**[MS-GPFAS]:**

**Group Policy: Firewall and Advanced Security Data Structure**

**Intellectual Property Rights Notice for Open Specifications Documentation**

* **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
* **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
* **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
* **Patents**. Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft [Open Specification Promise](http://go.microsoft.com/fwlink/?LinkId=214445) or the [Community Promise](http://go.microsoft.com/fwlink/?LinkId=214448). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
* **Trademarks**. The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
* **Fictitious Names**. The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights**. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

**Tools**. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

**Revision Summary**

| Date | Revision History | Revision Class | Comments |
| --- | --- | --- | --- |
| 6/4/2010 | 0.1 | Major | First Release. |
| 7/16/2010 | 0.1 | None | No changes to the meaning, language, or formatting of the technical content. |
| 8/27/2010 | 1.0 | Major | Updated and revised the technical content. |
| 10/8/2010 | 1.1 | Minor | Clarified the meaning of the technical content. |
| 11/19/2010 | 1.1 | None | No changes to the meaning, language, or formatting of the technical content. |
| 1/7/2011 | 1.1 | None | No changes to the meaning, language, or formatting of the technical content. |
| 2/11/2011 | 2.0 | Major | Updated and revised the technical content. |
| 3/25/2011 | 3.0 | Major | Updated and revised the technical content. |
| 5/6/2011 | 4.0 | Major | Updated and revised the technical content. |
| 6/17/2011 | 5.0 | Major | Updated and revised the technical content. |
| 9/23/2011 | 5.1 | Minor | Clarified the meaning of the technical content. |
| 12/16/2011 | 6.0 | Major | Updated and revised the technical content. |
| 3/30/2012 | 7.0 | Major | Updated and revised the technical content. |
| 7/12/2012 | 8.0 | Major | Updated and revised the technical content. |
| 10/25/2012 | 8.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 1/31/2013 | 8.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 8/8/2013 | 9.0 | Major | Updated and revised the technical content. |
| 11/14/2013 | 9.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 2/13/2014 | 10.0 | Major | Updated and revised the technical content. |
| 5/15/2014 | 10.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 6/30/2015 | 11.0 | Major | Significantly changed the technical content. |

Table of Contents

[1 Introduction 7](#_Toc423367291)

[1.1 Glossary 7](#_Toc423367292)

[1.2 References 8](#_Toc423367293)

[1.2.1 Normative References 8](#_Toc423367294)

[1.2.2 Informative References 9](#_Toc423367295)

[1.3 Protocol Overview (Synopsis) 9](#_Toc423367296)

[1.3.1 Background 9](#_Toc423367297)

[1.3.2 Firewall and Advanced Security Extension Encoding Overview 9](#_Toc423367298)

[1.4 Relationship to Other Protocols 11](#_Toc423367299)

[1.5 Prerequisites/Preconditions 11](#_Toc423367300)

[1.6 Applicability Statement 12](#_Toc423367301)

[1.7 Versioning and Capability Negotiation 12](#_Toc423367302)

[1.8 Vendor-Extensible Fields 12](#_Toc423367303)

[1.9 Standards Assignments 12](#_Toc423367304)

[2 Messages 13](#_Toc423367305)

[2.1 Transport 13](#_Toc423367306)

[2.2 Message Syntax 13](#_Toc423367307)

[2.2.1 Global Policy Configuration Options 13](#_Toc423367308)

[2.2.1.1 Disable Stateful FTP 13](#_Toc423367309)

[2.2.1.2 Disable Stateful PPTP 13](#_Toc423367310)

[2.2.1.3 Security Associations Idle Time 14](#_Toc423367311)

[2.2.1.4 Preshared Key Encoding 14](#_Toc423367312)

[2.2.1.5 IPsec Exemptions 14](#_Toc423367313)

[2.2.1.6 Certificate Revocation List Check 15](#_Toc423367314)

[2.2.1.7 IPsec Through NATs 15](#_Toc423367315)

[2.2.1.8 Policy Version 15](#_Toc423367316)

[2.2.1.9 Tunnel Remote Machine Authorization List 16](#_Toc423367317)

[2.2.1.10 Tunnel Remote User Authorization List 16](#_Toc423367318)

[2.2.1.11 Opportunistically Match Authentication Set Per Key Module 16](#_Toc423367319)

[2.2.1.12 Transport Remote Machine Authorization List 16](#_Toc423367320)

[2.2.1.13 Transport Remote User Authorization List 17](#_Toc423367321)

[2.2.1.14 Packet Queue 17](#_Toc423367322)

[2.2.2 Firewall Rule Messages 17](#_Toc423367323)

[2.2.2.1 Profile Tokens 17](#_Toc423367324)

[2.2.2.2 Port and Port Range Rules 18](#_Toc423367325)

[2.2.2.3 Port Keyword Rules 18](#_Toc423367326)

[2.2.2.4 Direction Tokens 18](#_Toc423367327)

[2.2.2.5 Action Tokens 19](#_Toc423367328)

[2.2.2.6 IfSecure Tokens 19](#_Toc423367329)

[2.2.2.7 Interfaces 19](#_Toc423367330)

[2.2.2.8 Interface Types 19](#_Toc423367331)

[2.2.2.9 IPV4 Address Ranges Rules 20](#_Toc423367332)

[2.2.2.10 IPV4 Address Subnet Rules 20](#_Toc423367333)

[2.2.2.11 IPV6 Address Range Rules 21](#_Toc423367334)

[2.2.2.12 IPV6 Address Subnet Rules 21](#_Toc423367335)

[2.2.2.13 Address Keyword Rules 22](#_Toc423367336)

[2.2.2.14 Boolean Rules 22](#_Toc423367337)

[2.2.2.15 Edge Defer Rules 22](#_Toc423367338)

[2.2.2.16 ICMP Type - Code Rules 23](#_Toc423367339)

[2.2.2.17 Platform Validity Rules 23](#_Toc423367340)

[2.2.2.18 Platform Validity Operators Rules 23](#_Toc423367341)

[2.2.2.19 Firewall Rule and the Firewall Rule Grammar Rule 24](#_Toc423367342)

[2.2.2.20 Trust Tuple Keyword Rules 30](#_Toc423367343)

[2.2.3 Per-Profile Policy Configuration Options 30](#_Toc423367344)

[2.2.3.1 Enable Firewall 30](#_Toc423367345)

[2.2.3.2 Disable Stealth Mode 31](#_Toc423367346)

[2.2.3.3 Shield Up Mode 31](#_Toc423367347)

[2.2.3.4 Disable Unicast Responses to Multicast and Broadcast Traffic 31](#_Toc423367348)

[2.2.3.5 Log Dropped Packets 32](#_Toc423367349)

[2.2.3.6 Log Successful Connections 32](#_Toc423367350)

[2.2.3.7 Log Ignored Rules 32](#_Toc423367351)

[2.2.3.8 Maximum Log File Size 33](#_Toc423367352)

[2.2.3.9 Log File Path 33](#_Toc423367353)

[2.2.3.10 Disable Inbound Notifications 33](#_Toc423367354)

[2.2.3.11 Allow Authenticated Applications User Preference Merge 34](#_Toc423367355)

[2.2.3.12 Allow Globally Open Ports User Preference Merge 34](#_Toc423367356)

[2.2.3.13 Allow Local Firewall Rule Policy Merge 34](#_Toc423367357)

[2.2.3.14 Allow Local IPsec Policy Merge 35](#_Toc423367358)

[2.2.3.15 Disabled Interfaces 35](#_Toc423367359)

[2.2.3.16 Default Outbound Action 35](#_Toc423367360)

[2.2.3.17 Default Inbound Action 36](#_Toc423367361)

[2.2.3.18 Disable Stealth Mode for IPsec Secured Packets 36](#_Toc423367362)

[2.2.4 Authentication Sets 36](#_Toc423367363)

[2.2.4.1 Version 37](#_Toc423367364)

[2.2.4.2 Name 37](#_Toc423367365)

[2.2.4.3 Description 38](#_Toc423367366)

[2.2.4.4 EmbeddedContext 38](#_Toc423367367)

[2.2.4.5 Suite Keys 38](#_Toc423367368)

[2.2.4.6 Phase 1 and Phase 2 Auth Suite Methods 38](#_Toc423367369)

[2.2.4.7 Phase 1 and Phase 2 Auth Suite Certificate Authority Names 39](#_Toc423367370)

[2.2.4.8 Phase 1 Auth Suite Preshared Key 40](#_Toc423367371)

[2.2.4.9 Phase 1 and Phase 2 Auth Suite Certificate Account Mapping 40](#_Toc423367372)

[2.2.4.10 Phase 1 Auth Suite Exclude CA Name 40](#_Toc423367373)

[2.2.4.11 Phase 1 and Phase 2 Auth Suite Health Cert 40](#_Toc423367374)

[2.2.4.12 Phase 1 and Phase 2 Auth Suite Skip Version 41](#_Toc423367375)

[2.2.4.13 Phase 1 and Phase 2 Auth Suite Other Certificate Signing 41](#_Toc423367376)

[2.2.4.14 Phase 1 and Phase 2 Auth Suite Intermediate CA 42](#_Toc423367377)

[2.2.4.15 Certificate Criteria Type Tokens 42](#_Toc423367378)

[2.2.4.16 Certificate Criteria Name Type Tokens 42](#_Toc423367379)

[2.2.4.17 Phase 1 and Phase 2 Auth Suite Certificate Criteria 43](#_Toc423367380)

[2.2.4.18 Phase 1 and Phase 2 Auth Suite Allow Kerberos Proxy 44](#_Toc423367381)

[2.2.4.19 Phase 1 and Phase 2 Auth Suite Kerberos Proxy Server 44](#_Toc423367382)

[2.2.5 Cryptographic Sets 44](#_Toc423367383)

[2.2.5.1 Version 45](#_Toc423367384)

[2.2.5.2 Name 45](#_Toc423367385)

[2.2.5.3 Description 46](#_Toc423367386)

[2.2.5.4 EmbeddedContext 46](#_Toc423367387)

[2.2.5.5 Phase 1 - Do Not Skip Deffie Hellman 46](#_Toc423367388)

[2.2.5.6 Phase 1 - Time Out in Minutes 46](#_Toc423367389)

[2.2.5.7 Phase 1 - Time Out in Sessions 47](#_Toc423367390)

[2.2.5.8 Phase 2 - Perfect Forward Secrecy 47](#_Toc423367391)

[2.2.5.9 Phase 1 - Suite Keys 48](#_Toc423367392)

[2.2.5.10 Phase 1 Suite - Key Exchange Algorithm 48](#_Toc423367393)

[2.2.5.11 Phase 1 Suite - Encryption Algorithm 49](#_Toc423367394)

[2.2.5.12 Phase 1 Suite - Hash Algorithm 49](#_Toc423367395)

[2.2.5.13 Phase 1 Suite Skip Version 50](#_Toc423367396)

[2.2.5.14 Phase 1 Suite - 2.1 Hash Algorithm 50](#_Toc423367397)

[2.2.5.15 Phase 1 Suite - 2.16 Key Exchange Algorithm 50](#_Toc423367398)

[2.2.5.16 Phase 2 - Suite Keys 51](#_Toc423367399)

[2.2.5.17 Phase 2 Suite - Protocol 51](#_Toc423367400)

[2.2.5.18 Phase 2 Suite - Encryption Algorithm 52](#_Toc423367401)

[2.2.5.19 Phase 2 Suite - AH Protocol Hash Algorithm 52](#_Toc423367402)

[2.2.5.20 Phase 2 Suite - ESP Protocol Hash Algorithm 52](#_Toc423367403)

[2.2.5.21 Phase 2 Suite - Time Out in Minutes 52](#_Toc423367404)

[2.2.5.22 Phase 2 Suite - Time Out in Kilobytes 53](#_Toc423367405)

[2.2.5.23 Phase 2 Suite - Skip Version 53](#_Toc423367406)

[2.2.5.24 Phase 2 Suite - 2.1 Encryption Algorithm 53](#_Toc423367407)

[2.2.5.25 Phase 2 Suite - 2.1 AH Hash Algorithm 54](#_Toc423367408)

[2.2.5.26 Phase 2 Suite - 2.1 ESP Hash Algorithm 54](#_Toc423367409)

[2.2.5.27 Phase 2 Suite - 2.9 Protocol 55](#_Toc423367410)

[2.2.5.28 Phase 2 - 2.16 Perfect Forward Secrecy 55](#_Toc423367411)

[2.2.6 Connection Security Rule Messages 56](#_Toc423367412)

[2.2.6.1 Connection Security Action Tokens 56](#_Toc423367413)

[2.2.6.2 Connection Security Rule and the Connection Security Rule Grammar Rule 56](#_Toc423367414)

[2.2.6.3 Keying Module Rules 62](#_Toc423367415)

[2.2.7 Main Mode Rule Messages 62](#_Toc423367416)

[2.2.7.1 Main Mode Rule and the Main Mode Rule Grammar Rule 62](#_Toc423367417)

[3 Protocol Details 65](#_Toc423367418)

[3.1 Administrative Plug-in Details 65](#_Toc423367419)

[3.1.1 Abstract Data Model 65](#_Toc423367420)

[3.1.2 Timers 65](#_Toc423367421)

[3.1.3 Initialization 65](#_Toc423367422)

[3.1.4 Higher-Layer Triggered Events 65](#_Toc423367423)

[3.1.5 Message Processing Events and Sequencing Rules 66](#_Toc423367424)

[3.1.5.1 Policy Administration Load Message Sequencing 66](#_Toc423367425)

[3.1.5.2 Policy Administration Update Message Sequencing 66](#_Toc423367426)

[3.1.6 Timer Events 67](#_Toc423367427)

[3.1.7 Other Local Events 67](#_Toc423367428)

[3.2 Client Details 67](#_Toc423367429)

[3.2.1 Abstract Data Model 67](#_Toc423367430)

[3.2.2 Timers 67](#_Toc423367431)

[3.2.3 Initialization 67](#_Toc423367432)

[3.2.4 Higher-Layer Triggered Events 67](#_Toc423367433)

[3.2.5 Message Processing Events and Sequencing Rules 67](#_Toc423367434)

[3.2.6 Timer Events 67](#_Toc423367435)

[3.2.7 Other Local Events 68](#_Toc423367436)

[3.2.7.1 Policy Application Event 68](#_Toc423367437)

[4 Protocol Examples 69](#_Toc423367438)

[4.1 Configuration Options Messages 69](#_Toc423367439)

[4.2 Firewall Rule Message 69](#_Toc423367440)

[4.3 Connection Security Rule Message 69](#_Toc423367441)

[4.4 Authentication Set Messages 70](#_Toc423367442)

[4.4.1 Authentication Set { 212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB } 70](#_Toc423367443)

[4.4.2 Authentication Set { D842F406-E895-406A-AC35-9837B6D499F4 } 72](#_Toc423367444)

[4.4.3 Authentication Set { A75A5046-E377-45CC-BD25-EC0F8E601CE1 } 73](#_Toc423367445)

[4.4.4 Authentication Set { 967F0367-F879-42EC-938B-C89FE8289B26 } 73](#_Toc423367446)

[4.4.5 Cryptographic Set Messages 75](#_Toc423367447)

[4.4.5.1 Cryptographic Set { CD863A4F-CD94-4763-AD25-69A1378D51EB } 75](#_Toc423367448)

[4.4.5.2 Cryptographic Set { E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F } 77](#_Toc423367449)

[5 Security 82](#_Toc423367450)

[5.1 Security Considerations for Implementers 82](#_Toc423367451)

[5.2 Index of Security Parameters 82](#_Toc423367452)

[6 Appendix A: Product Behavior 83](#_Toc423367453)

[7 Appendix B: Full ABNF Grammar 85](#_Toc423367454)

[8 Change Tracking 89](#_Toc423367455)

[9 Index 91](#_Toc423367456)

# Introduction

This document specifies the Group Policy: Firewall and Advanced Security Data Structure extension to the Group Policy: Registry Extension Encoding, as specified in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf), and provides a mechanism for an administrator to control any Firewall and Advanced Security behavior on a client using group policy-based settings.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in [[RFC2119]](http://go.microsoft.com/fwlink/?LinkId=90317). Sections 1.5 and 1.9 are also normative but do not contain those terms. All other sections and examples in this specification are informative.

## Glossary

The following terms are specific to this document:

**Active Directory**: A general-purpose network directory service. [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) also refers to the Windows implementation of a directory service. [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) stores information about a variety of objects in the network. Importantly, user accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-ADTS%5d.pdf) describes both forms. For more information, see [[MS-AUTHSOD]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-AUTHSOD%5d.pdf) section 1.1.1.5.2, Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Kerberos, and DNS.

**administrative template**: A file associated with a [**Group Policy Object (GPO)**](#gt_dec32233-8776-4151-91a0-8624a2b9abb0) that combines information on the syntax of registry-based policy settings with human-readable descriptions of the settings, as well as other information.

**client-side extension GUID (CSE GUID)**: A [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that enables a specific client-side extension on the Group Policy client to be associated with policy data that is stored in the logical and physical components of a [**Group Policy Object (GPO)**](#gt_dec32233-8776-4151-91a0-8624a2b9abb0) on the Group Policy server, for that particular extension.

**computer-scoped Group Policy Object path**: A scoped Group Policy Object (GPO) path that ends in "\Machine".

**distinguished name (DN)**: A name that uniquely identifies an object by using the relative distinguished name (RDN) for the object, and the names of container objects and domains that contain the object. The distinguished name (DN) identifies the object and its location in a tree.

**domain**: A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a domain controller (DC) and host a member list that identifies all members of the domain, as well as optionally hosting the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) service. The domain controller provides authentication (2) of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [MS-AUTHSOD] section 1.1.1.5 and [MS-ADTS].

**globally unique identifier (GUID)**: A term used interchangeably with universally unique identifier (UUID) in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [[RFC4122]](http://go.microsoft.com/fwlink/?LinkId=90460) or [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) must be used for generating the [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1). See also universally unique identifier (UUID).

**Group Policy Object (GPO)**: A collection of administrator-defined specifications of the policy settings that can be applied to groups of computers in a domain. Each GPO includes two elements: an object that resides in the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) for the domain, and a corresponding file system subdirectory that resides on the sysvol DFS share of the Group Policy server for the domain.

**policy setting**: A statement of the possible behaviors of an element of a domain member computer's behavior that can be configured by an administrator.

**registry**: A local system-defined database in which applications and system components store and retrieve configuration data. It is a hierarchical data store with lightly typed elements that are logically stored in tree format. Applications use the registry API to retrieve, modify, or delete registry data. The data stored in the registry varies according to the version of Windows.

**registry policy file**: A file associated with a [**Group Policy Object (GPO)**](#gt_dec32233-8776-4151-91a0-8624a2b9abb0) that contains a set of registry-based policy settings.

**tool extension GUID or administrative plug-in GUID**: A GUID defined separately for each of the user policy settings and computer policy settings that associates a specific administrative tool plug-in with a set of policy settings that can be stored in a [**Group Policy Object (GPO)**](#gt_dec32233-8776-4151-91a0-8624a2b9abb0).

**Unicode**: A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) standard [[UNICODE5.0.0/2007]](http://go.microsoft.com/fwlink/?LinkId=154659) provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (UTF-8, UTF-16, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [[RFC2119]](http://go.microsoft.com/fwlink/?LinkId=90317). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](http://msdn.microsoft.com/en-us/library/dn781092.aspx).

### Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[MS-FASP] Microsoft Corporation, "[Firewall and Advanced Security Protocol](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf)".

[MS-GPOL] Microsoft Corporation, "[Group Policy: Core Protocol](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf)".

[MS-GPREG] Microsoft Corporation, "[Group Policy: Registry Extension Encoding](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf)".

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, [http://www.rfc-editor.org/rfc/rfc2119.txt](http://go.microsoft.com/fwlink/?LinkId=90317)

[RFC4122] Leach, P., Mealling, M., and Salz, R., "A Universally Unique Identifier (UUID) URN Namespace", RFC 4122, July 2005, [http://www.ietf.org/rfc/rfc4122.txt](http://go.microsoft.com/fwlink/?LinkId=90460)

[RFC4234] Crocker, D., Ed., and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005, [http://www.rfc-editor.org/rfc/rfc4234.txt](http://go.microsoft.com/fwlink/?LinkId=90462)

[RFC4291] Hinden, R. and Deering, S., "IP Version 6 Addressing Architecture", RFC 4291, February 2006, [http://www.ietf.org/rfc/rfc4291.txt](http://go.microsoft.com/fwlink/?LinkId=90464)

### Informative References

[MSDN-RegisterGPNotification] Microsoft Corporation, "RegisterGPNotification function", [http://msdn.microsoft.com/en-us/library/aa374404(VS.85).aspx](http://go.microsoft.com/fwlink/?LinkId=217895)

## Protocol Overview (Synopsis)

The Group Policy: Firewall and Advanced Security Data Structure provides a mechanism for an administrator to control Firewall and Advanced Security behavior of the client through group policy using the Group Policy: Registry Extension Encoding specified in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf).

### Background

The Group Policy: Core Protocol (as specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf)) allows clients to discover and retrieve [**policy settings**](#gt_46c9430c-115a-4cbc-a527-ee8ca3deb79f) created by administrators of a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). These settings are persisted within [**Group Policy Objects (GPOs)**](#gt_dec32233-8776-4151-91a0-8624a2b9abb0) that are assigned to the policy target accounts in the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). On each client, each GPO is interpreted and acted upon by software components known as client plug-ins. The client plug-ins responsible for a given GPO are specified using an attribute on the GPO. This attribute specifies a list of [**globally unique identifier (GUID)**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) lists. The first GUID of each GUID list is referred to as a [**client-side extension GUID (CSE GUID)**](#gt_8a485508-83b4-4e14-aae9-7299a85fa879). Other GUIDs in the GUID list are referred to as [**tool extension GUIDs**](#gt_88ad7745-bee6-47f7-ae98-6fac7c5ef330). For each GPO that is applicable to a client, the client consults the CSE GUIDs listed in the GPO to determine which client plug-in on the client should handle the GPO. The client then invokes the client plug-in to handle the GPO.

[**Registry**](#gt_2d67ea57-10e6-422f-985e-694834945a02)-based settings are accessible from a GPO through the Group Policy: Registry Extension Encoding protocol, which is a client plug-in. The protocol provides mechanisms both for administrative tools to obtain metadata about registry-based settings and for clients to obtain applicable registry-based settings.

Group Policy: Firewall and Advanced Security Data Structure settings may be administered using [**administrative templates**](#gt_4e6de77d-87b5-487a-90db-46caf3bf6742) (as specified in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 2.2.2). An administrative template is a file associated with a GPO that combines information on the syntax of registry-based settings with human-readable descriptions of the settings as well as other information. Administrative tools use administrative templates to allow administrators to configure registry-based settings for applications on clients.

Group Policy: Registry Extension Encoding settings are specified using [**registry policy files**](#gt_3b5b5fef-af73-45f8-83a8-f1b5ed11ea20) (as specified in [MS-GPREG] section 2.2.1). An administrative tool uses the information within the administrative template to write out a registry policy file and associate it with a GPO. The Group Policy: Registry Extension Encoding plug-in on each client reads registry policy files specified by applicable GPOs and applies their contents to its registry.

Administrative templates support a limited subset of the syntax for registry policy files. As a result, not all registry-based settings may be expressed using administrative templates. Such registry-based settings may be implemented using a custom user-interface that does not rely on administrative templates. One example of such registry-based settings is those belonging to the Firewall and Advanced Security component, which are described in this document.

### Firewall and Advanced Security Extension Encoding Overview

Firewall and Advanced Security policies are configurable from a GPO through the Group Policy: Firewall and Advanced Security Data Structure. The Firewall and Advanced Security component has complex settings not expressible through administrative templates and for this reason it implements a custom UI that can author registry policy files containing the encodings of the settings described in this document. Because the Firewall and Advanced Security policies are applied to the whole machine, the Group Policy: Firewall and Advanced Security Data Structure protocol uses the Computer Policy Mode specified in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 1.3.2.

This protocol provides mechanisms both for Group Policy administrators to deploy policies and for clients to obtain the applicable policies to enforce them. Thus, the protocol consists of two components: an administrative plug-in and a client.

The Group Policy: Firewall and Advanced Security Data Structure administrative plug-in is invoked by an administrative tool. It is responsible for loading and updating the Firewall and Advanced Security settings contained within a specified GPO. It understands how to translate these settings to and from the encodings described in section [2.2](#Section_3adde782cd9d4bfdbb7b9f5b5ea54f85).

The Group Policy: Firewall and Advanced Security Data Structure client is responsible for applying the Firewall and Advanced Security settings configured through Group Policy to the local Firewall and Advanced Security Protocol server. Group Policy: Firewall and Advanced Security Data Structure does not implement its own Client-Side Extension as defined in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf) section 3.2.1.24; instead, it relies on the Group Policy: Registry Extension Encoding Client-Side Extension. Thus, the processing of Firewall and Advanced Security policies on the client computer is divided into two distinct stages. First, the Group Policy: Registry Extension Encoding client plug-in copies the settings from the GPO to the registry, and then the Group Policy: Firewall and Advanced Security Data Structure client reads the settings from the registry and applies them to the local Firewall and Advanced Security Protocol server.

