IPsec, VPNs and the Dynamic VPN Controller (DVC)

Michael Froh
Cinnabar Networks, Inc.

Cinnabar Networks, Inc.
265 Carling Avenue, Suite 200
Ottawa, Ontario
K1S 2E1

Contractor Report Number: **DRD004-001**
Contract Number: **W7714-3-2894**
Contract Scientific Authority: **S. Zeber (613) 991-1388**

Defence R&D Canada

Contract Report
DRDC Ottawa CR 2004-060
March 2004

National Defence | Défense nationale

Canada

TABLE OF CONTENTS

List of Figures

List of Tables

1 INTRODUCTION

IP Security (IPsec) protocols and Virtual Private Network (VPN) products that implement these protocols can provide authenticated secure network communication channels. Defence Research and Development Canada (DRDC) Ottawa has been studying the use of VPN technology to support secure communications for dynamic coalitions and has developed a prototype Dynamic VPN Controller (DVC) to demonstrate how this technology could be applied to dynamic coalitions.

The dynamic coalition environment requires flexible, scalable and secure solutions. Based on experience gained from implementing the DVC, there are several capabilities missing from existing IPsec implementations that are required to support dynamic coalitions.

1.1 OBJECTIVE

The objectives of this report are to:

- Articulate dynamic coalition usage scenarios and their VPN requirements;
- Highlight the capability maturity of IPsec products for use in dynamic coalitions;
- Evaluate the DVC prototype capabilities; and
- Identify further IPsec and VPN research areas to support dynamic coalitions.

1.2 APPROACH

The Statement of Work (SOW) required that a general review of IPsec and VPN technology be performed including a review of the DVC prototype developed by DRDC Ottawa. The approach taken in performing this work was the following:

- Conduct a general World Wide Web (WWW) search of IPsec papers and implementations;
- Review DVC documentation;
- Discussions with DVC implementers;
- Attend a DVC demo;
- Discussions with IT Security Authority within DND; and
- Synthesis of the above material into this report.

1.3 DOCUMENT STRUCTURE

The document is structured as follows:

- Section 2 contains an examination of various VPN deployment scenarios with particular attention to dynamic coalition VPNs and the Department of National Defence (DND);
- Section 3 examines the state of the IPsec standards efforts and a discussion of IPsec capabilities fundamental to deploying large scale dynamic coalition VPNs. This section also examines the capabilities of open-source IPsec implementations as well as those in commercial and military products;
- Section 4 provides a brief overview of the DRDC DVC prototype and examines limitations based on the dynamic coalition deployment scenarios described in Section 2;
- Section 5 concludes with some suggested areas of further research;

- Appendix A and Appendix B contain references and acronyms, respectively;
- Appendix C contains initial thoughts on a potential implementation of a DVC using Secure Shell (SSH) as a potential further research area; and
- Appendix D contains information found on the Internet about the National Security Agency's (NSA) High Assurance Internet Protocol Interoperability Standard (HAIPIS), which forms the basis of most of the military IPsec implementations found in Section 3.3.3.

2 VPN DEPLOYMENT SCENARIOS

A number of distinct VPN deployment scenarios are examined in this section ranging from Wide Area Networks (WAN) and Road-Warriors to dynamic coalitions.

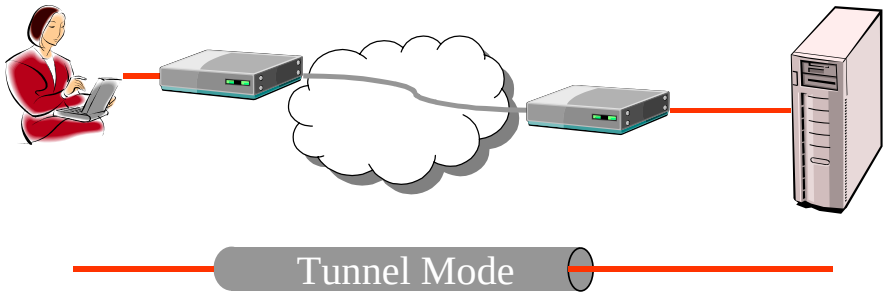
2.1 IPSEC VPN CONSTRUCTS

IPsec has two distinct protocols for protecting Internet Protocol (IP) information: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides integrity protection only to the IP header and the payload. ESP provides integrity and/or confidentiality protection to an inner (red) IP header and the payload but does not protect the outer (black) IP header. Each of these protocols can be used to protect communications in one of two distinct modes: transport and tunnel. By definition, security gateways can only act in tunnel mode whereas end-systems can use both tunnel and transport modes.

Communicating IPsec entities establish unidirectional sets of security parameters including keys in a construct called a Security Association (SA). Information is protected by either the AH or ESP transforms using the SA.

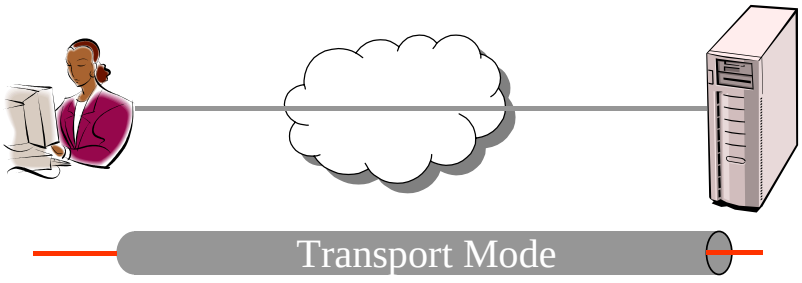
The “private” in IPsec VPN is somewhat unclear in that it could mean information protected using encryption or it could also mean the use of a private IP address space. The former only applies to the ESP transform that provides encryption and the latter case applies only to tunnel mode that encapsulates an inner “red” IP header.

Figure 1 shows a typical tunnel mode IPsec connection while Figure 2 shows a transport mode IPsec connection.



Information is protected only between gateways.

Figure 1 – Tunnel Mode VPN



Information is protected from client to server.

Figure 2 – Transport Mode VPN

It is possible to establish complex SA combinations, or bundles, where a single IPsec entity may need to perform multiple transforms on a packet of data on transmission or reception. Figure 3 shows an SA bundle constructed by applying a transport mode transform, then a tunnel mode transform on outgoing packets at the client.

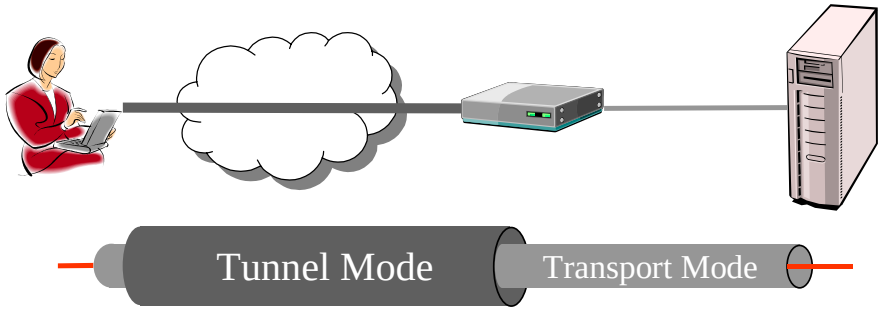


Figure 3 – Security Association (SA) Bundle VPN

IPsec is an address-aware protocol that requires address transparency as explained in [Carpenter]. That is, IPsec cannot tolerate any Network Address Translation (NAT) in its packets in transit since the selection of appropriate keying material is dependent on knowing the IP address of the remote peer IPsec entity. [Carpenter] further explains that the predominance of Intranet private networks protected by firewalls employing NAT has throttled the ability to deploy end-to-end IPsec protections.

2.2 WAN SCENARIOS

In a typical WAN scenario, multiple locations from a single organization establish wide area communication connections using IPsec ESP tunnels between firewall/gateway devices. This scenario has seen significant deployment in the last few years since it provides a significant Return on Investment (ROI) by eliminating the costs of leasing long-haul data communications links.

A typical WAN VPN is shown in Figure 4 with the following characteristics:

- Connections are usually fully meshed but could be hub & spoke (for example, all satellite offices connect to the Head Office location);
- Each site usually has an external (black) static IP address;
- Static keying configuration is often used;
- Static access configuration where typically any host can talk to any other host on a remote site; and
- Usually employs a privately managed IP address space.

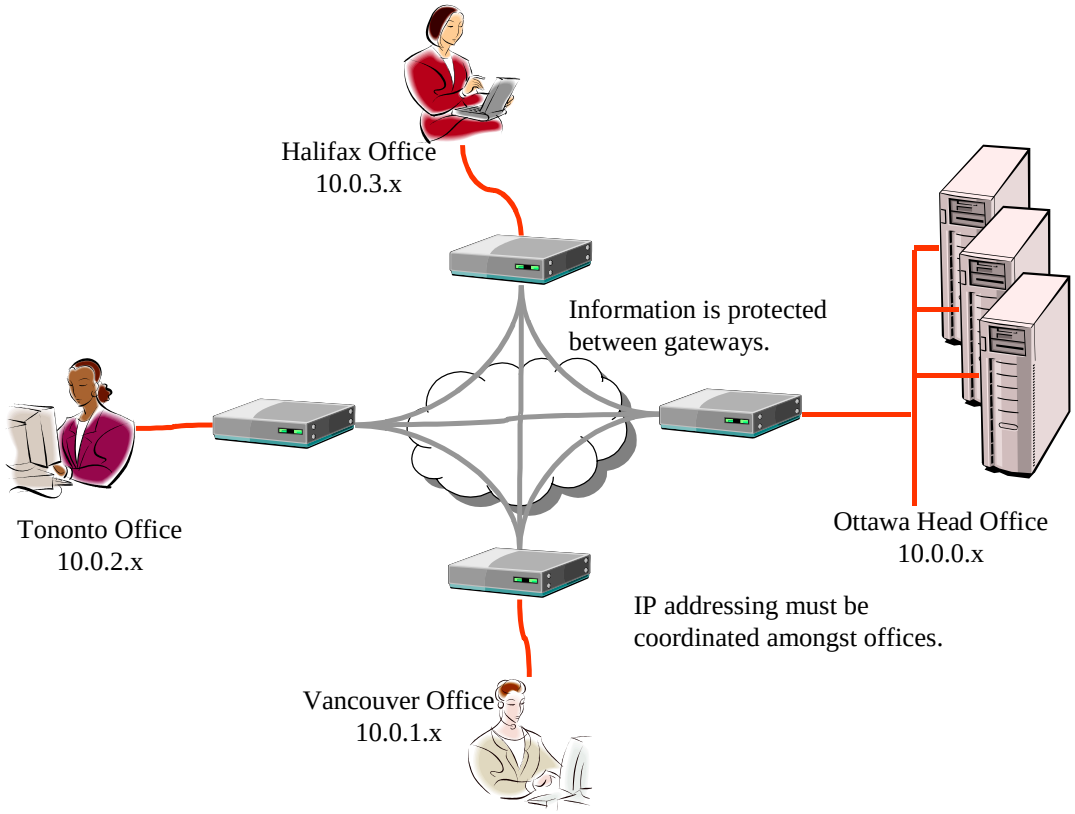


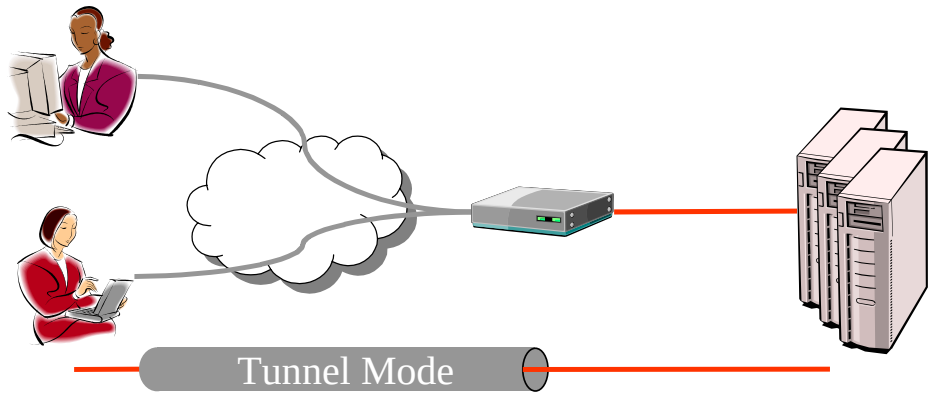
Figure 4 – Wide Area Network (WAN) VPN

2.3 ROAD-WARRIOR AND TELE-WORKING SCENARIOS

Typical road-warrior and Tele-working scenarios have employees of an enterprise connecting to their office either while traveling or from home (for example, [Denker]). This scenario has seen substantial deployment in the last few years since it provides a significant ROI by eliminating corporate modem pool maintenance and long distance dial-in costs.

