Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff’s Exhibit 39

⚓ Maniphest > T81543 ⊞ Create Task

☑ Enable IPSec between datacenters

☑ Closed, Resolved Public

Description

Traffic between our datacenters goes across fibers that are potentially surveilled. Since we terminate HTTPS immediately at the first hop, this means that user traffic gets across to the main datacenter in cleartext.

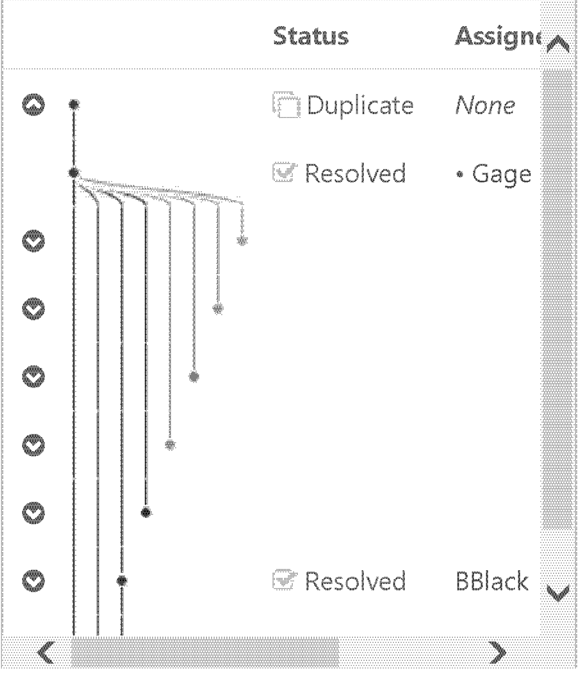
Details

Reference rt3536

Related Objects

Search... ▼

Task Graph Mentions



	Status	Assigne
	Duplicate	*None*
	☑ Resolved	• Gage
	☑ Resolved	BBlack

Tags

Interdatacenter-IPsec

Traffic (Done)

Operations

Subscribers

Matanya, faidon, greg and 9 others

Tokens

Assigned To

- **Gage**

Authored By

- **rtimport**, Sep 11 2012

Resolved	BBlack
Resolved	BBlack

• **rtimport** added a project: ~~ops-core~~. Dec 18 2014, 1:23 AM

• **rtimport** raised the priority of this task from to *Normal*.

• **rtimport** set Reference to rt3536.

• **rtimport** created this task. Sep 11 2012, 5:20 PM

faidon added a comment. Sep 11 2012, 9:07 PM

On Tue, Sep 11, 2012 at 05:20:36PM +0000, Ryan Lane via RT wrote:

> *Traffic between esams and the US datacenters goes across the WAN. This means HTTPS isn't actually encrypted for esams users. Also, we're*
> *sending IP information across the WAN, which is privacy information.*

Having IPsec tunnels between esams and the US means we're going to have
a lower MTU which is going to be a constant PITA. IPsec is also hard and
difficult to debug. I'd much prefer doing something like

stunnel or
pound and use plain ol' HTTPS.
Regards,
Faidon

rtimport added a comment.
Sep 11 2012, 9:07 PM

Status changed from 'new' to 'open' by RT_System

tstarling added a comment.
Jul 8 2013, 11:29 PM

For users geolocated in Europe,
HTTPS connections are
terminated in esams and
then the requests are forwarded
unencrypted to eqiad. This
compromises the
security of the system. Recent
news articles indicate that the
physical
security of the internet backbone
may not be as good as
previously assumed.
I propose buying dedicated IPsec
hardware for each DC, sufficient
to encrypt
cache-to-cache traffic and thus
protect the privacy of our users.

mark added a comment.
Jul 9 2013, 8:46 AM

On Mon Jul 08 23:29:10 2013, tstarling wrote:

> *For users geolocated in Europe, HTTPS connections are terminated in esams and then the requests are forwarded unencrypted to eqiad. This compromises the security of the system. Recent news articles indicate that the physical security of the internet backbone may not be as good as previously assumed.*
>
> *I propose buying dedicated IPsec hardware for each DC, sufficient to encrypt cache-to-cache traffic and thus protect the privacy of our users.*

Not just esams. Any link that leaves our data centers is equally suspect. So that also includes pmtpa vs eqiad, and soon ulsfo. Dedicated ipsec hardware is not very practical for this, and also pretty expensive. But I'd like to experiment with ipsec host-to-host (which is really what it was meant for) at some point...

