Traffic flow confidentiality in federated networks

Multi-topology routing and security options

Ole Ingar Bentstuen
Norwegian Defence Research Establishment (FFI)
Division Cyber Systems and Electronic Warfare
Norway
Ole-Ingar.Bentstuen@ffi.no

Per Carlén
Swedish Defence Materiel Administration (FMV)
Contractor from Peldakon
Sweden
pc@peldakon.se

Traffic Flow Confidentiality (TFC) aims to prevent analysis of traffic flows. According to the principles of Protected Core Networking (PCN), TFC should be provided as a service in the network and not implemented by the users. Since provisioning of TFC in the entire network might not be practical or economical feasible, solutions are required for forwarding traffic on paths where sufficient TFC is employed. There are mainly two challenges related to this, the first one is to establish different routing-topologies for TFC and non-TFC paths, and the second is how users should signal their requirements for TFC to the network. This paper discusses using multi-topology routing for path selection and then proposes a signalling scheme that is based on option-headers.

Keywords; Traffic flow confidentiality, MT-routing, security options

I. INTRODUCTION

The ITU-T X.800 recommendation [1] defines Traffic Flow Confidentiality (TFC) as follows: "*This service provides for the protection of the information which might be derived from observation of traffic flows*". X.800 lists three different mechanisms that are associated with the TFC service:

- traffic padding,
- encipherment and
- routing-control

Traffic padding contains both padding of each individual packet to a given length and inserting extra packets so that each flow has a given volume. Encipherment is required both to protect meta-information in packet headers and to hide the usage of traffic padding. Routing control ensures that data is conveyed only over routes that have the appropriate level of protection.

In the concept for Protected Core Networking (PCN [2]), there's a strict separation of the network from the users. If users require confidentiality protection for their information, they have to provide this themselves, which basically dissolves in encrypting traffic before it enters the network. Any TFC-requirement from the user is handled in the network by applying certain mechanisms which are invoked by user-signalling.

The NATO STO IST research task group IST-103 on *Selected challenges for PCN* [3] has primarily worked on TFC in relation to Quality of Service (QoS). The background and experiments described in this paper is done within the context of IST-103 and since PCN mostly focuses on the network-layer, this paper will focus on IPv4 and IPv6.

The main goal of PCN is to build a highly flexible and reliable federation of networks. Nations participating in a mission should be able to merge or coordinate their network resources so that they together meet the requirements of the mission. Therefore, all solutions for TFC within a national network should also work in a federated environment.

A. Traffic Flow Confidentiality

Depending on choice of technology for different parts of the network, the provided TFC may not always include full volume confidentiality. This is especially valid for shared mediums like Ethernet, which is not designed to deliver a constant bit rate. With this background, it is sensible to divide TFC in a number of levels, ranging from no TFC at all to full volume hiding. Five different levels of TFC are listed in [4]:

- no TFC,
- source/destination addresses concealment,
- precedence concealment,
- packet size concealment and
- traffic volume concealment

The levels are not necessarily successive; you could for instance imagine hiding the precedence but not the addresses, although the purpose of this might by unclear. However, in [4], these levels are cumulative.

IST-103 studied how and where these different levels can be implemented on different kind of links (wired, wireless etc) in a network, whereas this paper mostly focuses on (virtual) point-to-point links.

Following the OSI-layers; on layer 1, being optical, electrical or electromagnetic, all TFC-levels can be provided with proprietary means. On layer 2, when being Ethernet, TFC-levels 1 and 2 can be provided and together with suitable, proprietary solution for traffic padding, also levels 3 and 4.

DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

TFC-levels provided on layer 3 are the same as for layer 2. One important aspect of TFC-level 2 is that an underlying bearer-network may be unable to handle QoS properly since the bearer will not be able to differentiate traffic based on a field that is hidden. Due to the possible impact of this, precedence concealment on layer 3 should be avoided.

Users with strict TFC-requirements may not have enough trust in network-side TFC, and therefore chose to implement TFC themselves. An experiment [5] was performed to analyse the consequences of such approach. The results showed that if users are implementing TFC level 3 and 4, it can severely impact QoS for other traffic flowing in the network. The recommended action was to avoid situations where users implement their own TFC-solutions and rather use a TFC-service, provided in the network. This is in line with the principles in PCN.