A typical Tele-working VPN is shown in Figure 5 with the following characteristics:

- Hub & spoke configuration;
- Clients have external (black) dynamic IP addresses;
- Static keying only works for small configurations (<100 clients) with larger configurations requiring scaleable authentication mechanisms (mainly X.509 certificates);
- Static access configuration where the Tele-worker appears to be on the local work network; and
- Usually employs a privately managed IP address space but the work network must now issue a valid internal IP address.



Information is protected from client to gateway.

Figure 5 – Road-Warrior or Tele-work VPN

2.4 EXTRANETS

An extranet is typically used to allow business partners into a corporate network. The usual reason for establishing extranets is the establishment of supply chain management (that is, suppliers and buyers form trusted paths of communication). This scenario has seen limited deployment in the last few years since its ROI is typically the elimination of costly inventory. Note that extranets can also be built using non-IPsec technologies as well.

In cases where there are strong industry leading companies, hub and spoke VPNs can be established. For example, the three largest United States (US) automotive manufacturers established the Automotive Network eXchange (ANX), an IPsec hub-spoke VPN, to establish communications with its suppliers. [Messmer] notes that ANX is having interoperability problems with multiple vendors IPsec equipment.

The ANX network is shown in Figure 6[1] with approved Internet Service Providers (ISPs) providing connectivity (that is, the squares at end-systems are IPsec VPN devices). Extranets typically have these characteristics:

- Hub & spoke configuration;
- Clients usually have external (black) static IP addresses;
- Depending on the complexity of the supply chain, static keying can be used for authentication. Larger extranets need X.509 based authentication;
- Static access configuration where the supplier has access to only specific applications within the corporate network; and
- Usually employs privately managed IP address spaces at both the supplier and the buyer.

[1] Diagram is copyright © ANXeBusiness Corp. (Hhttp://www.anx.com/extranet/managed-services.html#networkH)

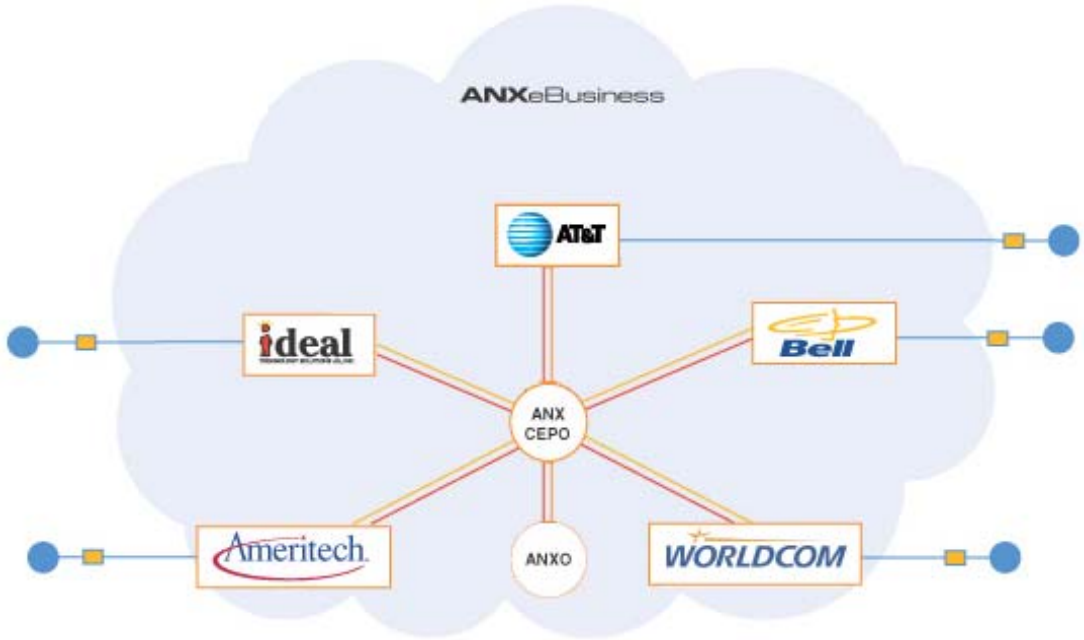


Figure 6 – Extranet VPN

2.5 COALITION SCENARIOS

Coalition is defined as "*a temporary alliance of distinct parties, persons, or states for joint action*":[2]

- *Temporary* implies that the VPN must be configured, used and then torn down. How quickly a situation changes will help determine the temporary nature of the coalition and how quickly the coalition needs to be configured and torn down;
- *Distinct Parties* implies that all participants are independent having their own IT infrastructure and policy. Therefore, there will be distinct security policy administrative domains that must negotiate a mutually acceptable policy for communication within the coalition. Coalitions will typically have a lead entity which may dictate aspects of security policy to which participants may decide to join or not join the coalition; and
- *Joint Action* implies that a coalition is formed for some distinct purpose and this implies that there is some need for joint information sharing to support the joint action. The nature of the information sharing will depend on the coalition and its purpose.

A significant aspect of establishing a dynamic coalition depends on whether the coalition involves the establishment of mobile or rapidly deployed sites as opposed to a dynamically formed coalition based on sharing strategic Information Technology (IT) assets. In almost all mobile or rapidly deployed transient cases, there will be a simultaneous requirement for connectivity from the mobile element back to a corporate or headquarters strategic entity. Therefore, dynamic coalitions will always include strategic entities and may include mobile or transient entities.

Examples of dynamic coalition VPNs include:[3]

[2] Merriam-Webster on-line dictionary, Hhttp://m-w.comH.

[3] Note that the scenarios examined here do not include consideration for examining higher level abstractions of multiple concurrent coalitions. For example, considerations on how to handle multiple coalitions, handling cross-coalition chatter, or defining meta-coalition policy is not examined and left for future study.

- Business teaming agreements for joint bids, product development, etc. These agreements typically define the nature of the information sharing in a Non-Disclosure Agreements (NDA). An NDA will typically define distinct entities within each party who are responsible for managing the information transfer under the NDA. That is, this entity will regulate what local information can flow to the remote party, and what local entities can access remote party information. Resulting VPNs will typically involve static IT assets and can be established for short to long time periods;
- Government and Non-Government Aid organizations distributing aid. These are typically rapid deployment scenarios that can be national or international in scope. United Nations (UN) organizations such as the World Food Program (WFP) will deploy to many needy nations around the world and require close coordination with non-Government Organizations (NGOs) to distribute food. Depending on the security of the environment, close coordination is also required with local police and military forces, as well as UN based forces;
- First Responders deploying to disaster sites. Police, fire and ambulance will respond to disaster sites and can establish local command posts. Coordination is required between all of the available first responders, as well as with other civilian (for example, industrial building owners) and government organizations (for example, municipal utilities or military ordinance experts);
- Military Forces working on joint military deployments. Examples include UN and North Atlantic Treaty Organization (NATO) deployments as well as ally-led coalitions such as the Gulf War. Coordination is required amongst deployed mobile units as well as each nation's strategic networks; and
- Military Forces working on *Aid to the Civil Power* deployments. These scenarios require close coordination between a nation's military and its national, provincial and municipal police forces in both a strategic and mobile setting. Coordination is also required at the strategic level to various levels of government.

A dynamic coalition VPN is shown in Figure 7 and has these characteristics:

- Fully meshed mobile deployments and strategic IT environments with hub and spoke strategic to mobile connectivity;
- Mobile elements may have external (black) dynamic IP addresses whereas strategic elements have static IP addresses;
- Static keying only works for small configurations (<20 parties) with larger configurations requiring scaleable X.509 authentication mechanisms;
- Relatively dynamic access configuration depending on how the joint action evolves; and
- Parties will likely employ privately managed IP address spaces.

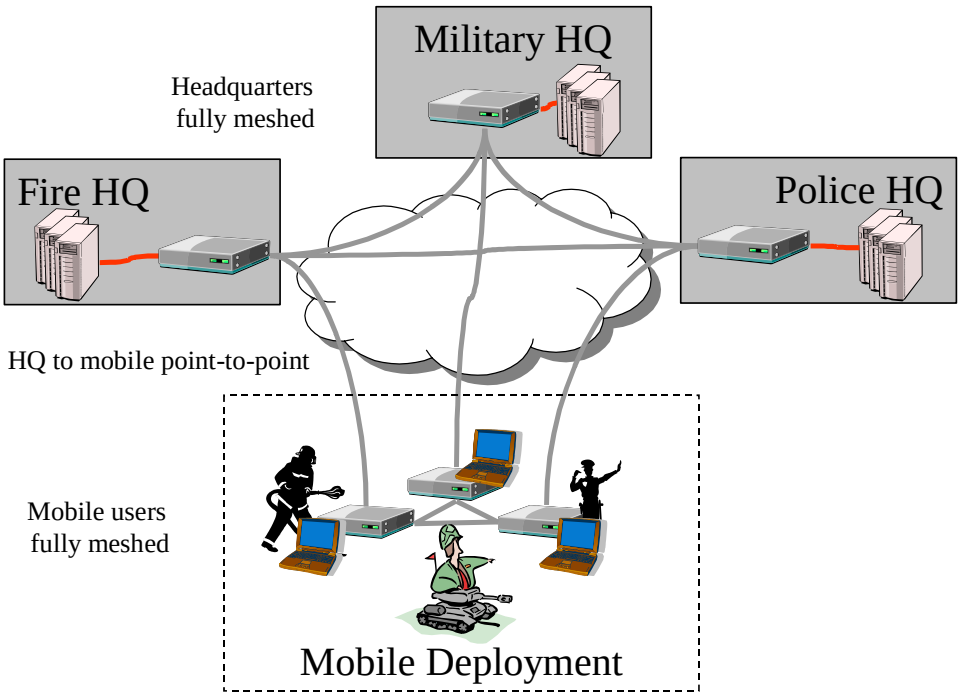


Figure 7 – Dynamic Coalition VPN

2.5.1 SERVER BASED OR EDGE COMPUTING MODELS

An important consideration in forming dynamic coalitions depends on the computing model used to share information within the coalition. As noted in [Carpenter], the use of edge computing requires address transparency. Therefore, the deployment of large-scale edge computing applications such as Voice over IP (VoIP) cannot be easily solved if NAT is present at coalition boundaries.

However, if the computing model is server based, then address transparency is not a requirement of the coalition.

Organizations that participate in dynamic coalitions will be faced with the dual requirements of wanting to deploy edge-computing applications, such as VoIP, versus the need for managing the risk to their IT infrastructures. The former requires end-to-end network transparency whereas the latter strives to expose only the required infrastructure elements needed to achieve the coalition actions.