The application of Firewall and Advanced Security policies is done as follows:

1. An administrator invokes a Group Policy Protocol Administrative Tool, as specified in [MS-GPOL] section 3.3.1.1, on the administrator's computer in order to administer the Firewall and Advanced Security settings of a GPO.
2. The administrative tool invokes the Group Policy: Firewall and Advanced Security Data Structure administrative plug-in to load the current policy settings. The administrative plug-in loads the settings through the Group Policy: Registry Extension Encoding administrative plug-in by invoking the Load Policy Settings event, as specified in [MS-GPREG] section 3.1.4.1.
3. The administrative tool displays these policy settings to the administrator in a custom UI, which enables the administrator to make changes if needed.
4. If the administrator makes any changes to the policy settings, the administrative tool invokes the Group Policy: Firewall and Advanced Security Data Structure administrative plug-in to update the settings in the GPO. The administrative plug-in updates the settings through the Group Policy: Registry Extension Encoding administrative plug-in by invoking the Update Policy Settings event, as specified in [MS-GPREG] section 3.1.4.2. During the processing of this event, the Group Policy: Registry Extension Encoding's CSE GUID is written to the GPO. After updating the settings, the administrative plug-in uses Group Policy: Core Protocol to update the version number associated with the GPO by invoking the Group Policy Extension Update event, as specified in [MS-GPOL] section 3.3.4.4.
5. A client computer affected by that GPO is started (or is connected to the network, if this happens after the client starts), and Group Policy: Core Protocol is invoked by the client to retrieve Policy Settings from the Group Policy server. As part of the processing of Group Policy: Core Protocol, the Group Policy: Registry Extension Encoding's CSE GUID is read from this GPO, and this instructs the client to invoke a Group Policy: Registry Extension Encoding client plug-in component for Policy Application.
6. In processing the Policy Application portion of Group Policy: Registry Extension Encoding, the client parses the settings and then saves the settings in the registry. The Firewall and Advanced Security policies are stored under the Software\Policies\Microsoft\WindowsFirewall\ registry key.
7. After all Client-Side Extensions (including the Group Policy: Registry Extension Encoding client plug-in) have completed processing, Group Policy: Core Protocol signals the Policy Application event, as specified in [MS-GPOL] section 3.2.7.3, to notify the Group Policy: Firewall and Advanced Security Data Structure client.
8. The Group Policy: Firewall and Advanced Security Data Structure client parses the Firewall and Advanced Security settings from the Software\Policies\Microsoft\WindowsFirewall\ registry key. The client then passes these settings to the Group Policy: Firewall and Advanced Security Data Structure server for enforcement by invoking the SetGroupPolicyRSoPStore abstract interface, as specified in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 3.1.6.4.

## Relationship to Other Protocols

This protocol depends on the Group Policy: Core Protocol (as specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf)) to provide a list of applicable GPOs.

Group Policy: Firewall and Advanced Security Data Structure configures settings that are used by the Firewall and Advanced Security Protocol specified in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf). These settings are defined in [MS-FASP] section 3.1.1.

For policy administration, the Group Policy: Firewall and Advanced Security Data Structure depends on the Group Policy: Registry Extension Encoding (specified in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf)) to store settings from in the GPO. For policy application, the Group Policy: Firewall and Advanced Security Data Structure depends on Group Policy: Registry Extension Encoding to retrieve settings from a GPO and to populate settings in the client registry. Group Policy: Registry Extension Encoding in turn depends on remote file access to read and write these settings from the GPO. Thus the Group Policy: Firewall and Advanced Security Data Structure has an indirect dependency on remote file access.

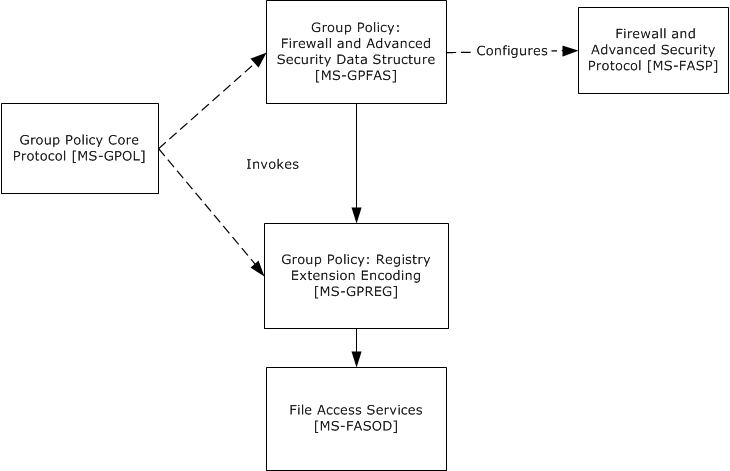


Figure : Group Policy: Firewall and Advanced Security Data Structure protocol relationship diagram

## Prerequisites/Preconditions

The prerequisites for this protocol are the same as those for the Group Policy: Registry Extension Encoding.

In addition, a client must have a system/subsystem capable of executing commands at startup/shutdown time because the Computer Policy Mode of the Group Policy: Registry Extension Encoding is used.

## Applicability Statement

Group Policy: Firewall and Advanced Security Data Structure is applicable only while transported under the Group Policy: Registry Extension Encoding and within the Group Policy: Core Protocol framework. Group Policy: Firewall and Advanced Security Data Structure can be used to express the required Firewall and Advanced Security policy of the client.

This protocol is also applicable only when the requirement is for many clients to get the same Firewall and Advanced Security policies. To configure individual clients with custom Firewall and Advanced Security policies, the Firewall and Advanced Security Protocol (as specified in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf)) can be used instead.

The protocol should not be used in any other context.

## Versioning and Capability Negotiation

This document covers versioning and capability negotiation issues in the following areas:

* Protocol Versions: This protocol has a policy version. This version (also called the inherent version of the component or the maximum supported schema version of the component), can be tied to policies and specific policy objects, as defined in section [2.2](#Section_3adde782cd9d4bfdbb7b9f5b5ea54f85).[<1>](#Appendix_A_1)
* Capability Negotiation: A configuration option defined in section 2.2 contains the maximum policy version encoded in the policy settings. Policy Objects also specify the policy version in which they are encoded. Lastly, a client component implementing the Group Policy: Firewall and Advanced Security Data Structure has an inherent maximum policy version it supports. Using this information, a client can understand what can and cannot be expected in these encodings, what must be parsed and what must be ignored. The settings in section 2.2 are defined in terms of these policy versions when appropriate. No other negotiation capabilities, version-specific or otherwise, are present in this protocol.

## Vendor-Extensible Fields

None.

## Standards Assignments

This protocol defines the administrative tool's extension GUID standards assignments, as specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf) section 1.8. It also defines a base registry key where the settings of this protocol are stored on registry policy files using Group Policy: Registry Extension Encoding. The assignments are as follows.

| Parameter | Value |
| --- | --- |
| Tool extension GUID | {b05566ac-fe9c-4368-be01-7a4cbb6cba11} |
| Policy Base registry key | Software\Policies\Microsoft\WindowsFirewall\ |

When a GPO is modified, the Tool Extension GUID value is written to the GPO by the administrative plug-in tools that are part of Windows.

# Messages

## Transport

The Group Policy: Firewall and Advanced Security Data Structure's administrative plug-in uses the transport specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf) to read and modify settings in the central policy store. Specifically, it uses remote file access for reading, updating, creating, and deleting the group policy settings. Information is retrieved from the policy store and written to the client's registry by the Group Policy: Registry Extension Encoding ([[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 3.2), using remote file access.

## Message Syntax

### Global Policy Configuration Options

The Global Policy Configuration Options are values that represent the enumeration values of the **FW\_GLOBAL\_CONFIG** enumeration type as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41. Note that the following global policy configuration options supported by the Firewall and Advanced Security Protocol specified in [MS-FASP] are read-only, and thus cannot be configured through this protocol:

* FW\_GLOBAL\_CONFIG\_POLICY\_VERSION\_SUPPORTED
* FW\_GLOBAL\_CONFIG\_CURRENT\_PROFILE
* FW\_GLOBAL\_CONFIG\_BINARY\_VERSION\_SUPPORTED

#### Disable Stateful FTP

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "DisableStatefulFTP"

Type: REG\_DWORD.

Size: Equal to the size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_DISABLE\_STATEFUL\_FTP** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Disable Stateful PPTP

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "DisableStatefulPPTP"

Type: REG\_DWORD.

Size: Equal to the size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_DISABLE\_STATEFUL\_PPTP** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Security Associations Idle Time

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "SAIdlTime"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: This field is an unsigned 32-bit integer value.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_SA\_IDLE\_TIME** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Preshared Key Encoding

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "PresharedKeyEncoding"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: This field is a 32-bit value consisting of the following value.

| Value | Meaning |
| --- | --- |
| 0x00000001 | This value represents the enumeration value **FW\_GLOBAL\_CONFIG\_PRESHARED\_KEY\_ENCODING\_UTF\_8** as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.39. |

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_PRESHARED\_KEY\_ENCODING** enumeration value as defined in [MS-FASP] section 2.2.41.

#### IPsec Exemptions

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecExempt"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: This field is a 32-bit value consisting of the bitwise OR of zero or more of the following flags.

| Value | Meaning |
| --- | --- |
| 0x00000001 | This value represents the **FW\_GLOBAL\_CONFIG\_IPSEC\_EXEMPT\_NEIGHBOR\_DISC** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.38. |
| 0x00000002 | This value represents the **FW\_GLOBAL\_CONFIG\_IPSEC\_EXEMPT\_ICMP** enumeration value as defined in [MS-FASP] section 2.2.38. |
| 0x00000004 | This value represents the **FW\_GLOBAL\_CONFIG\_IPSEC\_EXEMPT\_ROUTER\_DISC** enumeration value as defined in [MS-FASP] section 2.2.38. |
| 0x00000008 | This value represents the **FW\_GLOBAL\_CONFIG\_IPSEC\_EXEMPT\_DHCP** enumeration value as defined in [MS-FASP] section 2.2.38. |

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_PRESHARED\_KEY\_ENCODING** enumeration value as defined in [MS-FASP] section 2.2.41.

#### Certificate Revocation List Check

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "StrongCRLCheck"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: This field is a 32-bit value.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_CRL\_CHECK** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### IPsec Through NATs

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecThroughNAT"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: This field is a 32-bit value consisting of one of the following flags, all defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.40.

| Value | Meaning |
| --- | --- |
| 0x00000000 | This value represents the **FW\_GLOBAL\_CONFIG\_IPSEC\_THROUGH\_NAT\_NEVER** enumeration value. |
| 0x00000001 | This value represents the enumeration value **FW\_GLOBAL\_CONFIG\_IPSEC\_THROUGH\_NAT\_SERVER\_BEHIND\_NAT**. |
| 0x00000002 | This value represents the **FW\_GLOBAL\_CONFIG\_IPSEC\_THROUGH\_NAT\_SERVER\_AND\_CLIENT\_BEHIND\_NAT** enumeration value. |

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_IPSEC\_THROUGH\_NAT** enumeration value as defined in [MS-FASP] section 2.2.41.

#### Policy Version

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "PolicyVersion"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: This field is a 32-bit value.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_POLICY\_VERSION** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Tunnel Remote Machine Authorization List

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecTunnelRemoteMachineAuthorizationList"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A variable-length, null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_IPSEC\_TUNNEL\_REMOTE\_MACHINE\_AUTHORIZATION\_LIST** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Tunnel Remote User Authorization List

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecTunnelRemoteUserAuthorizationList"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A variable-length, null-terminated Unicode string.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_IPSEC\_TUNNEL\_REMOTE\_USER\_AUTHORIZATION\_LIST** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Opportunistically Match Authentication Set Per Key Module

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecOpportunisticallyMatchAuthSetPerKM"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_OPPORTUNISTICALLY\_MATCH\_AUTH\_SET\_PER\_KM** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Transport Remote Machine Authorization List

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecTransportRemoteMachineAuthorizationList"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A variable-length, null-terminated Unicode string.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_IPSEC\_TRANSPORT\_REMOTE\_MACHINE\_AUTHORIZATION\_LIST** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Transport Remote User Authorization List

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "IPsecTransportRemoteUserAuthorizationList"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A variable-length, null-terminated Unicode string.

This value represents the contents assigned to the configuration option represented by the **FW\_GLOBAL\_CONFIG\_IPSEC\_TRANSPORT\_REMOTE\_USER\_AUTHORIZATION\_LIST** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

#### Packet Queue

Key: Software\Policies\Microsoft\WindowsFirewall\

Value: "EnablePacketQueue"

Type: REG\_DWORD

Size: Equal to size of the Data field.

Data: This field is a 32-bit value.

This value represents the contents assigned to the configuration option represented by the FW\_GLOBAL\_CONFIG\_ENABLE\_PACKET\_QUEUE enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.41.

### Firewall Rule Messages

This section defines the grammars used to encode different portions of the firewall rules.

#### Profile Tokens

This grammar, as specified in [[RFC4234]](http://go.microsoft.com/fwlink/?LinkId=90462), is used to identify profile types.

PROFILE\_VAL = "Domain" / "Private" / "Public"

**Domain**: This token value represents the **FW\_PROFILE\_TYPE\_DOMAIN** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.2. The remaining token values in this list can be found in the same Protocol specification section.

**Private**: This token value represents the **FW\_PROFILE\_TYPE\_PRIVATE** enumeration value.

**Public**: This token value represents the **FW\_PROFILE\_TYPE\_PUBLIC** enumeration value.

#### Port and Port Range Rules

This grammar is used to identify ports.

1. PORT\_RANGE\_VAL = BEGINPORT "-" ENDPORT
2. PORT\_VAL = SINGLEPORT
3. BEGINPORT = PORT
4. ENDPORT = PORT
5. SINGLEPORT = PORT
6. PORT = 1\*5DIGIT

**PORT:** This rule represents a port number. Hence, its decimal value MUST NOT be greater than 65,535.

**BEGINPORT:** This rule describes a port number that represents the **wBegin** field of a **FW\_PORT\_RANGE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.12. The remaining rules in this list can be found in the same Protocol specification section.

**ENDPORT:** This rule describes a port number that represents the **wEnd** field of a **FW\_PORT\_RANGE** structure.

**SINGLEPORT:** This rule describes a port number that represents both the **wBegin** and the **wEnd** fields of a **FW\_PORT\_RANGE** structure.

**PORT\_VAL:** This rule describes a **FW\_PORT\_RANGE** structure as defined in [MS-FASP] section 2.2.12. The structure MUST comply with all requirements defined in that section.

#### Port Keyword Rules

This grammar is used to identify port keywords.

1. LPORT\_KEYWORD\_VAL = "RPC" / "RPC-EPMap" / "Teredo"
2. LPORT\_KEYWORD\_VAL\_2\_10 = "IPTLSIn" / "IPHTTPSIn"
3. LPORT\_KEYWORD\_VAL\_2\_20 = "Ply2Disc"
4. RPORT\_KEYWORD\_VAL\_2\_10 = "IPTLSOut" / "IPHTTPSOut"

**RPC:** This token represents the **FW\_PORT\_KEYWORD\_DYNAMIC\_RPC\_PORTS** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.14. The remaining token values in this list can be found in the same section.

**RPC-EPMap:** This token represents the **FW\_PORT\_KEYWORD\_RPC\_EP** enumeration value.

**Teredo:** This token represents the **FW\_PORT\_KEYWORD\_TEREDO\_PORT** enumeration value.

**IPHTTPSOut:** This token represents the **FW\_PORT\_KEYWORD\_IP\_TLS\_IN** enumeration value.

**IPHTTPSIn:** This token represents the **FW\_PORT\_KEYWORD\_IP\_TLS\_OUT** enumeration value.

**Ply2Disc:** This token represents the **FW\_PORT\_KEYWORD\_PLAYTO\_DISCOVERY** enumeration value.

#### Direction Tokens

This grammar is used to identify the direction of a network traffic flow.

DIR\_VAL = "In" / "Out"

**In:** This token value represents the **FW\_DIR\_IN** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.19.

**Out:** This token value represents the **FW\_DIR\_OUT** enumeration value as defined in [MS-FASP] section 2.2.19.

#### Action Tokens

This grammar is used to identify the actions available for firewall rules.

1. ACTION\_VAL = "Allow" / "Block" / "ByPass"

**Allow:** This token value represents the **FW\_RULE\_ACTION\_ALLOW** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.33. The remaining token values in this list can be found in the same Protocol specification section.

**Block:** This token value represents the **FW\_RULE\_ACTION\_BLOCK** enumeration value.

**ByPass:** This token value represents the **FW\_RULE\_ACTION\_ALLOW\_BYPASS** enumeration value.

#### IfSecure Tokens

This grammar is used to identify the security flags on firewall rules described in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.34.

1. IFSECURE\_VAL = "Authenticate" / "AuthenticateEncrypt"
2. IFSECUIRE2\_9\_VAL = "An-NoEncap"
3. IFSECURE2\_10\_VAL = "AnE-Nego"

**Authenticate:** This token value represents the **FW\_RULE\_FLAGS\_AUTHENTICATE** enumeration value as defined in [MS-FASP] section 2.2.34. The remaining token values in this list can be found in the same Protocol specification section.

**AuthenticateEncrypt:** This token value represents the **FW\_RULE\_FLAGS\_AUTHENTICATE\_WITH\_ENCRYPTION** enumeration value.

**An-NoEncap:** This token value represents the **FW\_RULE\_FLAGS\_AUTH\_WITH\_NO\_ENCAPSULATION** enumeration value.

**AnE-Nego:** This token value represents the **FW\_RULE\_FLAGS\_AUTH\_WITH\_ENC\_NEGOTIATE** enumeration value.

#### Interfaces

This grammar is used to identify the interfaces on firewall rules described in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.34.

1. IF\_VAL = GUID

**IF\_VAL:** This grammar rule represents a GUID that identifies an interface ([MS-FASP] section 2.2.34).

#### Interface Types

This grammar is used to identify the types of network adapters described in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.34.

1. IFTYPE\_VAL = "Lan" / "Wireless" / "RemoteAccess"

**Lan:** This token value represents the **FW\_INTERFACE\_TYPE\_LAN** enumeration value as defined in [MS-FASP] section 2.2.20. The remaining token values in this list can be found in the same Protocol specification section.

**Wireless:** This token value represents the **FW\_INTERFACE\_TYPE\_WIRELESS** enumeration value.

**RemoteAccess:** This token value represents the **FW\_INTERFACE\_TYPE\_REMOTE\_ACCESS** enumeration value.

#### IPV4 Address Ranges Rules

This grammar is used to identify IPv4 address ranges.

1. ADDRESSV4\_RANGE\_VAL = BEGINADDRV4 "-" ENDADDRV4
2. ADDRESSV4\_RANGE\_VAL = SINGLEADDRV4
3. BEGINADDRV4 = ADDRV4
4. ENDADDRV4 = ADDRV4
5. SINGLEADDRV4 = ADDRV4
6. ADDRV4 = 1\*3DIGIT "."1\*3DIGIT "."1\*3DIGIT "."1\*3DIGIT

**ADDRV4:** This rule represents an IPv4 address.

**BEGINADDRV4:** This rule describes an IPv4 address that represents the **dwBegin** field of a **FW\_IPV4\_ADDRESS\_RANGE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.8. The remaining rules in this list can be found in the same Protocol specification section.

**ENDADDRV4:** This rule describes an IPv4 address that represents the **dwEnd** field of a **FW\_IPV4\_ADDRESS\_RANGE** structure.

**SINGLEADDRV4:** This rule describes an IPv4 address that represents both the **dwBegin** and the **dwEnd** fields of a **FW\_IPV4\_ADDRESS\_RANGE** structure.

**ADDRESSV4\_RANGE\_VAL:** This rule represents a **FW\_IPV4\_ADDRESS\_RANGE** structure as defined in [MS-FASP] section 2.2.8. The structure MUST comply with all requirements defined in that section.

#### IPV4 Address Subnet Rules

This grammar is used to identify IPv4 subnets.

1. ADDRESSV4\_SUBNET\_VAL = SUBNET\_ADDRV4 "/" V4PREFIX\_LENGHT
2. ADDRESSV4\_SUBNET\_VAL = SUBNET\_ADDRV4 "/" MASK\_ADDRV4
3. V4PREFIX\_LENGTH = 1\*2DIGIT
4. SUBNET\_ADDRV4 = ADDRV4
5. MASK\_ADDRV4 = ADDRV4

**ADDRV4:** This rule represents an IPv4 address as defined in section [2.2.2.8](#Section_b75134ac1cc94f619553bfe49c5cf1a9).

**SUBNET\_ADDRV4:** This rule describes an IPv4 address that represents the **dwAddress** field of a **FW\_IPV4\_SUBNET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.4. The remaining rules in this list can be found in the same Protocol specification section.

**MASK\_ADDRV4:** This rule describes an IPv4 address mask that represents the **dwSubNetMask** field of a **FW\_IPV4\_SUBNET** structure.

**V4PREFIX\_LENGTH:** This rule describes a decimal number that MUST be less than 32 and that represents the **dwSubNetMask** field of a **FW\_IPV4\_SUBNET** structure. The way in which it represents it is a shortcut as it describes the number of high order consecutive bits that are set to 1 in the address mask.

**ADDRESSV4\_SUBNET\_VAL:** This rule represents a **FW\_IPV4\_SUBNET** structure as defined in [MS-FASP] section 2.2.4. The structure MUST comply with all requirements defined in that section.

#### IPV6 Address Range Rules

This grammar is used to identify IPv6 address ranges.

1. ADDRESSV6\_RANGE\_VAL = BEGINADDRV6 "-" ENDADDRV6
2. ADDRESSV6\_RANGE\_VAL = SINGLEADDRV6
3. BEGINADDRV6 = ADDRV6
4. ENDADDRV6 = ADDRV6
5. SINGLEADDRV6 = ADDRV6
6. ADDRV6 = a string representing an IPv6 address

**ADDRV6:** This rule represents an IPv6 address as defined in [[RFC4291]](http://go.microsoft.com/fwlink/?LinkId=90464).

**BEGINADDRV6:** This rule describes an IPv6 address that represents the **Begin** field of a **FW\_IPV6\_ADDRESS\_RANGE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.10. The remaining rules in this list can be found in the same Protocol specification section.

**ENDADDRV6:** This rule describes an IPv6 address that represents the **End** field of a **FW\_IPV6\_ADDRESS\_RANGE** structure.

**SINGLEADDRV6:** This rule describes an IPv6 address that represents both the **Begin** and the **End** fields of a **FW\_IPV6\_ADDRESS\_RANGE** structure.

**ADDRESSV6\_RANGE\_VAL:** This rule represents a **FW\_IPV6\_ADDRESS\_RANGE** structure as defined in [MS-FASP] section 2.2.10. The structure MUST comply with all requirements defined in that section.

#### IPV6 Address Subnet Rules

This grammar is used to identify IPv6 subnets.

1. ADDRESSV6\_SUBNET\_VAL = SUBNET\_ADDRV6 "/" V6PREFIX\_LENGHT
2. V6PREFIX\_LENGTH = 1\*3DIGIT
3. SUBNET\_ADDRV6 = ADDRV6

**ADDRV6:** This rule represents an IPv6 address as defined in section [2.2.2.10](#Section_32f9f12df3ee4db390ef0ccb2b794af8).

**SUBNET\_ADDRV6:** This rule describes an IPv4 address that represents the **Address** field of a **FW\_IPV6\_SUBNET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.6. The remaining rules in this list can be found in the same Protocol specification section.

**V6PREFIX\_LENGTH:** This rule describes a decimal number that MUST be less than 128 and that represents the **dwNumPrefixBits** field of a **FW\_IPV6\_SUBNET** structure.

**ADDRESSV6\_SUBNET\_VAL:** This rule represents a **FW\_IPV6\_SUBNET** structure as defined in [MS-FASP] section 2.2.6. The structure MUST comply with all requirements defined in that section.

#### Address Keyword Rules

This grammar is used to identify address keywords.

1. ADDRESS\_KEYWORD\_VAL = "LocalSubnet" / "DNS" / "DHCP" / "WINS" / "DefaultGateway"
2. ADDRESS\_KEYWORD\_VAL\_2\_20 = "IntrAnet" / "IntErnet" / "Ply2Renders" / "RmtIntrAnet"

**LocalSubnet:**  This token represents the **FW\_ADDRESS\_KEYWORD\_LOCAL\_SUBNET** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.21. The remaining token values in this list can be found in the same Protocol specification section.

**DNS:** This token represents the **FW\_ADDRESS\_KEYWORD\_DNS** enumeration value.

**DHCPL:** This token represents the **FW\_ADDRESS\_KEYWORD\_DHCP** enumeration value.

**WINS:** This token represents the **FW\_ADDRESS\_KEYWORD\_WINS** enumeration value.

**DefaultGateway:** This token represents the **FW\_ADDRESS\_KEYWORD\_DEFAULT\_GATEWAY** enumeration value.

**IntrAnet:** This token represents the **FW\_ADDRESS\_KEYWORD\_INTRANET** enumeration value.

**IntErnet:** This token represents the **FW\_ADDRESS\_KEYWORD\_INTERNET** enumeration value.

**Ply2Renders:** This token represents the **FW\_ADDRESS\_KEYWORD\_PLAYTO\_RENDERERS** enumeration value.

**RmtIntrAnet:** This token represents the **FW\_ADDRESS\_KEYWORD\_REMOTE\_INTERNET** enumeration value.

#### Boolean Rules

This grammar is used to identify Boolean values.