--
Mark Bergsma <mark at wikimedia>
Lead Operations Architect
Wikimedia Foundation

• **rtimport** added a comment.
Jul 9 2013, 8:46 AM

Status changed from 'new' to 'open' by RT_System

mark added a comment.
Jul 9 2013, 8:46 AM

Queue changed from procurement to core-ops by mark

mark added a comment.
Jul 9 2013, 9:06 AM

On Tue Jul 09 08:46:08 2013, mark wrote:

> *Dedicated ipsec hardware is not very practical for this, and also*
> *pretty*
> *expensive. But I'd like to experiment with ipsec host-to-host (which*
> *is really*
> *what it was meant for) at some point...*

I'd like to (re)try IPsec in Linux with ESP in "transport mode".

> The advantage here is that this doesn't need any routing changes, and avoids the significant complication of rerouting (all) traffic between these hosts with separate (policy) routing, which tends to break things for traffic that is not supposed to use the tunnel/VPN. In transport mode we can select exactly which traffic (payload only) we want to encrypt, and not the rest. We're already getting MPLS transport to esams to avoid some of this, but that doesn't (really) solve the encryption problem. If ESP in transport mode works well, that would solve it in a scaleable way. Fortunately we have sufficient configuration management in place that maintaining such a setup across many hosts is no longer a problem. With our MPLS links we'll be able to do Jumbo frames, so we will even be able to support MTU 1500 and up with IPsec. I've used IPsec with Linux about 10 years ago, and it had some problems then - especially in a mixed environment with other vendors such as Cisco routers. Rekey failures and negotiation problems. I'm hoping the

situation is better
now, especially in a uniform
Linux environment.
--
Mark Bergsma <mark at
wikimedia>
Lead Operations Architect
Wikimedia Foundation

faidon added a comment.
Jul 9 2013, 10:47 AM

On Tue, Jul 09, 2013 at 09:06:08AM +0000, Mark Bergsma via RT wrote:

> *We're already getting MPLS transport to esams to avoid some of this,*
> *but that doesn't (really) solve the encryption problem. If ESP in*
> *transport mode works well, that would solve it in a scaleable way.*
> *Fortunately we have sufficient configuration management in place that*
> *maintaining such a setup across many hosts is no longer a problem. With*
> *our MPLS links we'll be able to do Jumbo frames, so we will even be*
> *able to support MTU 1500 and up with IPsec.*

I don't have access to the contract but I asked Leslie yesterday and she said that our yet-to-be-established link will have an MTU of 1514.

> *I've used IPsec with Linux about 10 years ago, and it had some problems then - especially in a mixed environment with other vendors such as Cisco routers. Rekey failures and negotiation problems. I'm hoping the situation is better now, especially in a uniform Linux environment.*

I've tried to use it a few years back with Linux and it was incredibly messy. The software might have improved since, but I still expect a full dual-stack IPsec setup in transport mode between with two/three datacenters to be non-obvious in many ways and possibly fragile. An alternative would be to just do SSL, e.g. via stunnel. That also has a number of complexities, though.
Personally, I'd much rather prefer encryption be transparent to the hosts and be handled entirely on the network equipment level.
Faidon

tstarling added a comment.

Jul 9 2013, 12:41 PM

On Tue Jul 09 08:46:08 2013, mark wrote:

> *Dedicated ipsec hardware is not very practical for this, and also*
> *pretty expensive. But I'd like to experiment with ipsec host-to-host (which*
> *is really what it was meant for) at some point...*

This ticket came out of an IRC discussion:
<TimStarling> LeslieCarr: any guess what the cost of said equipment would be?
my googling has not yet been successful
<LeslieCarr> memory fails me :(if you open a ticket we can get some quotes

mark added a comment.

Jul 9 2013, 12:55 PM

On Jul 9, 2013, at 12:47 PM, "Faidon Liambotis via RT" <core-ops at rt> :)
--
Mark Bergsma <mark at wikimedia>
Lead Operations Architect
Wikimedia Foundation

mark added a comment.

Jul 12 2013, 12:29 PM

Merged into ticket #3536 by mark

mark added a comment.

Jul 12 2013, 12:29 PM

Merged into ticket #3536 by mark

jeremyb added a comment.

Aug 26 2013, 12:43 AM

AdminCc jeremyb added by jeremyb

tstarling added a comment.

Sep 10 2013, 1:11 AM

I don't understand why the MTU is important for IPsec feasibility. If it's only
for internal traffic, then MTU discovery will be efficient and reliable, right?
If we're just talking about the small performance loss due to lower TCP window
size etc., then surely that is better dealt with on a separate ticket, independently of IPsec.

tstarling added a comment.

Nov 1 2013, 10:43 AM

http://www.washingtonpost.com/wo
security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1

According to the a recent leak from Edward Snowden, the NSA has already been
using links between Google datacentres to collect private information in
plaintext, so it's not a big jump to imagine that they are doing it with us
too.

coren added a comment.