B. *Application of network level TFC*

Many links in core networks are Ethernet-based point-to-point links. With the current advances of Ethernet in service provider networks, implementing TFC on Ethernet is now a viable option. One suitable technology is IEEE 802.11ae (MACSec). It should be noted that there are currently no extensions for padding in the standard, which means that a proprietary technology needs to be added if a high level of TFC is required. Note that this type of link-protection may serve the purpose of protecting the network itself rather than the confidentiality of the information passed between users.

With these technologies, it is possible to implement TFC in the parts of the network where deemed necessary.

Fig. 1 shows a possible military network of today. Due to cost, the network can consist of some highly protected links owned and/or controlled by the defence as well as high capacity links, possibly Internet, across commercial service providers. Related to federated networks, different nations might or might not implement TFC in their networks. The example above is also valid for this scenario. A routing control mechanism, as detailed in X.800, is required to control the flow of traffic in such networks. Traffic that requires TFC should follow the upper path in Fig. 1 while traffic that does not require TFC may use the lower one.

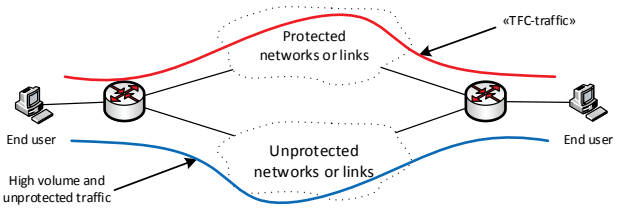

Fig. 1. Mixed TFC network

II. SIGNALING FOR TFC

In a network containing links operating on a range of TFC-levels, including "No TFC", there is a need for TFC-signalling between the end-user and the network in order for the network to choose the right path to fulfil the users requirements.

There are several aspects that have to be signalled for TFC. First, the five different levels need to be handled. It has sometimes been foreseen to merge level 1 (address hiding) and 2 (precedence hiding) to give four cumulative levels in total so signalling could fit into two bits. As mentioned earlier, the report from IST-103 discourages this, since hiding the precedence will prohibit the bearer from proper QoS-handling. Additionally, the signalling needs to handle strictness of the requirement. Like, should a packet be dropped if a link doesn't fulfil the requirement on TFC, or is the traffic so important that the network should forward the packet across a less protected link?

As defined in PCN, signalling can either be stateless or stateful. Stateless refers to where each node in the network treats each packet individually, and path- and forwarding behaviour may change from packet to packet. Hence the signalling needs to be per packet. Stateful means that each packet in a flow is treated based on a priori negotiated behaviour and over a fixed path where each node in the path is keeping the state for the flow. Mechanisms for both stateless and stateful signalling will be described next.

A. *Stateless signalling*

Traffic requiring TFC that traverses a network without any prior reservations has to be handled on a per-packet basis. This means that the TFC-requirement needs to be visible to forwarding nodes in every packet. There are a few alternatives for placing this information in the structures of IPv4 and IPv6; these will be further described below, with the aim of having similar signalling for the two protocols.

1) *DiffServ*

It has been suggested that the six DSCP (Differentiated Services Code Points) -bits, available in both IPv4 and IPv6, will not only carry information for QoS but also for TFC. In RD2933 [6], one bit is reserved for TFC future usage. With the number of TFC levels earlier mentioned and other dimensions like strictness of the TFC requirement, this one bit approach is apparently not sufficient. Signalling of TFC within the DSCP-field is also discouraged in the draft STANAG 4711 [7] for IOP QoS.

2) *IP Option/Hop-by-Hop options (IPv6)*

Another place that could be used for TFC-signalling is within an IP Option, which is a header field with commonalities existing for both for IPv4 and IPv6.

In IPv4, an IP Option is an optional field in the IP-header that is intended for control-functions, like time-stamping and source-routing. For IPv6, similar options are implemented as an extension header immediately following the IPv6 header, namely "Hop-by-Hop Options Header".

As for the choice of option-numbers, there are basically three approaches; selecting an IANA-assigned, use an experimental one, or apply for a new option. All alternatives will be covered in the following sections.

a) *Assigned options*

A possible header for signalling TFC in IPv6 is CALIPSO (RFC 5570) [8], which is mentioned in [3]. For IPv4, CIPSO

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

[9] is recognized as a good candidate for TFC signalling due to its high degree of resemblance to CALIPSO. The main usage, for both CIPSO and CALIPSO is Multiple Level Security (MLS) systems in trusted networks. CALIPSO even states that the extension header should be removed before packets are transmitted towards untrusted networks.

