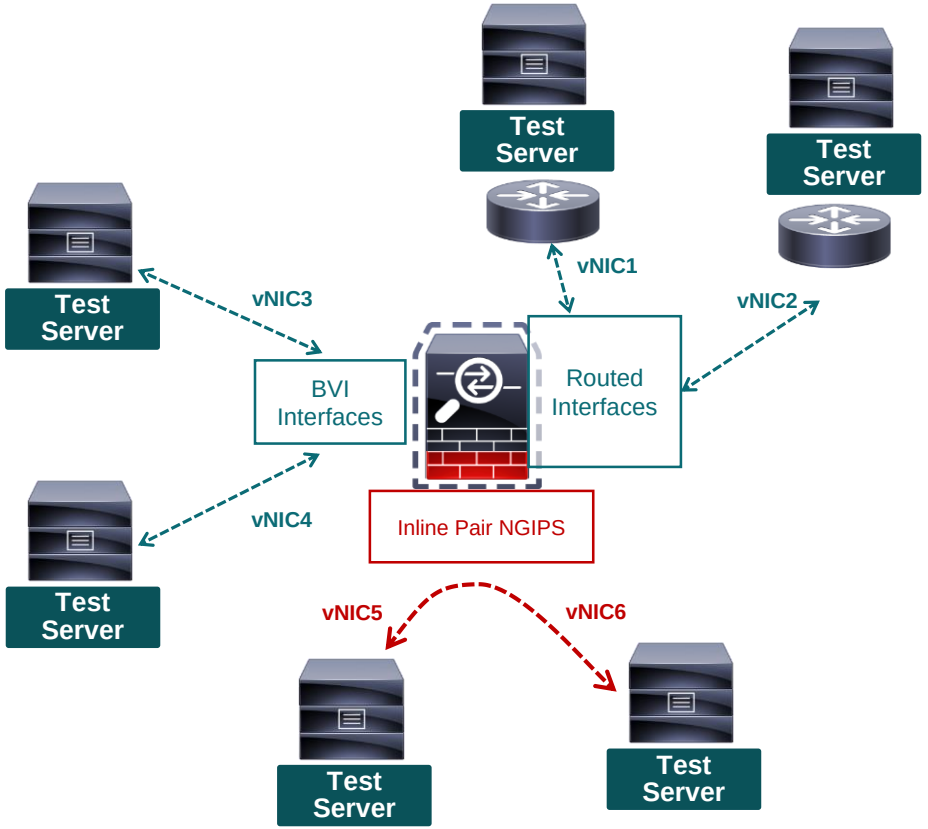
- L3 routed
- L2 transparent
- IPS Interface paired

One advantage of this environment over Public cloud is that more test tools are available here and you have more control to deploy as you normally would with physical appliances.

Private Cloud Example Setup of Cisco Firepower Threat Defense NGFWv for Testing

Testbed Setup allows testing of

- Routed or Transparent interfaces
- Interface Paired IPS interfaces



Public Cloud

Testing Challenges

One HUGE difference from on-premise testing is cost €. Since virtual security appliances operate in the 1-10 Gbps performance range, testing of those devices, if done without consideration, might cost thousands of dollars or more:

- Testing Internet to Web server performance using test clients located on the internet and Public cloud web servers
- Testing from one region to another
- Basically any transfer where the public cloud provider charges for sending or receiving data requires you to be very considerate about any sort of testing plan.

Each workload you create and run also generates a cost associated with it. Its not uncommon to spin up 20 or more VM's in on premise lab testing and let them generate large amounts of traffic. This can generate a large bill with your cloud provider if not careful.

