

P2P VPN Problem Statement

Discussion of Issues

History

10/14/2011 draft-nir-ipsecme-p2p-00.txt

ipsecme WG agreed to focus on use case 2

3/5/2012 draft-ietf-ipsecme-p2p-vpn-problem-00.txt

Use cases only for now. No requirements.
Discussed on ipsec list.

3/20/2012 Created 13 issues based on discussion.
Agreeing on issue resolutions.

Issue #210: What Should We Call This Effort?

- Postponed

211: We should talk more about why this is a hard problem

- Description
 - Explain more clearly what the hard parts are
- Proposed Resolution
 - Add Requirements to do this
- Response
 - Agreement

212: Section 2.2 should be more detailed

- Description
 - Gateway-to-Gateway P2P VPN Use Case Needs More Motivation and Explanation
- Proposed Resolution
 - Explain use case better, using VOIP traffic between branch offices as example
- Response
 - Agreement but don't add new acronyms

213: In use case 2.1, direct endpoint-to-endpoint connectivity may not be possible

- Description
 - In Endpoint-to-Endpoint P2P VPN Use Case, direct endpoint-to-endpoint connectivity may not be possible if both endpoints are NATed
- Proposed Resolution
 - Mention this in section 2.1
- Response
 - Can solve with existing NAT traversal techniques
- Revised Resolution
 - Mention existing NAT traversal techniques also

214: Should gateways figure things out completely or just punt endpoints to a closer gateway?

- Description
 - Two interpretations
 - Should “initial core gateway” be required to fully configure satellites or can it punt them to another gateway?
 - Should we cover cases where endpoint cannot communicate directly with another endpoint but must go through gateway?
- Proposed Resolution
 - First interpretation is solution-specific so premature
 - Second interpretation is covered by 213
- Response
 - Agreement

215: Should traffic flow through the gateway while a shortcut is being established?

- Description
 - Should traffic continue to flow through the gateway while a shortcut is being established?
- Proposed Resolution
 - This is solution-specific, unless we believe there's a requirement for it. Either way, it's not a use case.
- Response
 - No response. Means agreement?

216: Multiple interfaces or mobile endpoint

- Description
 - What if an endpoint has multiple interfaces and/or is mobile? Which tunnels should be torn down as this endpoint moves around, sometimes behind a gateway and sometimes not?
- Proposed Resolution
 - This is solution-specific
- Response
 - Or maybe there's some requirement here?

217: Temporary Credentials

- Description
 - Endpoints may require temporary credentials in order to establish a secure connection to another endpoint
- Proposed Resolution
 - Put this in the requirements section
- Response
 - Agreed. Discussion on PSK vs. PKI.

218: Exhaustive configuration

- Description
 - Exhaustive configuration can work fine if there are good automated configuration protocols
- Proposed Resolution
 - Exhaustive configuration doesn't scale for constrained devices in large networks. Explain this in section 3.1.
- Response
 - Agreed. Also, IP addresses and lists of authorized users change continuously, which causes serious problems for exhaustive configuration in a large network.

219: Star topology as an admin choice

- Description
 - Some admins prefer a star topology so they can inspect traffic. They may not want to use P2P VPN.
- Proposed Resolution
 - Mention this in the Security Considerations section.
- Response
 - Agreed, but note that admin may choose to allow P2P VPN for some purposes (e.g. VOIP, intra-organization, gateway-to-gateway).

220: Dangling Paragraph

- Description
 - The last paragraph of section 3.2 doesn't belong in that section
- Proposed Resolution
 - Delete that paragraph
- Response
 - No response. Means agreement?

221: IPsec Architecture and Proprietary Approaches

- Description
 - In section 3.3, we should say that proprietary approaches may not implement all the checks in the IPsec architecture
- Proposed Resolution
 - Add this to section 3.3
- Response
 - No response. Means agreement?

Next Steps

- March 26 Publish updated issue resolutions based on email discussions and WG meeting.
- IETF Week Verify WG consensus on resolutions. Agree on name.
- April 2 Publish revised I-D with updated use cases and name. Solicit requirements.
- April Discuss and agree on requirements.
- Early May Publish new I-D with requirements. Solicit solutions.
- End of June Proposed solutions due. Discuss on list and in Vancouver.
- August Decide on solution. Start refining.