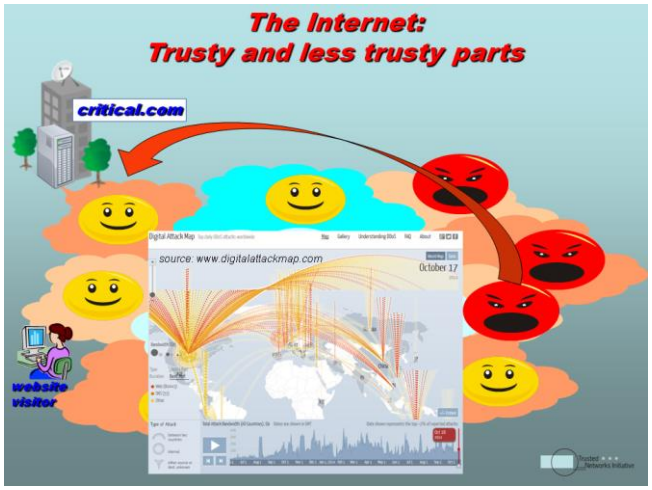
Trusted Networks Initiative

Summary

Version 01-04-2015

Trusted Networks Initiative

The Trusted Networks Initiative aims at a global trust concept that provides website-operators with a last-resort option in case a large or long-lasting distributed denial of service (DDoS) attacks can not be mitigated by other Anti-DDoS means.



Some DDoS-attacks may become too big to handle

The project is launched in The Netherlands by a group of critical-website operators, access networks, internet exchanges, governmental organizations and supporting institutes, who recently kicked off the initial Trusted Routing concept that currently operates in beta mode.

The principles of the solutions are simple: each participating network at its sole discretion can step to 'trusted internet only' if an emergency situation requires to temporary disconnect from the global internet.

Any network, content or access provider, can participate in the trusted domain as long as they commit to a certain minimum of:

- DDoS-preventing technology;
- sufficient organizational response to DDoS events, and;
- respect to common laws.

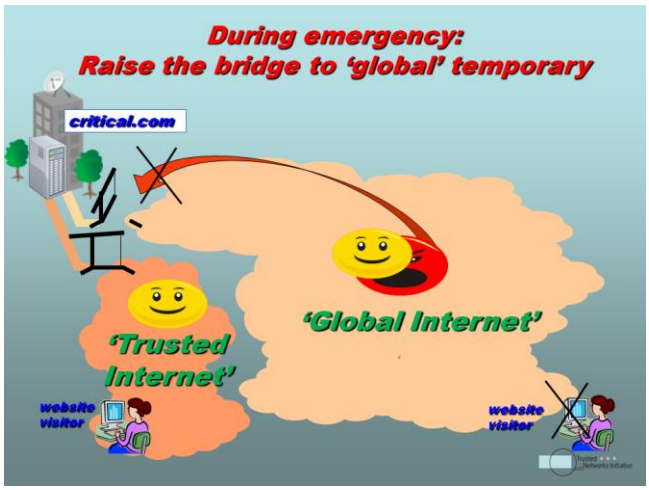
Trusted Routing Concept

Within the Trusted Routing concept the participating networks are connected to both 'the global Internet' and the 'trusted domain' of the Trusted Network Initiative.

The 'trusted domain' is available via a dedicated VLAN-112 and a dedicated Routeserver is configured at the Dutch internet exchanges NL-ix and AMS-IX.

Parties interested to join the 'trusted domain' can qualify at the independent Trusted Networks Initiative with a written statement that they will commit to the Trusted Network policy. and then get connected to these exchanges, to activate the Trusted Routing to other participants.

The Trusted Routing Routeserver is configured in standby-mode, and is only to be used in case of emergency. Participating networks should first try to solve the DDoS attacks with their own generic mitigation solutions, however have the last-resort option to reroute to the trusted domain if the attack becomes too big or too long to handle generically.