Public Cloud

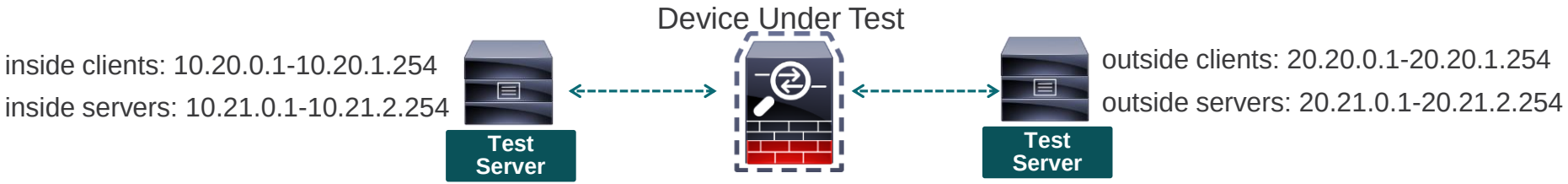
Differences and Challenges

- The Public cloud environment is VERY different. No L2 or L1 access means things have to be done differently. Each workload can generally only have 1 IP address in a subnet so test tools cannot be setup to use an entire class C or similar address space and generate connections using those ranges.
- Make sure your tools and setup are not the bottleneck before testing.
- Troubleshooting is a challenge because of limited scope of visibility into all the pieces being tested.
- Networking in the cloud can limit what the workload can see and process.
- Try to limit what components are in the design to control what pieces you have to troubleshoot during the test.

Public Cloud

Differences and Challenges

In typical on-premise testing of security devices, you use a large address space:



- 4 Class C address spaces on either of the DUT is common:
  - about 1000 IP addresses per side == huge number of unique tcp connections possible

In typical public cloud testing of security devices, you are limited because any workload can only have 1 IP address assigned to it, so every unique IP address is a unique workload. A public cloud test might only have 5-10 unique IP address per side (because of **€€€**) which requires 10-20 workloads just to run the testing tool! It's much harder to generate tests with hundreds much less thousands of unique IP address pairs.

Performance Tricks and Tips

Performance tricks and tips

"What techniques does a vendor use to accelerate their numbers silently?"

Cut-through or non-inspection

- What if a vendor was silently stopping inspection of a flow and bypassing it because it was impacting overall performance? If anybody claims single flow threat inspection at say 2 gbps or greater, for sure they are not inspecting the flow anymore!
- What if a product detected commercial test traffic and didn't apply the same inspection path? No way would anybody do that! Right?

Similarly to single flow performance, there are ways to enhance the performance of a box by either reducing the work it does per flow, or reducing the flows/packets you do the work on. Neither is really acceptable if done silently. Your security policy should drive the behavior of the security device.

