MIS 5214

Weeks 11 & 12

Agenda

- Team Project Presentation Schedule, Deliverables, Presentation timings
- Project Cloud System Security Plan
  - Section 2: Information System Categorization
    - E-Authentication Determination
      - Section 13: Minimum Security Controls
        - Control Baselines
        - Control Classes
          - Technical Control Families
            - Identity and Authentication Technical Control Family
  - Section 8: Information System Type
    - Cloud service models
    - Cloud deployment models
    - Leveraged authorizations
  - Section 13: Minimum Security Controls
      - Control Baselines
      - Control Classes
        - Technical Control Families
- Section 9: Review of Firewall types and IDS/IPS types

Team Project Presentation Schedule

Full Name	Team	Presentation
Lai, Chenhui	1	18-Apr
Liu, Yuan	1	18-Apr
Mu, Richard	1	18-Apr
You, Zirui	1	18-Apr
Chen, Xinteng	2	18-Apr
Huang, Haitao	2	18-Apr
Mays, Jason M.	2	18-Apr
Wang, Yingyan	2	18-Apr
Ahmed, Raisa	3	18-Apr
Roberts, Matthew	3	18-Apr
Wang, Dongjie	3	18-Apr
Yang, Qianru	3	18-Apr
Bonds, Monique O.	4	25-Apr
Chen, Qiyu	4	25-Apr
Rohrer, Frederic D.	4	25-Apr
Sun, Ping	4	25-Apr
Zhou, Hanqing	4	25-Apr
Dong, Xiaomin	5	25-Apr
Jiang, Jing	5	25-Apr
Raju, Jerrin	5	25-Apr
Selvaraju, Jayapreethi	5	25-Apr
Feldman, Joseph E.	6	25-Apr
Li, Yijiang	6	25-Apr
Ntokwane, Karabo	6	25-Apr
Wei, Zhixin	6	25-Apr

Full Name	Team	Date
Billups, Marsha	1	18-Apr
Gibbons, Michael	1	18-Apr
Mackowsky, Brandan	1	18-Apr
Tartaglione, Eugene A.	1	18-Apr
Collura, Michelangelo C.	1	18-Apr
Dong, Shi Yu	2	18-Apr
Greenwood, Fraser	2	18-Apr
Pitter, Tamekia	2	18-Apr
Thomas, Sheena L.	2	18-Apr
Chen, Linlan	3	18-Apr
Gaire, Binju	3	18-Apr
Nelson, Candace T.	3	18-Apr
Yakush, Ruslan I.	3	18-Apr
Tang, Rouying	3	18-Apr
Christian, Tiesha	4	25-Apr
Foggie, James T.	4	25-Apr
Nguyen, Duy N.	4	25-Apr
Toor, Parneet	4	25-Apr
Eidenzon, Tal	4	25-Apr
Butler, Jerry M.	5	25-Apr
Hoxhaj, Donald	5	25-Apr
Quitugua, Anthony	5	25-Apr
DiPentino, Vittorio C.	5	25-Apr
Keshtkar, Somayeh	6	25-Apr
Needle, Paul R.	6	25-Apr
Shirozian, Sevag	6	25-Apr
Cheung, Heiang Y.	6	25-Apr

Team Project Deliverables

Team deliverables: All files put in Team's Google Docs folder

1. Presentation file in PDF – name file with team # system name
   - Print document provided to Prof. Lanter prior to presentation

2. SSP Document in PDF – name file with "SSP" team # and system name

3. Lessons learned document in format (include lessons learned in presentation)
   - What went well
   - What did not go so well
   - What should be done better next time

Individual student deliverable: File put in your personal Google Docs folder

1. 360 degree review – name file with team# and your name
   - What I contributed and how I helped
   - What each other member of my team contributed and helped with

Presentation timings

- 15 minutes for presentation
- 20 minutes for questions and answers
  - Each non-presenting team has 5 minutes to ask questions & identify findings

Table of Contents

Table of Contents

2.3 E-AUTHENTICATION DETERMINATION

The e-Authentication information may be found in section: Section 15 Attachments E-Authentication Level Selection.

Note: Refer to OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies for more information on e-Authentica

e-Authentication Level

The e-authentication level is Choose an item.

Choose an item.
Level 1: Little or no confidence in the asserted identity's validity
Level 2: Some confidence in the asserted identity's validity
Level 3: High confidence in the asserted identity's validity
Level 4: Very high confidence in the asserted identity's validity.