Nov 1 2013, 2:00 PM

On Tue Jul 09 08:55:07 2013, mark wrote:

> *How about we try Linux IPsec, since it doesn't cost anything and isn't*
> *much work either. If it still sucks today, we can still buy expensive boxes or use stunnel... :)*

I agree with Mark without hesitation here; the Linux ipsec

> implementation is comparably robust to any hardware available, would be relatively simple to deploy thanks to configuration management and costs us little but time to deploy experimentally.
> Interestingly enough, I've used a simplified ipsec setup in the past where, since our endpoints were fixed, we simply used configuration management deployed keys (i.e.: no IKE) to great effect. With a bit of automation for key rotation, this meant rock-solid host to host IPsec with no dependency on networking or an externally maintained daemon to be stable -- at the cost of having to do key management ourselves (which we did through ssh). [in case you are curious, the use case included boxes deployed in networks presumed hostile and also integrated with TPM which should be unneeded in our case]
> The advantage of doing it this way is that there is no capital investment required, no routing changes needed at all, and only hosts pairs we deem necessary need use IPsec at all; it's easy to deploy and

experiment on a subset of hosts.

• **Gage** merged a task: Restricted Task.
Dec 18 2014, 6:51 PM

• **Gage** claimed this task.

• **Gage** added a subscriber: • **rtimport**.

faidon renamed this task from *Enable IPSec between esams and US datacenters* to *Enable IPSec between datacenters*.
Dec 22 2014, 9:40 AM

faidon updated the task description. **(Show Details)**

faidon raised the priority of this task from *Normal* to *High*.

faidon set Security to None.

Aklapper added a subscriber: **tstarling**. Dec 22 2014, 8:52 PM

• **Gage** added a comment.
Dec 24 2014, 3:45 PM

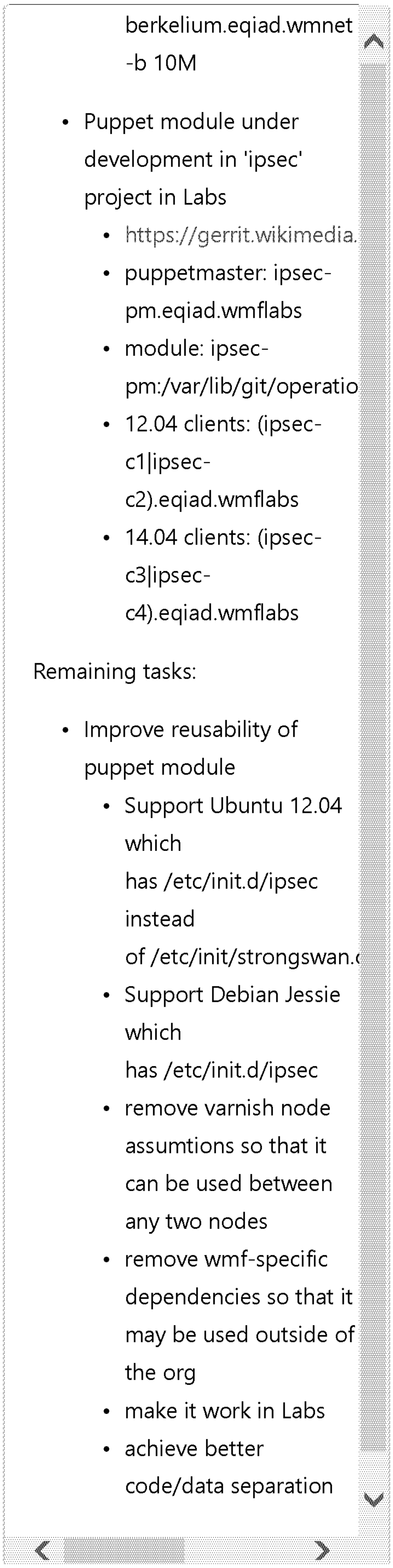
Decisions have been made to use:

- Host-to-host connections between Varnish nodes in cache sites and those in main colos
- Transport mode (ESP without AH): only the payload is encrypted;

IP/TCP headers are not authenticated
- Strongswan daemon for ISAKMP
- IKEv2 via reuse of Puppet client's SSL certs + keys
- Assumption: nodes will run Ubuntu 14.04

Current status:

- A test setup is running between (berkelium|curium).eqiad and (cp3001|cp3002).esams in transport mode
  - Manual configuration, derived from http://www.strongswan. transport/
  - Hosts are sending syslog events to Logstash
- Connection resilience tested: 10% packet loss in each direction on berkelium
  - sudo iptables -A OUTPUT -d cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP
  - sudo iptables -A INPUT -s cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP
  - 10MB/sec throughput over IPsec tests complete successfully: iperf -c