1. BOOL\_VAL = "TRUE" / "FALSE"

**TRUE:** This token represents a decimal value of 1 which has the meaning of the Boolean value of true.

**FALSE:** This token represents a decimal value of 0 which has the meaning of the Boolean value of false.

#### Edge Defer Rules

This grammar is used to identify Edge defer flags.

1. DEFER\_VAL = "App" / "User"

**App:** This token represents the FW\_RULE\_FLAGS\_ROUTEABLE\_ADDRS\_TRAVERSE\_DEFER\_APP flag as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.34. The meaning of the appearance of this token is a Boolean true.

**User:** This token represents the FW\_RULE\_FLAGS\_ROUTEABLE\_ADDRS\_TRAVERSE\_DEFER\_USER flag as defined in [MS-FASP] section 2.2.34. The meaning of the appearance of this token is a Boolean true.

#### ICMP Type - Code Rules

This grammar is used to identify ICMP protocol type and codes.

1. ICMP\_TYPE\_CODE\_VAL = TYPE ":" CODE
2. TYPE = 1\*3DIGIT
3. CODE = 1\*3DIGIT
4. CODE =/ "\*"

**TYPE:** This grammar rule represents the **bType** field of the **FW\_ICMP\_TYPE\_CODE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.16. The grammar rule encodes a decimal value which MUST be less than or equal to 255.

**CODE:** This grammar rule represents the **wCode** field of the **FW\_ICMP\_TYPE\_CODE** structure as defined in [MS-FASP] section 2.2.16. When the grammar rule encodes a decimal value, such value MUST be less than or equal to 255. When the grammar rule encodes a "\*" token, then the meaning is the same as a value of 0x100 in the **wCode** field.

**ICMP\_TYPE\_CODE\_VAL:** This rule represents a **FW\_ICMP\_TYPE\_CODE** structure as defined in [MS-FASP] section 2.2.16. The structure MUST comply with all requirements defined in that section.

#### Platform Validity Rules

This grammar is used to identify platform validity objects.

1. PLATFORM\_VAL = PLATFORM ":" OS\_MAJOR\_VER ":" OS\_MINOR\_VER
2. PLATFORM = 1DIGIT
3. OS\_MAJOR\_VER = 1\*3DIGIT
4. OS\_MINOR\_VER = 1\*3DIGIT

**PLATFORM:** This grammar rule represents the 3 least significant bits of the **bPlatform** field of the **FW\_OS\_PLATFORM** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.29. The grammar rule encodes a decimal value which MUST be less than or equal to 7.

**OS\_MAJOR\_VER:** This grammar rule represents the **bMajorVersion** field of the **FW\_OS\_PLATFORM** structure as defined in [MS-FASP] section 2.2.29. The grammar rule encodes a decimal value which MUST be less than or equal to 255.

**OS\_MINOR\_VER:** This grammar rule represents the **bMinorVersion** field of the **FW\_OS\_PLATFORM** structure as defined in [MS-FASP] section 2.2.29. The grammar rule encodes a decimal value which MUST be less than or equal to 255.

**PLATFORM\_VAL:** This rule represents a **FW\_OS\_PLATFORM** structure as defined in [MS-FASP] section 2.2.29, with the exception of the 5 most significant bits of the **bPlatform** field. The structure MUST comply with all requirements defined in that section.

#### Platform Validity Operators Rules

This grammar is used to identify platform validity objects.

1. PLATFORM\_OP\_VAL = "GTEQ"

**GTEQ:** This token represents the **FW\_OS\_PLATFORM\_GTEQ** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.28.

**PLATFORM\_OP\_VAL:** This rule represents the 5 most significant bits of the **bPlatform** field of the last **FW\_OS\_PLATFORM** structure entry (as defined in [MS-FASP] section 2.2.29), of the **pPlatforms** field of the **FW\_OS\_PLATFORM\_LIST** structure as defined in [MS-FASP] section 2.2.30.

#### Firewall Rule and the Firewall Rule Grammar Rule

Firewall rules are stored under the Software\Policies\Microsoft\WindowsFirewall\FirewallRules key.

Each value under the key is a firewall rule. The type of the value MUST be **REG\_SZ**. The data of each value is a string that can be parsed by the following grammar. This grammar represents a firewall rule as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.36, except for the **wszRuleId** field of the **FW\_RULE** structure which is instead represented by the name of the registry value.

1. RULE = "v" VERSION "|" 1\*FIELD
2. FIELD = TYPE\_VALUE "|"
3. TYPE\_VALUE =  "Action=" ACTION\_VAL
4. TYPE\_VALUE =/ "Dir=" DIR\_VAL
5. TYPE\_VALUE =/ "Profile=" PROFILE\_VAL
6. TYPE\_VALUE =/ "Protocol=" 1\*3DIGIT ; protocol is maximum 3 digits (255)
7. TYPE\_VALUE =/ "LPort=" ( PORT\_VAL / LPORT\_KEYWORD\_VAL )
8. TYPE\_VALUE =/ "RPort=" PORT\_VAL
9. TYPE\_VALUE =/ "LPort2\_10=" ( PORT\_RANGE\_VAL / LPORT\_KEYWORD\_VAL\_2\_10 )
10. TYPE\_VALUE =/ "RPort2\_10=" ( PORT\_RANGE\_VAL / RPORT\_KEYWORD\_VAL\_2\_10 )
11. TYPE\_VALUE =/ "Security=" IFSECURE\_VAL
12. TYPE\_VALUE =/ "Security2\_9=" IFSECURE2\_9\_VAL
13. TYPE\_VALUE =/ "Security2=" IFSECURE2\_10\_VAL
14. TYPE\_VALUE =/ "IF=" IF\_VAL
15. TYPE\_VALUE =/ "IFType=" IFTYPE\_VAL
16. TYPE\_VALUE =/ "App=" APP\_VAL
17. TYPE\_VALUE =/ "Svc=" SVC\_VAL
18. TYPE\_VALUE =/ "LA4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL )
19. TYPE\_VALUE =/ "RA4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
20. TYPE\_VALUE =/ "LA6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL )
21. TYPE\_VALUE =/ "RA6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
22. TYPE\_VALUE =/ "Name=" STR\_VAL
23. TYPE\_VALUE =/ "Desc=" STR\_VAL
24. TYPE\_VALUE =/ "EmbedCtxt=" STR\_VAL
25. TYPE\_VALUE =/ "Edge=" BOOL\_VAL
26. TYPE\_VALUE =/ "Defer=" DEFER\_VAL
27. TYPE\_VALUE =/ "LSM=" BOOL\_VAL
28. TYPE\_VALUE =/ "Active=" BOOL\_VAL
29. TYPE\_VALUE =/ "ICMP4=" ICMP\_TYPE\_CODE\_VAL
30. TYPE\_VALUE =/ "ICMP6=" ICMP\_TYPE\_CODE\_VAL
31. TYPE\_VALUE =/ "Platform=" PLATFORM\_VAL
32. TYPE\_VALUE =/ "RMauth=" STR\_VAL
33. TYPE\_VALUE =/ "RUAuth=" STR\_VAL
34. TYPE\_VALUE =/ "AuthByPassOut=" BOOL\_VAL
35. TYPE\_VALUE =/ "SkipVer=" VERSION
36. TYPE\_VALUE =/ "LOM=" BOOL\_VAL
37. TYPE\_VALUE =/ "Platform2=" PLATFORM\_OP\_VAL
38. TYPE\_VALUE =/ "PCross=" BOOL\_VAL
39. TYPE\_VALUE =/ "LUAuth=" STR\_VAL
40. TYPE\_VALUE =/ "RA42=" ADDRESS\_KEYWORD\_VAL\_2\_20
41. TYPE\_VALUE =/ "RA62=" ADDRESS\_KEYWORD\_VAL\_2\_20
42. TYPE\_VALUE =/ "LUOwn=" STR\_VAL
43. TYPE\_VALUE =/ "AppPkgId=" STR\_VAL
44. TYPE\_VALUE =/ "LPort2\_20=" LPORT\_KEYWORD\_VAL\_2\_20
45. TYPE\_VALUE =/ "TTK=" TRUST\_TUPLE\_KEYWORD\_VAL
46. TYPE\_VALUE =/ "LUAuth2\_24=" STR\_VAL
47. TYPE\_VALUE =/ "NNm=" STR\_ENC\_VAL
48. TYPE\_VALUE =/ "SecurityRealmId=" STR\_VAL
49. VERSION = MAJOR\_VER "." MINOR\_VER
50. MAJOR\_VER = 1\*3DIGIT
51. MINOR\_VER = 1\*3DIGIT
52. APP\_VAL = 1\*ALPHANUM
53. SVC\_VAL = "\*" / 1\*ALPHANUM
54. STR\_VAL = 1\*ALPHANUM

**MAJOR\_VER:** This grammar rule describes a decimal number that represents the high order 8 bits of the **wSchemaVersion** field of the **FW\_RULE** structure as defined in [MS-FASP] section 2.2.36. Because of this, the decimal value of this number MUST NOT be greater than 255. The following grammar rules can also be found in the previously mentioned [MS-FASP] section 2.2.36.

**MINOR\_VER:** This grammar rule describes a decimal number that represents the low order 8 bits of the **wSchemaVersion** field of the **FW\_RULE** structure. Because of this, the decimal value of this number MUST NOT be greater than 255.

**VERSION:** This grammar rule describes a decimal value whose low 8 order bits are those described in the MINOR\_VER grammar rule, and whose high 8 order bits are those described in the MAJOR\_VER grammar rule.

**Action=:** This token value represents the **Action** field of the **FW\_RULE** structure as defined in [MS-FASP] section 2.2.36. The ACTION\_VAL grammar rule represents the value contents of this field. This token MUST appear at most once in a rule string. The remaining token values in this list can be found in the same Protocol specification section except where noted.

**Dir=:** This token value represents the **Direction** field of the **FW\_RULE** structure. The DIR\_VAL grammar rule represents the value contents of this field. This token MUST appear at most once in a rule string.

**Profile=:** This token value represents the **dwProfiles** field of the **FW\_RULE** structure. The PROFILE\_VAL grammar rule represents a value content of such field. If this token appears more than once in a RULE grammar rule, then all the contents represented by the PROFILE\_VAL rule appearing next to them are included. If the **Profile=** token never appears in the rule string then it represents a value of FW\_PROFILE\_TYPE\_ALL as defined in [MS-FASP] section 2.2.2.

**Protocol=:** This token value represents the **wIpProtocol** field of the **FW\_RULE** structure. The 1\*3DIGIT grammar rule represents the value content of this field. Such value MUST NOT be greater than 255. The **Protocol** token MUST appear at most once in a RULE grammar rule. If a **Protocol** token does not appear in the rule string, then the meaning is the same as a value of 256 in the **wIpProtocol** field in [MS-FASP] section 2.2.36.

**LPort=:** This token value represents the **LocalPorts** field of the **FW\_RULE** structure. As such defined, **LocalPorts** is of type **FW\_PORTS**, which contains a **Ports** field of type **FW\_PORT\_RANGE\_LIST**, which also contains a pPorts array of type **FW\_PORT\_RANGE**. The PORT\_VAL grammar rule represents an entry in the **pPorts** field. The LPORT\_KEYWORD\_VAL grammar rule, however, represents the **wPortKeywords** field of the **LocalPorts** field (which is of type **FW\_PORTS**) of the **FW\_RULE** structure. If the **LPort=:** token appears multiple times in the rule string, then all the respective PORT\_VAL rules and LPORT\_KEYWORD\_VAL rules of such appearances are allowed.

**LPort2\_10=:** This token value represents the **LocalPorts** field of the **FW\_RULE** structure. Similarly to the case of the "LPort=" token, the PORT\_RANGE\_VAL grammar rule represents an entry in the **pPorts** field. The LPORT\_KEYWORD\_VAL\_2\_10 grammar rule, however, represents the **wPortKeywords** field of the **LocalPorts** field (which is of type **FW\_PORTS**) of the **FW\_RULE** structure. If the **LPort** token appears multiple times in the rule string, then all the respective PORT\_RANGE\_VAL rules and LPORT\_KEYWORD\_VAL\_2\_10 rules of such appearances are allowed.

**RPort=:** This token value represents the **RemotePorts** field of the **FW\_RULE** structure. As such defined, **RemotePorts** is of type **FW\_PORTS**, which contains a **Ports** field of type **FW\_PORT\_RANGE\_LIST**, which also contains a pPorts array of type **FW\_PORT\_RANGE**. The PORT\_VAL grammar rule represents an entry in the **pPorts** field. If the **RPort** token appears multiple times in the rule string, then all the PORT\_VAL rule of such are allowed.

**RPort2\_10=:** This token value represents the **RemotePorts** field of the **FW\_RULE** structure. Similarly to the case of the "RPort=" token, the PORT\_RANGE\_VAL grammar rule represents an entry in the **pPorts** field. The RPORT\_KEYWORD\_VAL\_2\_10 grammar rule however represents the **wPortKeywords** field of the **RemotePorts** field (which is of type **FW\_PORTS**) of the **FW\_RULE** structure. If the **RPort** token appears multiple times in the rule string, then all the respective PORT\_RANGE\_VAL rules and RPORT\_KEYWORD\_VAL\_2\_10 rules of such appearances are allowed.

**Security=:** This token value represents specific flags in the **wFlags** field of the **FW\_RULE** structure. The IFSECURE\_VAL grammar rule represents a flag of such field. This token MUST appear at most once in a rule string.

**Security2\_9=:** This token value represents specific flags in the **wFlags** field of the **FW\_RULE** structure. The IFSECURE\_VAL grammar rule represents a flag of such field. This token MUST appear at most once in a rule string. Also this token MUST appear only if the VERSION is a number greater than or equal to 0x0209.

**Security2=:** This token value represents specific flags in the **wFlags** field of the **FW\_RULE** structure. The IFSECURE\_VAL grammar rule represents a flag of such field. This token MUST appear at most once in a rule string. Also this token MUST appear only if the VERSION is a number greater than or equal to 0x020A.

**IF=:** This token represents an entry in the **LocalInterfaceIds** field of the **FW\_RULE** structure.

**IFType=:** This token represents the **dwLocalInterfaceType** field of the **FW\_RULE** structure.

**App=:** This token represents the **wszLocalApplication** field of the **FW\_RULE** structure. The grammar rule APP\_VAL represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Svc=:** This token represents the **wszLocalService** field of the **FW\_RULE** structure. The grammar rule SVC\_VAL represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**LA4=:** This token value represents the **LocalAddress** field of the **FW\_RULE** structure, specifically the v4 fields. As such defined **LocalAddress** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type FW\_IPV4\_RANGE\_LIST, which also contains a pRanges array of type FW\_IPV4\_ADDRESS\_RANGE, and lastly a **V4SubNets** field of type FW\_IPV4\_SUBNET\_LIST, which also contains a pSubNets array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. If the "LA4" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL and ADDRESSV4\_SUBNET\_VAL rules of such appearances are allowed.

**RA4=:** This token value represents the **RemoteAddress** field of the **FW\_RULE** structure, specifically the v4 fields. As such defined **RemoteAddress** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type **FW\_IPV4\_RANGE\_LIST**, which also contains a pRanges array of type **FW\_IPV4\_ADDRESS\_RANGE**, and lastly a **V4SubNets** field of type **FW\_IPV4\_SUBNET\_LIST**, which also contains a pSubNets array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV4AddressKeywords** field. If the "RA4" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**LA6=:** This token value represents the **LocalAddress** field of the **FW\_RULE** structure, specifically the v6 fields. As such defined **LocalAddress** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a pRanges array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly a **V6SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a pSubNets array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. If the "LA6" token appears multiple times in the rule string, then all the respective ADDRESSV6\_RANGE\_VAL and ADDRESSV6\_SUBNET\_VAL rules of such appearances are allowed.

**RA6=:** This token value represents the **RemoteAddress** field of the **FW\_RULE** structure, specifically the v6 fields. As such defined **RemoteAddress** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a pRanges array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly a **V6SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a pSubNets array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV6AddressKeywords** field. If the "RA6" token appears multiple times in the rule string, then all the respective ADDRESSV6\_RANGE\_VAL, ADDRESSV6\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**Name=:** This token represents the **wszName** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Desc=:** This token represents the **wszDescription** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**EmbedCtxt=:** This token represents the **wszEmbeddedContext** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Edge=:** This token represents the FW\_RULE\_FLAGS\_ROUTEABLE\_ADDRS\_TRAVERSE flag (as defined in [MS-FASP] section 2.2.34) of the **wFlags** field of the **FW\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section [2.2.2.14](#Section_2bdb10546ea04b088e51513f7a758011). If the "Edge=" token does not appear in the rule a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**Defer=:** This token represents the contents of the **wFlags** field of the **FW\_RULE** structure on the position defined by the FW\_RULE\_FLAGS\_ROUTEABLE\_ADDRS\_TRAVERSE\_APP and FW\_RULE\_FLAGS\_ROUTEABLE\_ADDRS\_TRAVERSE\_USER flag (as defined in [MS-FASP] section 2.2.34) The DEFER\_VAL grammar rule represents the Boolean contents of such flag as defined in section 2.2.2.14. If the "Defer=" token does not appear in the rule then a Boolean value false is assumed for both flags. Also this token MUST appear only if the VERSION is a number greater than or equal to 0x020A. This token MUST appear at most once in a rule string.

**LSM=:** This token represents the FW\_RULE\_FLAGS\_LOOSE\_SOURCE\_MAPPED flag (as defined in [MS-FASP] section 2.2.34) of the **wFlags** field of the **FW\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "LSM=" token does not appear in the rule a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**Active=:** This token represents the FW\_RULE\_FLAGS\_ACTIVE flag (as defined in [MS-FASP] section 2.2.34) of the **wFlags** field of the **FW\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "Active=" token does not appear in the rule a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**ICMP4=:** This token value represents the **V4TypeCodeList** field of the **FW\_RULE** structure. As such defined **V4TypeCodeList** is of type **FW\_ICMP\_TYPE\_CODE\_LIST**, it contains a pEntries array of type **FW\_ICMP\_TYPE\_CODE**. The ICMP\_TYPE\_CODE\_VAL grammar rule represents an entry in the **pEntries** field. If the "ICMP4=" token appears multiple times in the rule string, then all the respective ICMP\_TYPE\_CODE\_VAL grammar rules of such appearances are allowed.

**ICMP6=:** This token value represents the **V6TypeCodeList** field of the **FW\_RULE** structure. As such defined **V6TypeCodeList** is of type **FW\_ICMP\_TYPE\_CODE\_LIST**, it contains a pEntries array of type **FW\_ICMP\_TYPE\_CODE**. The ICMP\_TYPE\_CODE\_VAL grammar rule represents an entry in the **pEntries** field. If the "ICMP6=" token appears more than once in the rule string, then all the respective ICMP\_TYPE\_CODE\_VAL grammar rules of such appearances are allowed.

**Platform=:** This token value represents the **PlatformValidityList** field of the **FW\_RULE** structure. As such defined **PlatformValidityList** is of type **FW\_OS\_PLATFORM\_LIST**, it contains a pPlatforms array of type **FW\_OS\_PLATFORM**. The PLATFORM\_VAL grammar rule represents an entry in the **pPlatforms** field. If the "Platform=" token appears multiple times in the rule string, then all the respective PLATFORM\_VAL grammar rules of such appearances are allowed.

**RMAuth=:** This token represents the **wszRemoteMachineAuthorizationList** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**RUAuth=:** This token represents the **wszRemoteUserAuthorizationList** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**AuthByPassOut=:** This token represents the FW\_RULE\_FLAGS\_AUTHENTICATE\_BYPASS\_OUTBOUND flag (as defined in [MS-FASP] section 2.2.34) of the **wFlags** field of the **FW\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "AuthByPassOut=" token does not appear in the rule a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**SkipVer=:** The VERSION grammar rule following this token represents the highest inherent version of the Firewall and Advanced Security components that should ignore this rule string completely. The inherent version of a Firewall and Advanced Security component is the highest version that component supports.

**LOM=:** This token represents the FW\_RULE\_FLAGS\_LOCAL\_ONLY\_MAPPED flag (as defined in [MS-FASP] section 2.2.34) of the **wFlags** field of the **FW\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "LOM=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear only once in a rule string.

**Platform2=:** This token represents the operator to use on the last entry of the **PlatformValidityList** field of the **FW\_RULE** structure. Hence the PLATFORM\_OP\_VAL token represents the five most significant bits of the **bPlatform** field of the last **FW\_OS\_PLATFORM** structure entry (as defined in [MS-FASP] section 2.2.29) of the **pPlatforms** field of the **FW\_OS\_PLATFORM\_LIST** structure as defined in [MS-FASP] section 2.2.30.

**PCROSS=:** This token represents the FW\_RULE\_FLAGS\_ALLOW\_PROFILE\_CROSSING flag (as defined in [MS-FASP] section 2.2.34) of the **wFlags** field of the **FW\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "PCROSS=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear only once in a rule string.

**LUAuth=:** This token represents the **wszLocalUserAuthorizationList** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear only once in a rule string.

**RA42=:** This token value represents the **RemoteAddresses** field of the **FW\_RULE** structure, specifically the **dwV4AddressKeywords** field. The ADDRESS\_KEYWORD\_VAL\_2\_20 grammar rule represents a flag in the **dwV4AddressKeywords** field. If the "RA42=" token appears multiple times in the rule string, then all the respective ADDRESS\_KEYWORD\_VAL\_2\_20 rules of such appearances are allowed.

**RA62=:** This token value represents the **RemoteAddresses** field of the **FW\_RULE** structure, specifically the **dwTrustTupleKeywords** field. The ADDRESS\_KEYWORD\_VAL\_2\_20 grammar rule represents a flag in the **dwV6AddressKeywords** field. If the "RA62=" token appears multiple times in the rule string, then all the respective ADDRESS\_KEYWORD\_VAL\_2\_20 rules of such appearances are allowed.

**LUOwn=:** This token represents the **wszLocalUserOwner** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear only once in a rule string.

**AppPkgId=:** This token represents the **wszPackageId** field of the **FW\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear only once in a rule string.

**LPort2\_20=:** This token value represents the **LocalPorts** field of the **FW\_RULE** structure, specifically the **wPortKeywords** field. The LPORT\_KEYWORD\_VAL\_2\_20 grammar rule represents a flag in the **dwTrustTupleKeywords** field. If the "LPort2\_20=" token appears multiple times in the rule string, then all the respective LPORT\_KEYWORD\_VAL\_2\_20 rules of such appearances are allowed.

**TTK=:** This token value represents the **dwTrustTupleKeywords** field of the **FW\_RULE** structure. The TRUST\_TUPLE\_KEYWORD\_VAL grammar rule represents a flag in the **dwTrustTupleKeywords** field. If the "TTK=" token appears multiple times in the rule string, then all the respective TRUST\_TUPLE\_KEYWORD\_VAL rules of such appearances are allowed.

**LUAuth2\_24=:** This token value[<2>](#Appendix_A_2) represents the base64 encoded content of **wszLocalUserAuthorizationList** and it also adds the FW\_RULE\_FLAGS\_LUA\_CONDITIONAL\_ACE flag on the **wFlags** field of the FW\_RULE2\_24 structure ([MS-FASP] section 2.2.101). This token MUST appear only once in a rule string.

**NNm=:** This token value[<3>](#Appendix_A_3) represents the **OnNetworkNames** field of the FW\_RULE2\_24 structure ([MS-FASP] section 2.2.101). The STR\_ENC\_VAL grammar rule represents an encoded string that represents the contents of such field. This token MUST appear only once in a rule string.

**SecurityRealmId=**: This token[<4>](#Appendix_A_4) represents the **wszSecurityRealmId** field of the FW\_RULE2\_24 structure ([MS-FASP] section 2.2.101). The STR\_VAL grammar rule represents a Unicode string that represents the contents of the field. This token MUST appear only once in a rule string.

The "LPort=" token MUST appear only if a "Protocol=" token has appeared before it on the rule string AND the value of the "Protocol=" token is either 6 (for TCP) or 17 (for UDP). The same applies to the "RPort=", "LPort2\_10=" and "RPort2\_10=" tokens. The "ICMP4=" and "ICMP6=" tokens MUST appear only if the "Protocol=" token has appeared before it on the rule string and expressed a value of 1 for "ICMP4=" or of 58 for "ICMP6=". The "LPort=", "RPort=", "LPort2\_10=", and "RPort2\_10=" tokens cannot appear in a rule string where a "ICMP4=" or a "ICMP6=" token appears and vice versa.

The semantic checks described in [MS-FASP] section 2.2.36 are also applicable to the firewall rules described in this section after following the mapping in each of the preceding tokens.

#### Trust Tuple Keyword Rules

This grammar is used to identify trust tuple keywords.

1. TRUST\_TUPLE\_KEYWORD\_VAL = "Proximity" / "ProxSharing" / "WFDPrint" / "WFDDisplay" / "WFDDevices"

**Proximity:** This token represents the **FW\_TRUST\_TUPLE\_KEYWORD\_PROXIMITY** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.96. The remaining token values in this list can be found in the same section.