2.5.2 DYNAMIC COALITION VPN REQUIREMENTS

Based on the definition of a coalition, as well as reasoning from the dynamic coalition examples, the following are considered a reasonable set of dynamic coalition VPN requirements:

- Communications amongst coalition members must be secured from external threats;
- Local parties should have complete control over their local IT resources and people involved in the coalition. Changes to either the resources or people accessing the coalition should be not require further VPN policy negotiation with remote parties;
- Local parties should be able to deploy autonomously managed authentication schemes for authenticating their local users prior to providing access to the coalition resources;

- Local users should not have to acquire new authentication credentials in order to access remote coalition party resources. The distribution of new credentials can seriously hamper the rapid deployment of dynamic coalitions unless it can be done in a fully automated fashion;
- The establishment of a dynamic coalition should not require local parties to alter their physical strategic IT infrastructure. For example, membership in the coalition should not require the establishment of a physically isolated Local Area Network (LAN). The deployment of mobile assets necessarily implies that IT assets are physically re-located and configured;
- The establishment of a dynamic coalition should not require a priori coordination of the logical strategic IT infrastructure. For example, it should be possible to establish a coalition without having to change a private IPv4 address space. The deployment of mobile assets may require changes to the IT asset logical infrastructure;
- It is highly desirable that a coalition party can audit the information exchanged as part of the coalition from its coalition VPN gateway. Providing auditing at the gateway provides a more manageable scenario than auditing at all servers and edge-computing nodes within the party's coalition committed assets. This implies that end-to-end IPsec tunnels cannot be used in some coalition scenarios;
- It is desirable that mobile coalition deployments have the option of using locally provided communications assets (for example, local public telephone infrastructure, ISP, leased data lines, cellular network, etc.). Not all coalition parties that engage in mobile deployments will have autonomous WAN connectivity back to their strategic network (for example, using tactically deployed satellite). Hence, the outer (black) coalition addresses may be dynamically assigned from the local ISP IPv4 address pool; and
- It is highly desirable that the security policy negotiation amongst coalition parties be implemented with the least amount of *a priori* knowledge. This does imply that coalition members implement standards which provide:
    - a high-level security policy language,
    - gateway discovery,
    - policy discovery,
    - policy distribution,
    - policy resolution,
    - a model to translate high-level policies to IPsec SAs, and
    - a means of checking compliance of SAs to the high-level policy.[4]

2.6 DEPARTMENT OF NATIONAL DEFENCE (DND) DYNAMIC COALITIONS

DND currently deploys IPsec VPN technology in several parts of its IT Security Architecture as shown in Figure 8 [DDCEI]:

- Tele-worker VPN dial-in to the Defence Wide Area Network (DWAN);
- WAN Intranet using commercial IPsec VPN products for the DWAN;
- WAN Intranet using high-grade IPsec VPN products for the Classified Network (CNet);

[4] All of these are IPSP requirement [Blaze] objectives as noted in Section 3.2.2.

- Extranet DWAN connectivity with suppliers using commercial IPsec VPN products; and
- Extranet CNet connectivity with allies using high-grade crypto and commercial firewalls.

Note that blue and red lines represent Designated and Classified information, respectively.

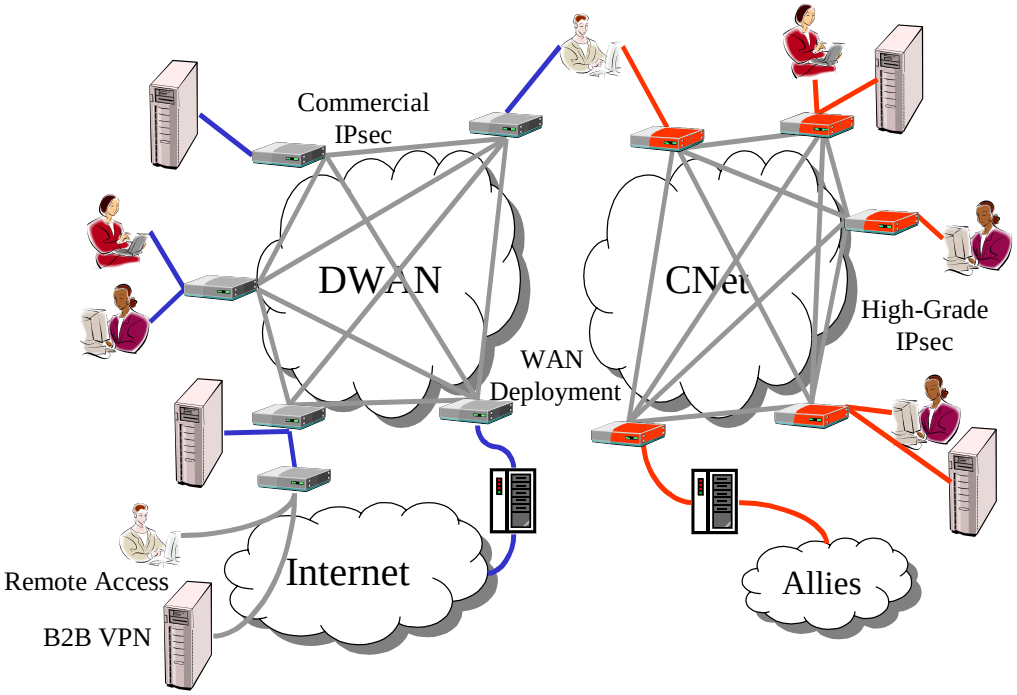


Figure 8 – DND IT Security Architecture

In general, the current DND IT Security Architecture employs the "crunchy outside, soft inside" approach as noted in [Carpenter]. It is interesting to note that the original architecture document [DDCEI] detailed end-to-end IPsec VPNs within the DWAN for specific hosts; however, this has not been implemented due to the management limitations of existing IPsec VPN products. Although the architecture calls for end-to-end IPsec VPNs, it only does so within a specific isolated private network within the architecture; therefore, end-to-end transparency is still not achieved, as noted in [Carpenter].

DND has the capability to deploy commercial satellite backhaul links from field deployments to their strategic IT infrastructure. However, local telecommunications are sometimes used (for example, local ISPs). In some cases, DND will participate in deployed allied networks, but these networks are a closed environment with no connectivity back to national network assets.

DND is unique within the Federal Government in the realm of Information Operations (IO) doctrine [IO]. IO is a multi-faceted approach, which aims at information supremacy during times of conflict. DND's unique role is that it will not only provide defensive IO measures to protect its IT assets from Computer Network Attack (CNA), but it also has an offensive IO capability as well. In light of the very strong emphasis on defensive IO within the department, it is unlikely that true end-to-end network transparency as described in [Carpenter] will ever be deployed. That is, DND will always maintain well-defined gateways into their networks as a primary element in deploying Defence in Depth [NSA]. For example, existing classified connections with allies provides no network visibility and limits services to email and web application proxies. Additionally, DND has deployed private IPv4 addresses on its internal networks so network transparency is not possible.

3 IPSEC VPN TECHNOLOGY

This section examines IPsec VPN technology as identified in the Security Architecture for the Internet Protocol [Kent]. Specifically, the state of the Internet Engineering Task Force (IETF) standards is examined, followed by a discussion of IPsec capabilities required by dynamic coalition VPNs, and closing with a brief view of available open-source, commercial and military IPsec products.

3.1 IPSEC STANDARDS

The following IETF Working Groups (WG) are producing standards related to IPsec:

- IP Security Protocol (ipsec) WG [ipsec] developed all of the existing IPsec standards. Their current short-term work items are to improve the existing key management protocol (Internet Key Exchange, IKE) and IPsec encapsulation protocols. Version 2 of these protocols is currently being worked on. Specific tasks include:
    - *"Changes to IKE to support NAT/Firewall traversal,*
    - *Changes to IKE to support [Stream Control Transmission Protocol] SCTP,*
    - *New cipher documents to support [Advanced Encryption Standard – Cipher Block Chaining] AES-CBC, [AES – Message Authentication Code] AES-MAC, [Secure Hash Algorithm] SHA-2, and a fast AES mode suitable for use in hardware encryptors,*
    - *IKE [Management Information Base] MIB documents,*
    - *Sequence number extensions to ESP to support an expanded sequence number space, and*
    - *Clarification and standardization of rekeying procedures in IKE."*;
- IP Security Policy (ipsp) WG [ipsp] has been ongoing since 1999. A proposed security policy protocol [Sanchez] was tabled but has since dropped from the WG. Therefore, the WG is only working on the IPsec modeling at the moment.
    - *"Specify a repository-independent Information Model for supporting IP security Policies. This model preferably derives from the Information Model as defined in the Policy Framework WG,*
    - *Develop or adopt an extensible policy specification language. The language should be generic enough to support policies in other protocol domains, but must provide the necessary security mechanisms that are vital to IPsec,*
    - *Provide guidelines for the provisioning of IPsec policies using existing policy distribution protocols. This includes profiles for distributing IPsec policies over protocols such as [Lightweight Directory Access Protocol] LDAP, [Common Open Policy Service] COPS, [Simple Network Management Protocol] SNMP, and [File Transfer Protocol] FTP,*
    - *Adopt or develop a policy exchange and negotiation protocol. The protocol must be capable of: i) discovering policy servers, ii) distributing and negotiating security policies, and; iii) resolving policy conflicts in both intra/inter domain environments. The protocol must be independent of any security protocol suite and key management protocol. Existing protocol work in the IETF, such as [Service Location Protocol] SLP, will be considered if such protocols meet the requirements of this work, and*
    - *Work with the "Policy Terminology" design team to define a common set of terms used in documents in the area of Policy Based (Network) Management."*;

- Profiling Use of PKI in IPSEC (pki4ipsec) WG [pki4ipsec] has just started and it hopes to delivery the following two items by Jan 2005:
    - "*A standards-track document that gives specific instructions on how X.509 certificates should be handled with respect to the IKEv1 and IKEv2 protocols. This document will include a certificate profile, addressing which fields in the certificate should have which values and how those values should be handled. This effort is the WG's primary priority, and*
    - *An informational document identifying and describing requirements for a profile of a certificate management protocol to handle PKI enrolment as well as certificate lifecycle interactions between IPsec VPN systems and PKI systems. Enrolment is defined as certificate request and retrieval. Certificate lifecycle interactions are defined as certificate renewals/changes, evocation, validation, and repository lookups.*";
- IKEv2 Mobility and Multihoming (mobike) WG [mobike] has just started and will focus on the extensions to the IKEv2 protocol required to enable its use in the context where there are multiple IP addresses per host (multihoming, SCTP) or where the IP addresses changes in the control of the IPsec host (mobility and roaming). It hopes to complete its mandate by Dec 2004 and is being supported by both Ericsson and Nokia. Its specific goals are:
    - *"IKEv2 mobile IP support for IKE SAs. Support for changing and authenticating the IKE SA endpoints IP addresses as requested by the host,*
    - *Updating IPsec SA gateway addresses. Support for changing the IP address associated with the tunnel mode IPsec SAs already in place, so that further traffic is sent to the new gateway address,*
    - *Multihoming support for IKEv2. Support for multiple IP addresses for IKEv2 SAs, and IPsec SAs created by the IKEv2. This should also include support for the multiple IP address for SCTP transport. This should also work together with the first two items, i.e. those addresses should be able to be updated too,*
    - *Verification of changed or added IP addresses. Provide way to verify IP address either using static information, information from certificates, or through the use of a return routability mechanism,*
    - *Reduction of header overhead involved with mobility-related tunnels. This is a performance requirement in wireless environments, and*
    - *Specification of PF_KEY extensions to support the IPsec SA movements and tunnel overhead reduction."*; and
- IPsec KEYing information resource record (ipseckey) WG has established what information is needed in an IPSEC-specific keying resource record. The content of the resource record includes a Domain Name Service (DNS) KEY record and other useful IPSEC information, such as that required for Opportunistic Encryption.