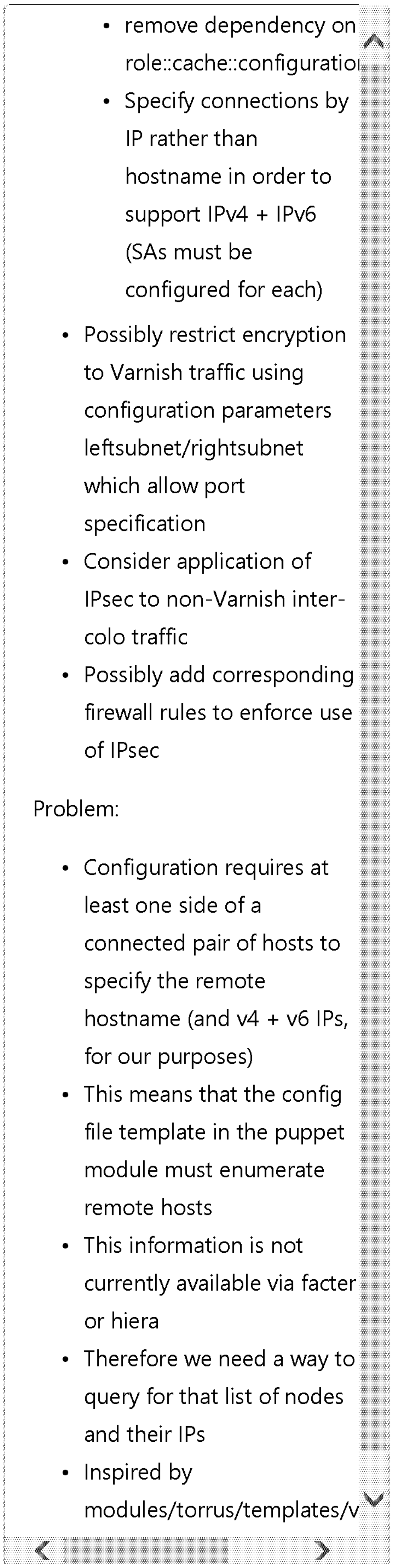


berkelium.eqiad.wmnet
-b 10M

- Puppet module under development in 'ipsec' project in Labs
    - https://gerrit.wikimedia.
    - puppetmaster: ipsec-pm.eqiad.wmflabs
    - module: ipsec-pm:/var/lib/git/operatio
    - 12.04 clients: (ipsec-c1|ipsec-c2).eqiad.wmflabs
    - 14.04 clients: (ipsec-c3|ipsec-c4).eqiad.wmflabs

Remaining tasks:

- Improve reusability of puppet module
    - Support Ubuntu 12.04 which has /etc/init.d/ipsec instead of /etc/init/strongswan.c
    - Support Debian Jessie which has /etc/init.d/ipsec
    - remove varnish node assumtions so that it can be used between any two nodes
    - remove wmf-specific dependencies so that it may be used outside of the org
    - make it work in Labs
    - achieve better code/data separation



  - remove dependency on role::cache::configuratio
  - Specify connections by IP rather than hostname in order to support IPv4 + IPv6 (SAs must be configured for each)
- Possibly restrict encryption to Varnish traffic using configuration parameters leftsubnet/rightsubnet which allow port specification
- Consider application of IPsec to non-Varnish inter-colo traffic
- Possibly add corresponding firewall rules to enforce use of IPsec

Problem:

- Configuration requires at least one side of a connected pair of hosts to specify the remote hostname (and v4 + v6 IPs, for our purposes)
- This means that the config file template in the puppet module must enumerate remote hosts
- This information is not currently available via facter or hiera
- Therefore we need a way to query for that list of nodes and their IPs
- Inspired by modules/torrus/templates/v

from manifests/role/cache.pp

- However that does not have clean code/data separation, and v4 + v6 IPs are not included

Solution?:

- Store data in Hiera: hostname, IPv4 address, IPv6 address, site and cluster membership for at least Varnish nodes