Performance tricks and tips

Cut-Through and non-inspection as part of the security policy

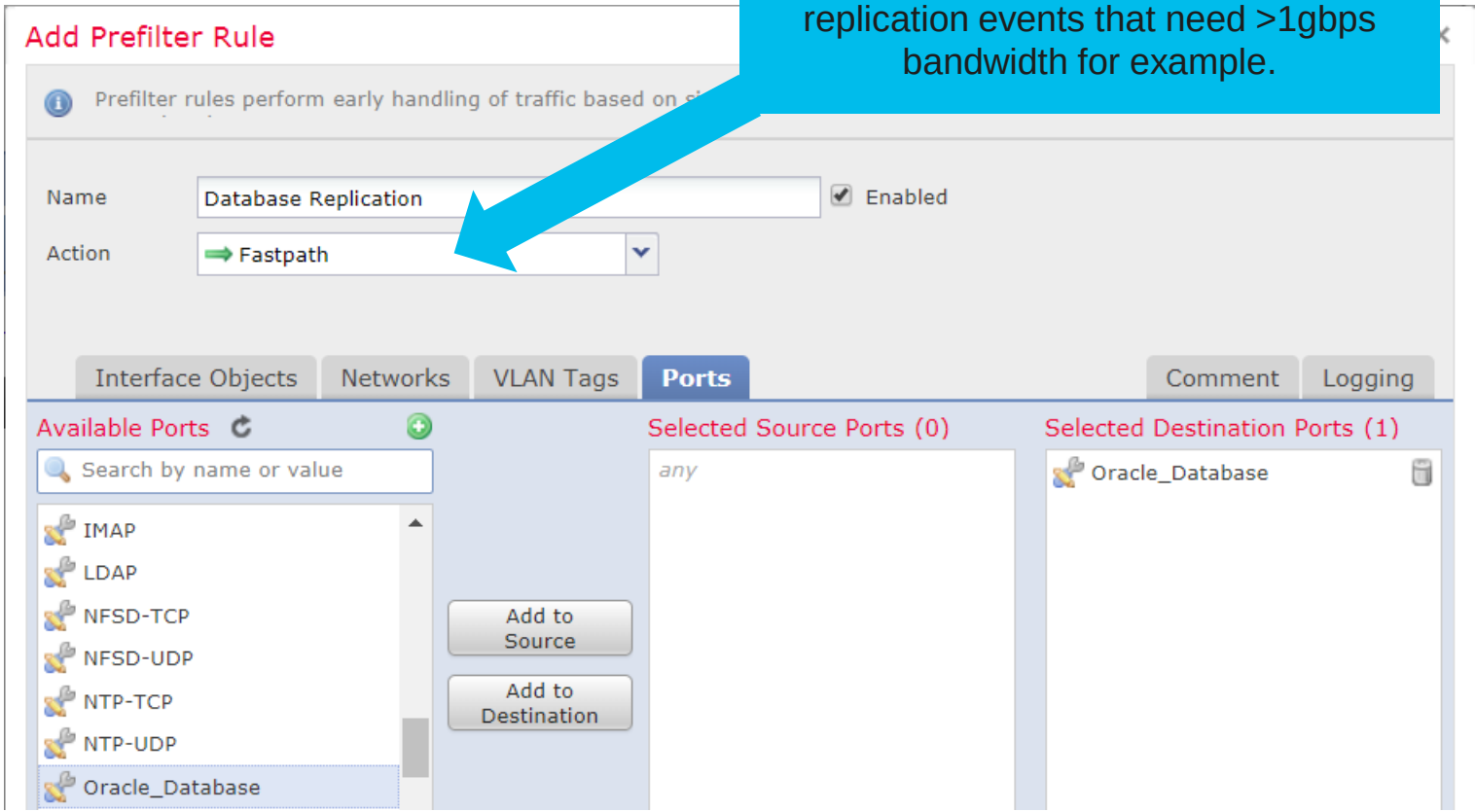
Sometimes, cut-through or non-inspection is ok or even desired. If you know about it and document it as part of your security policy, then it's clearly ok. Cisco has a variety of configuration options to change how much inspection occurs in FTD.

- Flow-offload: Firepower 4100 and 9300 have hardware offload capabilities that take prefilter rules and execute them in hardware for very fast speed and very low latency
- Prefilter rules: FTD has the concept of L3/L4 basic acls that can be defined to allow you to block or fastpath specific traffic without allowing further higher order threat inspection (IPS, AVC, AMP, URL, etc)

Prefilter Rules

Fastpath (or block) without inspection

Fastpath flows that need faster bandwidth or lower latency and can be trusted and are well defined: database replication events that need >1gbps bandwidth for example.