3.2 IPSEC CAPABILITIES FOR DYNAMIC COALITIONS

A number of key features or capabilities are required in IPsec product implementations in order to support generalized dynamic coalitions. Specifically, the areas of interest in each of the following sub-sections have been identified as being crucial to supporting large-scale dynamic coalitions.

3.2.1 ELECTRONIC KEY MANAGEMENT[5]

IPsec has IKE as a standard protocol for negotiating keying material between IPsec entities. IKE establishes ESP and AH keys at run-time based on Diffie Hellman key exchange. IKE supports two methods of authenticating the remote IPsec entity: pre-shared secrets and X.509 public key infrastructure (PKI) certificates.

Pre-shared secrets require the *a priori* establishment of (n)(n-1)/2 keys prior to the start of a fully meshed dynamic coalition. Since the manual key distribution scales at approximately n^2, pre-shared secrets are not suitable for large coalitions. By definition, the exchange of pre-shared requires both authenticity and secrecy.

PKI does not share the n^2 problem of pre-shared keys. Rather it requires the distribution of n certificates to coalition parties from one or more Certificate Authorities (CA). Certificate distribution requires an authenticated channel but does not require secret information exchange. However, a CA defines an administrative domain. By definition a dynamic coalition is composed of *distinct parties*, which implies multiple administrative domains, or multiple CAs in the PKI case. Some coalitions may define an overall administrative domain CA (for example, NATO). In truly dynamic coalitions, each party's CA must be cross-certified with every other coalition member, which requires cross-certifications of the order n^2. Like certificate distribution, cross-certification requires only an authenticated channel. Compared to the pre-shared key scenario, cross-certification requires only the authenticated exchange of certificates and does not require the exchange of secret information.

The Kerberized Internet Negotiation of Keys (kink) WG [kink] is working to standardize the use of Kerberos as a valid electronic keying mechanism for IKE. However, Kerberos is only suitable for a single administrative domain. Again, a dynamic coalition implies multiple administrative domains by definition. Note that Kerberos, or other identity management schemes, could be used by a coalition party to authenticate the people allowed access to the coalition resources. Like pre-shard secrets, Kerberos requires the distribution of authenticated and secret initial information.

In the context of large and truly dynamic coalitions, the term "electronic key management" refers to managing the identities of coalition members without the need for secret distribution of keying material. Therefore, pre-shared secrets and Kerberos are not feasible. PKI is left as the only viable alternative in establishing large dynamic coalitions and where the parties have not necessarily had previous relationships. PKI still requires a cross certification exercise of order n^2, where n is the number of coalition parties. The cross certification effort does require the authenticated exchange of CA certificates but no secret information exchanges.

3.2.2 POLICY BASED CONFIGURATION AND OPERATIONS

By definition, a dynamic coalition is composed of *distinct parties*, which implies distinct administrative domains. Therefore, a necessary part of establishing a dynamic coalition is the negotiation of mutually acceptable security policies amongst the coalition participants. Note that *mutually acceptable* does not necessarily imply that all coalition members agree to the same policy. Some coalitions may be governed by group-ratified policies (for example, adherence to NATO security policy for a NATO coalition). However, many coalitions will be governed by many bilateral policy agreements amongst the various members.

[Bacic] identifies that *"every policy expression must be relatively simple and it must be possible for anyone with a reasonable computer education and knowledge of security and policy*

[5] Note that group key management is not considered but may be applicable to some types of dynamic coalitions. This is left for further study.

particulars to define valid and strong policies … It is crucial that policy writing be made as easy as possible for the policy writer to define policies in the language of the policy engine … support a rich set of logical expressions."[6] IPsec implementations supporting dynamic coalitions must fulfil these requirements. Large-scale coalitions may involve hundreds of parties particularly if multiple parties are provided by single organizations (for example, the Canadian Forces might have several strategic and many tactical interfaces into a UN coalition). The ability for policy writers to clearly understand the aspects of a stated policy depend very heavily on the characteristics identified above.

As noted in [Bacic], IPsec VPN security policy is a specific network policy[7] that is defined in terms of low-level network constructs and requires the definition of IPsec detailed configuration (for example, cryptographic algorithms, ESP or AH transforms, tunnel or transport mode, etc.). If coalitions are structured with just IPsec tunnels between parties, then the granularity of control in policy that can be enforced by the IPsec product is source and destination IP addresses. If coalitions allow end-to-end IPsec tunnels between clients and servers, the policy granularity at these endpoints can be to X.509 certificate named entities; however, with all the conditions of end-to-end network addressing transparency (see Section 3.2.3).

IP Security Policy (IPSP) Requirements [Blaze] defines some generic requirements *"to provide a scalable, decentralized framework for managing, discovering and negotiating the host and network IPsec policies that govern access, authorization, cryptographic mechanisms, confidentiality, integrity, and other IPsec properties.*"[8]:

- "*A policy model with well-defined semantics that captures the relationship between IPsec SAs and higher-level security policies;*
- *A gateway discovery mechanism that allows hosts to discover where to direct IPsec traffic intended for a specific endpoint;*
- *A well-specified language for describing host policies;*
- *A means of distributing responsibility for different aspects of policy to different entities;*
- *A mechanism for discovering the policy of a host;*
- *A mechanism for resolving the specific IPsec parameters to be used between two hosts governed by different policies (and for determining whether any such parameters exist); and*
- *A well-specified mechanism for checking for compliance with a host's policy when SAs are created.*"[9]

The requirement to define high-level policies [Bacic, Blaze] also implies the need for analysis to ensure consistency [Bacic, Eronen, Fu] and conformance [Blaze], a means of negotiating that policy with peer entities [Blaze], and a means for translating into IPsec specific policies [Blaze]. All of these require automated methods to be truly effective.

The IPSP work to date has been complex [Baltatu00]. The WG has currently defined only the IPSP Requirements [Blaze] and the IPsec Configuration Policy Information Model [Jason]. The information model inherits its complex structure from the Distributed Management Task Force (DTMF) Common Information Model (CIM). While suitable for detailed IPsec entity configuration, the information model is not suitable for coalition policy expression.

[6] [Bacic], Section 1.
[7] [Bacic], Section 4.6.
[8] [Blaze], Section 2.
[9] [Blaze], Section 3.1.

Some early IPSP work to define a Security Policy Protocol (SPP) [Sanchez] was an initial attempt at an application layer protocol for the exchange of IPsec policy information. At least one prototype implementation was constructed [Baltatu01] which included some initial performance measurements. However, it was found to be too flexible and highly complex [Baltatu00, Fu]. Some of this early work on SPP [Baltatu01] found that secure gateway discovery cannot be policy constrained and that confidentiality protection of policies created complexity. Unconstrained gateway discovery and non-confidential policies may not be suitable for some dynamic coalitions.

> *"A critical aspect of the IPSP architecture [SPP] … is its flexibility, which results in the definition of a complex system, therefore a system whose functionality is not trivial to control and which can easily become unmanageable."*[10]

A NSA sponsored project performed in 2001-2002 by Network Associates Incorporated (NAI) Labs developed a scaleable IPsec policy configuration system [NAILabs1, NAILabs2, NAILabs3, NAILabs4]. This work examined several policy provisioning protocols including: LDAP, COPS, and SNMP. This study concluded that SNMP was a more appropriate protocol for IPsec provisioning since: it allowed multiple authorities to control a single IPsec device, and it also allowed fine-grained access control methods over particular IPsec policy attributes. The authors of this work produced an open-source implementation of their SNMP management structure [net-snmp] and provided input to the ipsp WG on their IPsec policy experiences. Note that this is a significant piece of work with related open-source code that is being actively developed. However, it still deals with detailed IPsec policies.

3.2.3 IPv6 Support

DRDC, and militaries in general, see IPv6 as an important aspect in their future networks. Support for IPv6 is highly desirable in dynamic coalitions. In particular, the US Department of Defense (DoD) Chief Information Officer has mandated a policy with a goal of transitioning all DoD intra and inter networking to IPv6 by the US government fiscal year 2008 [DoD].

IPv6 will be an important aspect to future networked communications. The extent to which IPv6 will be implemented within the global Internet is unclear for the reasons noted in [Carpenter]. A key issue noted is End-To-End Address Transparency. The following quotes from [Carpenter] identify a key dynamic coalition characteristic remains unresolved:

> *"Underlying a number of the specific developments mentioned below is the concept of an "Intranet", loosely defined as a private corporate network using [Transmission Control Protocol] TCP/IP technology, and connected to the Internet at large in a carefully controlled manner. The Intranet is presumed to be used by corporate employees for business purposes, and to interconnect hosts that carry sensitive or confidential information. It is also held to a higher standard of operational availability than the Internet at large. Its usage can be monitored and controlled, and its resources can be better planned and tuned than those of the public network. These arguments of security and resource management have ensured the dominance of the Intranet model in most corporations and campuses."*[11]
>
> *"Firewalls, by their nature, fundamentally limit transparency."*[12]

[10] [Baltatu01], Section 3.3.
[11] [Carpenter], Para. 3.1.
[12] [Carpenter], Para. 3.3.1.

> *"Note that private address space is sometimes asserted to be a security feature, based on the notion that outside knowledge of internal addresses might help intruders. This is a false argument, since it is trivial to hide addresses by suitable access control lists, even if they are globally unique - indeed that is a basic feature of a filtering router, the simplest form of firewall. A system with a hidden address is just as private as a system with a private address. There is of course no possible point in hiding the addresses of servers to which outside access is required."*[13]
>
> *"The loss of transparency at the Intranet/Internet boundary may be considered a security feature, since it provides a well defined point at which to apply restrictions. This form of security is subject to the "crunchy outside, soft inside" risk, whereby any successful penetration of the boundary exposes the entire Intranet to trivial attack. The lack of end-to-end security applied within the Intranet also ignores insider threats."*[14]

The parties identified in the example dynamic coalitions will all have moderate to high security concerns. Therefore, they will all likely retain the notion of an *Intranet* and tightly control the access. But these same parties will likely want to take advantage of address-aware applications like VoIP. When applications are made address aware, end-to-end address transparency is needed. For example, H.323 transmits addressing information in its application payloads; therefore, any loss of address transparency at a node within the network (for example, NAT at a firewall) requires a corresponding Application Layer Gateway (ALG), which is application protocol aware.

Note that militaries have two valid reasons for keeping end-to-end addressing information private:

- If they participate in offensive IO, they will require strong defensive IO positions. Network addressing schemes can provide a significant amount of intelligence about an organization; and
- Military forces have a great concern about traffic flow security and its observation in deriving valuable intelligence particularly with regard to tactical operations.

3.2.4 COMPLEXITY AND IMPLEMENTATION

Complexity seems to be the hallmark of the IPsec, IKE and now ipsp work [Baltatu00, Baltatu01, Ferguson, FreeS/WAN, Jason, Steffen]. Unfortunately, all the flexibility with its associated complexity is extremely detrimental to implementing and deploying secure systems.

[Ferguson] provides a cryptographic evaluation of IPsec and indicates that the protocols (ESP, AH, IKE, and Internet Security Association and Key Management Protocol, ISAKMP) are too flexible and too complex. Note that the FreeS/WAN open source initiative [FreeS/WAN] has implemented those [Ferguson] recommendations that are possible without breaking IPsec interoperability, which results in a non-compliant implementation but one with reduced complexity. As per the [Ferguson] recommendation, AH was removed from FreeS/WAN, and ESP has been modified to provide authentication in every case. Additionally, [Steffen] has tried to address some of the complexity in deploying IPsec VPNs through the development and maintenance of X.509 certificate support in FreeS/WAN.