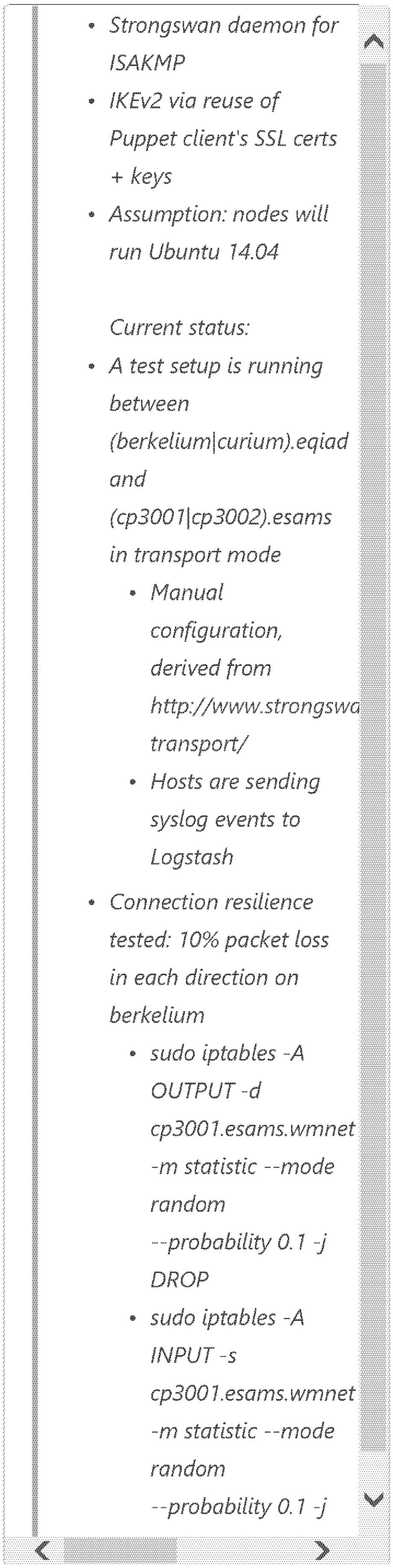
Documentation under development (to be moved to Wikitech): https://office.wikimedia.org/wiki/Use (WMF)/IPsec

mark added subscribers:

- **Gage**, **mark**.

Dec 29 2014, 1:47 PM

> In ~~T81543#943073~~,
> ○ **@Gage** wrote:
>
> *Decisions have been made to use:*
>
> - *Host-to-host connections between Varnish nodes in cache sites and those in main colos*
> - *Transport mode (ESP without AH): only the payload is encrypted; IP/TCP headers are not authenticated*



- *Strongswan daemon for ISAKMP*
- *IKEv2 via reuse of Puppet client's SSL certs + keys*
- *Assumption: nodes will run Ubuntu 14.04*

Current status:

- *A test setup is running between (berkelium|curium).eqiad and (cp3001|cp3002).esams in transport mode*
  - *Manual configuration, derived from http://www.strongswa transport/*
  - *Hosts are sending syslog events to Logstash*
- *Connection resilience tested: 10% packet loss in each direction on berkelium*
  - *sudo iptables -A OUTPUT -d cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP*
  - *sudo iptables -A INPUT -s cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j*

> - *10MB/sec throughput over IPsec tests complete successfully: iperf -c berkelium.eqiad.wmn -b 10M*

Thanks, this is very helpful!

> *Remaining tasks:*
>
> - *Improve reusability of puppet module*
>   - *Support Ubuntu 12.04 which has /etc/init.d/ipsec instead of /etc/init/strongswa*
>   - *Support Debian Jessie which has /etc/init.d/ipsec*
>   - *remove varnish node assumtions so that it can be used between any two nodes*
>   - *remove wmf-specific dependencies so that it may be used outside of the org*
>   - *make it work in Labs*
>   - *achieve better code/data separation*
>   - *remove dependency on role::cache::configurat*

> - - *Specify connections by IP rather than hostname in order to support IPv4 + IPv6 (SAs must be configured for each)*
> - *Possibly restrict encryption to Varnish traffic using configuration parameters leftsubnet/rightsubnet which allow port specification*
> - *Consider application of IPsec to non-Varnish inter-colo traffic*
> - *Possibly add corresponding firewall rules to enforce use of IPsec*

Could you create separate Phabricator tasks for (most of) these?

> *Documentation under development (to be moved to Wikitech): https://office.wikimedia.org/wiki/U (WMF)/IPsec*

Wouldn't it be better to develop this on Wikitech directly? You can just slap a draft template on the page to indicate it's not final/production ready yet.

• **Gage** added a comment.

Jan 5 2015, 6:13 PM

I feel that we need greater clarity about exactly who are we protecting our traffic from and how much effort is appropriate to expend on this goal.

From an article in Ars Technica dated Dec 30 2014 (http://ars.to/1B230yP):

"... in 2010, the NSA had already developed tools to attack the most commonly used VPN encryption schemes: Secure Shell (SSH), Internet Protocol Security (IPSec), and Secure Socket Layer (SSL) encryption."

This article discusses PSK, which we do not use, but also IKE:

"...trying to capture IPSec Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic during VPN handshakes to help build better attacks."

if that doesn't work, they try:

"...gathering more information on the systems of interest from other data collection sites or doing an end-run by calling on Tailored Access Operations to “create access points” through exploits of one of the endpoints of the VPN connection."

We must assume that this agency is not the only one with such capacity.

My question is: exactly who are we trying to secure our inter-colo communications from, and what is the feasibility of achieving that goal in the face of this information?

My impression is that adding IPsec can only potentially protect us from actors who can gain access to routers along our transit paths and record our traffic but do not have resources to apply the above methods.