In CALIPSO, there are a number of fields that can be used. There are two fields with a high degree of commonalities for CIPSO and CALIPSO, and these fields are therefore chosen as candidates for TFC-usage;

- DoI (Domain of Interpretation), which identifies the usage or system. The field is four octets long.
- Sensitivity Level, which describes a relative sensitivity within a DoI. They always have a specific ordering. The field is one octet long

Allocations of numbers for DoI are under IANA responsibility. There are ranges for usage in private networks as well as assignments to organizations. For TFC, a special DoI could be used with the sensitivity level indicating the requested TFC-level.

There are some possible drawbacks when using a header for TFC, that has a slightly different purpose in MLS;

- CIPSO has already been implemented in systems like Linux and Cisco IOS. An example of unwanted behaviour is the following: A Linux-host receives a packet with a CIPSO-header for TFC that is not understood. This packet will most likely be dropped due to policy in the kernel. To circumvent this, any CIPSO-label for TFC has to be removed before forwarding packets to the end host.
- Co-existence with MLS-systems will not work unless these systems reside behind tunnelling-devices, inserting a new CIPSO/CALIPSO option for TFC on the outer side. It should be noted that this architecture is not at all in line with the ones described in CALIPSO. Another option could be to share the header between MLS and TFC, but that may be a bit complicated given that the proposed standards already have been around for some time and that implementations already exist for MLS.
- As stated in the draft for CALIPSO/CIPSO, these are only intended to work in very strictly controlled networks. This is due to the fact that once in transport, there are no means in the protocol to protect against manipulation. This enables an adversary to alter a TFC-level without it being detected by intermediate nodes. The receiver may detect the alteration, if the sender applies integrity-protection to its packets, but then it's too late since the traffic already has traversed the network and possibly weakly protected links. On the other hand, if integrity-protection is implemented on links, hop-by-hop, with for instance MACSec or IPsec, a modification in a header would be recognized in the network, during transit, and countermeasures could be triggered.

b) Experimental options

In [10], an approach similar to CALIPSO is defined with the usage of an experimental Hop-by-Hop option. Here one octet with three different levels of TFC was specified. When looking for solutions for IPv4, an experimental IP option could be used to cover the same information.

When comparing experimental options with assigned ones, it is recognized that while the options still are susceptible to modifications once on the network, any problems related to co-existence with MLS seem to disappear. For IPv6 (RFC2460, page 6) however, it is stated that there can only be one Hop-by-Hop extension header in a packet. This leads to the conclusion that same obstacles as for CALIPSO exist for MLS-systems together with experimental Hop-by-Hop options.

IPv4 though, will allow a CIPSO-option together with an experimental option in the same IP header. There may however be some performance-issues with options in IPv4, since the actual position in the IP-header, for the experimental option, could vary and this requires more processing in intermediate nodes.

c) New option

The third alternative is to use a new assigned option for TFC. This would avoid one problem related to co-existence with MLS-systems. But again, it cannot be used at same time as CALIPSO since IPv6 only allows one hop-by-hop extension header.

3) Conclusions, stateless signaling

Since the space in the DSCP-field is considered too small to fit information for both QoS and TFC, and the fact that draft STANAG 4711 discourages from using the DSCP-field for TFC, it is not considered as an alternative.

As for signalling with options, very little differs in the choice whether it should be assigned by IANA or using experimental assignment. When using CIPSO/CALIPSO for TFC, there will be problems if MLS-systems also use the same framework. Even if experimental or new options are used, all problems related to co-existence still don't go away.

With this in mind, the recommendation leans towards placing signalling of TFC in options, but only if MLS-systems based on same approach is not in use.

B. Stateful signaling

With reservation-technology a TFC-provided path could be guaranteed throughout the network. For reservations to take place, signalling must indicate the requirements in advance. There are mainly two approaches for stateful signalling in IP networks; RSVP (Resource ReSerVation Protocol) (RFC 2205) and NSIS (Next Steps In Signaling) (RFC 4080).

1) RSVP

IntServ (Integrated Services) (RFC 1633) is a framework where network resources can be reserved and guaranteed for a flow, based on prior signalling. Nodes supporting IntServ also have to contain functionality for classifying, scheduling and admission-control. The latter two make sure that guarantees for the flows can be met, while the first one is more concerned on

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

identifying packets that are bound to a state. RSVP is the principal signalling protocol used in IntServ. With RSVP, a request with QoS-requirements passes every router on a path throughout the network from receiver to sender. If the requirements are met, a reserved path is set up.