Additional e-Authentication
Authentication Level Selecti

NIST 800 63-3: Digital Identity Guidelines

Table 6-1 Maximum Potential Impacts for Each Assurance Level

	Assurance Level		
Impact Categories	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Mod	High
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

From Week8 – Access Control's lecture

NIST 800-63A

NIST Special Publication 800-63A

Digital Identity Guidelines

Enrollment and Identity Proofing

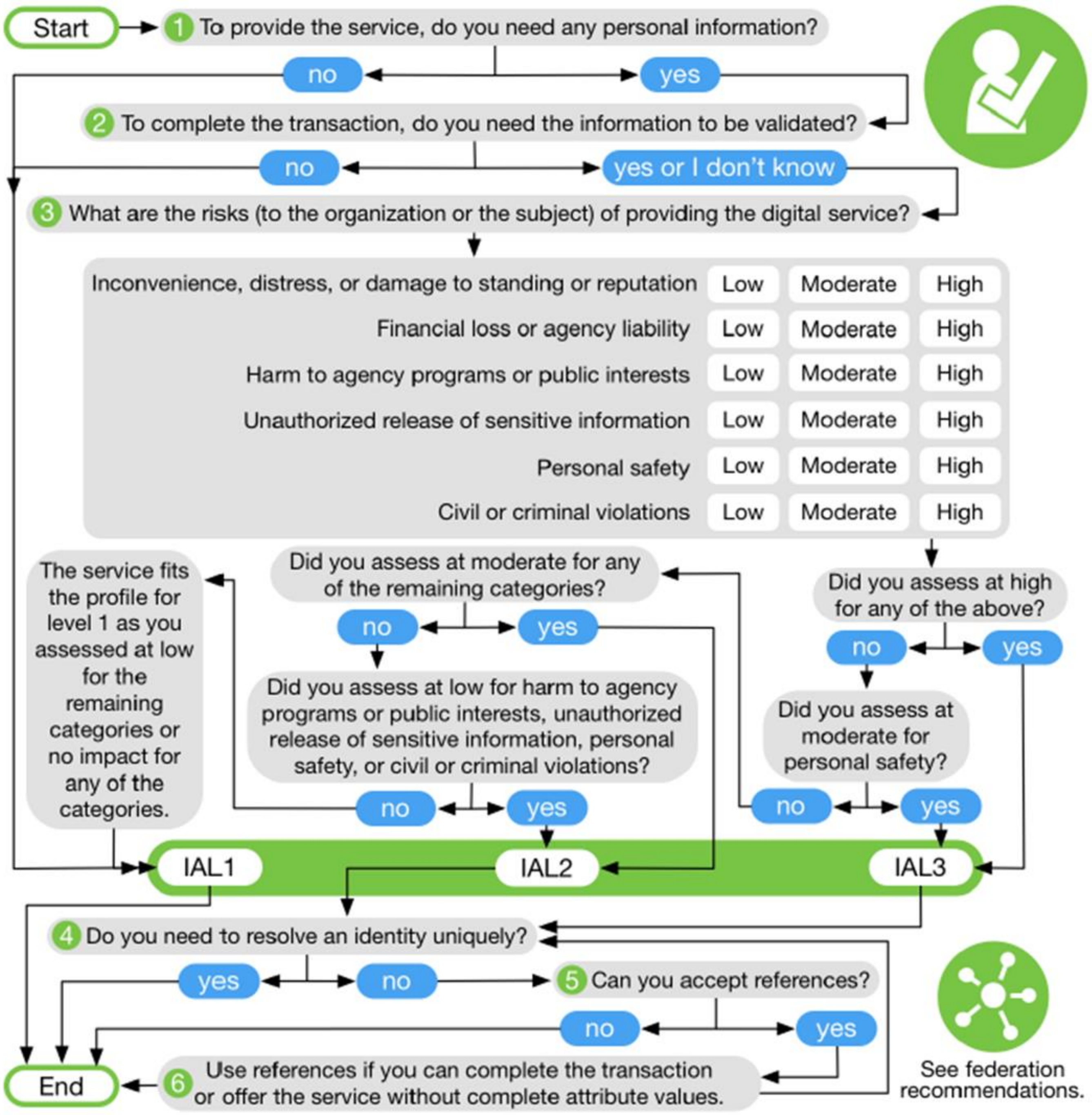
Paul A. Grassi
James L. Fenton

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:

https://doi.org/10.6028/NIST.SP.800-63a



NIST 800-63B

NIST Special Publication 800-63B

Digital Identity Guidelines

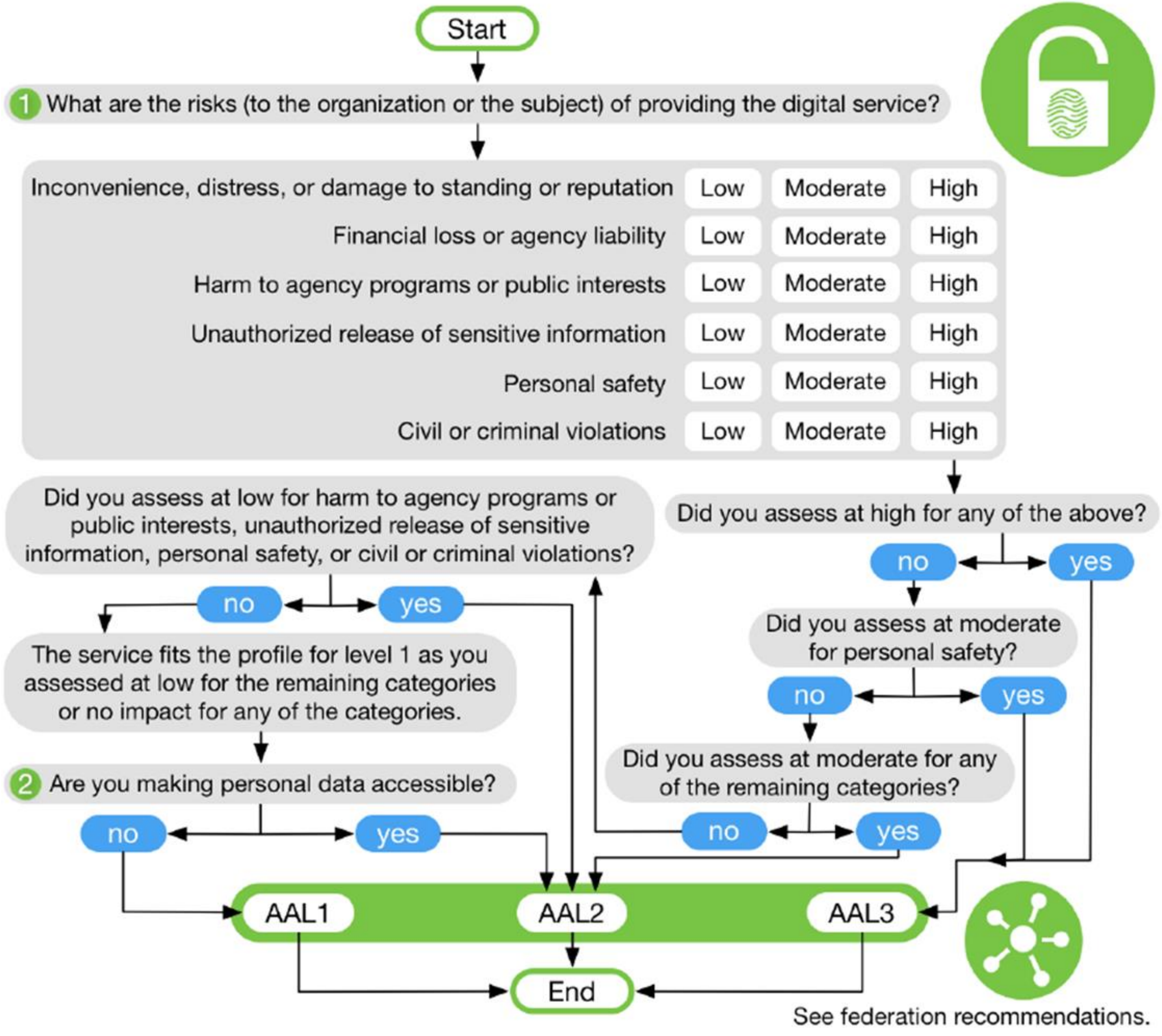
Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