**ProxSharing:** This token represents the **FW\_TRUST\_TUPLE\_KEYWORD\_PROXIMITY\_SHARING** enumeration value.

**WFDPrint:** This token represents the **FW\_TRUST\_TUPLE\_KEYWORD\_WFD\_Print** enumeration value.[<5>](#Appendix_A_5)

**WFDDisplay:** This token represents the **FW\_TRUST\_TUPLE\_KEYWORD\_WFD\_Display** enumeration value.[<6>](#Appendix_A_6)

**WFDDevices:** This token represents the **FW\_TRUST\_TUPLE\_KEYWORD\_WFD\_Devices** enumeration value. [<7>](#Appendix_A_7)

### Per-Profile Policy Configuration Options

The Per-Profile Configuration Options are values that represent the enumeration values of the **FW\_PROFILE\_CONFIG** enumeration type as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37. If neither the Software\Policies\Microsoft\WindowsFirewall\PrivateProfile nor the Software\Policies\Microsoft\WindowsFirewall\PublicProfile key exists, then the settings under the Software\Policies\Microsoft\WindowsFirewall\StandardProfile key are applied to both public and private profiles. On the other hand, if either the Software\Policies\Microsoft\WindowsFirewall\PrivateProfile or the Software\Policies\Microsoft\WindowsFirewall\PublicProfile key exists then the settings under the Software\Policies\Microsoft\WindowsFirewall\StandardProfile key are ignored and the settings under the Software\Policies\Microsoft\WindowsFirewall\PrivateProfile key and the Software\Policies\Microsoft\WindowsFirewall\PublicProfile key apply to the networks identified by the corresponding **FW\_PROFILE\_TYPE\_PRIVATE** and the **FW\_PROFILE\_TYPE\_PUBLIC** enumeration values as defined in [MS-FASP] section 2.2.2.

#### Enable Firewall

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile, Software\Policies\Microsoft\WindowsFirewall\StandardProfile

Value: "EnableFirewall"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_ENABLE\_FW** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Disable Stealth Mode

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile, Software\Policies\Microsoft\WindowsFirewall\StandardProfile

Value: "DisableStealthMode"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DISABLE\_STEALTH\_MODE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Shield Up Mode

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile, Software\Policies\Microsoft\WindowsFirewall\StandardProfile

Value: "DoNotAllowExceptions"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_SHIELDED** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Disable Unicast Responses to Multicast and Broadcast Traffic

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile, Software\Policies\Microsoft\WindowsFirewall\StandardProfile

Value: "DisableUnicastResponsesToMulticastBroadcast"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DISABLE\_UNICAST\_RESPONSES\_TO\_MULTICAST\_BROADCAST** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Log Dropped Packets

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\StandardProfile\Logging

Value: "LogDroppedPackets"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_LOG\_DROPPED\_PACKETS** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Log Successful Connections

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\StandardProfile\Logging

Value: "LogSuccessfulConnections"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_LOG\_SUCCESS\_CONNECTIONS** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Log Ignored Rules

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging. (This setting MUST NOT be present on Software\Policies\Microsoft\WindowsFirewall\StandardProfile\Logging)

Value: "LogIgnoredRules"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_LOG\_IGNORED\_RULES** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Maximum Log File Size

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\StandardProfile\Logging

Value: "LogFileSize"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: A 32-bit value that represents a number.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_LOG\_MAX\_FILE\_SIZE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Log File Path

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging, Software\Policies\Microsoft\WindowsFirewall\StandardProfile\Logging

Value: "LogFilePath"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A Unicode string.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_LOG\_FILE\_PATH** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Disable Inbound Notifications

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile, Software\Policies\Microsoft\WindowsFirewall\StandardProfile

Value: "DisableNotifications"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DISABLE\_INBOUND\_NOTIFICATIONS** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Allow Authenticated Applications User Preference Merge

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AuthorizedApplications, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\AuthorizedApplications, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\AuthorizedApplications, Software\Policies\Microsoft\WindowsFirewall\StandardProfile\AuthorizedApplications

Value: "AllowUserPrefMerge"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_AUTH\_APPS\_ALLOW\_USER\_PREF\_MERGE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Allow Globally Open Ports User Preference Merge

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyOpenPorts, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\GloballyOpenPorts, Software\Policies\Microsoft\WindowsFirewall\PublicProfile\GloballyOpenPorts, Software\Policies\Microsoft\WindowsFirewall\StandardProfile\GloballyOpenPorts

Value: "AllowUserPrefMerge"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_GLOBAL\_PORTS\_ALLOW\_USER\_PREF\_MERGE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Allow Local Firewall Rule Policy Merge

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile. (This setting MUST NOT be present on Software\Policies\Microsoft\WindowsFirewall\StandardProfile)

Value: "AllowLocalPolicyMerge"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_ALLOW\_LOCAL\_POLICY\_MERGE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Allow Local IPsec Policy Merge

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile. This setting MUST NOT be present on Software\Policies\Microsoft\WindowsFirewall\StandardProfile.

Value: "AllowLocalIPsecPolicyMerge"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_ALLOW\_LOCAL\_IPSEC\_POLICY\_MERGE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Disabled Interfaces

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile. (This setting MUST NOT be present on Software\Policies\Microsoft\WindowsFirewall\StandardProfile)

Value: "DisabledInterfaces"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A Unicode string encoded with the following INTERFACES\_VAL grammar rule:

1. INTERFACES\_VAL = [ \*1INTF\_FIELD / INTF\_FIELD 1\*INTF\_FIELD\_SEQ ]
2. INTF\_FIELD = "{" GUID "}"
3. INTF\_FIELD\_SEQ = "," INTF\_FIELD

Where GUID is the string representation of the globally unique identifier, as defined in [[RFC4122]](http://go.microsoft.com/fwlink/?LinkId=90460) section 3, used to identify the interface on the client.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DISABLED\_INTERFACES** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Default Outbound Action

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile. (This setting MUST NOT be present on Software\Policies\Microsoft\WindowsFirewall\StandardProfile)

Value: "DefaultOutboundAction"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: 0x00000000 means allow traffic and 0x00000001 means block traffic.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DEFAULT\_OUTBOUND\_ACTION** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Default Inbound Action

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile. (This setting MUST NOT be present on Software\Policies\Microsoft\WindowsFirewall\StandardProfile)

Value: "DefaultInboundAction"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: 0x00000000 means allow traffic and 0x00000001 means block traffic.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DEFAULT\_INBOUND\_ACTION** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

#### Disable Stealth Mode for IPsec Secured Packets

Keys: Software\Policies\Microsoft\WindowsFirewall\DomainProfile, Software\Policies\Microsoft\WindowsFirewall\PrivateProfile, Software\Policies\Microsoft\WindowsFirewall\PublicProfile, Software\Policies\Microsoft\WindowsFirewall\StandardProfile)

Value: "DisableStealthModeIPsecSecuredPacketExemption"

Type: REG\_DWORD.

Size: Equal to size of the **Data** field.

Data: An unsigned, 32-bit integer value for which possible values are 0x00000000 or 0x00000001.

This value represents the contents assigned to the configuration option represented by the **FW\_PROFILE\_CONFIG\_DISABLE\_STEALTH\_MODE\_IPSEC\_SECURED\_PACKET\_EXEMPTION** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.37.

### Authentication Sets

The Authentication Set represents **FW\_AUTH\_SET** structures (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.64). These objects are encoded under the Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets key or the Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets key. Authentication sets stored on the Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets key represent those that have a value of FW\_IPSEC\_PHASE\_1 (as defined in [MS-FASP] section 2.2.49) in the **IpSecPhase** field of the **FW\_AUTH\_SET** structure.

Authentication sets stored on the Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets key represent those that have a value of FW\_IPSEC\_PHASE\_2 (as defined in [MS-FASP] section 2.2.49) in the **IpSecPhase** field of the **FW\_AUTH\_SET** structure. Each key under these two authentication set keys represents a unique authentication set object, and the name of each key represents the value of the **wszSetId** field of the **FW\_AUTH\_SET** structure. Registry keys and values under each of these authentication set keys are described in the following sections. The semantic checks specified in [MS-FASP] section 2.2.64 are also applicable to the authentication sets described in this section after following the mapping of the following registry values and tokens.

The Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet\{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE3} and the Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet\{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE4} keys MUST NOT exist. Hence phase 1 set with a set Id equal to {E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE3} and phase 2 sets with a set id equal to {E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE4} MUST rename their Ids when encoded through this protocol. The original set id value of this set MUST be written to the following two corresponding registry values, which clients of this protocol will use to rename the sets back:

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet

Value: "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE3}"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value encodes a Unicode string containing the set id value to which a phase 1 set with an original set id of "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE3}" had to rename itself.

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet

Value: "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE4}"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value encodes a Unicode string containing the set id value to which a phase 2 set with an original set id of "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE4}" had to rename itself to.

#### Version

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet\<wszSetId>.

Value: "Version"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value encodes a Unicode string using the VERSION grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the values of the **wSchemaVersion** field of the **FW\_AUTH\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.64.

#### Name

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet\<wszSetId>,

Value: "Name"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszName** field of the **FW\_AUTH\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.64.

#### Description

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet\<wszSetId>,

Value: "Description"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszDescription** field of the **FW\_AUTH\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.64.

#### EmbeddedContext

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet\<wszSetId>,

Value: "EmbeddedContext"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszEmbeddedContext** field of the **FW\_AUTH\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.64.

#### Suite Keys

Each authentication set may contain a list of suites corresponding to the authentication proposals that will be negotiated. These suites can be stored in Software\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or in Software\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>, where the SuiteIndex is a 4 digit decimal value encoded as a string.

The suite keys represent the **pSuites** array field of the **FW\_AUTH\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.64.

The suites for phase1 authentication sets differ from those of phase 2 authentication sets. The following sections describe how these suites are encoded. The semantic checks described in [MS-FASP] section 2.2.62 are also applicable to the authentication suites described in this section after following the mapping of the following registry values and tokens.

#### Phase 1 and Phase 2 Auth Suite Methods

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>,

Value: "Method"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that uses the following grammar rules to encode an authentication method.

1. PHASE1\_AUTH\_METHOD\_VAL = "Anonymous" / "MachineKerb" / "MachineCert"
2. PHASE1\_AUTH\_METHOD\_VAL =/ "MachineSHKey" / "MachineNtlm"
3. PHASE2\_AUTH\_METHOD\_VAL = "Anonymous" / "MachineCert" / "UserKerb"
4. PHASE2\_AUTH\_METHOD\_VAL =/ "UserCert" / "UserNtlm"

**Anonymous** - this token represents the **FW\_AUTH\_METHOD\_ANONYMOUS** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.59. The remaining tokens can be found in the same Protocol specification section.

**MachineKerb** - this token represents the **FW\_AUTH\_METHOD\_MACHINE\_KERB** enumeration value.

**MachineCert** - this token represents the **FW\_AUTH\_METHOD\_MACHINE\_CERT** enumeration value.

**MachineSHKey** - this token represents the **FW\_AUTH\_METHOD\_MACHINE\_SHKEY** enumeration value.

**MachineNtlm** - this token represents the **FW\_AUTH\_METHOD\_MACHINE\_NTLM** enumeration value.

**UserKerb** - this token represents the **FW\_AUTH\_METHOD\_USER\_KERB** enumeration value.

**UserCert** - this token represents the **FW\_AUTH\_METHOD\_USER\_CERT** enumeration value.

**UserNtlm** - this token represents the **FW\_AUTH\_METHOD\_USER\_NTLM** enumeration value.

This value represents the **Method** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP] section 2.2.62. If the value is read from a phase 1 key then the PHASE1\_AUTH\_METHOD\_VAL grammar rule MUST be used. If the value is read from a phase 2 key then the PHASE2\_AUTH\_METHOD\_VAL grammar rule MUST be used.

#### Phase 1 and Phase 2 Auth Suite Certificate Authority Names

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>,

Value: "CAName"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszCAName** field of the **FW\_AUTH\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.62. If this value appears in the Suite Key, then the SHKey value defined in the next section MUST NOT appear.

#### Phase 1 Auth Suite Preshared Key

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>.

Value: "SHKey"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszSHKey** field of the **FW\_AUTH\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.62.

#### Phase 1 and Phase 2 Auth Suite Certificate Account Mapping

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>,

Value: "CertAccountMapping"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a Boolean value using the BOOL\_VAL grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the FW\_AUTH\_SUITE\_FLAGS\_PERFORM\_CERT\_ACCOUNT\_MAPPING flag (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.60) of the **wFlags** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP] section 2.2.62. If this value appears under the suite key, then the SHKey value defined in section 2.2.4.5.3 MUST NOT appear.

#### Phase 1 Auth Suite Exclude CA Name

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>.

Value: "ExcludeCAName"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a Boolean value using the BOOL\_VAL grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the FW\_AUTH\_SUITE\_FLAGS\_CERT\_EXCLUDE\_CA\_NAME flag (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.60) of the **wFlags** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP] section 2.2.62. If this value appears in the Suite Key, then the SHKey value defined in section 2.2.4.5.3 MUST NOT appear.

#### Phase 1 and Phase 2 Auth Suite Health Cert

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>,

Value: "HealthCert"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a Boolean value using the BOOL\_VAL grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the FW\_AUTH\_SUITE\_FLAGS\_HEALTH\_CERT flag (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.60) of the **wFlags** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP] section 2.2.62. If this value appears in the Suite Key, then the SHKey value defined in section 2.2.4.5.3 MUST NOT appear.

#### Phase 1 and Phase 2 Auth Suite Skip Version

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>,

Value: "SkipVersion"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a schema version using the VERSION grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

If the Firewall and Advanced Security component parsing this suite key has a schema version smaller than or equal to the version value in this value, then it MUST skip this suite altogether.

#### Phase 1 and Phase 2 Auth Suite Other Certificate Signing

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>,

Value: "OtherCertSigning"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string that uses the following grammar rules to encode certificate signing algorithms.

1. OTHER\_CERT\_SIGNING\_VAL = "ECDSA256" / "ECDSA384"

**ECDSA256**- this token represents the **FW\_AUTH\_SUITE\_FLAGS\_CERT\_SIGNING\_ECDSA256** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.60.

**ECDSA384**- this token represents the **FW\_AUTH\_SUITE\_FLAGS\_CERT\_SIGNING\_ECDSA384** enumeration value as defined in [MS-FASP] section 2.2.60.

This value represents the FW\_AUTH\_SUITE\_FLAGS\_CERT\_SIGNING\_ECDSA256 and the FW\_AUTH\_SUITE\_FLAGS\_CERT\_SIGNING\_ECDSA384 flags of the **wFlags** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP] section 2.2.62. This value MUST be present only if the schema version of the authentication set, as defined in section [2.2.4.1](#Section_e017c13fa8ef49348356486b6a214a0a), contains a version of 0x0201 or higher. Whenever this value is found in the suite key, a SkipVersion value MUST also be present, and MUST contain a version of 0x0200.

#### Phase 1 and Phase 2 Auth Suite Intermediate CA

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>, or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>.

Value: "IntermediateCA"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a Boolean value using the BOOL\_VAL grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the FW\_AUTH\_SUITE\_FLAGS\_INTERMEDIATE\_CA flag (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.60) of the **wFlags** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP] section 2.2.62. This value MUST be present only if the schema version of the authentication set as defined in section [2.2.4.1](#Section_e017c13fa8ef49348356486b6a214a0a) contains a version of 0x020A or higher. Whenever this value is found in the suite key, a SkipVersion value MUST also be present, and MUST contain a version of 0x0208.

#### Certificate Criteria Type Tokens

This grammar is used to identify the types of certificate criteria.

1. CRITERIA\_TYPE\_VAL = "Both" / "Select" / "Validate"

**Both**: This token value represents the FW\_CERT\_CRITERIA\_TYPE\_BOTH enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.55. The remaining token values in this list can be found in the same Protocol specification section.

**Select**: This token value represents the FW\_CERT\_CRITERIA\_TYPE\_SELECTION enumeration value.Validate: This token value represents the FW\_CERT\_CRITERIA\_TYPE\_VALIDATION enumeration value.

#### Certificate Criteria Name Type Tokens

This grammar is used to identify the type of a name used in certificate criteria.

1. CRITERIA\_NAME\_TYPE\_VAL = "DNS" / "UPN" / "RFC822" / "CN" / "OU" / "O" / "DC"

**DNS**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_DNS enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.56. The remaining token values in this list can be found in the same Protocol specification section.

**UPN**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_UPN enumeration value.

**RFC822**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_RFC822 enumeration value.

**CN**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_CN enumeration value.

**OU**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_OU enumeration value.

**O**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_O enumeration value.

**DC**: This token value represents the FW\_CERT\_CRITERIA\_NAME\_DC enumeration value.

#### Phase 1 and Phase 2 Auth Suite Certificate Criteria

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex> or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>

Value: "CertCriteria"

Type: REG\_SZ.Size: Equal to size of the Data field.

Data: This value is a Unicode string that uses the following grammar rules to encode certificate criteria.

1. CERT\_CRITERIA = "v" VERSION "|" 1\*FIELD
2. VERSION = MAJOR\_VER "." MINOR\_VER
3. MAJOR\_VER = 1\*3DIGIT
4. MINOR\_VER = 1\*3DIGIT
5. FIELD = TYPE\_VALUE "|"
6. TYPE\_VALUE = "CriteriaType=" CRITERIA\_TYPE\_VAL
7. TYPE\_VALUE =/ "NameType=" CRITERIA\_NAME\_TYPE\_VAL
8. TYPE\_VALUE =/ "Name=" STR\_VAL
9. TYPE\_VALUE =/ "Eku=" STR\_VAL
10. TYPE\_VALUE =/ "Hash=" STR\_VAL
11. TYPE\_VALUE =/ "FollowRenewal=" BOOL\_VAL

This value represents the criteria for selecting and validating certificates as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.58.

**MAJOR\_VER**: This grammar rule describes a decimal number that represents the 8 high-order bits of the **wSchemaVersion** field of the **FW\_CERT\_CRITERIA** structure as defined in [MS-FASP] section 2.2.58. Because of this, the decimal value of this number MUST NOT be greater than 255. The following grammar rules can also be found in the previously mentioned [MS-FASP] section 2.2.58.

**MINOR\_VER**: This grammar rule describes a decimal number that represents the 8 low-order bits of the **wSchemaVersion** field of the **FW\_CERT\_CRITERIA** structure. Because of this, the decimal value of this number MUST NOT be greater than 255.

**VERSION**: This grammar rule describes a decimal value whose 8 low-order bits are those described in the MINOR\_VER grammar rule, and whose 8 high-order bits are those described in the MAJOR\_VER grammar rule.

**CriteriaType=**: This token value represents the **CertCriteriaType** field of the **FW\_CERT\_CRITERIA** structure. The CRITERIA\_TYPE\_VAL grammar rule represents the value contents of this field. This token MUST appear only once in a certificate criteria string. The remaining token values in this list can be found in the same Protocol specification section except where noted.

**NameType=**: This token value represents the **NameType** field of the **FW\_CERT\_CRITERIA** structure. The CRITERIA\_NAME\_TYPE\_VAL grammar rule represents the value contents of this field. This token MUST appear only once in a certificate criteria string.

**Name=**: This token value represents the **wszName** field of the **FW\_CERT\_CRITERIA** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of this field. This token MUST appear only once in a certificate criteria string.

**Eku=**: This token value represents an entry in the array stored in the **Eku** and **ppEku** fields of the **FW\_CERT\_CRITERIA** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such entry. If the "Eku=" token appears multiple times in the certificate criteria string, then all the respective STR\_VAL rules of such appearances are allowed.

**Hash=**: This token value represents the **wszHash** field of the **FW\_CERT\_CRITERIA** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of this field. This token MUST appear only once in a certificate criteria string.

**FollowRenewal=**: This token represents the FW\_AUTH\_CERT\_CRITERIA\_FLAGS\_FOLLOW\_RENEWAL flag (as defined in [MS-FASP] section 2.2.57) of the **wFlags** field of the **FW\_CERT\_CRITERIA** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section [2.2.2.14](#Section_2bdb10546ea04b088e51513f7a758011). If the "FollowRenewal=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear only once in a certificate criteria string.

#### Phase 1 and Phase 2 Auth Suite Allow Kerberos Proxy

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex> or Software\Policies\...\Phase2AuthenticationSet\<wszSetId>\<SuiteIndex>

Value: "AllowProxy"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A Unicode string that encodes a Boolean value using the BOOL\_VAL grammar rule defined in section [2.2.2.14](#Section_2bdb10546ea04b088e51513f7a758011).

This value represents the FW\_AUTH\_SUITE\_FLAGS\_ALLOW\_PROXY flag (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.60) of the **wFlags** field of the **FW\_AUTH\_SUITE** structure as defined in [MS-FASP]section 2.2.62.

#### Phase 1 and Phase 2 Auth Suite Kerberos Proxy Server

Keys: Software\Policies\...\Phase1AuthenticationSet\<wszSetId>\<SuiteIndex>

Value: "ProxyServer"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: A Unicode string.

This value represents the **wszProxyServer** field of the **FW\_AUTH\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.62.

### Cryptographic Sets

The Cryptographic Sets represents **FW\_ CRYPTO\_SET** structures as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73. These objects are encoded under the Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet or the Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets key. Cryptographic sets stored on the Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet key represent those who have a value of FW\_IPSEC\_PHASE\_1 (as defined in [MS-FASP] section 2.2.49) in the **IpSecPhase** field of the **FW\_CRYPTO\_SET** structure as defined in [MS-FASP] section 2.2.73). Cryptographic sets stored on the Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets key represent those who have a value of FW\_IPSEC\_PHASE\_2 (as defined in [MS-FASP] section 2.2.49) in the **IpSecPhase** field of the **FW\_CRYTO\_SET** structure as defined in [MS-FASP] section 2.2.73). Every key under each of these two cryptographic sets keys represents a unique cryptographic set object, and the name of each key represents the value of the **wszSetId** field of the **FW\_CRYPTO\_SET** structure as defined in [MS-FASP] section 2.2.73. The semantic checks described in [MS-FASP] section 2.2.73 are also applicable to the cryptographic sets described in this section after the mapping of the registry values and tokens.

The Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE1} and the Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE2} keys MUST NOT exist. Hence phase 1 sets with a set Id equal to {E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE1} and phase 2 sets with a set id equal to {E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE2} MUST rename their Ids when encoded through this protocol. The original set id value of this set MUST be written to the following two corresponding registry values, which clients of this protocol will use to rename the sets back:

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet

Value: "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE1}"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value encodes a Unicode string containing the set id value to which a phase 1 set with an original set id of "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE1}" had to rename itself to.

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets

Value: "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE2}"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value encodes a Unicode string containing the set id value to which a phase 2 set with an original set id of "{E5A5D32A-4BCE-4E4D-B07F-4AB1BA7E5FE2}" had to rename itself to.

#### Version

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>.

Value: "Version"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value encodes a Unicode string using the VERSION grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the values of the **wSchemaVersion** field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

#### Name

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>.

Value: "Name"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszName** field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

#### Description

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>.

Value: "Description"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszDescription** field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

#### EmbeddedContext

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>, or Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>.

Value: "EmbeddedContext"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string.

This value represents the **wszEmbeddedContext** field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

#### Phase 1 - Do Not Skip Deffie Hellman

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>.

Value: "DoNotSkipDH"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a Boolean value using the BOOL\_VAL grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

This value represents the **FW\_PHASE1\_CRYPTO\_FLAGS\_DO\_NOT\_SKIP\_DH** enumeration flag (as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.71) of the **wFlags** field of the **FW\_CRYPTO\_SET** structure as defined in [MS-FASP] section 2.2.73.

#### Phase 1 - Time Out in Minutes

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>.

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string that encodes a decimal number using the following grammar rule:

1. TIMEOUT\_MIN\_VAL = 1\*8DIGIT

**TIMEOUT\_MIN\_VAL** = the decimal value of this grammar rule MUST NOT be bigger than the decimal value of 71582788.

This value represents the **dwTimeoutMinutes** field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

#### Phase 1 - Time Out in Sessions

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>.

Value: "TimeOutSessions"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string that encodes a decimal number using the following grammar rule:

1. TIMEOUT\_SESS\_VAL = 1\*10DIGIT

**TIMEOUT\_SESS\_VAL:** The decimal value of this grammar rule MUST NOT be bigger than the decimal value of 2147483647.

This value represents the **dwTimeoutSessions** field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

#### Phase 2 - Perfect Forward Secrecy

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>.

Value: "PFS"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. PFS\_VAL = "Disable" / "EnableDHFromPhase1" / "ReKeyDH1" / "ReKeyDH2" / "ReKeyDH2048"
2. PFS\_VAL =/ "ReKeyECDH256" / "ReKeyECDH384"

**Disable:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DISABLE** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.72. The remaining token values in this list can be found in the same Protocol specification section.

**EnableDHFromPhase1:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_PHASE1** enumeration value.

**ReKeyDH1:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH1** enumeration value.

**ReKeyDH2:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH2** enumeration value.

**ReKeyDH2048:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH2048** enumeration value.

**ReKeyECDH256:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_ECDH256** enumeration value.

**ReKeyECDH384:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_ECDH384** enumeration value.

This value represents the **Pfs** field of the **FW\_CRYPTO\_SET** structure as defined in [MS-FASP] section 2.2.73.

#### Phase 1 - Suite Keys

Each authentication set can contain a list of suites corresponding to the cryptographic proposals that will be negotiated. These suites are stored in Software\Policies\Microsoft\WindowsFirewall\Phase1CryptoSet\<wszSetId>\<SuiteIndex> where the SuiteIndex is a 4 digit decimal value encoded as a string.

The suite keys represent the pPhase1Suites array field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

The suites for phase 1 cryptographic sets differ from those of phase 2 authentication sets. The following sections describe how these phase 1 cryptographic suites are encoded. The semantic checks described in [MS-FASP] section 2.2.69 are also applicable to the cryptographic phase 1 suites described in this section after following the mapping of the registry values and tokens.