For intermediate nodes to know which traffic will be under reservation-policy, filters are used. These filters looks at specifics in the headers of the packets, in IPv4 only source and destination address together with ports (udp or tcp) are used. With an extension (RFC 2207) to RSVP, SPI(Security Parameters Index)-numbers are also covered, which to some extent cover reservations for IPsec-protected flows. If users behind an IP-crypto want to send traffic with different TFC-requirements, this needs to be reflected with different SPIs. This may not be feasible in all situations, considering the delay introduced; a new flow needs a certain level of TFC, therefore a new security association needs to be established, which could happen automatically given that such functionality exists in the IP-cryptos. After that, the reservation can be performed with the new SPI as a filter, and finally the actual traffic can be sent if the reservation was successful.

For IPv6, an additional header-field can be used. A 20-bit field called flow label seems sufficient for distinguishing flows with different requirements, whether QoS or TFC, without requiring any new security associations to be established. Hence, additional delay and complexity can be eliminated.

There is currently no extension for RSVP that could hold TFC requirements; this has to be developed if RSVP is to be used for TFC-signalling.

2) RSVP-TE

In MPLS (Multiprotocol Label Switching)-networks packets are labelled at the network-edge and then forwarded in the core only based on the contents of the label.

Together with TE (traffic engineering), RSVP with extensions can be used, which provides a more flexible way of handling flows. One example is that LSP (Label-switched path)–tunnels can be instantiated with constraint like bandwidth by RSVP-TE (RFC 3209). Another is ERO (Explicit Route Object), which is an object where the sender can specify a fixed path through a network, based on addresses. This implies that the sender already has computed a suitable path given the requirements. In [11], such path-computation elements perform this task in a multi-domain (federated) environment.

Within a domain, RSVP-TE needs to be integrated with a routing-protocol in order to achieve flexibility and provide information regarding TE attributes. Both IS-IS and OSPF have been extended (RFCs 5305 and 3630) in order to describe and convey the topology for TE. The focus has mostly been on bandwidth, but other properties, like TFC, could possibly be defined and assigned by IANA.

The target for RSVP-TE is mainly more or less static networks, and as such is unlikely to perform well in environments with a certain degree of mobility (RFC 4094) and re-routing. More research needs to be conducted to study the applicability of MPLS/RSVP-TE in deployable networks, for instance a tactical backbone.

3) NSIS

The framework for NSIS is aiming to be more generic than RSVP, by introducing two layers in the signalling protocol stack, a lower layer generic transport protocol (signalling transport) called the NSIS Transport Layer Protocol (NTLP) and a higher layer protocol (signalling application), called the NSIS Signalling Layer Protocol (NSLP). A signalling application could be QoS management, firewall control and so on, so NSIS can support more functionality than for instance QoS. There's a framework in place (RFC 5978) for defining additional NSLPs.

The IST-103 report [3] proposes two alternatives for using NSLP for signalling of TFC-requirement. Extend the QoS template for NSLP (RFC 5975), or define a new TFC NSLP according to RFC 5978.

4) Conclusions, stateful signaling

When considering federated heterogeneous networks, where each network runs with different routing and protocols for TE, stateful TFC-signalling is an area that needs to be developed. Nevertheless, extending the NSIS-framework seems like a good alternative for realizing stateful signalling of TFC.

III. MULTITOPOLOGY ROUTING

Multi-topology routing (MTR) was standardized in IETF, beginning in 2007. Multi-topology OSPF (RFC 4915) was ready in June 2007, with Multi-Topology IS-IS (RFC 5120) following in February 2008.

MTR is a framework for maintaining separate routing topologies over a network. A topology is a defined subset of routers and links in a network, for which a separate set of routes is calculated. The base topology is the topology containing all possible routers and links in the network. The different topologies can partly or fully overlap each other, and each topology is a subset of the base topology. A shortest path first (SPF) calculation is performed for each topology to discover the best routes within the topology. The cost of one link can be different for the different topologies. Only the links associated with the actual topology are included in the calculation. The results of the SPF calculation are stored in one forwarding table for each topology. Topologies can be defined to solve different purposes, but a common use is to define topologies holding links providing certain QoS-requirements. An example of this is letting voice traffic follow a path with low latency whereas large file transfers follow a path with low monetary cost.

MTR is mainly concerned with two tasks; building different independent topologies, and using traffic classification to map packets into these topologies, given the signalled properties.