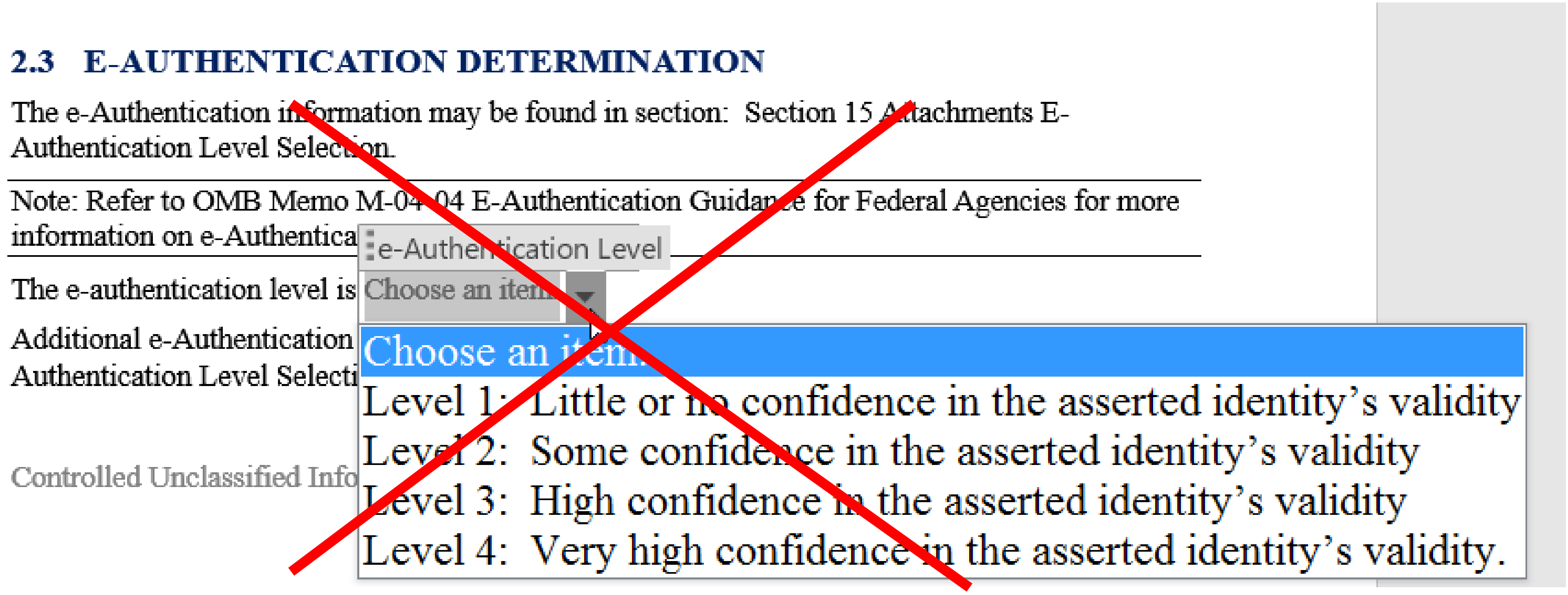
Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b



Replace the single e-authentication level value:



2.3 E-AUTHENTICATION DETERMINATION

The e-Authentication information may be found in section: Section 15 Attachments E-Authentication Level Selection.

Note: Refer to OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies for more information on e-Authentica

e-Authentication Level

The e-authentication level is Choose an item.

Additional e-Authentication
Authentication Level Selecti

Choose an item.
Level 1: Little or no confidence in the asserted identity's validity
Level 2: Some confidence in the asserted identity's validity
Level 3: High confidence in the asserted identity's validity
Level 4: Very high confidence in the asserted identity's validity.

Controlled Unclassified Info

With:

2.3 E-AUTHENTICATION DETERMINATION

Identity Authorization Level is: IAL1 *(or IAL2 or IAL3)*

Authentication Authorization Level is: AAL1 *(or AAL2 or AAL3)*

AAL = Authenticator Assurance Level

AAL1 : = 1 Factor

AAL2 : = 2 Factors

AAL3 : = 2 Factors: Hardware-based authenticator and an authenticator that provides verifier impersonation resistance