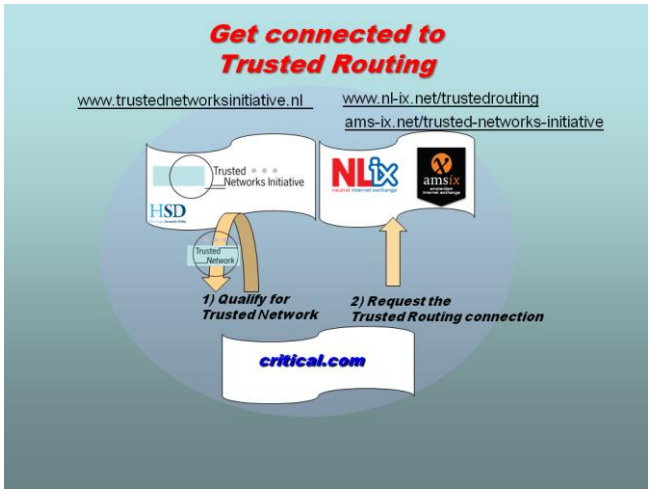
As a last-resort: Raise the bridge for attacks

Optionally, participants could also setup bilateral sessions with another network if both parties agree this is required.

empowered by HSD The Hague Security Delta nlnet FOUNDATION

How to join the Trusted Routing

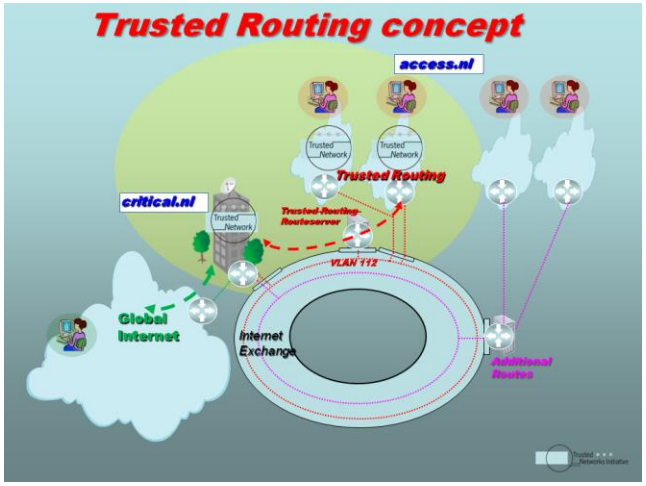
The Trusted Networks Initiative is focusing at content operators with (critical) websites using their own AS, IP and BGP4 routing facilities. Additionally the initiative is focusing at fixed and mobile access networks with a significant number of subscribers that should always be able to visit the (critical) websites. General information can be found at:
http://www.trustednetworksinitiative.nl/



Parties that meet the qualification requirements for being a Trusted Network, based upon the 'Trusted Networks Policy', can have themselves qualified by sending a Qualification Request to the chairman of the Trusted Networks Initiative. Both the Qualification-memo and Policy can be downloaded from:

http://www.trustednetworksinitiative.nl/

Being qualified, the party can request to the participating internet exchanges to be connected to the technical Trusted Routing infrastructure. The Trusted Routing is initially available at the Dutch internet exchanges NL-ix and AMS-IX.



Trusted Routing is available at NL-ix and AMS-IX

Specific information per exchange is available at:

http://www.nl-ix.net/trusted-routing

https://ams-ix.net/trusted-networks-initiative

Note that parties that already have a port at these exchanges may activate Trusted Routing at hardly more costs.

Frequently Asked Questions

Q: *Is the Trusted Routing the new alternative for existing mitigation and scrubbing solutions?*
A: No, Trusted Routing is an additional last resort solution on top of existing solutions.

Q: *Is the Trusted Routing to other 'Trusted Networks', activated centrally and collectively, or decentralized and independently ?*
A: The Trusted Routing is activated independently by each individual network. There is no 'central authority'.

Q: *Is it true that internet users at non-Trusted Networks may not be able to reach a website at a Trusted Network during a large DDoS attack ?*
A: Yes, however other internet users at the Trusted Networks can still reach that website, which is far better than not being reachable at all.

More information

http://www.trustednetworksinitiative.nl/
info@trustednetworksinitiative.nl