Currently, extensions for MTR exists as RFCs for two intra-domain routing protocols, IS-IS and OSPF. For BGP, being the major inter-domain protocol, there are currently no separate extensions for MTR and this makes federated MTR a bit complicated. Without these extensions, there are mainly two approaches with BGP, using scopes or communities. BGP scopes are based on separate sessions being established

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

between BGP speakers, one per topology. Communities can be seen as tags that are attached to a prefix. There are several aspects to consider for inter-domain MTR. The actual interworking between BGP and an IGP (Interior Gateway Protocol); advertising the properties of internal prefixes to the outside, and applying received prefixes and properties to an IGP. As mentioned earlier, a routing-protocol is not alone sufficient; traffic classification also has to take place to forward the traffic in the right topology. This classification needs to take place in border-routers as well as in routers inside a domain, operating an IGP only.

From a convergence-perspective one can question whether BGP is suitable for the dynamicity that may arise within domains in deployed networks, especially when introducing path diversity.

As mentioned earlier in relation with RSVP-TE, path-computation elements could be utilized to circumvent the lack of inter-domain MTR. In these cases a path from sender to receiver is calculated in advance and then this path could either be attached to every packet as source-routing or utilized in stateful signalling.

Another interesting topic is the actual number of topologies. Should the number of TFC-levels equal the number of TFC-topologies and what if different QoS-topologies also exist? A high number of topologies will lead to both overhead of routing as well as management-issues, the need for an optimization is obvious.

As seen, there are still a few issues to be resolved. The focus for this paper is mainly on signalling, how all the aspects of inter-domain MTR are solved, is considered as future work.

IV. EXPERIMENTS

Without a guaranteed TFC-provisioned path, reserved either statically or dynamically throughout the network, stateless handling is the only option to fall back on. With this approach every packet contains some information that will instruct intermediate routers how to forward the packet. Since there are no guarantees, routers can either drop or forward the packet when a path doesn't meet the signalled requirements. A suitable solution for stateless TFC could be MT-routing, where different levels of TFC are mapped on matching topologies. In order to validate this, experimentation was carried out.

The IST-103 members from Norway and Sweden decided to independently perform experiments with multi-topology and TFC during the end of 2013. The Norwegian experiment used MTR OSPF with TFC-signalling in DSCP whereas Sweden used multiple independent OSPF-processes with CALIPSO-based signalling. No TFC-protection was actually applied in the experiments, since it was regarded as insignificant given the purpose. TFC level 1 and 2 could however easily been achieved either by using IEEE 802.11ae (MACsec) or IPv6-in-IPv6 tunnelling together with IPsec as described in [5].

A. MT-OSPF and TFC-signalling in DSCP

Norwegian Defence Research Establishment has, over several years, developed an experimental tactical router that includes support for MTR. Experiments with this solution have been done both in lab [12] and as part of the CoNSIS [13][14] multinational experiment. The implementation is done in a Linux router based on Vyatta[1], and has an implementation with multi-topology OSPF (RFC 4915).

The main idea behind this experiment was to show that MTR can be used for Traffic Flow Confidentiality. Instead of marking each link with QoS-properties, each link was marked with TFC-properties. For the experiment, each link could have the property TFC or no TFC.

1) Experiment setup

Fig. 2 shows the setup for the experiment. There are two hosts, acting as source (S1) and sink (S2), and four routers, named R1 trough R4, with multi-topology routing enabled.

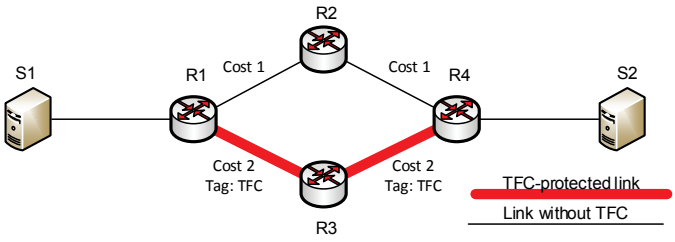

Fig. 2. TFC experiment setup

An OSPF cost was associated with each link in order to force base routing to choose the upper path (R1-R2-R4) between the two hosts. In addition, each link on the lower path (R1-R3-R4) had a MTR-tag "TFC", to indicate that these links were TFC-protected.

2) Differentiated Services

This experiment used the DSCP-field to signal requirement for TFC. In section II, signalling of TFC in the DSCP-field is described and discouraged, nevertheless it was used here since the main focus lied within the principles of signalling together with MTR rather than the choosing the most appropriate signalling method for TFC.