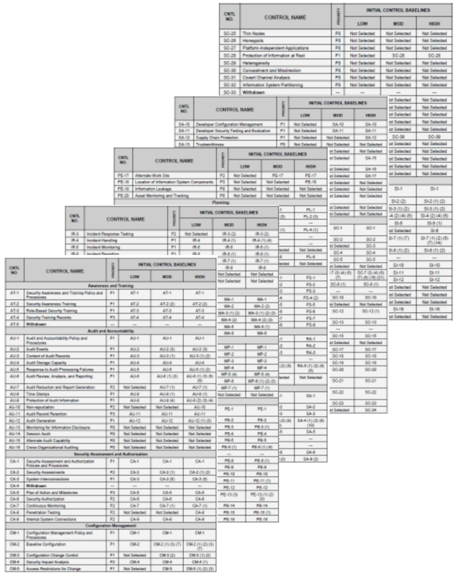
Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM Resistance	Required	Required	Required
Verifier-Impersonation Resistance	Not required	Not required	Required
Verifier-Compromise Resistance	Not required	Not required	Required
Replay Resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
	Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
	Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
	Incident Response				
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)



NIST 800-53R4

13. Minimum Security Controls: *Technical Controls*

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson
Joan Hash
Pauline Bowen

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Identification and Authentication (IA)

Control	Control Name	Control Baseline		
		Low	Moderate	High
IA-1	Identification and Authentication Policy and Procedures	L	M	H
IA-2	Identification and Authentication (Organizational Users)	L (1) (12)	M (5)	H (5)
IA-3	Device Identification and Authentication		M	H
IA-4	Identifier Management	L	M (4)	H (4)
IA-5	Authenticator Management	L (1) (11)	M (4) (6) (7)	H (4) (6) (7) (8) (13)
IA-6	Authenticator Feedback	L	M	H
IA-7	Cryptographic Module Authentication	L	M	H
IA-8	Identification and Authentication (Non-Organizational Users)	L (1) (2) (3) (4)	M	H

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret

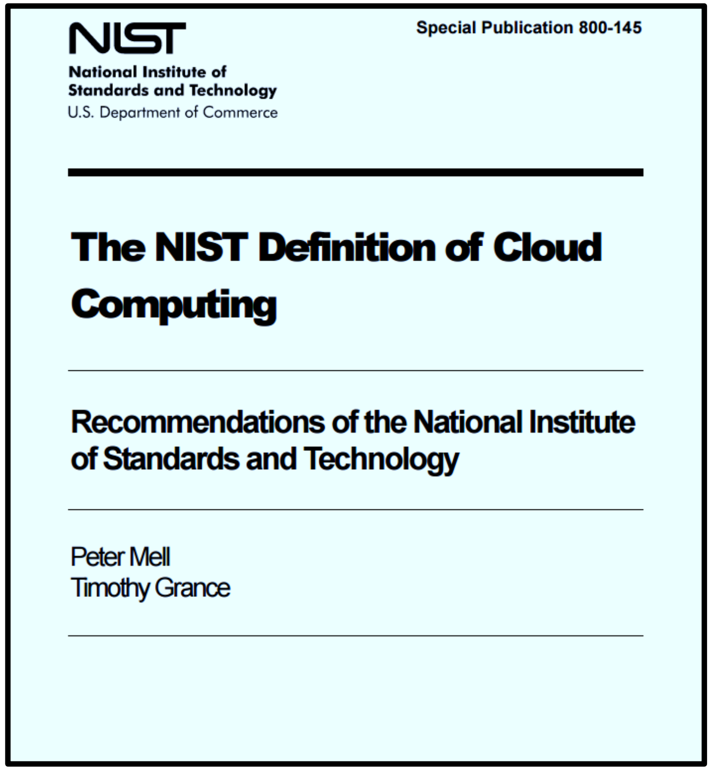
Table of Contents

Cloud computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

NIST's cloud model is composed of:

- 5 essential characteristics
- 3 service models
- 4 deployment models


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

5 Essential Characteristics of Cloud Computing

1. **On-demand self-service**
2. **Broad network access**
3. **Resource pooling**
4. **Rapid elasticity**
5. **Measured service**

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

5 Essential Characteristics of Cloud Computing

1. **On-demand self-service**
2. **Broad network access**
3. **Resource pooling (multi-tenant)**
4. **Rapid elasticity**
5. **Measured service (pay per use, charge per use)**

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3 Service Models of Cloud Computing

1. **Infrastructure as a Service (IaaS)**
2. **Platform as a Service (PaaS)**
3. **Software as a Service (SaaS)**

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Which Service Model(s) of cloud computing is your project's information system providing to your end users?

Table 8-1 Service Layers Represented in this SSP

Service Provider Architecture Layers		
☐	Software as a Service (SaaS)	Major Application
☐	Platform as a Service (PaaS)	Major Application
☐	Infrastructure as a Service (IaaS)	General Support System
☐	Other	Explain: Click here to enter text.