#### Phase 1 Suite - Key Exchange Algorithm

Keys: Software\Policies\...\Phase1CryptoSet\<wszSetId>\<SuiteIndex>.

Value: "KeyExchange"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. KEY\_EXCHANGE\_VAL = "DH1" / "DH2" / "DH2048" / "ECDH-256" / "ECDH-384"

**DH1:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH1** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.65. The remaining token values in this list can be found in the same Protocol specification section except where noted.

**DH2:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH2** enumeration value.

**DH2048:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH2048** enumeration value.

**ECDH-256:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_ECDH256** enumeration value.

**ECDH-384:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_ECDH384** enumeration value.

This value represents the **KeyExchange** field of the **FW\_PHASE1\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.69.

#### Phase 1 Suite - Encryption Algorithm

Keys: Software\Policies\...\Phase1CryptoSet\<wszSetId>\<SuiteIndex>.

Value: "Encryption"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. ENCRYPTION\_VAL = "DES" / "3DES" / "AES-128" / "AES-192" / "AES-256"

**DES** = this token represents the **FW\_CRYPTO\_ENCRYPTION\_DES** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.66. The remaining token values in this list can be found in the same Protocol specification section except where noted.

**3DES:** This token represents the **FW\_CRYPTO\_ ENCRYPTION\_3DES** enumeration value.

**AES-128:** This token represents the **FW\_CRYPTO\_ ENCRYPTION\_AES128** enumeration value.

**AES-192:** This token represents the **FW\_CRYPTO\_ ENCRYPTION\_AES192** enumeration value.

**AES-256:** This token represents the **FW\_CRYPTO\_ ENCRYPTION\_AES256** enumeration value.

This value represents the **Encryption** field of the **FW\_PHASE1\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.69.

#### Phase 1 Suite - Hash Algorithm

Keys: Software\Policies\...\Phase1CryptoSet\<wszSetId>\<SuiteIndex>.

Value: "Hash"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. HASH\_VAL = "MD5" / "SHA1"

**MD5:** This token represents the **FW\_CRYPTO\_HASH\_MD5** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.67.

**SHA1:** This token represents the **FW\_CRYPTO\_ HASH\_SHA1** enumeration value as defined in [MS-FASP] section 2.2.67.

This value represents the **Hash** field of the **FW\_PHASE1\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.69.

#### Phase 1 Suite Skip Version

Keys: Software\Policies\...\Phase1CryptoSet\<wszSetId>\<SuiteIndex>.

Value: "SkipVersion"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a schema version using the VERSION grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

If the Firewall and Advanced Security component parsing this suite key has a schema version smaller than or equal to the version value in this value, then it MUST skip this suite altogether.

#### Phase 1 Suite - 2.1 Hash Algorithm

Keys: Software\Policies\...\Phase1CryptoSet\<wszSetId>\<SuiteIndex>.

Value: "2\_1Hash"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. HASH2\_1\_VAL = "SHA256" / "SHA384"

**SHA256:** This token represents the **FW\_CRYPTO\_HASH\_SHA256** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.67.

**SHA384:** This token represents the **FW\_CRYPTO\_ HASH\_SHA384** enumeration value as defined in [MS-FASP] section 2.2.67.

This value represents the **Hash** field of the **FW\_PHASE1\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.69. If this value appears in the suite key, then a SkipVersion value with a version of 0x0200 or higher MUST be present.

#### Phase 1 Suite - 2.16 Key Exchange Algorithm

Keys: Software\Policies\...\Phase1CryptoSet\<wszSetId>\<SuiteIndex>.

Value: "2\_16KeyExchange"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: This value is a Unicode string encoded using the following grammar rule:

1. KEY\_EXCHANGE\_VAL = "DH1" / "DH2" / "DH2048" / "ECDH-256" / "ECDH-384" / "DH24"

**DH1:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH1** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.65. The remaining token values in this list can be found in the same Protocol specification section except where noted.

**DH2:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH2** enumeration value.

**DH2048:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH2048** enumeration value.

**ECDH-256:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_ECDH256** enumeration value.

**ECDH-384:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_ECDH384** enumeration value.

**DH24:** This token represents the **FW\_CRYPTO\_KEY\_EXCHANGE\_DH24** enumeration value.

This value represents the **KeyExchange** field of the **FW\_PHASE1\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.69.

#### Phase 2 - Suite Keys

Each authentication set could contain a list of suites which express cryptographic proposals that will be negotiated. These suites can be stored in Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>\<SuiteIndex> where the SuiteIndex is a 4 digit decimal value encoded as a string.

The suite keys represent the **pPhase2Suites** array field of the **FW\_CRYPTO\_SET** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.73.

The suites for phase 2 cryptographic sets differ from those of phase 1 authentication sets. The following sections describe how these phase 2 cryptographic suites are encoded. The semantic checks described in [MS-FASP] section 2.2.70 are also applicable to the cryptographic phase 2 suites described in this section after following the mapping of the registry values and tokens.

#### Phase 2 Suite - Protocol

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "Protocol"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. PROTOCOL\_VAL = "AH" / "ESP" / "AH&ESP"

**AH:** This token represents the **FW\_CRYPTO\_PROTOCOL\_AH** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.68. The remaining token values in this list can be found in the same Protocol specification section.

**ESP:** This token represents the **FW\_CRYPTO\_PROTOCOL\_ESP** enumeration value.

**AH&ESP:** This token represents the **FW\_CRYPTO\_PROTOCOL\_BOTH** enumeration value.

This value represents the **Protocol** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.70.

#### Phase 2 Suite - Encryption Algorithm

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "Encryption"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the ENCRYPTION\_VAL grammar rule defined in section [2.2.5.11](#Section_fd1455f1f8774460ae4eb4342944e065).

This value represents the **Encryption** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.70.

#### Phase 2 Suite - AH Protocol Hash Algorithm

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "AhHash"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the HASH\_VAL grammar rule defined in section [2.2.5.12](#Section_e07275e9e351491b803dc2c1fb544ddd).

This value represents the **AhHash** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.70.

#### Phase 2 Suite - ESP Protocol Hash Algorithm

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "EspHash"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the HASH\_VAL grammar rule defined in section [2.2.5.12](#Section_e07275e9e351491b803dc2c1fb544ddd).

This value represents the **EspHash** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.70.

#### Phase 2 Suite - Time Out in Minutes

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string that encodes a decimal number using the following grammar rule:

1. PHASE2\_SUITE\_TIMEOUT\_MIN\_VAL = 1\*4DIGIT

**PHASE2\_SUITE\_TIMEOUT\_MIN\_VAL** = the decimal value of this grammar rule MUST NOT be bigger than the decimal value of 2880.

This value represents the **dwTimeoutMinutes** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.70.

#### Phase 2 Suite - Time Out in Kilobytes

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string that encodes a decimal number using the following grammar rule:

1. PHASE2\_SUITE\_TIMEOUT\_KBYTES\_VAL = 1\*10DIGIT

**PHASE2\_SUITE\_TIMEOUT\_MIN\_VAL** = the decimal value of this grammar rule MUST NOT be bigger than the decimal value of 2147483647.

This value represents the **dwTimeoutKBytes** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.70.

#### Phase 2 Suite - Skip Version

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "SkipVersion"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: a Unicode string that encodes a schema version using the VERSION grammar rule defined in section [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16).

If the Firewall and Advanced Security component parsing this suite key has a schema version smaller than or equal to the version value in this value, then it MUST skip this suite altogether.

#### Phase 2 Suite - 2.1 Encryption Algorithm

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "2\_1Encryption"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. ENCRYPTION2\_1\_VAL = "AES-GCM128" / "AES-GCM192" / "AES-GCM256"

**AES-GCM128:** This token represents the **FW\_CRYPTO\_ENCRYPTION\_AES\_GCM128** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.66.

**AES-GCM192:** This token represents the **FW\_CRYPTO\_ENCRYPTION\_AES\_GCM192** enumeration value as defined in [MS-FASP] section 2.2.66.

**AES-GCM256:** This token represents the **FW\_CRYPTO\_ENCRYPTION\_AES\_GCM256** enumeration value as defined in [MS-FASP] section 2.2.66.

This value represents the **Encryption** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.70. If this value appears in the suite key, then a SkipVersion value with a version of 0x0200 MUST be present.

#### Phase 2 Suite - 2.1 AH Hash Algorithm

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "2\_1AhHash"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. AH\_ESP\_HASH2\_1\_VAL = "SHA256" / "AES-GCM128" / "AES-GCM192" / "AES-GCM256"

**SHA256:** This token represents the **FW\_CRYPTO\_HASH\_SHA256** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.67. The remaining token values in this list can be found in the same Protocol specification section.

**AES-GCM128:** This token represents the **FW\_CRYPTO\_HASH\_AES\_GMAC128** enumeration value.

**AES-GCM192:** This token represents the **FW\_CRYPTO\_HASH\_AES\_GMAC192** enumeration value.

**AES-GCM256:** This token represents the **FW\_CRYPTO\_HASH\_AES\_GMAC256** enumeration value.

This value represents the **AhHash** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.70. If this value appears in the suite key, then a SkipVersion value with a version of 0x0200 MUST be present.

#### Phase 2 Suite - 2.1 ESP Hash Algorithm

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "2\_1EspHash"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the AH\_ESP\_HASH2\_1\_VAL grammar rule defined in section [2.2.5.25](#Section_deb0f275e34f4ac593870e588f90d084).

This value represents the **EspHash** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.70. If this value appears in the suite key, then a SkipVersion value with a version of 0x0200 MUST be present.

#### Phase 2 Suite - 2.9 Protocol

Keys: Software\Policies\...\Phase2CryptoSets\<wszSetId>\<SuiteIndex>.

Value: "2\_9Protocol"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: this value is a Unicode string encoded using the following grammar rule:

1. PROTOCOL2\_9\_VAL = "AUTH\_NO\_ENCAP"

**AUTH\_NO\_ENCAP:** This token represents the **FW\_CRYPTO\_PROTOCOL\_AUTH\_NO\_ENCAP** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.68.

This value represents the **Protocol** field of the **FW\_PHASE2\_CRYPTO\_SUITE** structure as defined in [MS-FASP] section 2.2.70. If this value appears in the suite key, then a SkipVersion value with a version of 0x0209 MUST be present.

#### Phase 2 - 2.16 Perfect Forward Secrecy

Keys: Software\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\<wszSetId>.

Value: "2\_16PFS"

Type: REG\_SZ.

Size: Equal to size of the **Data** field.

Data: This value is a Unicode string encoded using the following grammar rule:

1. PFS\_VAL = "Disable" / "EnableDHFromPhase1" / "ReKeyDH1" / "ReKeyDH2" / "ReKeyDH2048"
2. PFS\_VAL =/ "ReKeyECDH256" / "ReKeyECDH384" / "ReKeyDH24"

**Disable:** This token represents the FW\_PHASE2\_CRYPTO\_PFS\_DISABLE enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.72. The remaining token values in this list can be found in the same protocol specification section.

**EnableDHFromPhase1:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_PHASE1** enumeration value.

**ReKeyDH1:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH1** enumeration value.

**ReKeyDH2:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH2** enumeration value.

**ReKeyDH2048:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH2048** enumeration value.

**ReKeyECDH256:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_ECDH256** enumeration value.

**ReKeyECDH384:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_ECDH384** enumeration value.

**ReKeyDH24:** This token represents the **FW\_PHASE2\_CRYPTO\_PFS\_DH24** enumeration value.

This value represents the Pfs field of the **FW\_CRYPTO\_SET** structure as defined in [MS-FASP] section 2.2.73.

### Connection Security Rule Messages

This section defines the grammars used to encode different portions of the Connection Security rules.

#### Connection Security Action Tokens

This grammar is used to identify the actions available for firewall rules.

1. CS\_ACTION\_VAL = "SecureServer" / "Boundary" / "Secure" / "DoNotSecure"

**SecureServer:** This token value represents the **FW\_CS\_RULE\_ACTION\_SECURE\_SERVER** enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.51. The remaining token values in this list can be found in the same Protocol specification section.

**Boundary:** This token value represents the **FW\_CS\_RULE\_ACTION\_BOUNDARY** enumeration value.

**Secure:** This token value represents the **FW\_CS\_RULE\_ACTION\_SECURE** enumeration value.

**DoNotSecure:** This token value represents the **FW\_CS\_RULE\_ACTION\_DO\_NOT\_SECURE** enumeration value.

#### Connection Security Rule and the Connection Security Rule Grammar Rule

Connection security rules are stored under the Software\Policies\Microsoft\WindowsFirewall\ConSecRules key.

Each value under the key is a connection security rule. The type of the value MUST be REG\_SZ. The data of each value is a string that can be parsed by the following grammar. This grammar represents a connection security rule as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.54, except for the **wszRuleId** field of the **FW\_CS\_RULE** structure which is instead represented by the name of the registry value.

1. CSRULE = "v" VERSION "|" 1\*FIELD
2. FIELD = TYPE\_VALUE "|"
3. TYPE\_VALUE = "Action=" CS\_ACTION\_VAL
4. TYPE\_VALUE =/ "Profile=" PROFILE\_VAL
5. TYPE\_VALUE =/ "Protocol=" 1\*3DIGIT ; protocol is maximum 3 digits (255)
6. TYPE\_VALUE =/ "EP1Port=" PORT\_VAL
7. TYPE\_VALUE =/ "EP2Port=" PORT\_VAL
8. TYPE\_VALUE =/ "EP1Port2\_10=" PORT\_RANGE\_VAL
9. TYPE\_VALUE =/ "EP2Port2\_10=" PORT\_RANGE\_VAL
10. TYPE\_VALUE =/ "IF=" IF\_VAL
11. TYPE\_VALUE =/ "IFType=" IFTYPE\_VAL
12. TYPE\_VALUE =/ "Auth1Set=" STR\_VAL
13. TYPE\_VALUE =/ "Auth2Set=" STR\_VAL
14. TYPE\_VALUE =/ "Crypto2Set=" STR\_VAL
15. TYPE\_VALUE =/ "EP1\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
16. TYPE\_VALUE =/ "EP2\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
17. TYPE\_VALUE =/ "EP1\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
18. TYPE\_VALUE =/ "EP2\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
19. TYPE\_VALUE =/ "Name=" STR\_VAL
20. TYPE\_VALUE =/ "Desc=" STR\_VAL
21. TYPE\_VALUE =/ "EmbedCtxt=" STR\_VAL
22. TYPE\_VALUE =/ "Active=" BOOL\_VAL
23. TYPE\_VALUE =/ "Platform=" PLATFORM\_VAL
24. TYPE\_VALUE =/ "SkipVer=" VERSION
25. TYPE\_VALUE =/ "Platform2=" PLATFORM\_OP\_VAL
26. TYPE\_VALUE =/ "SecureInClearOut=" BOOL\_VAL
27. TYPE\_VALUE =/ "ByPassTunnel=" BOOL\_VAL
28. TYPE\_VALUE =/ "Authz=" BOOL\_VAL
29. TYPE\_VALUE =/ "RTunnel4=" ADDRV4
30. TYPE\_VALUE =/ "RTunnel6=" ADDRV6
31. TYPE\_VALUE =/ "LTunnel4=" ADDRV4
32. TYPE\_VALUE =/ "LTunnel6=" ADDRV6
33. TYPE\_VALUE =/ "RTunnel4\_2=" ADDRV4
34. TYPE\_VALUE =/ "RTunnel6\_2=" ADDRV6
35. TYPE\_VALUE =/ "LTunnel4\_2=" ADDRV4
36. TYPE\_VALUE =/ "LTunnel6\_2=" ADDRV6
37. TYPE\_VALUE =/ "RTunnelFqdn=" STR\_VAL
38. TYPE\_VALUE =/ "RTunEndpts4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
39. TYPE\_VALUE =/ "RTunEndpts6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
40. TYPE\_VALUE =/ "KeyMod=" KEY\_MOD\_VAL
41. TYPE\_VALUE =/ "KeyManagerDictate=" BOOL\_VAL
42. TYPE\_VALUE =/ "KeyManagerNotify=" BOOL\_VAL
43. TYPE\_VALUE =/ "FwdLifetime=" 1\*10DIGIT
44. TYPE\_VALUE =/ "TransportMachineAuthzSDDL=" STR\_VAL
45. TYPE\_VALUE =/ "TransportUserAuthzSDDL=" STR\_VAL
46. TYPE\_VALUE =/ "SecurityRealmEnabled=" BOOL\_VAL
47. STR\_VAL = 1\*ALPHANUM
48. BOOL\_VAL = "TRUE" / "FALSE"

**Action=:** This token value represents the **Action** field of the **FW\_CS\_RULE** structure as defined in [MS-FASP] section 2.2.54. The CS\_ACTION\_VAL grammar rule represents the value contents of such field. This token MUST appear at most once in a rule string. The remaining token values in this list can be found in the same Protocol specification section except where noted.

**Profile=:** This token value represents the **dwProfiles** field of the **FW\_CS\_RULE** structure. The PROFILE\_VAL grammar rule represents a value content of such field. If this token appears several times in a CSRULE grammar rule, then all the contents represented by the PROFILE\_VAL rule appearing next to them are included. If the "Profile=" token never appears in the rule string, then it represents a value of FW\_PROFILE\_TYPE\_ALL as defined in [MS-FASP] section 2.2.2.

**Protocol=:** This token value represents the **wIpProtocol** field of the **FW\_CS\_RULE** structure. The 1\*3DIGIT grammar rule represents a value content of such field. Such value MUST NOT be greater than 255. The "Protocol" token MUST appear at most once in a CSRULE grammar rule. If a "Protocol" token does not appear in the rule string, then the meaning is the same as a value of 256 in the **wIpProtocol** field in [MS-FASP] section 2.2.54.

**EP1Port=:** This token value represents the **Endpoint1Ports** field of the **FW\_CS\_RULE** structure. As such defined **Endpoint1Ports** is of type **FW\_PORTS**, which contains a **Ports** field of type **FW\_PORT\_RANGE\_LIST**, which also contains a **pPorts** array of type **FW\_PORT\_RANGE**. The PORT\_VAL grammar rule represents an entry in the **pPorts** field. If the "EP1Port" token appears multiple times in the rule string, then all the respective PORT\_VAL rules of such appearances are allowed.

**EP1Port2\_10=:** This token value represents the **Endpoint1Ports** field of the **FW\_CS\_RULE** structure. As in the case of the "EP1Port=" token, the PORT\_RANGE\_VAL grammar rule represents an entry in the **pPorts** field. If the "EP1Port2\_10" token appears multiple times in the rule string, then all the respective PORT\_RANGE\_VAL rules of such appearances are allowed.

**EP2Port=:** This token value represents the **Endpoint2Ports** field of the **FW\_CS\_RULE** structure. As such defined **Endpoint2Ports** is of type **FW\_PORTS**, which contains a **Ports** field of type **FW\_PORT\_RANGE\_LIST**, which also contains a **pPorts** array of type **FW\_PORT\_RANGE**. The PORT\_VAL grammar rule represents an entry in the **pPorts** field. If the **EP2Port** token appears multiple times in the rule string, then all the PORT\_VAL rule of such are allowed.

**EP2Port2\_10=:** This token value represents the **Endpoint2Ports** field of the **FW\_CS\_RULE** structure. As in the case of the "EP2Port=" token, the PORT\_RANGE\_VAL grammar rule represents an entry in the **pPorts** field. If the **EP2Port2\_10** token appears multiple times in the rule string, then all the respective PORT\_RANGE\_VAL rules of such appearances are allowed.

**IF=:** This token represents an entry in the **LocalInterfaceIds** field of the **FW\_CS\_RULE** structure.

**IFType=:** This token represents the **dwLocalInterfaceType** field of the **FW\_CS\_RULE** structure.

**EP1\_4=:** This token value represents the **Endpoint1** field of the **FW\_CS\_RULE** structure, specifically the v4 fields. As such defined **Endpoint1** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type **FW\_IPV4\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV4\_ADDRESS\_RANGE**, and lastly a **V4SubNets** field of type **FW\_IPV4\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV4AddressKeywords** field. If the "EP1\_4" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**EP2\_4=:** This token value represents the **Endpoint2** field of the **FW\_CS\_RULE** structure, specifically the v4 fields. As such defined **Endpoint2** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type **FW\_IPV4\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV4\_ADDRESS\_RANGE**, and lastly a **V4SubNets** field of type **FW\_IPV4\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV4AddressKeywords** field. If the "EP2\_4" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**EP1\_6=:** This token value represents the **Endpoint1** field of the **FW\_CS\_RULE** structure, specifically the v6 fields. As such defined **Endpoint1** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly a **V6SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV6AddressKeywords** field. If the "EP1\_6" token appears multiple times in the rule string, then all the respective ADDRESSV6\_RANGE\_VAL, ADDRESSV6\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**EP2\_6=:** This token value represents the **Endpoint2** field of the **FW\_CS\_RULE** structure, specifically the v6 field. As such defined **Endpoint2** is of type **FsW\_ADDRESSES**, it contains the following 3 fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly a **V6SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV6AddressKeywords** field. If the "EP2\_6" token appears multiple times in the rule string, then all the respective ADDRESSV6\_RANGE\_VAL, ADDRESSV6\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**Name=:** This token represents the **wszName** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Desc=:** This token represents the **wszDescription** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**EmbedCtxt=:** This token represents the **wszEmbeddedContext** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Active=:** This token represents the FW\_CS\_RULE\_FLAGS\_ACTIVE flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the **FW\_CS\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section [2.2.2.14](#Section_2bdb10546ea04b088e51513f7a758011). If the "Active=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**Platform=:** This token value represents the **PlatformValidityList** field of the **FW\_CS\_RULE** structure. As such defined **PlatformValidityList** is of type **FW\_OS\_PLATFORM\_LIST**, it contains a **pPlatforms** array of type **FW\_OS\_PLATFORM**. The PLATFORM\_VAL grammar rule represents an entry in the **pPlatforms** field. If the **Platform=** token appears multiple times in the rule string, then all the respective PLATFORM\_VAL grammar rules of such appearances are allowed.

**SkipVer=:** The VERSION grammar rule following this token represents the highest inherent version of the Firewall and Advanced Security components that should ignore this rule string completely. The inherent version of a Firewall and Advanced Security component is the highest version such component supports.

**Platform2=:** This token represents the operator to use on the last entry of the **PlatformValidityList** field of the **FW\_CS\_RULE** structure. Hence the PLATFORM\_OP\_VAL token represents the 5 most significant bits of the **bPlatform** field of the last FW\_OS\_PLATFORM structure entry (as defined in [MS-FASP] section 2.2.29) of the **pPlatforms** field of the **FW\_OS\_PLATFORM\_LIST** structure as defined in [MS-FASP] section 2.2.30.

**Auth1Set=:** This token represents the **wszPhase1AuthSet** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Auth2Set=:** This token represents the **wszPhase2AuthSet** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Crypto2Set=:** This token represents the **wszPhase2CryptoSet** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**SecureInClearOut=:** This token represents the FW\_CS\_RULE\_OUTBOUND\_CLEAR flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the **FW\_CS\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "SecureInClearOut=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**ByPassTunnel=:** This token represents the FW\_CS\_RULE\_TUNNEL\_BYPASS\_IF\_ENCRYPTED flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the **FW\_CS\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the **ByPassTunnel=** token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**Authz=:** This token represents the FW\_CS\_RULE\_FLAGS\_APPLY\_AUTHZ flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the **FW\_CS\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the **"Authz="** token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**RTunnel4=:** This token represents the **dwLocalTunnelEndpointV4** field of the **FW\_CS\_RULE** structure. The ADDRV4\_VAL grammar rule represents the contents of such field. This token MUST appear at most once in a rule string.

**RTunnel6=:** This token represents the **LocalTunnelEndpointV6** field of the **FW\_CS\_RULE** structure. The ADDRV6\_VAL grammar rule represents the contents of such field. This token MUST appear at most once in a rule string.

**LTunnel4=:** This token represents the **dwRemoteTunnelEndpointV4** field of the **FW\_CS\_RULE** structure. The ADDRV4\_VAL grammar rule represents the contents of such field. This token MUST appear at most once in a rule string.

**LTunnel6=:** This token represents the **RemoteTunnelEndpointV6** field of the **FW\_CS\_RULE** structure. The ADDRV6\_VAL grammar rule represents the contents of such field. This token MUST appear at most once in a rule string.

**RTunnel4\_2=:** This token represents the **dwRemoteTunnelEndpointV4** field of the **FW\_CS\_RULE** structure, with the additional meaning that it also represents a value of true in the FW\_CS\_RULE\_FLAGS\_DTM flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the same **FW\_CS\_RULE** structure. The ADDRV4\_VAL grammar rule represents the contents of the **dwRemoteTunnelEndpointV4** field. This token MUST appear at most once in a rule string.

**RTunnel6\_2=:** This token represents the **RemoteTunnelEndpointV6** field of the **FW\_CS\_RULE** structure, with the additional meaning that it also represents a value of true in the FW\_CS\_RULE\_FLAGS\_DTM flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the same **FW\_CS\_RULE** structure. The ADDRV6\_VAL grammar rule represents the contents of the **RemoteTunnelEndpointV6** field. This token MUST appear at most once in a rule string.