• **Gage** closed subtask Restricted Task as *Resolved*.
Jan 11 2015, 4:13 PM

• **Gage** added a comment.
Jan 12 2015, 4:51 AM

More on the 12/2014 leaked info, from a Libreswan developer: "If you configure your IPsec based VPN properly, you are not affected. Always use Perfect Forward Secrecy and avoid PreSharedKeys.": https://nohats.ca/wordpress/blog/2(stop-using-ipsec-just-yet/

In Strongswan: "IKEv2 always uses PFS for IKE_SA rekeying whereas for CHILD_SA rekeying PFS is enforced by defining a Diffie-Hellman dhgroup in the esp parameter.": https://wiki.strongswan.org/projects, https://wiki.strongswan.org/projects,

> esp = <cipher suites>
> The notation is encryption-integrity[-dhgroup][-esnmode]
> Defaults to aes128-sha1,3des-sha1
> As a responder both daemons accept the first supported proposal received from the peer. In order to restrict a responder to only accept specific cipher suites, the strict flag (!, exclamation mark)
>
> Currently configured value:
> esp=aes256-sha512-modp4096!
>
> Input on cipher suite selection is solicited.

faidon mentioned this in ~~**T86663: Expand HTTP frontend clusters with new hardware**~~. Jan 13 2015, 2:41 PM

Dzahn added a subscriber: **Dzahn**. Jan 20 2015, 7:26 PM

BBlack added a subscriber: **BBlack**. Jan 20 2015, 7:27 PM

chasemp added a project: ~~**Interdatacenter-IPsec**~~. Jan 20 2015, 7:42 PM

• **Gage** mentioned this in **rOPUP917a7be9e69a: Strongswan: IPsec Puppet module**. Mar 1 2015, 11:19 PM

Jdforrester-WMF added a subscriber: **Jdforrester-WMF**.
Mar 10 2015, 6:50 PM

greg added a subscriber: **greg**.
Mar 11 2015, 2:49 AM

Dzahn awarded a token.
Mar 11 2015, 3:07 AM

• **Gage** closed subtask 🔒 Restricted Task as *Resolved*.
Mar 13 2015, 5:35 AM

• **Gage** closed subtask 🔒 Restricted Task as *Resolved*.

BBlack added a subtask: ~~**T96854: Reboot caches for kernel 3.19.6 globally**~~.
Apr 22 2015, 2:30 PM

BBlack added a subtask: ~~**T94417: Fix ipv6 autoconf issues**~~. Apr 22 2015, 2:35 PM

BBlack added a comment.
Apr 27 2015, 8:05 PM

Where are we at on this, aside from my blockers for final rollout re: kernel updates + IPv6 SLAAC?

BBlack added a parent task: ~~**T86718: Upgrade eqiad-misc varnish cluster from 2 to 4 systems.**~~. Apr 27 2015, 8:05 PM

BBlack added a subscriber: **faidon**.

May 3 2015, 11:19 PM

I've been going over the Interdatacenter-IPsec tasks today trying to get a picture of the overall situation and what's blocking various stages of deployment. This is a basic rundown of how I see things now:

I don't think we need or want crypto-traffic-only enforcement at this stage. Let's get this rolled out in a form where we still fall back to working, unencrypted traffic and simply have good monitoring in place that will alert us to this fallback condition. We can explore whether and how we want to force encryption at a later date. It could well be the case that ipsec with hostpair associations is not how we address our traffic crypto problems in the very long term view anyways. What we need now is just basically-reliable protection and alerting.

Tickets that can probably be ignored/dropped for now and not block deployment:

1. **T85823** - firewall rules - see above re: enforcement
2. T85827 - opportunistic encryption - seems dead-for-now upstream, so not really an available option

3. T85822 - restricting crypto to specific ports' traffic - does not seem necessary. The bastions won't be among the hostpairs involved, so SSH via them will always work fine. The traffic we'd want protected is the bulk of the traffic for any given hostpair, so efficiency isn't a big concern here either. If anything, not restricting by-port is a more secure-by-default solution anyways.

Nits that can probably easily be cleaned up / closed / ready:

1. ~~T96111~~ - Previous reauth failure investigation - seems ready to close, modulo ensuring we've discovered/applied sane runtime production values for various related parameters like lifetime and margin.
2. ~~T92604~~ - Rollout plan - seems sane, although the primary ticket text is a bit mixed/dated (we don't have it applied on all esams text caches, for instance, and wouldn't as a first step...). But yes, the general idea here to test on one hostpair only in production and then gradually enable the others is sane.
3. T95373 - Update Puppet CA cert - doesn't seem to be a

true blocker, more like "if we're going to fix this, let's do it now instead of later". Shouldn't be hard, right? If not, let's get it over with. If it is, then let's not block IPSec on it.