[13] [Carpenter], Para. 3.4.
[14] [Carpenter], Para. 7.

3.3 IPSEC IMPLEMENTATIONS

The following sub-sections examine the status and direction of IPsec implementations in the open-source, commercial and military communities. The following table provides a brief summary of the various implementations' capabilities (as identified in Section 3.2 above). Blank cells indicate uncertainty in the capability support. Note the following regarding table entries:

- Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) are elements of X.509 PKI support;
- *Scale* is a rough indication of whether the product policy management (Policy Mgmt) scheme is able to scale to large numbers; and
- Network Address Translation – Traversal (NAT-T) supports IPsec through NAT.

Table 1 - IPsec Implementation Capabilities

Implementation	X.509[15]	CRL	OCSP	Policy Mgmt	Scale	IPv6	NAT-T
FreeS/WAN	✓	✓	✓	✓[16]	✓		✓
KAME	✓					✓	
USAGI						✓	
Avaya	×	×	×	✓	✓		
Checkpoint	18 listed in OPSEC Alliance			✓	✓	✓	
Cisco PIX	Baltimore Entrust Verisign	✓	✓	✓	✓		✓
Cisco IOS	Baltimore Entrust Verisign	✓	✓	✓	✓	✓	✓
Military				✓		✓	

3.3.1 OPEN SOURCE

3.3.1.1 FREES/WAN ON LINUX

FreeS/WAN [FreeS/WAN] is an open-source IPsec implementation for Linux consisting of Kernel Level IPsec (KLIPS) and an IKE daemon (Pluto). FreeS/WAN is shutting down its development cycle since they do not believe their goal of Opportunistic Encryption will be implemented any time soon. StrongSec GmbH in Zurich provides X.509 certificate support patches to FreeS/WAN maintained at the Zurich University of Applied Sciences in Winterthur [FreeS/WAN_X509]. The patch(s) include:

- Virtual IP and Dynamic Host Control Protocol, DHCP-over-IPsec protocol for road-warriors;
- Protocol and port selectors in KLIPS;

[15] X.509 refers to basic X.509 certificate processing as part of the IKE daemon.
[16] Using IPsec keys in DNSSEC (RFC 2535).

- Dynamic CRL checking via http, ftp, file and LDAP Universal Resource Indicators (URI);
- OCSP support;
- NAT-T support;
- AES, Twofish, Blowfish, and Serpent encryption algorithms for use in IKE and IPsec ESP; and
- Layer 2 Tunnelling Protocol (L2TP) over IPsec support with Windows 95 / 98 / ME / NT4.0 / 2000 / XP.

A pre-patched version of FreeS/WAN, which includes the X.509, NAT-T, and algorithm patches, is available at [SuperFreeS/WAN].

Interoperability testing is achieved through the FreeS/WAN user community. X.509 certificate interoperability has been achieved with the following implementations:

- OpenBSD isakmpd,
- KAME,
- McAfee VPN (was PGPNet),
- Microsoft Windows 2000/XP,
- SSH Sentinel,
- Safenet SoftPK/SoftRemote,
- 6Wind,
- CheckPoint FW-1/VPN-1,
- Equinux VPN Tracker (Mac OS X),
- Gauntlet GVPN,
- Netasq, netcelo,
- Nortel Contivity, and
- Sun Solaris.[17]

Additional interoperability test results are contained in [Labouret].

3.3.1.2 KAME ON BSD

KAME is the open-source development effort of five Japanese companies. They have a development plan up to Mar 2004 [KAME]. Their IPsec implementation includes both a kernel IPsec engine and an IKE daemon (Racoon). Their implementation is regularly integrated into four stable Berkeley Software Distribution (BSD) releases (FreeBSD 4.0+, OpenBSD 2.7+, NetBSD 1.5+, and BSD/OS 4.2+). This is an active development group with weekly snapshot development releases.

KAME includes support for IPv6.

KAME is conformance tested by the TAHI Project [TAHI]. Interoperability information is not available via their website.

[17] Hhttp://www.freeswan.org/freeswan_trees/freeswan-2.05/doc/interop.htmlH

3.3.1.3 USAGI ON LINUX

UniverSAl playground for Ipv6 (USAGI) is a joint open-source development to deliver production quality IPv6 and IPsec (for both IPv4 and IPv6) protocol stack for Linux [USAGI]. USAGI is being run by a large number of corporate Japanese contributors and is tightly integrated with both KAME and TAHI. It is not clear from their website whether an IKE daemon is supplied.

Interoperability information is not available via their website.

3.3.2 COMMERCIAL

This section includes only a sampling of the available IPsec vendors (for a more complete list see http://vpninsider.com/html/vpnList.php).

3.3.2.1 AVAYA

Avaya (www.avaya.com) provides a series of high capacity IPsec VPN gateways (firewall included) and VPN Service Units (VPN only). There is no claim of X.509 certificate support although Remote Authentication Dial-In User Service (RADIUS) is supported.

Their VPNmanager product can manage an unlimited number of their products. It consists of a management console with IPsec policies pushed to a Netscape LDAP directory. Gateways and remote users then retrieve the policy from the LDAP directory.

Interoperability is claimed with Cisco IOS, 3000 series concentrators, and Netscreen products.

3.3.2.2 CHECKPOINT

Checkpoint (www.checkpoint.com) offers software IPsec VPN products on multiple hardware platforms. This same software is also offered on other system integrator products (for example, Nokia). The Checkpoint IPsec software supports PKI X.509 certificate authentication only between sites and not from remote access users. Remote users have a number of other authentication mechanisms including: RADIUS, SecurID, LDAP, Microsoft Active Directory, Terminal Access Controller Access Control System (TACACS) and XAUTH. Checkpoint announced in a press release on 22nd Dec. 2003 that it delivered its Firewall/VPN product on a Solaris 9 UltraSparc running IPv6. Nokia security products also support IPv6. Checkpoint has a Security Management Architecture that allows the management of large-scale Checkpoint products.

3.3.2.3 CISCO

Cisco (www.cisco.com) provides a number of IPsec enabled products including IOS based routers, 3000 series concentrators, and PIX firewalls. As a sample, the PIX 525 enterprise level firewall was examined. IPsec endpoint authentication can be provided by TACACS, RADIUS or with leading PKI X.509 certificates (Baltimore, Entrust, and Verisign). It was not clear if the PIX firewall supports IPv6. Cisco provides a PIX Device Manager to manage PIX devices; its capabilities are not clear but likely to scale well.

Cisco provides both IPv6, PKI X.509 certificate support, and scalable manageability in its IOS router software.

3.3.3 MILITARY

All of the military (that is, high-grade cryptographic) IPsec implementations found on the Internet were based in the US. All of the products found seem to have been developed under a NSA

High Assurance Internet Protocol Interoperability Standard (HAIPIS). More information on HAIPIS is found in Appendix D. From the various product pages, HAIPIS implies that these products support the following IPsec elements:

- ESP in tunnel mode[18];
- IKE;
- Some form of traffic flow security[19]; and
- Support for US Government Type 1 cryptographic algorithms.

The table below lists products found on the Internet with their capabilities, pricing and HAIPIS certification dates[20].

Table 2 - Military IPsec Implementations

Company	Device	KG	Mbps	# SA	HAIPIS	Cost	Ref
GDC4	FASTLANE	75					[FASTLANE]
GDC4	TACLANE Classic	175	7		Oct04	$10K	[TACLANE]
GDC4	TACLANE E100	175	160		Oct04	$10K	[TACLANE]
GDC4	Sectera INE	235	20		Feb04	$16K	[Sectera]
GDC4			1000		May05		
Viasat	Altasec	250	100		Jan04	$10K	[AltaSec]
Viasat			1000		May05		
Red Eagle	PETRA HAIPIS		0.056				[IASWS03]
Red Eagle	Talon		10	10			[IASWS03]
Red Eagle	INE 100	240	100	512	Dec03	$17K	[IASWS03]
Red Eagle	GX		1000	10000	Jul04		[IASWS03]
Red Eagle			10000		May05		

Additionally, a Communication Security Establishment (CSE) website has an on-line form for ordering cryptographic key material (keymat) suitable for Secure Data Network System (SDNS) cryptographic products [CSE]. This form implies that the Canadian government has deployed the following IPsec-capable products:

- Canadian Network Encryption System (CNES)[21];
- Electronic Key Management System (EKMS) Key Processor (KP/KOK-22A)[22];
- Secure Telephone Equipment (STE/KOV-14C)[23];

[18] ESP is explicitly stated and tunnel mode is inferred based on all product diagrams showing the products as security gateways. It is interesting to note that HAIPIS seems to have implemented two significant recommendations in the IPsec cryptanalysis provided by [Ferguson] which is also the objective of [FreeS/WAN].

[19] IPsec ESP in tunnel mode does provide confidentiality of the red IP headers and multiplexing of multiple data flows between end-systems within the red networks connected by a gateway. The author believes this is the extent of the traffic flow security provided with the possible addition of individual data packet padding.

[20] The speeds, HAIPIS dates, and cost (US dollars) were mainly found in [Lentz], slide 24.

[21] CNES is a Canadian variant of Motorola's Network Encryption System (NES), which is deployed within DND.

[22] The Communications Security Establishment (CSE) has adopted the US Electronic Key Management System (EKMS), which greatly reduces the manual handling of key material. The EKMS employs key processor workstations that require initial keying material before they can generate keys themselves.

- OMNI; and
- GSM SWT[24].

[23] The Secure Telephone Equipment (STE/KOV-14C) is the new replacement for the existing Subscriber Terminal Unit, Third Generation (STU-III). Note that it also uses SDNS keymat.

[24] The author could not ascertain the type of Communication Security (COMSEC) equipment OMNI and GSM SWT are, nor what the acronyms mean.

4 DYNAMIC VPN CONTROLLER (DVC)

The DVC is a DRDC Ottawa funded research prototype developed by NRNS Incorporated [NRNS1, NRNS2, NRNS3, NRNS4, NRNS5, NRNS6]. The prototype, which was derived from the concepts and ideas behind X-Bone [Touch] has been deployed at several international sites to test interoperability issues related to the deployment of dynamic coalitions.

The DVC is built on a FreeBSD platform with a number of additional open source elements:

- OpenSSL for certificate issuance and Secure Sockets Layer (SSL) connections for DVC control;
- X-Bone perl modules to facilitate SSL control sessions;
- KAME for IPsec;
- IP Filter for packet filtering firewall to control access;
- Bind to create name-address bindings in the DNS;
- Zebra to support dynamic routing injection of routes into the local routing domain;
- Apache + mod_ssl to support a DVC user interface;
- *isakmpd* to support key management for IPsec; and
- Keynote as a trust management system.

The first DVC prototype [NRNS1, NRNS2] was completed in 2002 and was functional but rudimentary. Security policies were defined as flat files. A DVC operator web interface provided the local operator with the ability to join and leave coalitions. During coalition establishment, the receiving operator had to explicitly acknowledge the initiating policy. The DVC employs two levels of PKI CA: a DVC project CA that signs the certificates identifying each DVC to the coalition, and a DVC CA, which is a local private CA, that signs the web interface and operator certificates. The DVC is a single platform prototype that includes all the necessary elements to establish a dynamic coalition including:

- Automatic coalition firewall configuration;
- Automatic coalition services DNS update;
- Automatic update of local routing table with coalition routes;
- Automatic configuration of IPsec protection on coalition traffic;
- A local policy definition capability;
- A policy negotiation capability;
- An operator interface to start/stop participation in coalitions; and
- Automatic status reporting on the health of coalition connectivity.