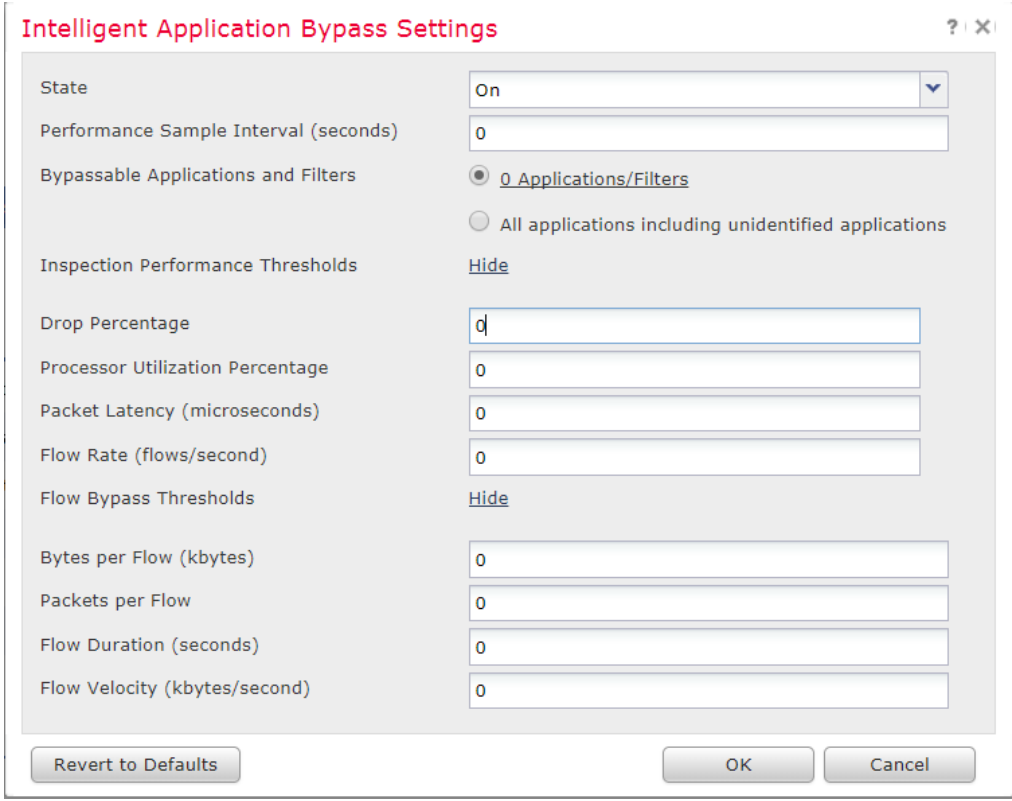


Performance tricks and tips

Cut Through and non-inspection

Intelligent Application Bypass (IAB)

- IAB gives an ability to dynamically fastpath a flow if it hits some thresholds of dropped packets, cpu load, latency etc.
- Allows you to choose to bypass a flow if it gets impacted or if it is a certain size.
- Understand that this is dynamic flow bypassing so holes in inspection could potentially opened up by malicious actors. You should be very careful using this!



Other Testing Types

Testing other Parameters

Exploit testing (Security coverage)

- Testing of the security coverage is also not easy
- When you run an exploit strikepack of say 1000 exploits, and get say 1000 events, its not easy to go through and make sure that each event was blocked (1 to 1 correlation) and produced an event related to the exploit in question (specific accuracy)

Protocol testing (false negative)

- Testing the ability of the device for false positives and evasion techniques.
- Requires either:
  - generally a deep understanding of the protocol and an ability to generate samples that test specific conditions
  - Or a tool that can do that intelligently and correctly (sometimes tools are badly written!)

Wrap up

or
Last chance to change your mind!

Am I going to do my own performance testing?

Questions you should ask:

- Should you take on the task of testing?
- Time required, gear required, expertise?
  - Time: Acquiring gear, setting up lab, building test cases, understanding the test gear and the test themselves, running tests, data analysis
  - Gear: Do you have a lab with the required switching gear, traffic generation gear, etc?
  - Are you capable?
    - Understanding the test tools
    - Have a deep understanding of the device under test and configuration of it
    - Understanding the results

Best Practices for Testing Security Devices

1. Traffic
   - Your network traffic is unique and in many cases the only true way to test performance
   - If that isn't feasible than make sure the test traffic you use is well understood, and that it activates the features you will be using and forces the device to pass the test traffic through the device to its fullest limits.
2. Features
   - Know what features you will be using and test with those features deployed and configured appropriately.
3. Configuration
   - Make sure you understand the product and have it configured as it would be in deployment. Deploy the same policies on each feature as you would in production or, at the minimum, a policy that exercises the same data path and forces the box to do work.

Cisco Firepower Sessions: Building Blocks

Tuesday	**BRKSEC-2050** Firepower NGFW Internet Edge Deployment Scenarios	**BRKSEC-2051** Deploying AnyConnect SSL VPN with ASA (and Firepower Threat Defense)	**BRKSEC-2058** A Deep Dive into using the Firepower Manager
Wednesday	**BRKSEC-2064** NGFWv and ASAv in Public Cloud (AWS and Azure)	**BRKSEC-2056** Threat Centric Network Security	**BRKSEC-3300** Advanced IPS Deployment
Thursday	**BRKSEC-3667** Advanced Firepower SSL policy troubleshooting	**BRKSEC-3035** Firepower Platform Deep Dive	**BRKSEC-3455** Dissecting Firepower NGFW “Installation & Troubleshooting