**LTunnel4\_2=:** This token represents the **dwLocalTunnelEndpointV4** field of the **FW\_CS\_RULE** structure, with the additional meaning that it also represents a value of true in the FW\_CS\_RULE\_FLAGS\_DTM flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the same **FW\_CS\_RULE** structure. The ADDRV4\_VAL grammar rule represents the contents of the **dwLocalTunnelEndpointV4** field. This token MUST appear at most once in a rule string.

**LTunnel6\_2=:** This token represents the **LocalTunnelEndpointV6** field of the **FW\_CS\_RULE** structure, with the additional meaning that it also represents a value of true in the FW\_CS\_RULE\_FLAGS\_DTM flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the same **FW\_CS\_RULE** structure. The ADDRV6\_VAL grammar rule represents the contents of the **LocalTunnelEndpointV6** field. This token MUST appear at most once in a rule string.

**RTunnelFqdn=:** This token represents the **wszRemoteTunnelEndpointFqdn** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear only once in a rule string.

**RTunEndpts4=:** This token value represents the **RemoteTunnelEndpoints** field of the **FW\_CS\_RULE** structure, specifically the v4 fields. As such defined **RemoteTunnelEndpoints** is of type **FW\_ADDRESSES**, it contains the following three fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type **FW\_IPV4\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV4\_ADDRESS\_RANGE**, and lastly, a **V4SubNets** field of type **FW\_IPV4\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV4AddressKeywords** field. If the "RTunEndpts4=" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**RTunEndpts6=:** This token value represents the **RemoteTunnelEndpoints** field of the **FW\_CS\_RULE** structure, specifically the v6 fields. As such defined **RemoteTunnelEndpoints** is of type **FW\_ADDRESSES**, it contains the following three fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly, a **V4SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV6AddressKeywords** field. If the "RTunEndpts6=" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**KeyMod=:** This token value represents the **dwKeyModules** field of the **FW\_CS\_RULE** structure. The KEY\_MOD\_VAL grammar rule represents a flag in the **dwKeyModules** field. If the "KeyMod=" token appears multiple times in the rule string, then all the respective KEY\_MOD\_VAL rules of such appearances are allowed.

**KeyManagerDictate=:** This token represents the FW\_CS\_RULE\_FLAGS\_KEY\_MANAGER\_ALLOW\_DICTATE\_KEY flag (as defined in [MS-FASP] section 2.2.50) of the wFlags field of the **FW\_CS\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "KeyManagerDictate=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear only once in a rule string.

**KeyManagerNotify=:** This token represents the FW\_CS\_RULE\_FLAGS\_KEY\_MANAGER\_ALLOW\_NOTIFY\_KEY flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the **FW\_CS\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the "KeyManagerNotify=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear only once in a rule string.

**FwdLifetime=:** This token represents the **FwdPathSALifetime** field of the **FW\_CS\_RULE** structure. Its decimal value MUST NOT be greater than 4,294,967,295. If the "FwdLifetime=" token does not appear in the rule, a value of zero is assumed. This token MUST appear only once in a rule string.

**TransportMachineAuthzSDDL=:** This token represents the **wszTransportMachineAuthzSDDL** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear only once in a rule string.

**TransportUserAuthzSDDL=:** This token represents the **wszTransportUserAuthzSDDL** field of the **FW\_CS\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear only once in a rule string.

**SecurityRealmEnabled=**: This token[<8>](#Appendix_A_8) represents the FW\_CS\_RULE\_FLAGS\_SECURITY\_REALM flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the FW\_CS\_RULE structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section 2.2.2.14. If the SecurityRealmEnabled= token does not appear in the rule, a Boolean value of FALSE is assumed. This token MUST appear only once in a rule string.

The semantic checks defined in [MS-FASP] section 2.2.54 are also applicable to the connection security rules described in this section after following the mapping in each of the preceding tokens.

#### Keying Module Rules

This grammar is used to identify keying modules.

1. KEY\_MOD\_VAL = "KeyModDefault" / "IkeV1" / "AuthIP" / "IkeV2"

**KeyModDefault:** This token represents the FW\_KEY\_MODULE\_DEFAULT enumeration value as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.95. The remaining token values in this list can be found in the same Protocol specification section.

**IkeV1:** This token represents the FW\_KEY\_MODULE\_IKEv1 enumeration value.

**AuthIP:** This token represents the FW\_KEY\_MODULE\_AUTHIP enumeration value.

**IkeV2:** This token represents the FW\_KEY\_MODULE\_IKEv2 enumeration value.

### Main Mode Rule Messages

This section defines the grammars used to encode different portions of the Main Mode rules. Main Mode rules are available on schema version 0x0208 and later.

#### Main Mode Rule and the Main Mode Rule Grammar Rule

Main mode rules are stored under the Software\Policies\Microsoft\WindowsFirewall\MainModeRules key.

Each value under the key is a main mode rule. The type of the value MUST be REG\_SZ. The data of each value is a string that can be parsed by the following grammar. This grammar represents a main mode rule as defined in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 2.2.84, except for the **wszRuleId** field of the **FW\_MM\_RULE** structure, which is instead represented by the name of the registry value.

1. MMRULE = "v" VERSION "|" 1\*FIELD
2. FIELD = TYPE\_VALUE "|"
3. TYPE\_VALUE =/ "Profile=" PROFILE\_VAL
4. TYPE\_VALUE =/ "Auth1Set=" STR\_VAL
5. TYPE\_VALUE =/ "Crypto1Set=" STR\_VAL
6. TYPE\_VALUE =/ "EP1\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
7. TYPE\_VALUE =/ "EP2\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
8. TYPE\_VALUE =/ "EP1\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
9. TYPE\_VALUE =/ "EP2\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
10. TYPE\_VALUE =/ "Name=" STR\_VAL
11. TYPE\_VALUE =/ "Desc=" STR\_VAL
12. TYPE\_VALUE =/ "EmbedCtxt=" STR\_VAL
13. TYPE\_VALUE =/ "Active=" BOOL\_VAL
14. TYPE\_VALUE =/ "Platform=" PLATFORM\_VAL
15. TYPE\_VALUE =/ "SkipVer=" VERSION
16. TYPE\_VALUE =/ "Platform2=" PLATFORM\_OP\_VAL
17. STR\_VAL = 1\*ALPHANUM
18. BOOL\_VAL = "TRUE" / "FALSE"

**Profile=:** This token value represents the **dwProfiles** field of the **FW\_MM\_RULE** structure as defined in [MS-FASP] section 2.2.84. The PROFILE\_VAL grammar rule represents a value content of such field. If this token appears several times in an MMRULE grammar rule, then all the contents represented by the PROFILE\_VAL rule appearing next to them are included. If the "Profile=" token never appears in the rule string then it represents a value of **FW\_PROFILE\_TYPE\_ALL** as defined in [MS-FASP] section 2.2.2.

**EP1\_4=:** This token value represents the **Endpoint1** field of the **FW\_MM\_RULE** structure, specifically the v4 fields, as defined in [MS-FASP] section 2.2.84. As such defined **Endpoint1** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type **FW\_IPV4\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV4\_ADDRESS\_RANGE**, and lastly a **V4SubNets** field of type **FW\_IPV4\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV4AddressKeywords** field. If the "EP1\_4" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**EP2\_4=:** This token value represents the **Endpoint2** field of the **FW\_MM\_RULE** structure, specifically the v4 fields, as defined in [MS-FASP] section 2.2.84. As such defined **Endpoint2** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV4AddressKeyword** field, a **V4Ranges** field of type **FW\_IPV4\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV4\_ADDRESS\_RANGE**, and lastly a **V4SubNets** field of type **FW\_IPV4\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV4\_SUBNET**. The ADDRESSV4\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV4\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV4AddressKeywords** field. If the "EP2\_4" token appears multiple times in the rule string, then all the respective ADDRESSV4\_RANGE\_VAL, ADDRESSV4\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**EP1\_6=:** This token value represents the **Endpoint1** field of the **FW\_MM\_RULE** structure, specifically the v6 fields, as defined in [MS-FASP] section 2.2.84. As such defined **Endpoint1** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly a **V6SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV6AddressKeywords** field. If the "EP1\_6" token appears multiple times in the rule string, then all the respective ADDRESSV6\_RANGE\_VAL, ADDRESSV6\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**EP2\_6=:** This token value represents the **Endpoint2** field of the **FW\_MM\_RULE** structure, specifically the v6 fields, as defined in [MS-FASP] section 2.2.84. As such defined **Endpoint2** is of type **FW\_ADDRESSES**, it contains the following 3 fields: a **dwV6AddressKeyword** field, a **V6Ranges** field of type **FW\_IPV6\_RANGE\_LIST**, which also contains a **pRanges** array of type **FW\_IPV6\_ADDRESS\_RANGE**, and lastly a **V6SubNets** field of type **FW\_IPV6\_SUBNET\_LIST**, which also contains a **pSubNets** array of type **FW\_IPV6\_SUBNET**. The ADDRESSV6\_RANGE\_VAL grammar rule represents an entry in the **pRanges** field. The ADDRESSV6\_SUBNET\_VAL grammar rule represents an entry in the **pSubNets** field. The ADDRESS\_KEYWORD\_VAL grammar rule, however, represents the **dwV6AddressKeywords** field. If the "EP2\_6" token appears multiple times in the rule string, then all the respective ADDRESSV6\_RANGE\_VAL, ADDRESSV6\_SUBNET\_VAL, and the ADDRESS\_KEYWORD\_VAL rules of such appearances are allowed.

**Name=:** This token represents the **wszName** field of the **FW\_MM\_RULE** structure as defined in [MS-FASP] section 2.2.84. The remaining token values in this list can be found in the same Protocol specification section. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Desc=:** This token represents the **wszDescription** field of the **FW\_MM\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**EmbedCtxt=:** This token represents the **wszEmbeddedContext** field of the **FW\_MM\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Active=:** This token represents the FW\_CS\_RULE\_FLAGS\_ACTIVE flag (as defined in [MS-FASP] section 2.2.50) of the **wFlags** field of the **FW\_MM\_RULE** structure. The BOOL\_VAL grammar rule represents the Boolean meaning of such flag as defined in section [2.2.2.14](#Section_2bdb10546ea04b088e51513f7a758011). If the "Active=" token does not appear in the rule, a Boolean value of false is assumed. This token MUST appear at most once in a rule string.

**Platform=:** This token value represents the **PlatformValidityList** field of the **FW\_MM\_RULE** structure. As such defined **PlatformValidityList** is of type **FW\_OS\_PLATFORM\_LIST**, it contains a **pPlatforms** array of type **FW\_OS\_PLATFORM**. The PLATFORM\_VAL grammar rule represents an entry in the **pPlatforms** field. If the "Platform=" token appears multiple times in the rule string, then all the respective PLATFORM\_VAL grammar rules of such appearances are allowed.

**SkipVer=:** The VERSION grammar rule following this token represents the highest inherent version of the Firewall and Advanced Security components that should ignore this rule string completely. The inherent version of a Firewall and Advanced Security component is the highest version such component supports.

**Platform2=:** This token represents the operator to use on the last entry of the **PlatformValidityList** field of the **FW\_MM\_RULE** structure. Hence the PLATFORM\_OP\_VAL token represents the five most significant bits of the **bPlatform** field of the last **FW\_OS\_PLATFORM** structure entry (as defined in [MS-FASP] section 2.2.29) of the pPlatforms field of the **FW\_OS\_PLATFORM\_LIST** structure as defined in [MS-FASP] section 2.2.30.

**Auth1Set=:** This token represents the **wszPhase1AuthSet** field of the **FW\_MM\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

**Crypto1Set=:** This token represents the **wszPhase1CryptoSet** field of the **FW\_MM\_RULE** structure. The STR\_VAL grammar rule represents a Unicode string that represents the contents of such field. This token MUST appear at most once in a rule string.

The semantic checks described in [MS-FASP] section 2.2.84 are also applicable to the main mode rules described in this section after following the mapping in each of the preceding tokens.

# Protocol Details

## Administrative Plug-in Details

The administrative plug-in mediates between the user interface (UI) and a remote data store that contains the Firewall and advanced security group policy extension settings. Its purpose is to receive Firewall and Advanced Security policy information from a UI and to write the same policy information to a remote data store.

### Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to explain how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that specified in this document.

The Firewall and Advanced Security Group Policy administrative plug-in relies on a collection of settings specified in section [2.2](#Section_3adde782cd9d4bfdbb7b9f5b5ea54f85) and stored as a Unicode configuration file ([[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 2.2) in a GPO using the Group Policy: Core Protocol specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf). The administrative plug-in parses and encodes these settings as specified in section 2.2 to perform its functions.

The Firewall and Advanced Security Group Policy administrative plug-in reads in these settings from the remote storage location GPO and displays them to an administrator through a UI.

An administrator can then use the UI to make further configuration changes, and the Firewall and Advanced Security Group Policy administrative plug-in will make corresponding changes to the name-value pairs stored in the aforementioned Unicode configuration file following the conventions of the grammars rules, registry values, and keys specified in section 2.2.

This conceptual data can be implemented using a variety of techniques. An implementation can implement such data using any method.[<9>](#Appendix_A_9)

This protocol also includes one ADM element, **Administered GPO (Public)**, which is directly accessed from Group Policy: Core Protocol, as specified in [MS-GPOL] section 3.3.1.3.

### Timers

None.

### Initialization

None.

### Higher-Layer Triggered Events

The Firewall and Advanced Security Group Policy administrative plug-in is invoked when an administrator launches the Group Policy Protocol Administrative Tool, as specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf) section 3.3.1.1. The Group Policy Protocol Administrative Tool passes the following parameters to the plug-in, as specified in [MS-GPOL] section 3.3.4.7.

| Parameter | Description |
| --- | --- |
| GPO DN | The [**distinguished name (DN)**](#gt_1175dd11-9368-41d5-98ed-d585f268ad4b) for the GPO that is being updated. This is the **Administered GPO (Public)** ADM element, as specified in section [3.1.1](#Section_11ea3ad7cad0434b87bc66b3578f0dd1). |
| Is User Policy | A Boolean value indicating whether this update is for user policy mode. If set to FALSE, this update is for computer policy mode. This parameter is ignored. |

The plug-in displays the current settings to the administrator, and when the administrator requests a change in settings, it updates the stored configuration appropriately as specified in section [2.2](#Section_3adde782cd9d4bfdbb7b9f5b5ea54f85), after performing additional checks and actions as noted in this section.

The administrative plug-in SHOULD[<10>](#Appendix_A_10) take measures in its UI to ensure that the user cannot unknowingly set the Firewall and Advanced Security policy settings to an invalid value. It SHOULD also make sure all references necessary for an object to work are appropriately configured (for example: ensure that non-default sets, which a connection security rule references, are also configured in the policy).

### Message Processing Events and Sequencing Rules

The Firewall and Advanced Security (FASP) Group Policy administrative plug-in reads extension-specific data from the **Administered GPO** (as defined in section [3.1.1](#Section_11ea3ad7cad0434b87bc66b3578f0dd1)) and will then pass that information to a UI to display the current settings to an administrator. The operations that the Firewall and Advanced Security Group Policy administrative plug-in uses to read extension-specific data from a GPO are detailed in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 3.1.5.3.

It will also write the extension-specific configuration data to the **Administered GPO** if the administrator makes any changes to the existing configuration. The operations that the Firewall and Advanced Security Group Policy administrative plug-in uses to create, update, or delete the extension-specific data to a GPO are detailed in section [3.1.5.2](#Section_4c9891c9ea48423da58ee5f70a9a4016).

Any additional entries in the configuration data that do not pertain to the configuration options specified in section [2.2](#Section_3adde782cd9d4bfdbb7b9f5b5ea54f85), or that are not supported by the particular implementation, MUST be ignored by the plug-in.

The FASP Group Policy administrative plug-in queries and persists these settings in the "registry.pol" registry policy file under the [**computer-scoped Group Policy Object path**](#gt_75cdc562-983e-442d-9387-54845be74fcc). The "registry.pol" file is loaded and updated by invoking the events in [MS-GPREG] sections 3.1.4.1 and 3.1.4.2. No other policy files are accessed by this plug-in. The plug-in MUST use the registry policy file format specified in [MS-GPREG] section 2.2.1 to query and update the policy entries described in section 2.2 in the "registry.pol" file.

#### Policy Administration Load Message Sequencing

The Group Policy: Firewall and Advanced Security Data Structure invokes the Load Policy Settings Event ([[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf), section 3.1.4.1), computer-scoped Group Policy Object path of the **Administered GPO**, and receives a Policy Setting State ([MS-GPREG], section 3.2.1.1).

#### Policy Administration Update Message Sequencing

To update the Group Policy: Firewall and Advanced Security Data Structure settings, the administrative plug-in MUST perform the following operations, in order:

1. The administrative plug-in MUST invoke the Update Policy Event ([[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 3.1.4.2), specifying the computer-scoped Group Policy Object path of the **Administered GPO** and the new Policy Setting State ([MS-GPREG] section 3.2.1.1).
2. The administrative plug-in MUST invoke the Group Policy Extension Update event specified in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf) section 3.3.4.4 with the following parameters:
   * "GPO DN" is set to the distinguished name (DN) of the **Administered GPO**.
   * "Is User Policy" is set to FALSE.
   * "CSE GUID" is set to the Group Policy: Registry Extension Encoding CSE GUID (defined in [MS-GPREG] section 1.9).
   * "TOOL GUID" is set to the Group Policy: Firewall and Advanced Security Data Structure Tool extension GUID (defined in section [1.9](#Section_963c05dddf8b47e09abbe948be167fec)).

### Timer Events

None.

### Other Local Events

None.

## Client Details

### Abstract Data Model

The Group Policy: Firewall and Advanced Security Data Structure client maintains no state. However, it directly accesses the Policy Setting State from the Group Policy: Registry Extension Encoding, as specified in [[MS-GPREG]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPREG%5d.pdf) section 3.2.1.1.

### Timers

None.

### Initialization

The Group Policy: Firewall and Advanced Security Data Structure client initializes when the host machine starts. The client MUST use an implementation-specific[<11>](#Appendix_A_11) method to register for notification of the Policy Application event, as defined in [[MS-GPOL]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-GPOL%5d.pdf) section 3.2.7.3. The client MUST then query the registry using the key and value names defined in sections [2.2.1](#Section_48e60b2e345645a4af40c77711bd6398) through [2.2.7](#Section_e8bbe80b3de14816be9188f4068b601d) to retrieve the initial policy settings. It MUST use the grammar rules defined in the same section to parse the values when necessary. Based on the data retrieved for these settings, the client MUST invoke the abstract interface SetGroupPolicyRSoPStore() (as specified in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 3.1.6.4) to modify the internal state of the Firewall and Advanced Security component.

### Higher-Layer Triggered Events

None.

### Message Processing Events and Sequencing Rules

None.

### Timer Events

None.

### Other Local Events

#### Policy Application Event

When Group Policy: Core Protocol signals the Policy Application event, the Group Policy: Firewall and Advanced Security Data Structure client MUST query the registry using the key and value names defined in sections [2.2.1](#Section_48e60b2e345645a4af40c77711bd6398) through [2.2.7](#Section_e8bbe80b3de14816be9188f4068b601d) to retrieve the updated policy settings. It MUST use the grammar rules defined in the same section to parse the values when necessary. Based on the data retrieved for these settings, the client MUST invoke the abstract interface SetGroupPolicyRSoPStore() (as specified in [[MS-FASP]](file:///E:\Target\Windows\Published\Books\MS-GPFAS\%5bMS-FASP%5d.pdf) section 3.1.6) to modify the internal state of the Firewall and Advanced Security component.

# Protocol Examples

## Configuration Options Messages

The following is an example of options that are configured to both enable the firewall and block inbound connections by default on the public profile.

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile

Value: "EnableFirewall"

Type: REG\_DWORD.

Size: 4

Data: 00000001

Value: "DefaultInboundAction"

Type: REG\_DWORD.

Size: 4

Data: 00000001

## Firewall Rule Message

The following is an example of a settings message that encodes a firewall rule object to be applied on client computers.

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules.

Value: "{F7EE5C6D-6C90-456B-9166-E301B1305A56}"

Type: REG\_SZ.

Size: 540

Data: "v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|Profile=Public|LPort=RPC|RPort=49000|LA4=192.168.1.0/255.255.255.0|LA4=192.168.0.0/255.255.255.0|RA4=LocalSubnet|RA6=LocalSubnet|App=c:\\path\\foo.exe|Name=Firewall Rule Test|Security=Authenticate|Security2\_9=An-NoEncap|"

## Connection Security Rule Message

The following is an example of a settings message that encodes connection security rule objects to be applied on client computers.

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\ConSecRules.

Value: "{06BD9C7F-E80A-4A68-92A2-CCBF5351A60A}"

Type: REG\_SZ.

Size: 912

Data: "v2.10|Action=Secure|Active=TRUE|Profile=Private|Profile=Public|EP2\_6=2006:1601::/32|EP2\_6=2a01:110::/31|EP2\_6=2001:4898::-2001:4898:a0:5084:ffff:ffff:ffff:ffff|EP2\_6=2001:4898:e0:7025::-2001:4898:ffff:ffff:ffff:ffff:ffff:ffff|RTunnel6\_2=2001:4898:e0:3084::2|Name=Tunnel From Internet To Corp|Desc=|Auth1Set={D842F406-E895-406A-AC35-9837B6D499F4}|Auth2Set={A75A5046-E377-45CC-BD25-EC0F8E601CE1}|Crypto2Set={CD863A4F-CD94-4763-AD25-69A1378D51EB}|EmbedCtxt=|"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\ConSecRules.

Value: "{797404C9-EEE0-4793-9271-9F09C834B902}"

Type: REG\_SZ.

Size: 480

Data: "v2.10|Action=DoNotSecure|Protocol=6|Active=TRUE|EP1Port=5357|EP1Port=5358|EP1Port=5363|EP2\_4=157.56.56.23|EP2\_4=157.56.59.42|EP2\_4=157.56.56.92|EP2\_4=157.56.59.49|EP2\_4=157.56.61.37|Name=Exempt TCP Ports on Specific boxes|Desc=|EmbedCtxt=|"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\ConSecRules.

Value: "{840A0BA7-40F7-4ECE-A1E8-F9E8652F354B }"

Type: REG\_SZ.

Size: 462

Data: "v2.10|Action=SecureServer|Active=TRUE|Name=Domain Isolation Rule|Desc=AuthIP policy|Auth1Set={212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}|Auth2Set={967F0367-F879-42EC-938B-C89FE8289B26}|Crypto2Set={E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}|"

## Authentication Set Messages

The following are an example of a settings message that encodes authentication set objects to be applied on client computers and used by the connection security rule example in section [4.3](#Section_bcabd549c6f4401cbd65e3488620565e).

### Authentication Set { 212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB }

The following messages encode a phase 1 authentication set with set id {212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}:

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}.

Value: "Version"

Type: REG\_SZ.

Size: 10

Data: "2.10"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}.

Value: "Name"

Type: REG\_SZ.

Size: 96

Data: "AuthIP Domain Isolation Rule - Phase 1 Auth Set"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}\0000

Value: "Method"

Type: REG\_SZ.

Size: 24

Data: "MachineKerb"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}\0001

Value: "Method"

Type: REG\_SZ.

Size: 24

Data: "MachineCert"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}\0001

Value: "HealthCert"

Type: REG\_SZ.

Size: 12

Data: "FALSE"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}\0001

Value: "CAName"

Type: REG\_SZ.

Size: 104

Data: "O=Contoso Corporation, CN=Contoso Corporate Root CA"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}\0001

Value: "CertAccountMapping"

Type: REG\_SZ.

Size: 12

Data: "FALSE"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{212D4E36-DB6E-4EAE-A65F-1C4615EBFDDB}\0001

Value: "ExcludeCAName"

Type: REG\_SZ.

Size: 12

Data: "FALSE"

### Authentication Set { D842F406-E895-406A-AC35-9837B6D499F4 }

The following messages encode a phase 1 authentication set with set id {D842F406-E895-406A-AC35-9837B6D499F4}:

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{D842F406-E895-406A-AC35-9837B6D499F4}.

Value: "Version"

Type: REG\_SZ.

Size: 10

Data: "2.10"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{D842F406-E895-406A-AC35-9837B6D499F4}\0000

Value: "Method"

Type: REG\_SZ.

Size: 24

Data: "MachineCert"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{D842F406-E895-406A-AC35-9837B6D499F4}\0000

Value: "HealthCert"

Type: REG\_SZ.

Size: 12

Data: "FALSE"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{D842F406-E895-406A-AC35-9837B6D499F4}\0000

Value: "CAName"

Type: REG\_SZ.

Size: 104

Data: "O=Contoso Corporation, CN=Contoso Corporate Root CA"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{D842F406-E895-406A-AC35-9837B6D499F4}\0000

Value: "CertAccountMapping"

Type: REG\_SZ.

Size: 12

Data: "FALSE"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase1AuthenticationSets\{D842F406-E895-406A-AC35-9837B6D499F4}\0000

Value: "ExcludeCAName"

Type: REG\_SZ.

Size: 12

Data: "FALSE"

### Authentication Set { A75A5046-E377-45CC-BD25-EC0F8E601CE1 }

The following messages encode a phase 2 authentication set with set id {A75A5046-E377-45CC-BD25-EC0F8E601CE1}:

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{A75A5046-E377-45CC-BD25-EC0F8E601CE1}.

Value: "Version"

Type: REG\_SZ.

Size: 10

Data: "2.10"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{A75A5046-E377-45CC-BD25-EC0F8E601CE1}\0000

Value: "Method"

Type: REG\_SZ.