Each packet that required TFC was marked with a value of 0x28 in the DSCP-field. This number was arbitrary chosen, and should be seen as an example only. On each router, a filter was inserted with Vyatta tools to force traffic marked with 0x28 into the topology for TFC. All traffic with other DS-field values should use the base topology.

3) Setup, No path available

Vyatta was configured such that if the TFC-topology didn't have a path to the end-node, the router would drop the packet and send an ICMP-message with value "Destination Unreachable / No route to destination". It is possible to configure Vyatta so that for a given DS-field value, the router chooses a TFC-path if it's available, and then falls back to another topology or base topology as last resort.

4) Verification of setup

Verification of the setup was done by inspecting the routing tables in each of the nodes, and using 'ping' and 'traceroute'-

[1] http://www.vyatta.org

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

utilities between the hosts and the routers. The base routing table in router R1 showed a route through R2 to reach S2. Likewise inspecting the topology for TFC showed a route from R1 to S2 through R3. A traceroute with unmarked packets from S1 to S2, showed a path through router R2.

A network analysis tool (wireshark) was installed on all links between the routers. This gave the ability to check which paths different traffic used through the network.

Several trials with traffic from source to sink were performed to validate the configuration. The tests were performed using the 'ping'- and 'traceroute'-tools and the MGEN[2] traffic generator. After successfully verification, the actual testing took place.

a) Unmarked traffic

First test performed was to send traffic from S1 to S2 without any DSCP-field marking. Network analysis tool showed that traffic followed the path R1-R2-R4. Likewise, traffic from source to router R2 and R4 followed the upper path. This was in line with what was expected.

b) Marked traffic

Next test was to send traffic marked with TFC-requirement from S1 to S2. The network analysing tool showed that traffic followed the lower path R1-R3-R4. Addressing the routers R3 and R4 from S1 also indicated a path selection from R1 to R3 and eventually R4. Addressing router R2 from S1 gave an ICMP-reply with "no route to destination from router R1. This was also in line with what was expected.

5) Further testing

Further testing was done by moving S2 to router R2. When S1 now tried to send packets marked with TFC-requirement to S2, router R1 returned "no route to destination". Unmarked traffic arrived as expected. Then TFC was enabled on the link between R4 and R2. Tests showed that marked traffic from S1 to S2 followed the long path through R1-R3-R4-R2 between S1 and S2. The results were as expected.

6) MT-OSPF and DSCP, conclusions and further work

This experiment clearly shows that multi-topology can be used to enable TFC in a network where only selected paths have TFC properties. Although the experiment only supported one level of TFC, it is possible in this framework to implement different levels of TFC on each link, and thereby supporting different topologies. Depending on how signalling for TFC is carried out, it is also possible to support both a strict requirement for TFC and a request for “TFC if available”. When the user signals a strict requirement for TFC, the network will return a message if there is no route with that level available.

The next possible extension of this experiment is to explore a multi-dimensional approach to MTR. Is it possible to have both TFC and QoS-tags on each link? The routing process in each router will then have to consider both QoS- and TFC-requirements when making the topologies. Instead of making a topology for each combination of QoS and TFC, one option could be to make this a two-stage process, where the router first considers all TFC-paths, and then looks at possible QoS-paths within applicable TFC-topologies.

B. MT-OSPF and TFC-signalling in CALIPSO-header

The aim of the experiment was to see if MT-routing and signalling of TFC within CALIPSO-header could be a suitable solution for choosing a path in accordance to signalled requirement and further explore the usage of the headers together with IP-cryptos.

1) Experiment, setup

All devices were built in a virtualized environment with Debian-based servers as hosts and routers. In the setup, seen in Fig. 3, the routers (R1-R4) contained software for IPv6 routing on multiple topologies.

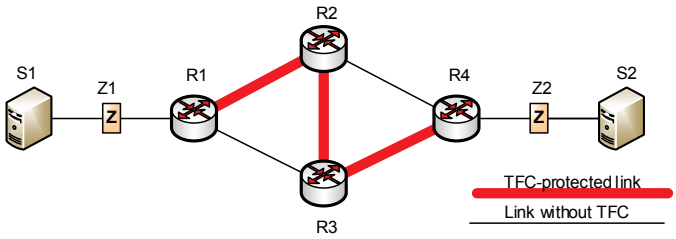

Fig. 3. CALIPSO-based TFC experiment

Modifications to Quagga[3] source-code were made in order to allow multiple instances of the OSPF-daemon running concurrently to handle the separate topologies. The separation of the instances was realized by letting them use different Internet Protocol numbers. It should be noted that even if running multiple OSPF-instances does serve the purpose of this MTR-experiment, the caused overhead compared to running one OSPF-instance with MTR extensions will most likely make it the least attractive alternative of the two.