3 Service Models of Cloud Computing

Infrastructure as a Service (IaaS)

Provides processing, storage, networks, and other fundamental computing resources

Consumer is able to deploy and run arbitrary software, which can include operating systems and applications

- The consumer does not manage or control the underlying cloud infrastructure,
  - but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3 Service Models of Cloud Computing

Platform as a Service (PaaS)

Consumer is provided capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider

- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage,
  - but has control over the deployed applications and possibly configuration settings for the application-hosting environment

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3 Service Models of Cloud Computing

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure

- The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

4 Deployment Models of Cloud Computing

1. **Private cloud**
2. **Community cloud**
3. **Public cloud**
4. **Hybrid cloud**

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

4 Deployment Models of Cloud Computing

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units)

- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

4 Deployment Models of Cloud Computing

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)

- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

4 Deployment Models of Cloud Computing

Public cloud

The cloud infrastructure is provisioned for open use by the general public

- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

4 Deployment Models of Cloud Computing

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities

- …but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Which cloud deployment model is your project's information system based on?

8.2 CLOUD DEPLOYMENT MODELS

Information systems are made up of different deployment models. The deployment models of the Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2 Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table 8-2 Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
☐	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
☐	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
☐	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
☐	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

Security Control Inheritance

Security control inheritance exist when

an information system or application receives protection from security controls that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application

- *entities either internal or external to the organization where the system or application resides.*

NIST SP 800-53 Revision 4

Control Inheritance

Many of the controls needed to protect organizational information systems are inheritable by other systems, e.g.

- Security awareness training
- Incident response plans
- Physical access to facilities
- Rules of behavior
- Public Key Infrastructure [PKI]
- Authorized secure standard configurations for clients/servers
- Access control systems
- Boundary protection
- Cross-domain solutions

- By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of inheritable controls, security costs can be amortized across multiple information systems

Leveraged Authorizations (SSP Section 8.3)

Security control implementations can only be inherited (leveraged) from a Cloud Service Offering (CSO) that has been approved and granted a FedRAMP Provisional Authorization to Operate (P-ATO) or an Agency ATO

Table 8-3 Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
<Enter Leveraged information system name1>	<Enter service provider owner1>	<Date>
<Enter Leveraged information system name2>	<Enter service provider owner2>	<Date>
<Enter Leveraged information system name3>	<Enter service provider owner3>	<Date>

Leveraged Security Controls

IA-5 (3)	Control Summary Information
Responsible Role:	
Parameter IA-5(3)-1:	
Parameter IA-5(3)-2:	
Parameter IA-5(3)-3:	
Parameter IA-5(3)-4:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

Leveraged Security Controls

The FedRAMP SSP templates have a section for each control, labeled, "Control Origination"

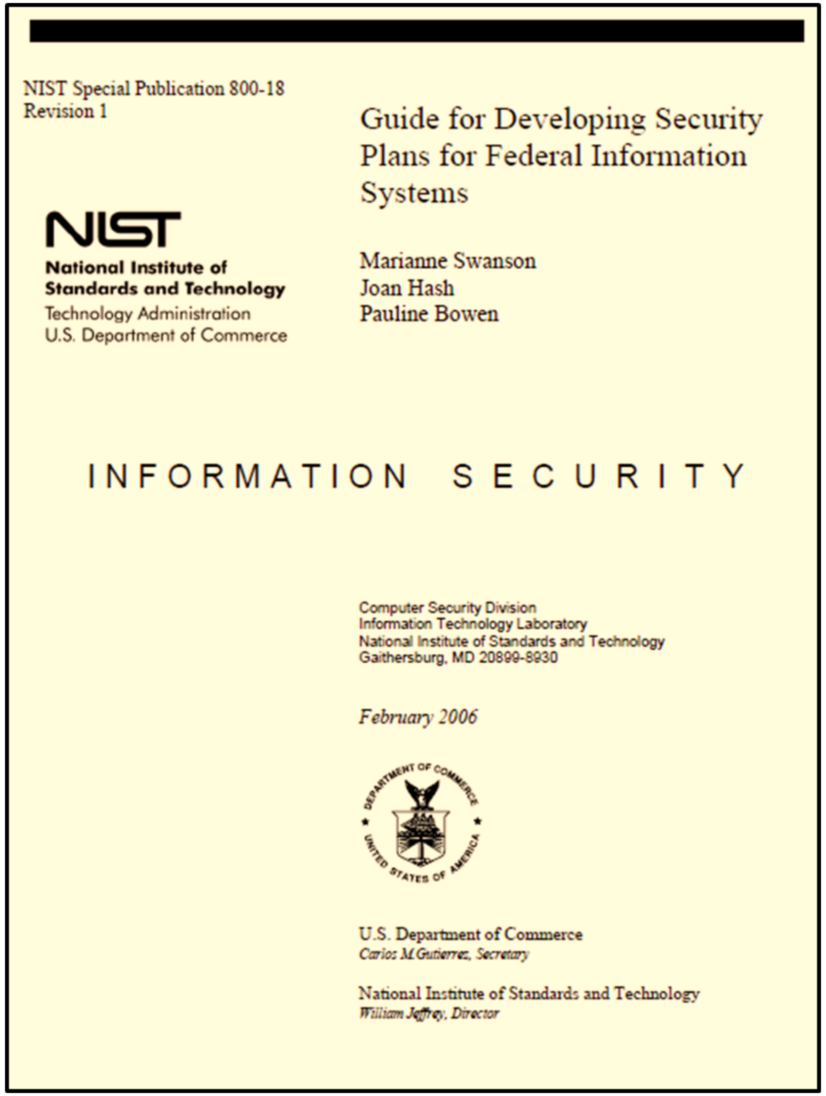
Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization

- The SSP writer should clearly indicate what sections of the security control are inherited and provide a description of what is inherited
- If an entire control is inherited, it must be clear to the Assessor what is inherited
- The writer does not need to describe how the leveraged service is performing the particular function
  - That detail is found in the SSP of the leveraged system from which the control is inherited

If a policy has been published and is referenced as is the basis for the implementation of the inherited security control, make sure that published document is provided as an attachment, or a supporting artifact with the SSP when submitted for FedRAMP review

https://www.fedramp.gov/weekly-tips-cues-february-15-2017/

13. Minimum Security Controls: *Technical Controls*



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Technical Controls

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Identification and Authentication (IA)

Control	Control Name	Control Baseline		
		Low	Moderate	High
IA-1	Identification and Authentication Policy and Procedures	L	M	H
IA-2	Identification and Authentication (Organizational Users)	L **(1) (12)**	M **(5)**	H **(5)**
IA-3	Device Identification and Authentication		M	H
IA-4	Identifier Management	L	M **(4)**	H **(4)**
IA-5	Authenticator Management	L **(1) (11)**	M **(4) (6) (7)**	H **(4) (6) (7) (8) (13)**
IA-6	Authenticator Feedback	L	M	H
IA-7	Cryptographic Module Authentication	L	M	H
IA-8	Identification and Authentication (Non-Organizational Users)	L **(1) (2) (3) (4)**	M	H

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Access Control (AC)

Control	Control Name	Control Baseline		
		Low	Moderate	High
AC-1	Access Control Policy and Procedures	L	M	H
AC-2	Account Management	L	M **(5) (7) (9) (10) (12)**	H **(7) (9)**
AC-3	Access Enforcement	L	M	H
AC-4	Information Flow Enforcement		M **(21)**	H **(8) (21)**
AC-5	Separation of Duties		M	H
AC-6	Least Privilege		M	H **(7) (8)**
AC-7	Unsuccessful Logon Attempts	L	M	H **(2)**
AC-8	System Use Notification	L	M	H
AC-10	Concurrent Session Control		**M AC-10**	H
AC-11	Session Lock		M	H
AC-12	Session Termination		M	H **(1)**
AC-13	Withdrawn			
AC-14	Permitted Actions Without Identification or Authentication	L	M	H
AC-15	Withdrawn			
AC-16	Security Attributes			
AC-17	Remote Access	L	M **(9)**	H **(9)**
AC-18	Wireless Access	L	M	H **(3)**
AC-19	Access Control For Mobile Devices	L	M	H
AC-20	Use of External Information Systems	L	M	H
AC-21	Information Sharing		M	H
AC-22	Publicly Accessible Content		M	H

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Audit and Accountability (AU)