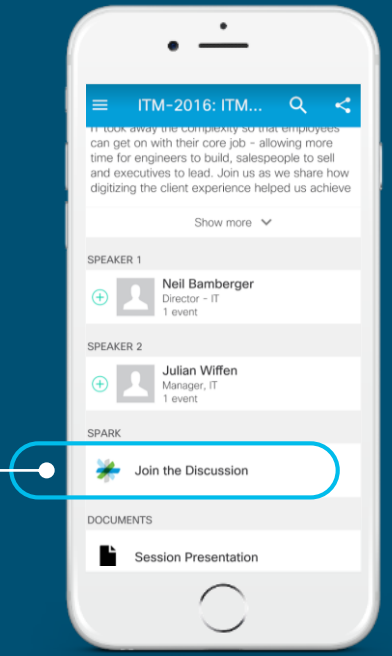
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

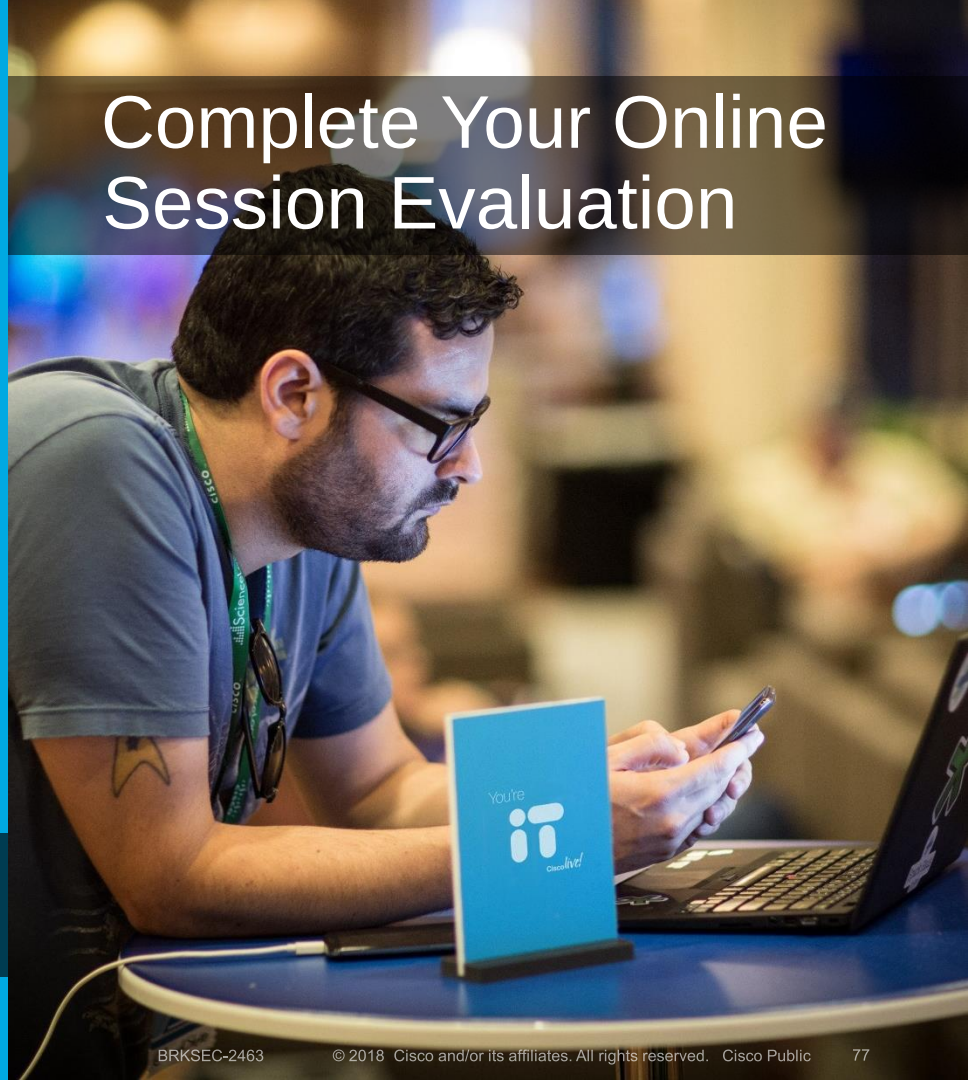


cs.co/ciscolivebot#BRKSEC-2463

Complete Your Online Session Evaluation

- Please complete your Online Session Evaluations after each session
- Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.



Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you


You're
Cisco live!