Normally Quagga installs learned routes in kernel routing table, but since a more advanced type of routing was required, this was disabled. Instead, a perl-script was written that periodically scanned the different topologies and if necessary modified rule-based routing-tables. IPtables was used to, internally to the server, mark the packets according to signalled TFC in CALIPSO-header. This marking was then utilized by the rule-based routing to find the correct routing table, corresponding to a certain topology.

Three topologies were built;

- noTFC, which contained all possible links.
- TFCplease, which contained all possible links but cost-parameters were trimmed to prefer TFC-protected over unprotected links.
- TFCrequired, which only contained TFC-protected links.

[2] https://www.nrl.navy.mil/itd/ncs/products/mgen

[3] http://www.nongnu.org/quagga

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

It should be noted that no relation to the provisioned TFC-level was made, whether a link was protected or not.

The servers (S1-S2) and IP-cryptos (Z1-Z2) contained software for adding or modifying CALIPSO-headers. A feature in IPtables was used to grab packets based on specified conditions and pass it out to a user-space application. This application, again a perl-script, added or modified a CALIPSO-header depending on configuration. The sensitivity-field of the header was used to indicate required level of TFC, where "1" meant "TFC please" and "2", "TFC required".

As implied, the IP-cryptos were capable of encrypting traffic by transforming clear-text packets into IPsec.

2) Experiment, execution and results

The following subchapters briefly describe the performed experiments.

a) Basic test

In this test, the IP-cryptos only forwarded traffic without encryption. S1 sent both "unmarked" traffic (without CALIPSO-header) as well as traffic marked with "TFC Required" towards S2. With packet-captures on all links, it could be observed that unmarked traffic traversed R1-R3-R4 due to lowest configured cost, while marked traffic was forwarded on R1-R2-R3-R4. As such, the results imply both that multiple topologies exist and that the correct topology was chosen based on signalling in packets.

b) TFC please

This test as well was performed without encryption. Now S1 sent both traffic marked "TFC Required", and "TFC Please" towards S2. Packet-captures showed that both types of traffic traversed the TFC-protected path (R1-R2-R3-R4).

After that, this TFC-protected path was broken by taken down the link between R2 and R3. What happened was that traffic marked with "TFC Required" was dropped in R1 since no suitable topology existed for its traffic. "TFC Please"-traffic, now took the path R1-R3-R4 and successfully arrived at S2. This was the expected result.

c) Header protection

Still without encryption, but this time the servers were integrity-protecting their traffic with AH (Authentication Header) (RFC 4302). ESP (Encapsulating Security Protocol) [RFC 4303)] was not used since the intermediate routers need to be able to inspect the CALIPSO-header in order to correctly forward traffic on the different topologies, and ESP would have prevented that. An adversary with the means to modify CALIPSO-headers could thereby impact the path that a packet traverses, possibly steering traffic to links with weak TFC-protection.

The AH-protected traffic, also containing a CALIPSO-header, successfully traversed the network from S1 to S2.

Then, modification of CALIPSO-headers was performed in R1, effectually down-marking traffic from being "TFC Required" to "TFC please". Traffic marked with "TFC Required" from S1, was now dropped at S2, due to integrity-protection being aware of modification in the packets. More important, packets were forwarded on "TFC please"-topology although signalled as "TFC required", since they had been successfully downgraded in transit.

d) Crypto, header handling

This time, encryption as well as CALIPSO-handling was enabled in the IP-cryptos. Different modes of handling was tested; one where the IP-cryptos inserted a header in the encrypted packet and another where the header on the cipher-side was reflecting the signalled value on the clear-text side.

Insertion of a header in a packet with ESP posed no problem, the routers correctly forwarded traffic according to signalled level and the receiving IP-crypto successfully decrypted the packet. Reflecting the signalling from clear-text to crypto-side was also successfully done.

3) MT-OSPF and CALIPSO, conclusions

The main conclusion is that stateless signalling of TFC within CALIPSO-header and a related MTR is a feasible solution.