4. ~~T88536~~ - Implement a big IPsec off switch - core script seem to already be merged and presumably basically works? There's a followup commit dating back to ~2w ago with some nits/bugfix traffic, not yet merged. What's stalling on this? https://gerrit.wikimedia.org/

Functional core IPsec things that definitely need to be working for deployment, and may need some serious work-time on them:

1. ~~T92603~~ - Monitoring - Seems we have some work here, but is missing (in my opinion) "ip xfrm" correlation, plus reviewing for smaller nits and such, and actual testing. Critical due to lack of real traffic enforcement, so that we're aware if things break down.
2. ~~T92602~~ - Stats traffic protection - Critical IMHO, as we're still leaking way too much information without this. Needs: identify the list of kafka brokers involved, figure out if they're already on jessie or

pre-req for our current working test configs), sort out puppet bits for including them in the configured hostpairs for tier2 DCs as well. If they're not jessie yet, this could be a pretty major holdup. We could go ahead without this initially just to get some protection in place, but we really need this ASAP regardless.

External blockers (not IPSec-specific, but block full production rollout):

1. ~~T94417~~ - Fix ipv6 autoconf issues - @faidon and I should be able to sort this out one way or another before the rest above is done.
2. ~~T96854~~ - cache reboots for kernel updates - We should be able to kick off this process later this week, and thus would expect completion by circa May 22 at the outside? We can overlap this with the first phases of rollout by ensuring we get a few key hosts rebooted early in the process that can be used for the initial production hostpairs.

Is there anything else missing that's not captured in all of the above?

• **Gage** closed subtask 🔒 Restricted Task as *Declined*.

May 4 2015, 5:43 PM

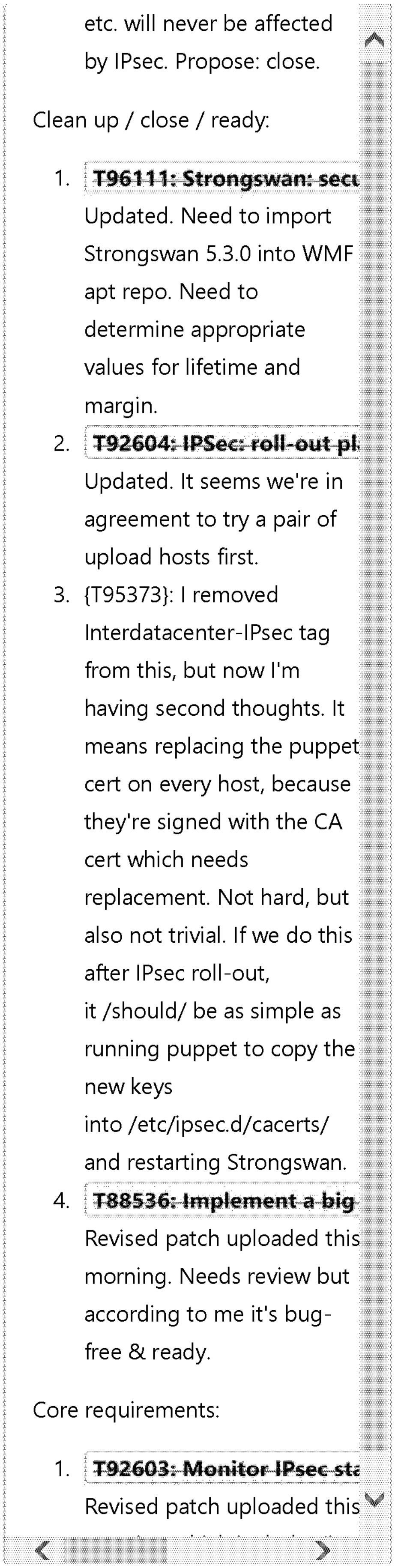
• **Gage** added a comment.

May 4 2015, 5:52 PM

Thanks, Brandon. I'll reply in order:

Proposed for ignore/drop:

1. ~~**T85823: IPsec: add firewall r**~~ Agreed, we don't need this right now. However I suspect we'll want this someday. Not a blocker. Propose: keep open with lowest priority.
2. {T85827}: Agreed, no movement upstream. It's a nice idea which could have made configuration easier, but we've already done the config work so now this would represent a config change rather than a savings in effort. I've closed it.
3. {T85822}: I opened this per Mark's request but personally I don't think we'll ever need this. The goal was to minimize potential impact of IPsec, but as BBlack has pointed out this is sufficiently taken care of by the hostpairs in use: DNS lookups, SSH from bastions,



etc. will never be affected by IPsec. Propose: close.