A number of minor improvements implemented in Version 2 in the same year [NRNS3] provided a more stable prototype.

isakmpd proved to be too unstable for the prototype so it was replaced with manual static keying in another version in Jan. 2003 [NRNS4]. This release also saw some additional features in the DVC operator web interface.

In Oct. 2003 a DVC Policy Editor was created as a separate application external to the DVC [NRNS5]. The editor rationalizes the duplication of the flat file configuration in an object-oriented editor where service, local network, local domain, local server, and permitted traffic objects are defined once. These objects are then used to construct site level policies within a coalition. The editor also allows local policies to include expectations that remote policies will include and exclude specific services. Once the policy is defined it can be pushed to the local DVC for automatic renegotiation with its remote peers.

Work is ongoing with the DVC prototype and IPv6 has recently been included. Connectivity is being tested with University College London (UCL) and the University of Murcia (UMU), Spain. As part of this work, [NRNS6] explains how the DVC might integrate with IPv6 PKI and Policy Based Network Management (PBNM) work being done at UMU [Gomez]. The report recommends that the DVC be integrated into the UMU work as a policy negotiator.

4.1 EVALUATION OF DVC CAPABILITIES

The DVC project has provided some excellent prototypes to study the problem of establishing secure dynamic coalitions and the author notes that it is far easier to comment than to create. Notwithstanding, the following evaluation against the established dynamic coalition capabilities are offered:

Table 3 – DVC Evaluation Against the Dynamic Coalition Requirements

Requirement	DVC Evaluation
Coalition communications must be secured.	Provided through the use of IPsec.
Local parties should have complete control over their local IT resources and people involved in the coalition.	Provided in the local policy configuration file; however, any changes to local elements requires a re-negotiation of the policy with the remote DVC.
Local parties should be able to deploy autonomously managed authentication schemes for authenticating their local users prior to providing access to the coalition resources.	Not really applicable since the current DVC prototype does not attempt to authenticate users trying to access the coalition. This is a new requirement.
Local people should not have to acquire new authentication credentials in order to access remote coalition party resources.	Not applicable since the current DVC does not authenticate users.
The establishment of a dynamic coalition should not require local parties to alter its physical strategic IT infrastructure.	Supported.
The establishment of a dynamic coalition should not require a priori coordination of the logical strategic IT infrastructure.	The IPv4 version of the DVC would require the re-assignment of the local IP address space in the event that coalition members had overlapping private IP address spaces.
Coalition parties should be able to audit the information exchanged at the VPN gateway.	The DVC does not provide an audit capability but there is nothing preventing this feature from being added. However, if end-to-end IPsec tunnels are supported in the future this will not be the case.
Mobile coalition deployments should have the option of using locally provided communications assets including dynamically assigned IPs.	The DVC cannot handle this situation, as it requires both the remote DNS name and static IP address within its policy file.
Minimize the *a priori* knowledge required amongst coalition parties.	The DVC must exchange the following a priori information between each DVC pair before it can

Requirement	DVC Evaluation
	negotiate coalitions: • Common class of IPsec parameters. • Remote DNS names and static IP addresses. • Coordination of offered and expected services.

The following additional comments on the DVC prototype are offered:

- The DVC policy negotiation is too brittle. If the local services that are offered are disallowed remotely, or the local party does not offer a remotely expected service, the entire negotiation fails. A more graceful negotiation could potentially allow negotiation of some partial set of agreed upon services. One might also consider defining service dependencies so associated groups of services can either succeed or fail. For example, the Post Office Protocol (POP) will not be negotiated unless the Simple Mail Transfer Protocol (SMTP) is also provided;
- The local and remote DVC both end up enforcing the same policy after negotiation. A more flexible approach (shown in Figure 9 below) would be to have each local party define who can access the remote DVC (that is, out-bound client communication is controlled by the local DVC) and what services are offered remotely (that is, in-bound access attempts to a local service are controlled by the local DVC). This would provide more flexibility for a party within a coalition to manage its IT resources as the situation evolves;
- In situations where coalition parities want to maintain the privacy of their Intranet, the current DVC policy negotiation reveals too much local network information (that is, the local subnets that will access remote services). If the enhanced DVC access control were implemented as shown in Figure 9 below, then the only network information to be revealed would be server addresses. Note that to hide the local IP address space effectively, one also needs to provide ALGs and/or NAT at the local DVC;
- The DVC implements source IP address based client control to coalition resources. This is too limited a design but the best that IPsec selectors can provide. Being able to allow individuals access is highly desirable. For example, an authenticating outgoing proxy as part of the DVC would allow local users to be strongly authenticated using any number of authentication schemes before being allowed access to the coalition. Note that this would also prevent the local private Intranet IP address space from being exposed to the remote DVC; and
- The current DVC tries to build an entire coalition management view with link and node reporting via the operator interface. The interface will not scale. Network mapping and health status might better be left to a red SNMP management approach, which has a richer set of network management tools.

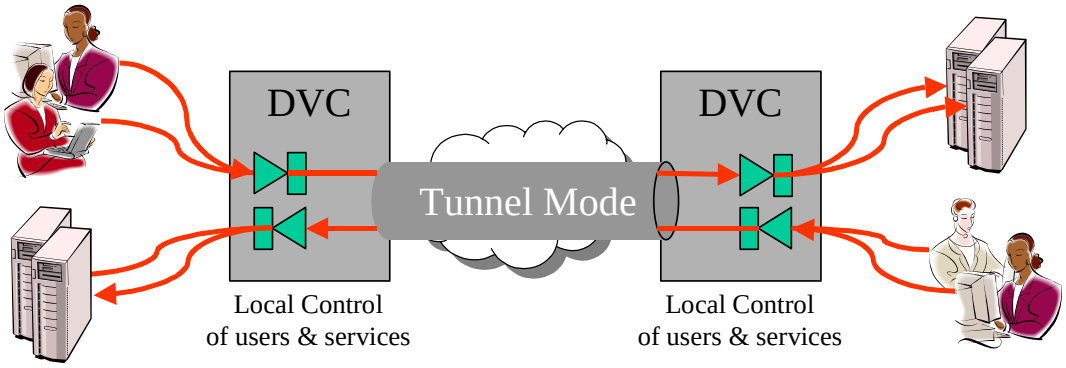


Figure 9 – Enhanced DVC Access Control Approach

4.2 DVC MILITARY DEPLOYMENTS

In a military context, the DVC would likely be used for operational traffic, which is typically classified. As such, it would require military grade cryptos front-ending the DVC. These might be IPsec cryptos (for example, TACLANE KG-175) or they could be link cryptos (KG-84) into a routed red network. It is envisioned that a DVC would be deployed immediately behind a military grade crypto on its red side.

The deployment of military grade cryptos will place all coalition DVCs within an isolated red IP network and provide protection against threats in the interconnecting network. As such, the DVC IPsec protection is redundant. Specifically, there is no need for integrity protection since the military grade crypto provides this service. The use of encryption might possibly be used to provide need-to-know separation within the protected network; however, if the encryption endpoint is just the DVC, and not end-systems, then this may be of limited value.[25] The remaining DVC functions (policy definition, policy negotiation, firewall, DNS, and routing updates) still remain valid functions behind the military grade crypto. However, these functions are now reduced to a more traditional firewall deployment albeit one with dynamic configuration.

[25] Note that in cases where the DVC is not immediately behind the military grade crypto, then its IPsec functions are not redundant.

5 FURTHER RESEARCH

Additional DVC related research is suggested below in a number of areas (in no specific order). Each of the listed research areas would complement the lessons learned from the existing DVC approach.

5.1 DVC POLICY NEGOTIATION

- Examine distributed in-band and out-of-band methods of IPsec policy negotiation in support of client to server tunnels within dynamic coalition networks. Several approaches might be examined:
    - In-band IPsec policy negotiation as suggested in [Froh],
    - Out-of-Band IPsec policy negotiation as suggested in [Sanchez], or
    - Out-of-Band device (and policy) discovery as alluded to by HAIPIS having an Internet Assigned Numbers Authority (IANA) allocated port 3623 entitled HAIPIS Dynamic Discovery; and
- Study and possibly try to influence the work of the following new IETF working Groups to the benefit of the DVC project:
    - Profiling Use of PKI in IPSEC (pki4ipsec) WG [pki4ipsec], and
    - IKEv2 Mobility and Multihoming (mobike) WG [mobike].

5.2 DVC TRUST / IDENTITY / NAMESPACE MANAGEMENT

- Study the management of Coalition DNS/LDAP namespaces in various deployment scenarios. The study should include an examination of the use of dynamic push technologies to update the namespace remotely (for example, using Transaction Signatures (TSIG) authenticated dynamic DNS updates);
- Study the use of alternate local authentication technologies that will support user authenticated coalition participation rather than machine address based participation. This should include examining the alternatives of providing authenticated participant identity to the local DVC, the remote DVC, and possibly the remote information server. Several technology alternatives might be examined:
    - Permanent X.509 based certificates issued by a local CA,
    - Temporary X.509 certificate issued by a coalition CA,
    - Local domain Kerberos[26] authentication with cross-realm authentication being using DVC X.509 certificates, and
    - Temporary Kerberos credentials issued by a remote coalition Key Distribution Centre (KDC) based on locally issued X.509 certificates;
- Study the issue of implementing individual identity X.509 certificates versus position based X.509 identity certificates;[27]
- Study various methods of achieving trust amongst coalition parties. Items to be considered include:
    - Establishing a coalition PKI CA,

[26] Note that Kerberos is an excellent authentication mechanism for use within a single administrative domain. As such, it might be applicable to authenticating local participants in a coalition.

[27] Note that DND has issued ~65,000 individual PKI identities. However, with the deployment of their Military Message Handling System, they will be issuing ~5,000 position based PKI identities.

  - Cross Certification of each party's strategic PKIs,
  - Study the ability to cross-certify on-the-fly using an OCSP portal as part of a DVC, and
  - Study the ability to establish trust through Attribute Authorities that issue Attribute Certificates; and
- Study the extension of the DVC policy language to include Service Level Agreement (SLA) notions for negotiating expectations amongst coalition parties including:
  - Allowed transactions,
  - Disallowed transactions,
  - Availability commitments, and
  - Quality of Service (QoS) commitments.

5.3 HARDEN EXISTING DVC

- Develop an alternate DVC implementation in order to clarify existing DVC protocol and API specifications. Specifically, implementations using alternate operating systems, scripting languages, IPsec implementations, and local policy definition would be emphasized;
- Conduct a Network Based Attack on the existing DVC configuration to determine potential weaknesses;
- Examine issues with porting the DVC to evaluated or alternate operating systems. Two possible candidates include:
  - SuSE Linux achieved a Common Criteria (CC) Evaluation Assurance Level (EAL) 2 rating in Jul 2003 [SuSE_eal2] and a subsequent EAL-3 rating in Jan 2004 [SuSE_eal3], and
  - NSA's Information Assurance Research Group has implemented a Secure Linux patch, which incorporates Mandatory Access Controls (MAC) capable of implementing flexible security policies [SELinux]; and
- Study the NSA's HAIPIS standard and its applicability to dynamic coalitions.

5.4 DVC COALITION SCENARIO DEVELOPMENT

- Study multiple coalition scenarios as a higher-level abstraction. Items to be examined include:
  - Technical considerations on how to handle multiple coalitions (for example, how does one handle routing to a remote entity when they are part of two coalitions),
  - Handling cross-coalition chatter, and
  - Defining meta-coalition policy; and
- Study the implications of group based key management with regard to dynamic coalitions (for example, could a central trusted policy server, such as Secure Realms, be used?).