Size: 18

Data: "UserKerb"

### Authentication Set { 967F0367-F879-42EC-938B-C89FE8289B26 }

The following messages encode a phase 2 authentication set with set id {967F0367-F879-42EC-938B-C89FE8289B26}:

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}.

Value: "Version"

Type: REG\_SZ.

Size: 10

Data: "2.10"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}.

Value: "Name"

Type: REG\_SZ.

Size: 96

Data: "AuthIP Domain Isolation Rule - Phase 2 Auth Set"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}\0000

Value: "Method"

Type: REG\_SZ.

Size: 18

Data: "UserKerb"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}\0001

Value: "Method"

Type: REG\_SZ.

Size: 18

Data: "UserNTLM"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}\0002

Value: "Method"

Type: REG\_SZ.

Size: 18

Data: "UserCert"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}\0002

Value: "CAName"

Type: REG\_SZ.

Size: 24

Data: "CN=TPM Root"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}\0002

Value: "CertAccountMapping"

Type: REG\_SZ.

Size: 10

Data: "TRUE"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2AuthenticationSets\{967F0367-F879-42EC-938B-C89FE8289B26}\0003

Value: "Method"

Type: REG\_SZ.

Size: 20

Data: "Anonymous"

### Cryptographic Set Messages

The following are an example of a settings message that encodes authentication set objects to be applied on client computers and used by the connection security rule example in section [4.3](#Section_bcabd549c6f4401cbd65e3488620565e).

#### Cryptographic Set { CD863A4F-CD94-4763-AD25-69A1378D51EB }

The following messages encode a phase 2 cryptographic set with set id {CD863A4F-CD94-4763-AD25-69A1378D51EB}:

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}.

Value: "Version"

Type: REG\_SZ.

Size: 10

Data: "2.10"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}.

Value: "Name"

Type: REG\_SZ.

Size: 100

Data: "Tunnel From Internet To Corp - Phase 2 Crypto Set"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}.

Value: "PFS"

Type: REG\_SZ.

Size: 16

Data: "Disable"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0000

Value: "Protocol"

Type: REG\_SZ.

Size: 8

Data: "ESP"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0000

Value: "Encryption"

Type: REG\_SZ.

Size: 16

Data: "AES-128"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0000

Value: "EspHash"

Type: REG\_SZ.

Size: 10

Data: "SHA1"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0000

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: 6

Data: "60"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0000

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: 14

Data: "100000"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0001

Value: "Protocol"

Type: REG\_SZ.

Size: 8

Data: "ESP"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0001

Value: "Encryption"

Type: REG\_SZ.

Size: 10

Data: "3DES"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0001

Value: "EspHash"

Type: REG\_SZ.

Size: 10

Data: "SHA1"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0001

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: 6

Data: "60"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{CD863A4F-CD94-4763-AD25-69A1378D51EB}\0001

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: 14

Data: "100000"

#### Cryptographic Set { E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F }

The following messages encode a phase 2 cryptographic set with set id {E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}:

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}.

Value: "Version"

Type: REG\_SZ.

Size: 10

Data: "2.10"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}.

Value: "Name"

Type: REG\_SZ.

Size: 100

Data: "AuthIP Domain Isolation Rule - Phase 2 Crypto Set"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}.

Value: "PFS"

Type: REG\_SZ.

Size: 16

Data: "Disable"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0000

Value: "Protocol"

Type: REG\_SZ.

Size: 8

Data: "ESP"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0000

Value: "EspHash"

Type: REG\_SZ.

Size: 10

Data: "SHA1"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0000

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: 6

Data: "60"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0000

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: 22

Data: "2147483647"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0001

Value: "Protocol"

Type: REG\_SZ.

Size: 8

Data: "ESP"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0001

Value: "2\_1EspHash"

Type: REG\_SZ.

Size: 22

Data: "AES-GCM128"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0001

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: 6

Data: "60"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0001

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: 22

Data: "2147483647"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0001

Value: "SkipVersion"

Type: REG\_SZ.

Size: 8

Data: "2.0"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0002

Value: "Protocol"

Type: REG\_SZ.

Size: 6

Data: "AH"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0002

Value: "AhHash"

Type: REG\_SZ.

Size: 10

Data: "SHA1"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0002

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: 6

Data: "60"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0002

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: 22

Data: "2147483647"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0003

Value: "Protocol"

Type: REG\_SZ.

Size: 8

Data: "ESP"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0003

Value: "Encryption"

Type: REG\_SZ.

Size: 10

Data: "3DES"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0003

Value: "EspHash"

Type: REG\_SZ.

Size: 10

Data: "SHA1"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0003

Value: "TimeOutMinutes"

Type: REG\_SZ.

Size: 6

Data: "60"

Key: SOFTWARE\Policies\Microsoft\WindowsFirewall\Phase2CryptoSets\{E9A15CB6-DFC4-41F8-8D14-CA62A4EC708F}\0003

Value: "TimeOutKbytes"

Type: REG\_SZ.

Size: 22

Data: "2147483647"

# Security

## Security Considerations for Implementers

Implementers SHOULD NOT transmit passwords or other sensitive data through this protocol. The primary reason for this restriction is that the protocol provides no encryption, and therefore sensitive data transmitted through this protocol can be intercepted easily by an unauthorized user with access to the network carrying the data. For example, if a network administrator configured a Group Policy: Registry Extension Encoding setting in a GPO to instruct a computer to use a specific password when accessing a certain network resource, this protocol would send that password unencrypted to those computers. A person gaining unauthorized access, intercepting the protocol's network packets in this case, would then discover the password for that resource that would then be unprotected from the unauthorized person.

## Index of Security Parameters

None.

# Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs.

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

* Windows Vista operating system
* Windows Server 2008 operating system
* Windows 7 operating system
* Windows Server 2008 R2 operating system
* Windows 8 operating system
* Windows Server 2012 operating system
* Windows 8.1 operating system
* Windows Server 2012 R2 operating system
* Windows 10 operating system
* Windows Server 2016 Technical Preview operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

[<1> Section 1.7](#Appendix_A_Target_1): The maximum supported schema versions (the inherent schema version) for each Windows operating system is as follows:

* Windows Vista uses version 0x0200.
* Windows Vista operating system with Service Pack 1 (SP1) and later and Windows Server 2008 use version 0x0201.
* Windows 7 and Windows Server 2008 R2 use version 0x020A.
* Windows 8 and Windows Server 2012 use version 0x0214.
* Windows 8.1 and Windows Server 2012 R2 use version 0x0216.
* Windows 10 and Windows Server 2016 Technical Preview use version 0x0218.

[<2> Section 2.2.2.19](#Appendix_A_Target_2): LUAuth2\_24= is available in Windows 10 and Windows Server 2016 Technical Preview.

[<3> Section 2.2.2.19](#Appendix_A_Target_3): NNm= is available in Windows 10 and Windows Server 2016 Technical Preview.

[<4> Section 2.2.2.19](#Appendix_A_Target_4): SecurityRealmId= is available in Windows 10 and Windows Server 2016 Technical Preview.

[<5> Section 2.2.2.20](#Appendix_A_Target_5): WFDPrint is only available on Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 Technical Preview.

[<6> Section 2.2.2.20](#Appendix_A_Target_6): WFDDisplay is only available on Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 Technical Preview.

[<7> Section 2.2.2.20](#Appendix_A_Target_7): WFDDevices is only available on Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 Technical Preview.

[<8> Section 2.2.6.2](#Appendix_A_Target_8): The SecurityRealmEnabled= token is available in Windows 10 and Windows Server 2016 Technical Preview.

[<9> Section 3.1.1](#Appendix_A_Target_9): The Firewall and Advanced Security configuration data is stored in registry keys of the managed computer as specified in section [2.2.1](#Section_48e60b2e345645a4af40c77711bd6398) and its subsections.

[<10> Section 3.1.4](#Appendix_A_Target_10): Windows administrative tools verify the validity of the objects as defined in section [2.2](#Section_3adde782cd9d4bfdbb7b9f5b5ea54f85) before writing them to the remote store through Group Policy: Registry Extension Encoding.

[<11> Section 3.2.3](#Appendix_A_Target_11): The Windows implementation of the Group Policy: Firewall and Advanced Security Data Structure client uses the RegisterGPNotification API to receive a notification when there is a change in policy (for more information, see [[MSDN-RegisterGPNotification]](http://go.microsoft.com/fwlink/?LinkId=217895)).

# Appendix B: Full ABNF Grammar

The following sections list the complete grammar rules of the policy setting that are encoded using ABNF syntax for implementers of Group Policy: Firewall and Advanced Security Group Policy Extension Encoding.

1. PROFILE\_VAL = "Domain" / "Private" / "Public"
2. PORT\_RANGE\_VAL = BEGINPORT "-" ENDPORT
3. PORT\_VAL = SINGLEPORT
4. BEGINPORT = PORT
5. ENDPORT = PORT
6. SINGLEPORT = PORT
7. PORT = 1\*5DIGIT
8. LPORT\_KEYWORD\_VAL = "RPC" / "RPC-EPMap" / "Teredo"
9. LPORT\_KEYWORD\_VAL\_2\_10 = "IPTLSIn" / "IPHTTPSIn"
10. RPORT\_KEYWORD\_VAL\_2\_10 = "IPTLSOut" / "IPHTTPSOut"
11. DIR\_VAL = "In" / "Out"
12. ACTION\_VAL = "Allow" / "Block" / "ByPass"
13. IFSECURE\_VAL = "Authenticate" / "AuthenticateEncrypt"
14. IFSECUIRE2\_9\_VAL = "An-NoEncap"
15. IFSECURE2\_10\_VAL = "AnE-Nego"
16. IF\_VAL = GUID
17. IFTYPE\_VAL = "Lan" / "Wireless" / "RemoteAccess"
18. ADDRESSV4\_RANGE\_VAL = BEGINADDRV4 "-" ENDADDRV4
19. ADDRESSV4\_RANGE\_VAL = SINGLEADDRV4
20. BEGINADDRV4 = ADDRV4
21. ENDADDRV4 = ADDRV4
22. SINGLEADDRV4 = ADDRV4
23. ADDRV4 = 1\*3DIGIT "."1\*3DIGIT "."1\*3DIGIT "."1\*3DIGIT
24. ADDRESSV4\_SUBNET\_VAL = SUBNET\_ADDRV4 "/" V4PREFIX\_LENGHT
25. ADDRESSV4\_SUBNET\_VAL = SUBNET\_ADDRV4 "/" MASK\_ADDRV4
26. V4PREFIX\_LENGHT = 1\*2DIGIT
27. SUBNET\_ADDRV4 = ADDRV4
28. MASK\_ADDRV4 = ADDRV4
29. ADDRESSV6\_RANGE\_VAL = BEGINADDRV6 "-" ENDADDRV6
30. ADDRESSV6\_RANGE\_VAL = SINGLEADDRV6
31. BEGINADDRV6 = ADDRV6
32. ENDADDRV6 = ADDRV6
33. SINGLEADDRV6 = ADDRV6
34. ADDRESSV6\_SUBNET\_VAL = SUBNET\_ADDRV6 "/" V6PREFIX\_LENGHT
35. V6PREFIX\_LENGHT = 1\*3DIGIT
36. SUBNET\_ADDRV6 = ADDRV6
37. ADDRESS\_KEYWORD\_VAL = "LocalSubnet" / "DNS" / "DHCP" / "WINS" / DefaultGateway"
38. BOOL\_VAL = "TRUE" / "FALSE"
39. DEFER\_VAL = "App" / "User"
40. ICMP\_TYPE\_CODE\_VAL = TYPE ":" CODE
41. TYPE = 1\*3DIGIT
42. CODE = 1\*3DIGIT
43. CODE =/ "\*"
44. PLATFORM\_VAL = PLATFORM ":" OS\_MAJOR\_VER ":" OS\_MINOR\_VER
45. PLATFORM = 1DIGIT
46. OS\_MAJOR\_VER = 1\*3DIGIT
47. OS\_MINOR\_VER = 1\*3DIGIT
48. PLATFORM\_OP\_VAL = "GTEQ"
49. RULE = "v" VERSION "|" 1\*FIELD
50. FIELD = TYPE\_VALUE "|"
51. TYPE\_VALUE = "Action=" ACTION\_VAL
52. TYPE\_VALUE =/ "Dir=" DIR\_VAL
53. TYPE\_VALUE =/ "Profile=" PROFILE\_VAL
54. TYPE\_VALUE =/ "Protocol=" 1\*3DIGIT ; protocol is maximum 3 digits (255)
55. TYPE\_VALUE =/ "LPort=" ( PORT\_VAL / LPORT\_KEYWORD\_VAL )
56. TYPE\_VALUE =/ "RPort=" PORT\_VAL
57. TYPE\_VALUE =/ "LPort2\_10=" ( PORT\_RANGE\_VAL / LPORT\_KEYWORD\_VAL\_2\_10 )
58. TYPE\_VALUE =/ "RPort2\_10=" ( PORT\_RANGE\_VAL / RPORT\_KEYWORD\_VAL\_2\_10 )
59. TYPE\_VALUE =/ "Security=" IFSECURE\_VAL
60. TYPE\_VALUE =/ "Security2\_9=" IFSECURE2\_9\_VAL
61. TYPE\_VALUE =/ "Security2=" IFSECURE2\_10\_VAL
62. TYPE\_VALUE =/ "IF=" IF\_VAL
63. TYPE\_VALUE =/ "IFType=" IFTYPE\_VAL
64. TYPE\_VALUE =/ "App=" APP\_VAL
65. TYPE\_VALUE =/ "Svc=" SVC\_VAL
66. TYPE\_VALUE =/ "LA4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL )
67. TYPE\_VALUE =/ "RA4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
68. TYPE\_VALUE =/ "LA6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL )
69. TYPE\_VALUE =/ "RA6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
70. TYPE\_VALUE =/ "Name=" STR\_VAL
71. TYPE\_VALUE =/ "Desc=" STR\_VAL
72. TYPE\_VALUE =/ "EmbedCtxt=" STR\_VAL
73. TYPE\_VALUE =/ "Edge=" BOOL\_VAL
74. TYPE\_VALUE =/ "Defer=" DEFER\_VAL
75. TYPE\_VALUE =/ "LSM=" BOOL\_VAL
76. TYPE\_VALUE =/ "Active=" BOOL\_VAL
77. TYPE\_VALUE =/ "ICMP4=" ICMP\_TYPE\_CODE\_VAL
78. TYPE\_VALUE =/ "ICMP6=" ICMP\_TYPE\_CODE\_VAL
79. TYPE\_VALUE =/ "Platform=" PLATFORM\_VAL
80. TYPE\_VALUE =/ "RMauth=" STR\_VAL
81. TYPE\_VALUE =/ "RUAuth=" STR\_VAL
82. TYPE\_VALUE =/ "AuthByPassOut=" BOOL\_VAL
83. TYPE\_VALUE =/ "SkipVer=" VERSION
84. VERSION = MAJOR\_VER "." MINOR\_VER
85. MAJOR\_VER = 1\*3DIGIT
86. MINOR\_VER = 1\*3DIGIT
87. APP\_VAL = 1\*ALPHANUM
88. SVC\_VAL = "\*" / 1\*ALPHANUM
89. STR\_VAL = 1\*ALPHANUM
90. INTERFACES\_VAL = [ \*1INTF\_FIELD / INTF\_FIELD 1\*INTF\_FIELD\_SEQ ]
91. INTF\_FIELD = "{" GUID "}"
92. INTF\_FIELD\_SEQ = "," INTF\_FIELD
93. PHASE1\_AUTH\_METHOD\_VAL = "Anonymous" / "MachineKerb" / "MachineCert"
94. PHASE1\_AUTH\_METHOD\_VAL =/ "MachineSHKey" / "MachineNtlm"
95. PHASE2\_AUTH\_METHOD\_VAL = "Anonymous" / "MachineCert" / "UserKerb"
96. PHASE2\_AUTH\_METHOD\_VAL =/ "UserCert" / "UserNtlm"
97. TIMEOUT\_MIN\_VAL = 1\*8DIGIT
98. TIMEOUT\_SESS\_VAL = 1\*10DIGIT
99. PFS\_VAL = "Disable" / "EnableDHFromPhase1" / "ReKeyDH1" / "ReKeyDH2" / "ReKeyDH2048"
100. PFS\_VAL =/ "ReKeyECDH256" / "ReKeyECDH384"
101. KEY\_EXCHANGE\_VAL = "DH1" / "DH2" / "DH2048" / "ECDH-256" / "ECDH-384"
102. ENCRYPTION\_VAL = "DES" / "3DES" / "AES-128" / "AES-192" / "AES-256"
103. HASH\_VAL = "MD5" / "SHA1"
104. HASH2\_1\_VAL = "SHA256" / "SHA384"
105. PROTOCOL\_VAL = "AH" / "ESP" / "AH&ESP"
106. ENCRYPTION2\_1\_VAL = "AES-GCM128" / "AES-GCM192" / "AES-GCM256"
107. AH\_ESP\_HASH2\_1\_VAL = "SHA256" / "AES-GCM128" / "AES-GCM192" / "AES-GCM256"
108. PROTOCOL2\_9\_VAL = "AUTH\_NO\_ENCAP"
109. CS\_ACTION\_VAL = "SecureServer" / "Boundary" / "Secure" / "DoNotSecure"
110. CSRULE = "v" VERSION "|" 1\*FIELD
111. FIELD = TYPE\_VALUE "|"
112. TYPE\_VALUE = "Action=" CS\_ACTION\_VAL
113. TYPE\_VALUE =/ "Profile=" PROFILE\_VAL
114. TYPE\_VALUE =/ "Protocol=" 1\*3DIGIT ; protocol is maximum 3 digits (255)
115. TYPE\_VALUE =/ "EP1Port=" PORT\_VAL
116. TYPE\_VALUE =/ "EP2Port=" PORT\_VAL
117. TYPE\_VALUE =/ "EP1Port2\_10=" PORT\_RANGE\_VAL
118. TYPE\_VALUE =/ "EP2Port2\_10=" PORT\_RANGE\_VAL
119. TYPE\_VALUE =/ "IF=" IF\_VAL
120. TYPE\_VALUE =/ "IFType=" IFTYPE\_VAL
121. TYPE\_VALUE =/ "Auth1Set=" STR\_VAL
122. TYPE\_VALUE =/ "Auth2Set=" STR\_VAL
123. TYPE\_VALUE =/ "Crypto2Set=" STR\_VAL
124. TYPE\_VALUE =/ "EP1\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
125. TYPE\_VALUE =/ "EP2\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
126. TYPE\_VALUE =/ "EP1\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
127. TYPE\_VALUE =/ "EP2\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
128. TYPE\_VALUE =/ "Name=" STR\_VAL
129. TYPE\_VALUE =/ "Desc=" STR\_VAL
130. TYPE\_VALUE =/ "EmbedCtxt=" STR\_VAL
131. TYPE\_VALUE =/ "Active=" BOOL\_VAL
132. TYPE\_VALUE =/ "Platform=" PLATFORM\_VAL
133. TYPE\_VALUE =/ "SkipVer=" VERSION
134. TYPE\_VALUE =/ "Platform2=" PLATFORM\_OP\_VAL
135. TYPE\_VALUE =/ "SecureInClearOut=" BOOL\_VAL
136. TYPE\_VALUE =/ "ByPassTunnel=" BOOL\_VAL
137. TYPE\_VALUE =/ "Authz=" BOOL\_VAL
138. TYPE\_VALUE =/ "RTunnel4=" ADDRV4
139. TYPE\_VALUE =/ "RTunnel6=" ADDRV6
140. TYPE\_VALUE =/ "LTunnel4=" ADDRV4
141. TYPE\_VALUE =/ "LTunnel6=" ADDRV6
142. TYPE\_VALUE =/ "RTunnel4\_2=" ADDRV4
143. TYPE\_VALUE =/ "RTunnel6\_2=" ADDRV6
144. TYPE\_VALUE =/ "LTunnel4\_2=" ADDRV4
145. TYPE\_VALUE =/ "LTunnel6\_2=" ADDRV6
146. MMRULE = "v" VERSION "|" 1\*FIELD
147. FIELD = TYPE\_VALUE "|"
148. TYPE\_VALUE =/ "Profile=" PROFILE\_VAL
149. TYPE\_VALUE =/ "Auth1Set=" STR\_VAL
150. TYPE\_VALUE =/ "Crypto1Set=" STR\_VAL
151. TYPE\_VALUE =/ "EP1\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
152. TYPE\_VALUE =/ "EP2\_4=" ( ADDRESSV4\_RANGE\_VAL / ADDRESSV4\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
153. TYPE\_VALUE =/ "EP1\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
154. TYPE\_VALUE =/ "EP2\_6=" ( ADDRESSV6\_RANGE\_VAL / ADDRESSV6\_SUBNET\_VAL / ADDRESS\_KEYWORD\_VAL )
155. TYPE\_VALUE =/ "Name=" STR\_VAL
156. TYPE\_VALUE =/ "Desc=" STR\_VAL
157. TYPE\_VALUE =/ "EmbedCtxt=" STR\_VAL
158. TYPE\_VALUE =/ "Active=" BOOL\_VAL
159. TYPE\_VALUE =/ "Platform=" PLATFORM\_VAL
160. TYPE\_VALUE =/ "SkipVer=" VERSION

# Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

* A document revision that incorporates changes to interoperability requirements or functionality.
* The removal of a document from the documentation set.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the technical content of the document is identical to the last released version.

Major and minor changes can be described further using the following change types:

* New content added.
* Content updated.
* Content removed.
* New product behavior note added.
* Product behavior note updated.
* Product behavior note removed.
* New protocol syntax added.
* Protocol syntax updated.
* Protocol syntax removed.
* New content added due to protocol revision.
* Content updated due to protocol revision.
* Content removed due to protocol revision.
* New protocol syntax added due to protocol revision.
* Protocol syntax updated due to protocol revision.
* Protocol syntax removed due to protocol revision.
* Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

* **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
* **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

| Section | Tracking number (if applicable) and description | Major change (Y or N) | Change type |
| --- | --- | --- | --- |
| [2.2.2.19](#Section_2efe0b767b4a41ff90501023f8196d16) Firewall Rule and the Firewall Rule Grammar Rule | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [2.2.6.2](#Section_885f236b39f54a83bac83c5459e88a9a) Connection Security Rule and the Connection Security Rule Grammar Rule | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [6](#Section_3b205aa6975b439389fbda56a971598f) Appendix A: Product Behavior | Updated product behavior notes for Windows 10 and Windows Server 2016 Technical Preview. | Y | Product behavior note updated. |
| 6 Appendix A: Product Behavior | Added Windows 10 to applicability list. | Y | Content update. |

# Index

**A**

[ABNF grammars](#section_cc6fa99b2d054810a1b42063889b3785) 85

Abstract data model

[administrative plug-in](#section_11ea3ad7cad0434b87bc66b3578f0dd1) 65

[client](#section_2f7a01d0bdde43f193f308475323edce) 67

[Action tokens](#section_20c71cdf5e6d4709a6138485cb746134) 19

[Address keyword rules](#section_b8f635e9910147f9a0b9f9bb02cfb8b5) 22

Administrative plug-in

[abstract data model](#section_11ea3ad7cad0434b87bc66b3578f0dd1) 65

[higher-layer triggered events](#section_604200400565443dabeb76461358528c) 65

[initialization](#section_1bf4f10d3b8d4a53bde6e691b670a25c) 65

[local events](#section_044626ad524b40bf856c5804e4a36ef1) 67

message processing

[overview](#section_39cc067fccac4da4bb7da42c3b08407e) 66

policy administration

[load message sequencing](#section_9e8ca48ef23744a8892f93cd83964044) 66

[update message sequencing](#section_4c9891c9ea48423da58ee5f70a9a4016) 66

[overview](#section_12ccb8222e2842c2bcf57d149e68af19) 65

sequencing rules

[overview](#section_39cc067fccac4da4bb7da42c3b08407e) 66

policy administration

[load message sequencing](#section_9e8ca48ef23744a8892f93cd83964044) 66

[update message sequencing](#section_4c9891c9ea48423da58ee5f70a9a4016) 66

[timer events](#section_97b9c59bcfb9478a8f5004b4cd47ba84) 67

[timers](#section_6895bbd0c6c746f9ac333a78adbbf10f) 65

Allow

[authenticated applications user preference merge](#section_d2c56e4bfb684f0abfac44ec8532c8b6) 34

[globally open ports user preference merge](#section_e032e09eacce49899dc5f42a9913ab0e) 34

[local firewall rule policy merge](#section_2c979624900a4b6eb4ef09b387cd62ab) 34

[local IPsec policy merge](#section_8df03d27ae4e46d5b7b92fc3056ba8fd) 35

[Applicability](#section_209aa10f7c5845f692f80a29eae428b1) 12

Authentication

[set messages example](#section_82e1037c2e0a4918baa227b80bf1f781) 70

[sets](#section_5a63628bdb8144ca8a7bdfc4458c6022) 36

[Authentication Sets message](#section_5a63628bdb8144ca8a7bdfc4458c6022) 36

**B**

[Boolean rules](#section_2bdb10546ea04b088e51513f7a758011) 22

**C**

[Capability negotiation](#section_4e3a2af7642b46aca2536d530db323c8) 12

[Certificate revocation list check](#section_c312ded50b2c43edb4db14420fcd6530) 15