Clean up / close / ready:

1. ~~**T96111: Strongswan: secu**~~ Updated. Need to import Strongswan 5.3.0 into WMF apt repo. Need to determine appropriate values for lifetime and margin.
2. ~~**T92604: IPSec: roll-out pl**~~ Updated. It seems we're in agreement to try a pair of upload hosts first.
3. {T95373}: I removed Interdatacenter-IPsec tag from this, but now I'm having second thoughts. It means replacing the puppet cert on every host, because they're signed with the CA cert which needs replacement. Not hard, but also not trivial. If we do this after IPsec roll-out, it /should/ be as simple as running puppet to copy the new keys into /etc/ipsec.d/cacerts/ and restarting Strongswan.
4. ~~**T88536: Implement a big**~~ Revised patch uploaded this morning. Needs review but according to me it's bug-free & ready.

Core requirements:

1. ~~**T92603: Monitor IPsec sta**~~ Revised patch uploaded this

xfrm' checking and addresses syntax issues. Review requested.

2. **~~T92602: Secure inter-datacer~~**
   I agree that this is important. Kafka brokers are still on Precise, so they will need to be reinstalled. I'll talk to Otto about this.

External blockers:

1. **~~T94417: Fix ipv6 autoconf is~~**
   I've tested & given my feedback in support of the token-based approach. Seems like we're waiting on feedback from Paravoid.
2. **~~T96854: Reboot caches for k~~**
   This is BBlack & Moritz's issue, I agree with the plan to overlap with first phases of rollout. We need at least 3.19.3, which works with the current plan to deploy 3.19.6.

I'm not aware of any other related issues.

• **Gage** closed subtask 🔒 Restricted Task as *Declined*.

May 6 2015, 5:53 PM

• **Gage** removed a subtask: **~~T85823: IPsec: add firewall rules~~**.

BBlack closed subtask **~~T96854: Reboot caches for kernel 3.19.6 globally~~** as *Resolved*.

May 26 2015, 12:47 PM

BBlack closed subtask **~~T94417: Fix ipv6 autoconf issues~~** as *Resolved*.
May 28 2015, 6:53 PM

BBlack removed a parent task: **~~T86718: Upgrade eqiad-misc varnish cluster from 2 to 4 systems.~~**. Jun 4 2015, 12:01 AM

BBlack added a parent task: **~~T101339: Expand misc cluster into cache PoPs~~**.
Jun 4 2015, 12:05 AM

BBlack added a subtask: **~~T92604: IPSec: roll-out plan~~**.
Jul 29 2015, 1:27 AM

Restricted Application added a subscriber: **Matanya**. · View Herald Transcript
Jul 29 2015, 1:27 AM

BBlack mentioned this in **rOPUPc86d5d45df63: enable ipsec for all codfw caches**.
Jul 30 2015, 10:16 PM

BBlack mentioned this in **rOPUP651418a26dca: enable ipsec for half eqiad text caches**.

BBlack mentioned this in **rOPUP390b3d7b7047: enable ipsec for all eqiad text caches**.

BBlack closed subtask ~~**T92604: IPSec: roll-out plan**~~ as *Resolved*.

Aug 3 2015, 3:56 PM

BBlack added a subtask: ~~**T92602: Secure inter-datacenter web request log (Kafka) traffic**~~.

Aug 3 2015, 4:06 PM

BBlack added a comment.

Aug 3 2015, 4:09 PM

So, the basic cache<->cache work for tier2 is complete and functioning in practice (modulo ongoing operational improvements). We're still missing protection of other traffic (critically, kafka data, blocker added to previously merely referenced ticket), and we still have no answer for the traffic that crosses DCs through an LVS (critically in the near future: codfw caches -> eqiad appservers. Beyond that, it is desirable to let tier2-frontend caches bypass flowing through tier2-backend+tier1-backend for fixed "pass" traffic, but we're not there yet and this basically blocks it.

BBlack mentioned this in ~~**T110065: Switch codfw caches to tier2, begin**~~

~~**pushing some traffic through them to test**~~.
Aug 24 2015, 5:02 PM

BBlack removed a subtask: ~~**T92602: Secure inter-datacenter web request log (Kafka) traffic**~~.
Aug 27 2015, 3:01 AM

BBlack added a project: **Traffic**.

BBlack closed this task as *Resolved*.
Aug 27 2015, 3:29 AM

I split off the last blocker as a separate Traffic-tagged ticket. It's important, but there's no clear priority vs other projects, and we may solve it without IPSec anyways. The rest of the work here has been functional for a while and it's time for this long-standing meta-task to die.

BBlack moved this task from **Triage** to ~~**Done**~~ on the **Traffic** board. Sep 22 2015, 1:57 PM

faidon changed the visibility from "**WMF-NDA** (Project)" to "Public (No Login Required)".
Dec 13 2017, 5:09 PM

faidon changed the edit policy from "**WMF-NDA** (Project)" to "All Users".

Log In to Comment