There are however a few things that need to be kept in mind, which is also somewhat covered in the related RFCs. CALIPSO-headers should be used in trusted environments, where the meaning of trusted together with the results of the experiment have to be interpreted as networks with mechanisms for integrity-protection on the links in the network. An adversary must not be able to remove or downgrade a signalled TFC-level, without the network noticing it.

The consequence of this is that all forwarding devices need suitable protection that prevents altering TFC-level by configuration or by malicious code. Also, all TFC-protected links require integrity-protection to mitigate header-modifications. This, in turn, implicitly sets the minimum requirement for TFC-provisioned links.

V. Conclusions and Recommendations

Both experiments described in section IV clearly show that multi-topology can be used to enable TFC in a network where only selected paths have TFC properties.

When signalling with CIPSO/CALIPSO, there are some drawbacks related to the possible collision with MLS-systems. If this can be avoided, there is sufficient space for adding strictness, like a wanted as well as an acceptable TFC-level.

Based on discussions and performed experiments, the recommendation for stateless signalling is to add new primitives to CIPSO/CALIPSO for TFC requirements. These should contain both the wanted level and the minimum accepted level.

Since the headers are sensitive to modifications, only networks with integrity-control can be used. Also, if transiting any public networks, the headers should not be visible. This could be achieved either by removal of headers or by tunnelling with encryption.

Two areas where more work is needed, before drawing any solid conclusions, are stateful signalling with NSIS and inter-

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20

domain MTR. For NSIS, adding a new TFC-specific NSLP according to RFC 5978 looks like a promising alternative. For inter-domain MTR, more research is needed before going into the process of standardization.

ACKNOWLEDGMENT

We wish to thank Mr Maurizio Bisio from Selex ES in Italy and Ms Åshild Grønstad Solheim from the Norwegian Defence Research Establishment, who did most of the theoretical work on TFC in the IST-103 working group.

REFERENCES

[1] ITU/CCITT, "Security Architecture for Open Systems Interconnection for CCITT Applications," Recommendation X.800, Geneva, 1991.

[2] NATO STO, "Requirements for a Protected Core Networking (PCN) Interoperability Specification (ISpec)," RTO-TR-IST-069, AC/323(IST-069)TP/424, pp, 1-258, July 2012.

[3] NATO STO, "Selected Challenges for Protected Core Networknig," STO-TR-IST-103, (draft, unpublished).

[4] G. Hallingstad and F. Micevski Scharf, "Provision of multiple levels of traffic flow confidentiality-service in protected core networks," RTO IA Symposium, Ljubljana, Slovenia, October 2008.

[5] P. Carlen, "Traffic Flow Confidentiality mechanisms and their impact on traffic," Military Communications and Information Systems Conference (MCC), Saint-Malo, France, October 2013.

[6] R.M. van Selm, G. Szabo, R. van Engelshoven and R. Goode, "IP QoS Standardisation for the INI," NCIA RD2933, (draft), AC/322(CP/1)N(2011)0037-Annex 2, February 2011.

[7] "Interoperability point quality of service (IOP QoS), "STANAG 4711 (Draft, unpublished), February 2014.

[8] All RFCs are published by IAB, IETF, ISE or IRSG. All RFCs are available at http://rfc-editor.org.

[9] IETF CIPSO Working Group, "Commercial IP security option (CIPSO 2.2)," Internet Draft, 16 July 1992.

[10] M. Lies, D. Dahlberg, P. Steinmetz, G. Hallingstad and P. Calvez, "The protected core networking (PCN) interoperability specification (ISPEC)," Technical Report 2013/SPW008905/13, September 2013.

[11] ETNA Ethernet Transport Networks, Architectures of Networking, "WP2 Network Architecture," November 15 2008.

[12] M. Hauge, M. A. Brose, J. Sander and J. Anderson, "Multi-topology Routing for Improved Network Resource Utilization in Mobile Tactical Networks," Military Communications Conference (MILCOM), San Jose, 2010.

[13] A. Eggen, M. Hauge, O.E. Hedenstad, K. Lund, A. Legaspi, H. Seifert, P. Sevenich and P. Simon, "Coalition Networks for Secure Information Sharing (CoNSIS)," (Invited paper) Military Communications Conference (MILCOM), San Diego, 2013.

[14] M. Hauge, M. A. Brose, J. Sander and J. Anderson, "Multi-topology Routing for QoS support in the CoNSIS convoy MANET," Military Communications Conference (MILCOM), Orlando, 2012.

DOI til publisert versjon / DOI to published version: 10.1109/MILCOM.2014.20