5.5 DVC ALTERNATE ARCHITECTURES

The following suggested research areas take a different architectural approach to solving dynamic coalitions. That is, they keep the coalition party networks as private Intranets and study how to provide coalition shared services and applications:

- Develop an alternate DVC approach that keeps the local parties IT infrastructure as private within the coalition. This would mean that the coalition party offers set services at the coalition boundary instead of general network routing. Several technology alternatives might be examined:
    - Using SSH technology to establish remote service entry points to coalition offered services (see 0 for more details), and
    - Using ALGs in a firewall environment as a means of hiding the private IT infrastructure. The use of Zorp [Zorp] should be considered as an extensible application proxy. Particular attention could be paid to edge-computing protocol support, such as VoIP[28];
- Study how various edge-computing applications could be handled by non-IPsec DVC alternative technologies; and
- Investigate other non-IPsec, or non-standard IPsec, VPN offerings that might be able to support dynamic coaltions (for example, VisEdge by Yo Inc. [Yo]).

[28] Note that both Avaya and Cisco emphasize VoIP in their firewall/VPN products; however, it is not clear if this support is on their firewall only, or whether it is integrated with the VPN.

Appendix A – References

AltaSec	http://www.viasat.com/secure/kg250/documents/KG-2507-03_000.pdf
Bacic	Eugen Bacic, "Options for the Policy Server Component of the DRDC Architecture for Secure Access Management", Version 2.0, 02 Apr 2003.
Baltatu00	Baltatu, M., A. Lioy, et al, "Security Policy System: status and perspective", *ICONN-2000: IEEE International Conference on Networks*, Sep 2000, pp. 278-284. http://security.polito.it/publications
Baltatu01	Baltatu, M., A. Lioy, et al, "Towards a Policy System for Ipsec: issues and an experimental implementation", *ICONN-2001: IEEE International Conference on Networks 2001*, Oct 2001, pp. 146-151. http://security.polito.it/publications
Blaze	Blaze, M., A. Keromytis, et al, "IP Security Policy (IPSP) Requirements", RFC3586, Aug 2003. http://www.ietf.org/rfc/rfc3586.txt
Carpenter	Carpenter, B., "Internet Transparency", RFC2775, Feb 2000. http://www.ietf.org/rfc/rfc2775.txt
CSE	http://www.cse-cst.gc.ca/en/documents/knowledge_centre/gov_publications/itsb/sdns.pdf
DDCEI	DDCEI 3-5, *DND Information Technology Security Architecture*, Version 4.0, 2102-132 (DDCEI 3-5), 18 Aug 2000. http://img.mil.ca/dgimo/ddcei/DDCEI_3/DDCEI_3_5/documents/secDocs/docITSec_e.htm
Denker	Denker, John, S. Bellovin, et al, "Moat: a Virtual Private Network Appliance and Services Platform", *Proceedings of LISA XIII*, Seattle, Nov 1999, pp 251-260. http://www.research.att.com/~smb/papers/index.html
DoD	Stenbit, John, Letter from US Department of Defence Chief Information Officer to the Chairman of the Joint Chiefs of Staff (and others) with subject "Internet Protocol V6 (IPv6)", 09 Jun 2003.
Eronen	Eronen, P. and J. Zitting, "An expert system for analyzing firewall rules", Helsinki University of Technology, *6th Nordic Workshop on Secure IT Systems (NordSec 2001)*, Nov 2001, pp 100-107. http://www.nixu.com/company/publications/nordsec_2001.pdf
Ferguson	Ferguson, N. and B. Schneier, "A Cryptographic Evaluation of Ipsec", Counterpane Internet Security Inc., no date. http://www.counterpane.com/ipsec.pdf
FASTLANE	http://www.gdc4s.com/Products/fastlane2.html
FreeS/WAN	http://www.freeswan.org
FreeS/WAN_X509	http://www.strongsec.com/freeswan/
Froh	Froh, M., "Business Proposition – Defensor Management of IPsec", Version 003, CyberSafe Canada, 21 Oct 1998.
Fu	Fu, Zhi and Felix Wu, "Automatic Generation of IPSec/VPN Security Policies In an Intra-Domain Environment", *12th International Workshop on Distributed Systems, Operations and Management (DSOM)*, Oct 2001. http://argos.csc.ncsu.edu/papers.htm
GDC4	General Dynamics C4 Systems http://www.gdc4s.com
Gerber	Gerber, Cheryl, "Converging on Network Security", *Military Information Technology – Online Edition*, Volume 8, Issue 1, 09 Feb 2004. http://www.mit-kmi.com/articles.cfm?DocID=384
Gomez	Gomez, A., G. Martinez, and O. Canovas, "New Security Services based on PKI", no date.
IASWS03	"2003 Information Assurance Solutions Working Symposium Program". http://www.laevents.com/iasws03/Login/DESC.cfm

ipsec	Internet Engineering Task Force, IP Security Protocol (ipsec) Working Group http://www.ietf.org/html.charters/ipsec-charter.html
ipsp	Internet Engineering Task Force, IP Security Policy (ipsp) Working Group http://www.ietf.org/html.charters/ipsp-charter.html
IO	Department of National Defence, *CF Information Operations*, B-GG-005-004/AF-010, 15 Mar 1998.
Jason	Jason, J., L. Rafalow, and E. Vyncke, "IPsec Configuration Policy Information Model", RFC3585, Aug 2003. http://www.ietf.org/rfc/rfc3585.txt
KAME	http://www.kame.net
Kent	Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RF2401, Nov 1998. http://www.ietf.org/rfc/rfc2401.txt
kink	Internet Engineering Task Force, Kerberized Internet Negotiation of Keys (kink) Working Group http://www.ietf.org/html.charters/kink-charter.html
Labouret	Labouret, Ghislaine, "Ipsec 2001 Interop Demo", *IPsec 2001 Global Summit*, Oct 2001. http://www.hsc.fr/resources/ipsec/ipsec2001
Lentz	Lentz, Robert, "FIAC – Transforming Information Assurance: DoD's Roadmap for the Future", *Keynote address to the Federal Information Assurance Conference (FIAC)*, 2003 (slide 24). http://www.fbcinc.com/fiac/sessions03/keynote_lentz.pdf
Messmer	Messmer, Ellen, "Car makers rev up new e-commerce initiatives", *Network World Fusion*, 02 Sep 2002. http://www.nwfusion.com/news/2002/0902autotech.html?docid=2047
mobike	Internet Engineering Task Force, IKEv2 Mobility and Multihoming (mobike) Working Group http://www.ietf.org/html.charters/mobike-charter.html
NAILabs1	NAILabs, "Current Ipsec Policy Configuration Options", Feb 2001. [29] http://net-policy.sourceforge.neet/SMIP/01-existing-solutions.pdf
NAILabs2	NAILabs, "A Scaleable IPsec Policy Configuration System", Nov 2001. http://net-policy.sourceforge.neet/SMIP/02-architecture.pdf
NAILabs3	NAILabs, "Benchmarking results of SMIP project software components", date unclear. http://net-policy.sourceforge.neet/SMIP/03-benchmarks.pdf
NAILabs4	NAILabs, "Current Ipsec Policy Configuration Options", Jul 2002. http://net-policy.sourceforge.neet/SMIP/04-lessons-learned.pdf
net-snmp	http://net-snmp.sourceforge.net/
NRL	http://www.itd.nrl.navy.mil/itd_accomp_ipsec.pdf
NRNS1	NRNS Inc., "Dynamic VPN Controller (DVC)", presentation slides, no date.
NRNS2	NRNS Inc., "Dynamic VPN Controller (DVC) Demonstrator – Project Report", Version 1.2, Oct 2002.
NRNS3	NRNS Inc., "Dynamic VPN Controller (DVC) Demonstrator – Addendum Report", Version 1.0, Oct 2002.
NRNS4	NRNS Inc., "Dynamic VPN Controller (DVC) Demonstrator – Addendum 2 Report", Version 1.0, Jan 2003.
NRNS5	NRNS Inc., "Dynamic VPN Controller (DVC) Demonstrator – Policy Editor User Manual", Version 1.0, Oct 2003.
NRNS6	NRNS Inc., "Integration of the DVC Demonstrator with the UMU-PKIv6 and UMU-PBNM Systems", DRAFT Version 0.1, Mar 2004.

[29] Although the NAILabs references indicate a publication date of 15 Sep 2003 on their title page, they self-reference where the dates are in the 2001 and 2002 timeframes. A best effort actual date is listed for each.

NSA	National Security Agency, “Defense in Depth”, no date. http://www.nsa.gov/snac/support/defenseindepth.pdf
pki4ipsec	Internet Engineering Task Force, Profiling Use of PKI in IPSEC (pki4ipsec) Working Group http://www.ietf.org/html.charters/pki4ipsec-charter.html
Sanchez	Sanchez, L. and M. Condell, “Security Policy Protocol”, <draft-ietf-ipsp-spp-01.txt>, 29 Jan 2002. [No longer listed in IETF site] http://www.ir.bbn.com/~mcondell/papers/draft-ietf-ipsp-spp.txt
Sectera	http://www.gdc4s.com/Products/sectera.htm
SELinux	National Security Agency, Security-Enhanced Linux website http://www.nsa.gov/selinux/
Steffen	Steffen, Andreas, “Virtual Private Networks – Coping With Complexity”, *Published in “Security, E-Learning – 17. DFN-Arbeitstagung uber Kommunikationsnetze in Dusseldorf”*, 2003, pp. 289-302. http://security.zhwin.ch/DRN_VPN.pdf
SuperFreeS/WAN	http://www.freeswan.ca/
SuSE	SuSE, *Security – Security Certification*. http://www.suse.com/de/security/certification/index.html
SuSE_eal2	Bundesamt fur Sicherheit in der Informationstechnik, “Certification Report – BSI-DSZ-CC-0216-2003 for SuSE Linux Enterprise Server V8 with certification-sles-eal2 package from SuSE Linux AG”, 28 Jul 2003. http://www.bsi.bund.de/zertifiz/zert/reporte/0216a.pdf
SuSE_eal3	Bundesamt fur Sicherheit in der Informationstechnik, “Certification Report – BSI-DSZ-CC-0234-2004 for SuSE Linux Enterprise Server V8 – Service Pack 3, RC4 with certification-sles-eal3 package from SuSE Linux AG”, 14 Jan 2004.
TACLANE	http://www.gdc4s.com/Products/taclane.html
TAHI	http://www.tahi.org/
Touch	Touch, Joe, “Dynamic Internet Overlay Deployment and Management Using the X-Bone”, *Computer Networks*, Jul 2002, pp. 117-135.
USAGI	http://www.linux-ipv6.org/
Viasat	Viasat Government Systems http://www.viasat.com
Yo	http://yo.com
Zorp	http://www.balabit.com/products/zorp/