[Change tracking](#section_1c4ac237e0a14494945ada8089c8fa1d) 89

Client

[abstract data model](#section_2f7a01d0bdde43f193f308475323edce) 67

[higher-layer triggered events](#section_1135aaae031743b8b427d0e1d71238b6) 67

[initialization](#section_9456019985a64cb9b79828c4ee1c2431) 67

[local events - policy application](#section_d12c1900a915432db812fe84971eaa94) 68

[message processing](#section_e881218ee0744be081c705cc9b3e732c) 67

[sequencing rules](#section_e881218ee0744be081c705cc9b3e732c) 67

[timer events](#section_8d5ed08dcbfa4917b6eabe85e6bbf6b4) 67

[timers](#section_1ec0ee8ca08f44a19c1a58866169e31e) 67

[Configuration options messages example](#section_c1bd84228d0c45e18cb3d4f4aeed9b79) 69

Connection security

[action tokens](#section_a41d8e9967c842ca9344011bf1a9ef41) 56

[rule](#section_885f236b39f54a83bac83c5459e88a9a) 56

[rule grammar rule](#section_885f236b39f54a83bac83c5459e88a9a) 56

[rule message example](#section_bcabd549c6f4401cbd65e3488620565e) 69

[rule messages](#section_9c1bd02f755e4783af0c5c2ecb8bc5a0) 56

[Connection Security Rule Messages message](#section_9c1bd02f755e4783af0c5c2ecb8bc5a0) 56

[Cryptographic sets](#section_c89c075873f84be8b902a48cf0198a68) 44

[Cryptographic Sets message](#section_c89c075873f84be8b902a48cf0198a68) 44

**D**

Data model - abstract

[administrative plug-in](#section_11ea3ad7cad0434b87bc66b3578f0dd1) 65

[client](#section_2f7a01d0bdde43f193f308475323edce) 67

Default

[inbound action](#section_5f0dde47643145618bac2efe8465f1e3) 36

[outbound action](#section_bccac98d197349d09100aceb3bf557df) 35

Description

[authentication sets](#section_5fe0fe2d0e4546fd8674440844d2c450) 38

[cryptographic sets](#section_db1ddfc9c3aa447b823991a3164c107c) 46

[Direction tokens](#section_32d37578740140c287028584bc7c7c23) 18

Disable

[inbound notifications](#section_b84a7360e8644df79fcb249461fbb23a) 33

stateful

[FTP](#section_acb214f8e2c845b6b1ba0d902ca40eb6) 13

[PPTP](#section_15e30d4e01394ca7aff138546b3971ab) 13

[stealth mode](#section_e0e681d304684796b541c5f9945041d8) 31

[unicast responses to multicast and broadcast traffic](#section_ce0afeb1d9fb4e8cb79722991ebd6658) 31

[Disabled interfaces](#section_7a2c97daf6de419f99bd5286cb6a3e61) 35

**E**

[Edge defer rules](#section_af98f4a157484516b04b95af4acee566) 22

EmbeddedContext

[authentication sets](#section_fbe9023d6e2b44768d48f7ae1f02378e) 38

[cryptographic sets](#section_317eb9eea9414eea94bbbf4cfd6d3483) 46

[Enable firewall](#section_2100c5527f374a7f9fa02a864ab87212) 30

Examples

[authentication set messages](#section_82e1037c2e0a4918baa227b80bf1f781) 70

[configuration options messages](#section_c1bd84228d0c45e18cb3d4f4aeed9b79) 69

[connection security rule message](#section_bcabd549c6f4401cbd65e3488620565e) 69

[firewall rule message](#section_2889ae25f3294462a295dbb15bcc186a) 69

**F**

[Fields - vendor-extensible](#section_a3d0864714ff4ea5b3325b9927d6e0f2) 12

Firewall

[rule](#section_2efe0b767b4a41ff90501023f8196d16) 24

[rule grammar rule](#section_2efe0b767b4a41ff90501023f8196d16) 24

[rule message example](#section_2889ae25f3294462a295dbb15bcc186a) 69

[rule messages](#section_4c194907125349fd8642fa58260c40a1) 17

[Firewall Rule Messages message](#section_4c194907125349fd8642fa58260c40a1) 17

[Full ABNF grammars](#section_cc6fa99b2d054810a1b42063889b3785) 85

**G**

[Global policy configuration options](#section_48e60b2e345645a4af40c77711bd6398) 13

[Global Policy Configuration Options message](#section_48e60b2e345645a4af40c77711bd6398) 13

[Glossary](#section_92bc46e53a7c4df7ac422c6b901f519c) 7

**H**

Higher-layer triggered events

[administrative plug-in](#section_604200400565443dabeb76461358528c) 65

[client](#section_1135aaae031743b8b427d0e1d71238b6) 67

**I**

[ICMP type code rules](#section_c3032c754a3a43abac85b8e723697635) 23

[IfSecure tokens](#section_bf0c0257cda542e2bd981c7173c875a7) 19

[Implementer - security considerations](#section_660eda77ad8f40ce9164f00b65dc2458) 82

[Index of security parameters](#section_cfa68b80a9a740c5b198a48085bcbb3a) 82

[Informative references](#section_4974785c919542be8bff0639a364de6e) 9

Initialization

[administrative plug-in](#section_1bf4f10d3b8d4a53bde6e691b670a25c) 65

[client](#section_9456019985a64cb9b79828c4ee1c2431) 67

[Interface types](#section_b75134ac1cc94f619553bfe49c5cf1a9) 19

[Interfaces](#section_c8c7544367364e79bef57a372c3d696d) 19

[Introduction](#section_d09e86381d4344cf97f06b52378ce987) 7

IPsec

[exemptions](#section_483b655210fb4eaa8cf368ee07b55ced) 14

[through NATs](#section_bd06c6ece0d141038e7790777112ff75) 15

IPV4 address

[range rules](#section_4f7cdd39d47d4963b0a784f739e8d53f) 20

[subnet rules](#section_32f9f12df3ee4db390ef0ccb2b794af8) 20

IPV6 address

[range rules](#section_07c718846d5b4422bb71bc14647a5f65) 21

[subnet rules](#section_43f8de90bd3049f884305a0b896cf4df) 21

**L**

Local events

[administrative plug-in](#section_044626ad524b40bf856c5804e4a36ef1) 67

[client - policy application](#section_d12c1900a915432db812fe84971eaa94) 68

Log

[dropped packets](#section_1726ae365ec8401ab716a8dd38218b41) 32

[file path](#section_e3c69589ae5345bb83553084c1f3d481) 33

[ignored rules](#section_425b411736e44828a1f6c884b0c646fe) 32

[successful connections](#section_58ce0d4aea6d4738a75344f8a0cf002b) 32

**M**

Main mode

[rule](#section_35c464bee8b04a2ea1fa1bfffce2d117) 62

[rule grammar rule](#section_35c464bee8b04a2ea1fa1bfffce2d117) 62

[rule messages](#section_e8bbe80b3de14816be9188f4068b601d) 62

[Main Mode Rule Messages message](#section_e8bbe80b3de14816be9188f4068b601d) 62

[Maximum log file size](#section_067ce0bfd98444cb88b502725378eee1) 33

Message processing

administrative plug-in

[overview](#section_39cc067fccac4da4bb7da42c3b08407e) 66

policy administration

[load message sequencing](#section_9e8ca48ef23744a8892f93cd83964044) 66

[update message sequencing](#section_4c9891c9ea48423da58ee5f70a9a4016) 66

[client](#section_e881218ee0744be081c705cc9b3e732c) 67

Messages

[action tokens](#section_20c71cdf5e6d4709a6138485cb746134) 19

[address keyword rules](#section_b8f635e9910147f9a0b9f9bb02cfb8b5) 22

allow

[authenticated applications user preference merge](#section_d2c56e4bfb684f0abfac44ec8532c8b6) 34

[globally open ports user preference merge](#section_e032e09eacce49899dc5f42a9913ab0e) 34

[local firewall rule policy merge](#section_2c979624900a4b6eb4ef09b387cd62ab) 34

[local IPsec policy merge](#section_8df03d27ae4e46d5b7b92fc3056ba8fd) 35

[Authentication Sets](#section_5a63628bdb8144ca8a7bdfc4458c6022) 36

[Boolean rules](#section_2bdb10546ea04b088e51513f7a758011) 22

[certificate revocation list check](#section_c312ded50b2c43edb4db14420fcd6530) 15

connection security

[action tokens](#section_a41d8e9967c842ca9344011bf1a9ef41) 56

[rule](#section_885f236b39f54a83bac83c5459e88a9a) 56

[rule grammar rule](#section_885f236b39f54a83bac83c5459e88a9a) 56

[rule messages](#section_9c1bd02f755e4783af0c5c2ecb8bc5a0) 56

[Connection Security Rule Messages](#section_9c1bd02f755e4783af0c5c2ecb8bc5a0) 56

[Cryptographic Sets](#section_c89c075873f84be8b902a48cf0198a68) 44

default

[inbound action](#section_5f0dde47643145618bac2efe8465f1e3) 36

[outbound action](#section_bccac98d197349d09100aceb3bf557df) 35

description

[authentication sets](#section_5fe0fe2d0e4546fd8674440844d2c450) 38

[cryptographic sets](#section_db1ddfc9c3aa447b823991a3164c107c) 46

[direction tokens](#section_32d37578740140c287028584bc7c7c23) 18

disable

[inbound notifications](#section_b84a7360e8644df79fcb249461fbb23a) 33

stateful

[FTP](#section_acb214f8e2c845b6b1ba0d902ca40eb6) 13

[PPTP](#section_15e30d4e01394ca7aff138546b3971ab) 13

[stealth mode](#section_e0e681d304684796b541c5f9945041d8) 31

[unicast responses to multicast and broadcast traffic](#section_ce0afeb1d9fb4e8cb79722991ebd6658) 31

[disabled interfaces](#section_7a2c97daf6de419f99bd5286cb6a3e61) 35

[edge defer rules](#section_af98f4a157484516b04b95af4acee566) 22

EmbeddedContext

[authentication sets](#section_fbe9023d6e2b44768d48f7ae1f02378e) 38

[cryptographic sets](#section_317eb9eea9414eea94bbbf4cfd6d3483) 46

[enable firewall](#section_2100c5527f374a7f9fa02a864ab87212) 30

firewall

[rule](#section_2efe0b767b4a41ff90501023f8196d16) 24

[rule grammar rule](#section_2efe0b767b4a41ff90501023f8196d16) 24

[rule messages](#section_4c194907125349fd8642fa58260c40a1) 17

[Firewall Rule Messages](#section_4c194907125349fd8642fa58260c40a1) 17

[Global Policy Configuration Options](#section_48e60b2e345645a4af40c77711bd6398) 13

[ICMP type code rules](#section_c3032c754a3a43abac85b8e723697635) 23

[IfSecure tokens](#section_bf0c0257cda542e2bd981c7173c875a7) 19

[interface types](#section_b75134ac1cc94f619553bfe49c5cf1a9) 19

[interfaces](#section_c8c7544367364e79bef57a372c3d696d) 19

IPsec

[exemptions](#section_483b655210fb4eaa8cf368ee07b55ced) 14

[through NATs](#section_bd06c6ece0d141038e7790777112ff75) 15

IPV4 address

[range rules](#section_4f7cdd39d47d4963b0a784f739e8d53f) 20

[subnet rules](#section_32f9f12df3ee4db390ef0ccb2b794af8) 20

IPV6 address

[range rules](#section_07c718846d5b4422bb71bc14647a5f65) 21

[subnet rules](#section_43f8de90bd3049f884305a0b896cf4df) 21

log

[dropped packets](#section_1726ae365ec8401ab716a8dd38218b41) 32

[file path](#section_e3c69589ae5345bb83553084c1f3d481) 33

[ignored rules](#section_425b411736e44828a1f6c884b0c646fe) 32

[successful connections](#section_58ce0d4aea6d4738a75344f8a0cf002b) 32

main mode

[rule](#section_35c464bee8b04a2ea1fa1bfffce2d117) 62

[rule grammar rule](#section_35c464bee8b04a2ea1fa1bfffce2d117) 62

[rule messages](#section_e8bbe80b3de14816be9188f4068b601d) 62

[Main Mode Rule Messages](#section_e8bbe80b3de14816be9188f4068b601d) 62

[maximum log file size](#section_067ce0bfd98444cb88b502725378eee1) 33

name

[authentication sets](#section_15d6267187334fe4915307f96d03e7f2) 37

[cryptographic sets](#section_b285461e250a443aab392d0dad8feea7) 45

[Per-Profile Policy Configuration Options](#section_abe4eb0fe3a048ccbde35dc89b81b40b) 30

phase 1

[do not skip Deffie Hellman](#section_8c9e2bed4fda4a08a19c250e380a6743) 46

[suite keys](#section_f6db07d4951c414391545b2974284ff8) 48

[time out in minutes](#section_011876a587ae4711b597e8b2cdfc2a8f) 46

[time out in sessions](#section_90a94a58aad04febbf6d9e066ecbcb19) 47

phase 1 auth suite

[certificate account mapping](#section_74a8294109964c1ca9942bbed2f9a5a8) 40

[certificate authority names](#section_c77199d8e01d4e0d9dce14fda4ffe0df) 39

[exclude CA name](#section_362a1bfb72b94a2f90e0d5b66ff1c68d) 40

[health cert](#section_80cd9769955d4cd1a8cbdb7b93078387) 40

[intermediate CA](#section_3ecf1f1bdc5a4c97a5bba3e6354e4765) 42

[methods](#section_a6ed36beb3de43ccbe8fcdf56616a33f) 38

[other certificate signing](#section_47cc2759fe50464c92872ac58fd42dfb) 41

[preshared key](#section_93b10090bcbb49a689d8793bf522e6ea) 40

[skip version](#section_ea14c4ee0f1a47c4ad4923a6555a4122) 41

phase 1 suite

[2.1 hash algorithm](#section_4dd68cc5ef7f4703815482c91c9111b0) 50

[encryption algorithm](#section_fd1455f1f8774460ae4eb4342944e065) 49

[hash algorithm](#section_e07275e9e351491b803dc2c1fb544ddd) 49

[key exchange algorithm](#section_59df1def474f4f4c95395e664d5238e2) 48

[skip version](#section_8bf1979d613e443fa7fb6af182d78d89) 50

phase 2

[perfect forward secrecy](#section_6053e57e20624261b92cdea714b7ab50) 47

[suite keys](#section_f5d484d26d164a9bafe8dbe6b2671c31) 51

phase 2 auth suite

[certificate account mapping](#section_74a8294109964c1ca9942bbed2f9a5a8) 40

[certificate authority names](#section_c77199d8e01d4e0d9dce14fda4ffe0df) 39

[health cert](#section_80cd9769955d4cd1a8cbdb7b93078387) 40

[intermediate CA](#section_3ecf1f1bdc5a4c97a5bba3e6354e4765) 42

[methods](#section_a6ed36beb3de43ccbe8fcdf56616a33f) 38

[other certificate signing](#section_47cc2759fe50464c92872ac58fd42dfb) 41

[preshared key](#section_93b10090bcbb49a689d8793bf522e6ea) 40

[skip version](#section_ea14c4ee0f1a47c4ad4923a6555a4122) 41

phase 2 suite

[2.1 AH hash algorithm](#section_deb0f275e34f4ac593870e588f90d084) 54

[2.1 encryption algorithm](#section_b4003406103c43c1b498c3172767b320) 53

[2.1 ESP hash algorithm](#section_ae16e0f304f747838f5d90c52a40d7c5) 54

[2.9 protocol](#section_8c4fa272f8ed43a59ecb7f7cce3e47a1) 55

[AH protocol hash algorithm](#section_3fcf0447d9d445eb851bac21387319b8) 52

[encryption algorithm](#section_3f4418116c6945f38607cc490e9b587c) 52

[ESP protocol hash algorithm](#section_cf731c13803645d382c20b5fde8319f4) 52

[protocol](#section_16f08224cb984e158a301500e1e52d95) 51

[skip version](#section_b223a837c0bb47b095bfbf7b9e3fbd29) 53

[time out in kilobytes](#section_01ba85fec3bb4edb9cfdcb1c6e37b2e0) 53

[time out in minutes](#section_1109661d1bd444e4bd54dd1bbdfccaed) 52

platform validity

[operators rules](#section_d72b6779e2d843cf93e49cd6d95f8937) 23

[rules](#section_b69c1aea027d45edb362797f04441649) 23

[policy version](#section_15ab2dd9cbb34450a4591759aa20e9f7) 15

[port and port range rules](#section_0d077a8f49c445bf9080dd8b68285126) 18

[port keyword rules](#section_304ed01752664600b8f2c38fa17984b4) 18

[preshared key encoding](#section_c61edb2f4b954d6ea6f2e22e8ea692d5) 14

[profile tokens](#section_f614b363140b4ea7bc71e55f4e382993) 17

[security associations idle time](#section_89407952862b4415879c9e9e4b4c16de) 14

[shield up mode](#section_6cf6175225224f83864c71357a1249db) 31

[suite keys](#section_647fb1e7a6ac41c4bff0e8c25d440ea9) 38

[transport](#section_bfcb5d5087694dc0880c43322fa881ce) 13

tunnel remote

[machine authorization list](#section_859001baa20a48788a45a0fc88b0a9b2) 16

[user authorization list](#section_9aec6dbaf5ae4a53b4debd58fffa9813) 16

version

[authentication sets](#section_e017c13fa8ef49348356486b6a214a0a) 37

[cryptographic sets](#section_dded7724b5ce457782b461093aa8b7ed) 45

**N**

Name

[authentication sets](#section_15d6267187334fe4915307f96d03e7f2) 37

[cryptographic sets](#section_b285461e250a443aab392d0dad8feea7) 45

[Normative references](#section_6a938c80c2494383a59246681b634f16) 8

**O**

Overview

[background](#section_c2a9ef4cf03348a0af734ccaadc129af) 9

[firewall and advanced security extension encoding](#section_11efd46c2b934cb59a5d7da2f35da86d) 9

[synopsis](#section_06b136f262fe4f57b6c623d758522763) 9

[Overview (synopsis)](#section_06b136f262fe4f57b6c623d758522763) 9

**P**

[Parameters - security index](#section_cfa68b80a9a740c5b198a48085bcbb3a) 82

[Per-profile policy configuration options](#section_abe4eb0fe3a048ccbde35dc89b81b40b) 30

[Per-Profile Policy Configuration Options message](#section_abe4eb0fe3a048ccbde35dc89b81b40b) 30

Phase 1

[do not skip Deffie Hellman](#section_8c9e2bed4fda4a08a19c250e380a6743) 46

[suite keys](#section_f6db07d4951c414391545b2974284ff8) 48

[time out in minutes](#section_011876a587ae4711b597e8b2cdfc2a8f) 46

[time out in sessions](#section_90a94a58aad04febbf6d9e066ecbcb19) 47

Phase 1 auth suite

[certificate account mapping](#section_74a8294109964c1ca9942bbed2f9a5a8) 40

[certificate authority names](#section_c77199d8e01d4e0d9dce14fda4ffe0df) 39

[exclude CA name](#section_362a1bfb72b94a2f90e0d5b66ff1c68d) 40

[health cert](#section_80cd9769955d4cd1a8cbdb7b93078387) 40

[intermediate CA](#section_3ecf1f1bdc5a4c97a5bba3e6354e4765) 42

[methods](#section_a6ed36beb3de43ccbe8fcdf56616a33f) 38

[other certificate signing](#section_47cc2759fe50464c92872ac58fd42dfb) 41

[preshared key](#section_93b10090bcbb49a689d8793bf522e6ea) 40

[skip version](#section_ea14c4ee0f1a47c4ad4923a6555a4122) 41

Phase 1 suite

[2.1 hash algorithm](#section_4dd68cc5ef7f4703815482c91c9111b0) 50

[encryption algorithm](#section_fd1455f1f8774460ae4eb4342944e065) 49

[hash algorithm](#section_e07275e9e351491b803dc2c1fb544ddd) 49

[key exchange algorithm](#section_59df1def474f4f4c95395e664d5238e2) 48

[skip version](#section_8bf1979d613e443fa7fb6af182d78d89) 50

Phase 2

[perfect forward secrecy](#section_6053e57e20624261b92cdea714b7ab50) 47

[suite keys](#section_f5d484d26d164a9bafe8dbe6b2671c31) 51

Phase 2 auth suite

[certificate account mapping](#section_74a8294109964c1ca9942bbed2f9a5a8) 40

[certificate authority names](#section_c77199d8e01d4e0d9dce14fda4ffe0df) 39

[health cert](#section_80cd9769955d4cd1a8cbdb7b93078387) 40

[intermediate CA](#section_3ecf1f1bdc5a4c97a5bba3e6354e4765) 42

[methods](#section_a6ed36beb3de43ccbe8fcdf56616a33f) 38

[other certificate signing](#section_47cc2759fe50464c92872ac58fd42dfb) 41

[preshared key](#section_93b10090bcbb49a689d8793bf522e6ea) 40

[skip version](#section_ea14c4ee0f1a47c4ad4923a6555a4122) 41

Phase 2 suite

[2.1 AH hash algorithm](#section_deb0f275e34f4ac593870e588f90d084) 54

[2.1 encryption algorithm](#section_b4003406103c43c1b498c3172767b320) 53

[2.1 ESP hash algorithm](#section_ae16e0f304f747838f5d90c52a40d7c5) 54

[2.9 protocol](#section_8c4fa272f8ed43a59ecb7f7cce3e47a1) 55

[AH protocol hash algorithm](#section_3fcf0447d9d445eb851bac21387319b8) 52

[encryption algorithm](#section_3f4418116c6945f38607cc490e9b587c) 52

[ESP protocol hash algorithm](#section_cf731c13803645d382c20b5fde8319f4) 52

[protocol](#section_16f08224cb984e158a301500e1e52d95) 51

[skip version](#section_b223a837c0bb47b095bfbf7b9e3fbd29) 53

[time out in kilobytes](#section_01ba85fec3bb4edb9cfdcb1c6e37b2e0) 53

[time out in minutes](#section_1109661d1bd444e4bd54dd1bbdfccaed) 52

Platform validity

[operators rules](#section_d72b6779e2d843cf93e49cd6d95f8937) 23

[rules](#section_b69c1aea027d45edb362797f04441649) 23

[Policy version](#section_15ab2dd9cbb34450a4591759aa20e9f7) 15

[Port and port range rules](#section_0d077a8f49c445bf9080dd8b68285126) 18

[Port keyword rules](#section_304ed01752664600b8f2c38fa17984b4) 18

[Preconditions](#section_1a26b6be53754ababed2f8478968cbec) 11

[Prerequisites](#section_1a26b6be53754ababed2f8478968cbec) 11

[Preshared key encoding](#section_c61edb2f4b954d6ea6f2e22e8ea692d5) 14

[Product behavior](#section_3b205aa6975b439389fbda56a971598f) 83

[Profile tokens](#section_f614b363140b4ea7bc71e55f4e382993) 17

**R**

[References](#section_4ff40c8570014385bfa7111ed627c822) 8

[informative](#section_4974785c919542be8bff0639a364de6e) 9

[normative](#section_6a938c80c2494383a59246681b634f16) 8

[Relationship to other protocols](#section_f8909f182a4b4590bdf7320f30e7a6d1) 11

**S**

Security

[implementer considerations](#section_660eda77ad8f40ce9164f00b65dc2458) 82

[parameter index](#section_cfa68b80a9a740c5b198a48085bcbb3a) 82

[Security associations idle time](#section_89407952862b4415879c9e9e4b4c16de) 14

Sequencing rules

administrative plug-in

[overview](#section_39cc067fccac4da4bb7da42c3b08407e) 66

policy administration

[load message sequencing](#section_9e8ca48ef23744a8892f93cd83964044) 66

[update message sequencing](#section_4c9891c9ea48423da58ee5f70a9a4016) 66

[client](#section_e881218ee0744be081c705cc9b3e732c) 67

[Shield up mode](#section_6cf6175225224f83864c71357a1249db) 31

[Standards assignments](#section_963c05dddf8b47e09abbe948be167fec) 12

[Suite keys](#section_647fb1e7a6ac41c4bff0e8c25d440ea9) 38

**T**

Timer events

[administrative plug-in](#section_97b9c59bcfb9478a8f5004b4cd47ba84) 67

[client](#section_8d5ed08dcbfa4917b6eabe85e6bbf6b4) 67

Timers

[administrative plug-in](#section_6895bbd0c6c746f9ac333a78adbbf10f) 65

[client](#section_1ec0ee8ca08f44a19c1a58866169e31e) 67

[Tracking changes](#section_1c4ac237e0a14494945ada8089c8fa1d) 89

[Transport](#section_bfcb5d5087694dc0880c43322fa881ce) 13

Triggered events

[administrative plug-in](#section_604200400565443dabeb76461358528c) 65

[client](#section_1135aaae031743b8b427d0e1d71238b6) 67

Triggered events - higher-layer

[client](#section_1135aaae031743b8b427d0e1d71238b6) 67

Tunnel remote

[machine authorization list](#section_859001baa20a48788a45a0fc88b0a9b2) 16

[user authorization list](#section_9aec6dbaf5ae4a53b4debd58fffa9813) 16

**V**

[Vendor-extensible fields](#section_a3d0864714ff4ea5b3325b9927d6e0f2) 12

Version

[authentication sets](#section_e017c13fa8ef49348356486b6a214a0a) 37

[cryptographic sets](#section_dded7724b5ce457782b461093aa8b7ed) 45

[Versioning](#section_4e3a2af7642b46aca2536d530db323c8) 12