Appendix B – Acronyms

ACCORDIAN	[US type 1 key management algorithm]
AES	Advanced Encryption Standard
AH	[IPsec] Authentication Header
ALG	Application Layer Gateway
ANX	Automotive Network eXchange
BATON	[US type 1 cryptographic algorithm]
BSD	Berkeley Software Distribution
CA	[PKI] Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CF	Canadian Forces
CIM	Common Information Model
CNA	Computer Network Attack
CNES	Canadian Network Encryption System
CNet	[DND] Classified Network
COMSEC	Communication Security
COPS	Common Open Policy Service
CRL	Certificate Revocation List
CSE	Canadian Security Establishment
DHCP	Dynamic Host Control Protocol
DND	Department of National Defence
DES	Data Encryption Standard
DNS	Domain Name Service
DoD	[US] Department of Defense
DRDC	Defence Research and Development Canada
DTMF	Distributed Management Task Force
DVC	Dynamic VPN Controller
DWAN	[DND] Defence Wide Area Network
EAL	[Common Criteria] Evaluation Assurance Level
EIAU	[HAIPE] End Information Assurance Unit
EKMS	Electronic Key Management System
ESP	[IPsec] Encapsulating Security Protocol
FIREFLY	[US type 1 key management algorithm]
FTP	File Transfer Protocol
HAIPE	High Assurance IP Encryption
HAIPIS	High Assurance IP Interface Specification
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
INE	In-Line Encryptor
IO	Information Operations
ipsec	[IETF] IP Security Protocol [Working Group]
ipseckey	[IETF] IPSEC KEYing information resource record [Working Group]
IPsec	Internet Protocol Security
ipsp	[IETF] IP Security Policy [Working Group]
IPSP	Internet Protocol Security Policy
ISAKMP	Internet Security Association and Key Management Protocol
isakmpd	[BSD] ISAKMP daemon
ISP	Internet Service Provider
IT	Information Technology
KAME	[BSD IPv6 and IPsec implementation project name]
KDC	Key Distribution Centre
KEY	[DNS key record]
keymat	Keying Material
kink	[IETF] Kerberized Internet Negotiation of Keys [Working Group]
KLIPS	[FreeS/WAN] Kernel Level IPsec module
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Controls
MAC	Message Authentication Code [as in AES-MAC]
MEDLEY	[US type 1 cryptographic algorithm]
MIB	Management Information Base
mobike	[IETF] IKEv2 Mobility and Multihoming [Working Group]
NAI	Network Associates Incorported
NAT	Network Address Translation
NAT-T	Network Address Translation – Traversal
NATO	North Atlantic Treaty Organization
NDA	Non-Disclosure Agreement
NES	[Motorola's] Network Encryption System
NGO	Non-Government Organization
NRL	[US] Naval Research Laboratory
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
OTNK	[HAIPIS] Over the Network Keying

PBNM	Policy Based Network Management
PF_KEY	[BSD socket protocol family used for key management]
PKI	Public Key Infrastructure
pki4ipsec	[IETF] Profiling Use of PKI in IPSEC [Working Group]
Pluto	[FreeS/WAN IKE daemon]
POP	Post Office Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
ROI	Return on Investment
SA	Security Association
SCTP	Stream Control Transmission Protocol
SDNS	Secure Data Network System
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SLP	Service Location Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCKS	[IETF proxy protocol for firewall transversal]
SPP	Security Policy Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STE	Secure Telephone Equipment
STU-III	Subscriber Terminal Unit, Third Generation
TACACS	Terminal Access Controller Access Control System
TAHI	[IPv6 conformance testing project]
TCP	Transmission Control Protocol
TSIG	[DNS] Transaction Signatures
UCL	University College London
UMU	University of Murcia [Spain]
UN	United Nations
URI	Universal Resource Indicator
US	United States
USAGI	UniverSAl playGround for Ipv6
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEASEL	[US type 1 cryptographic algorithm]
WFP	World Food Program
WG	Working Group
WWW	World Wide Web

Appendix C – Dynamic Coalition VPN Using SSH

Some preliminary thoughts on establishing dynamic coalition Virtual Private Networks (VPNs) using Secure Shell (SSH) as an underlying technology are presented below. This might be considered in cases where the local coalition party wants to keep their local Information Technology (IT) infrastructure private from the coalition but still offer flexible services to the coalition.

- SSH can hides the local network through connection forwarding;
- SSH doesn't handle dynamically assigned ports very well (for example, File Transfer Protocol (FTP) or H.323) and may have to be integrated with Application Layer Gateways (ALGs);
- Existing client SSH implementations cannot alter connection forwarding configuration once the client starts an SSH session with the server; although there is nothing in the SSH protocol to prevent this;
- SSH multiplexes many Transmission Control Protocol (TCP) connections over a single secured TCP connection; therefore, the traffic flow security provided by IPsec is also available;
- OpenSSH supports both Internet Protocol (IP) v4 and IPv6;
- SSH does not support User Datagram Protocol (UDP) based applications and may have to be integrated with something like SOCKS; and
- Existing SSH client implementations have course granularity of local connection forwarding binding to existing interfaces. That is, the default binding is to localhost and all interfaces can be specified using the –g (gateway ports) option. A DVC like device would need to bind to only the red side interface for forwarded ports. Restricting the binding to the red interface might be achieved using altered SSH client code or other technologies like tcp-wrappers and/or Linux netfilter.

Appendix D – High Assurance Internet Protocol Interoperability Standard (HAIPIS)

Many of the high-grade IPsec encryption devices refer to being High Assurance IP Encryption (HAIPE) compliant. This appears to be a National Security Agency (NSA) program for the development of high-grade in-line network encryptor (INE) products as explained in [Gerber]:

> *"To address network convergence and the growing dependence on IP-based networks, the agency [NSA] created the High Assurance Internet Protocol Interoperability Standard (HAIPIS) to support future generations of IP-based network encryptors and a suite of secure, IP-based applications, such as Secure Voice Over IP."*

[IASWS03] refers to Version 2 of HAIPIS as having over the network keying (OTNK)[30]:

> *"High Assurance IP Encryption (HAIPE) devices provide security services for Internet Protocol (IP) traffic for tactical and strategic network applications. Version 1 HAIPE devices are manually keyed, but Version 2 devices will support over-the-network keying. This presentation will provide an overview of the advanced key management concepts for keying HAIPE End Information Assurance Units (EIAUs), including key ordering, EIAU registration, over-the-network key delivery directly to an EIAU, and staged key delivery through a management workstation."*[31]

HAIPIS is also referred to in a US Navy Research Laboratory [NRL] diagram implying that is a modified version of IPsec standards developed in 2002.

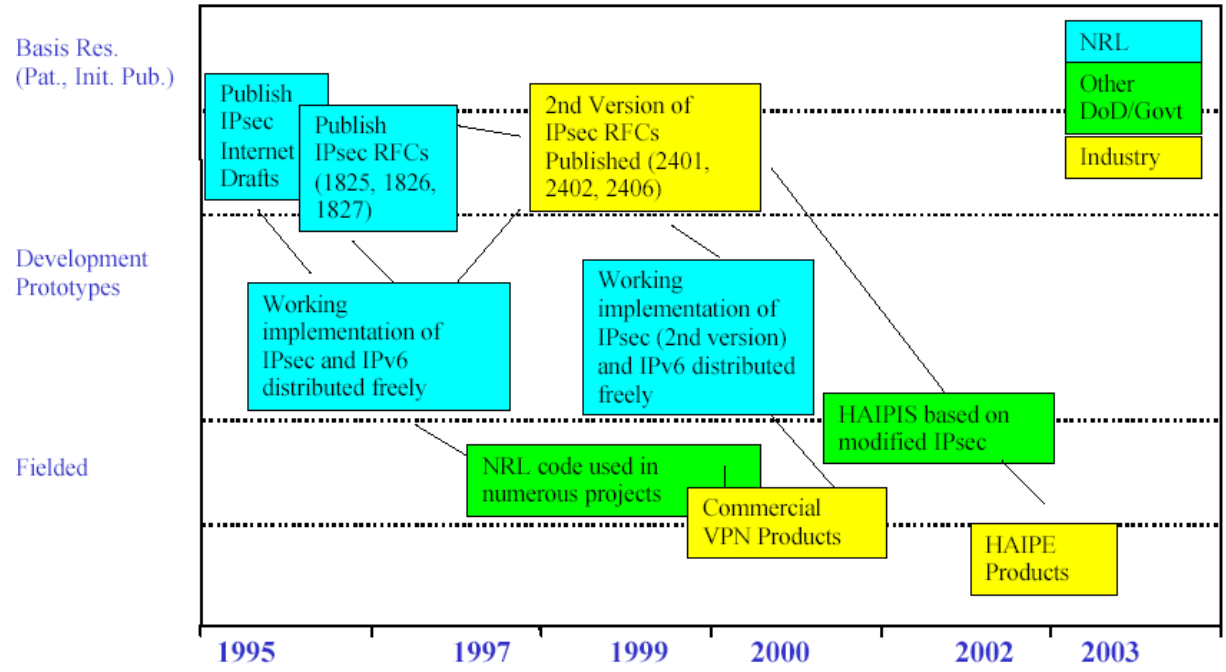


Figure 10 - NRL Involvement in IPsec Standards [NRL]

[30] OTNK seems to be a derivative of the Secure Data Network System (SDNS) Key Management Protocol (KMP) work based on the description provided here (that is, direct and staged key delivery).

[31] [IASWS03], Key Management Infrastructure (KMI) Session "HAIPE Key Management" abstract.

It is interesting to note that [IASWS03] also refers to the Advanced Encryption Standard (AES) as both a valid Type 3 (commercial) and a Type 1 (high-grade) cryptographic algorithm[32]:

> *"The SafeXcel-3140 is capable of performing commercial grade (Type 3) cryptographic algorithms ([Data Encryption Standard] DES, [Triple-DES] TDES, AES) and provides all the necessary cryptographic functions required for IPSec compatibility as well as the security critical design for FIPS 140-2 Certification.*
>
> *The SafeXcel-3340 is capable of performing U.S. government (Type 1) cryptographic algorithms (AES, BATON, MEDLEY, WEASEL), advanced key management (ACCORDIAN, FIRFELY, Benign Fill) functions and provides all the necessary cryptographic functions required for HAIPE compatibility as well as all the security critical design required for NSA Certification."*

[32] [IASWS03], SafeNet Workshop Session, "Gigabit VPN ASIC for Commercial, Defense and Homeland Security Applications.... Bridging the gap between Government and Commercial" abstract.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Cinnabar Networks
265 Carling Ave, Suite 200
Ottawa, Ontario, CANADA K1S 2E1

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

IPsec, VPNs and the Dynamic VPN Controller (DVC) (U)

4. AUTHORS (Last name, first name, middle initial)

Froh, Michael J.

5. DATE OF PUBLICATION (month and year of publication of document)

March 2004

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

37

6b. NO. OF REFS (total cited in document)

61

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical report on the current status of Internet Protocol Security (IPsec) standards and implementations, Virtual Private Networks (VPNs) and the DRDC prototype Dynamic VPN Contoller (DVC).

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Dr. Steve Zeber, Network Information Operations Section
DRDC Ottawa, 3701 Carling Avenue, Ottawa, ON K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15BF27

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

W7714-3-2894

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRD004-001

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

DRDC Ottawa CR 2004-060

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(Y) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

(U) IP Security (IPsec) protocols and Virtual Private Network (VPN) products that implement these protocols can provide authenticated secure communication channels. Defence Research and Development Canada Ottawa has been studying the use of VPN technology to support secure communications for dynamic coalitions and has developed a prototype Dynamic VPN Controller (DVC) to demonstrate how this technology could be applied to dynamic coalitions. This report proposes dynamic coalition usage scenarios and derives previously unarticluated VPN requirements, or capabilities. A brief survey of IPsec standards development, open-source IPsec implementations, commercial IPsec implementations, and military IPsec implementations is provided. The IPsec standards and implementations are examined for their support of capabilities required by dynamic coalition VPNs. The DVC prototype is then evaluated against the dynamic coalition VPN capabilities. The report concludes with suggestions for additional research to further develop: DVC policy negotiation; DVC trust, identity, and namespace management; DVC prototype hardening; DVC coalition scenario development; and alternate DVC technical architectures.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Internet Protocol Security, IPsec, Virtual Private Network, VPN, policy, security policy, security policy negotiation, information systems, IS, information technology, IT, coalition, military coalition, communications securtiy, COMSEC, open-source, GNU Public License, GPL, Internet Engineering Task Force, IETF, Request for Comment, RFC, IT Management, electronic key management, EKMS, Internet Protocol Version 6, IPv6, Public Key Infrastructure, PKI, Certificate Authority, CA