Control	Control Name	Control Baseline		
		Low	Moderate	High
AU-1	Audit and Accountability Policy and Procedures	L	M	H
AU-2	Audit Events	L	M	H
AU-3	Content of Audit Records	L	M	H
AU-4	Audit Storage Capacity	L	M	H
AU-5	Response to Audit Processing Failures	L	M	H
AU-6	Audit Review, Analysis and Reporting		M	H **(4) (7) (10)**
AU-7	Audit Reduction and Report Generation	L	M	H
AU-8	Time Stamps	L	M	H
AU-9	Protection of Audit Information	L	M **(2)**	H
AU-10	Non-repudiation		M	H
AU-11	Audit Record Retention	L	M	H
AU-12	Audit Generation	L	M	H

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

System and Communications Protection

Control	Control Name	Control Baseline		
		Low	Moderate	High
SC-1	System and Communications Protection Policy and Procedures	L	M	H
SC-2	Application Partitioning		M	H
SC-3	Security Function Isolation			H
SC-4	Information in Shared Resources		M	H
SC-5	Denial of Service Protection	L	M	H
SC-6	Resource Availability		**M SC-6**	**H SC-6**
SC-7	Boundary Protection	L	M **(8) (12) (13) (18)**	H **(10) (12) (13) (20)**
SC-8	Transmission Confidentiality and Integrity		M	H
SC-10	Network Disconnect		M	H
SC-12	Cryptographic Key Establishment and Management	L	M **(2) (3)**	H **(2) (3)**
SC-13	Cryptographic Protection	L	M	H
SC-15	Collaborative Computing Devices	L	M	H
SC-17	Public Key Infrastructure Certificates		M	H
SC-18	Mobile Code		M	H
SC-19	Voice Over Internet Protocol		M	H
SC-20	Secure Name /Address Resolution Service (Authoritative Source	L	M	H
SC-21	Secure Name /Address Resolution Service (Recursive or Caching	L	M	H
SC-22	Architecture and Provisioning for Name/Address Resolution Ser	L	M	H
SC-23	Session Authenticity		M	H **(1)**
SC-24	Fail in Known State			H
SC-28	Protection of Information at Rest		M **(1)**	H **(1)**
SC-39	Process Isolation	L	M	SC-39

Agenda

✓ Project Cloud System Security Plan
- Section 2: Information System Categorization
  - E-Authentication Determination
- Section 13: Minimum Security Controls
  - Control Baselines
  - Control Classes
    - Technical Control Families
      - Identity and Authentication Technical Control Family

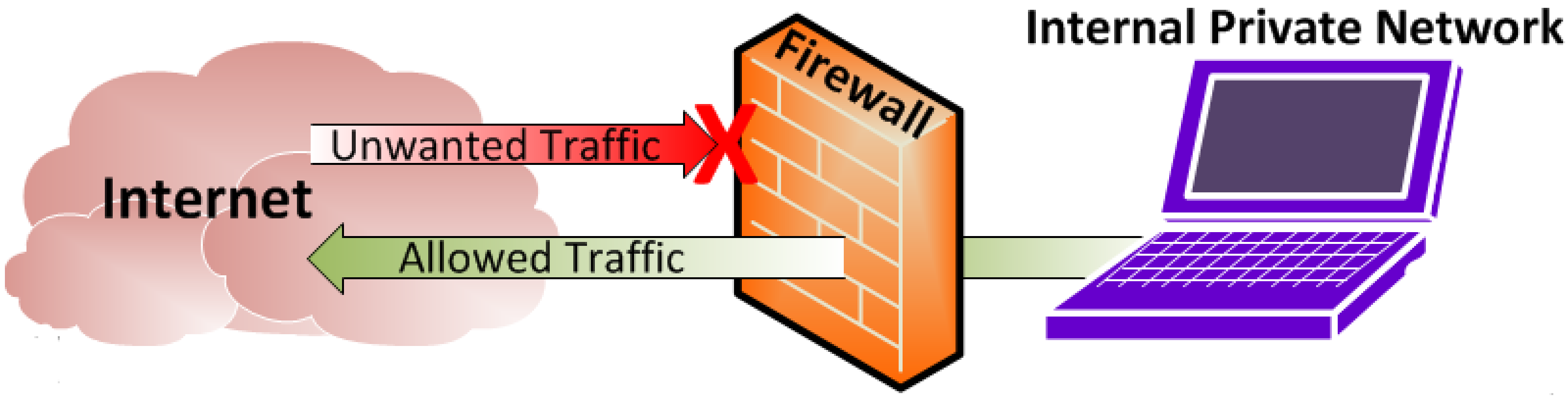
✓ Section 8: Information System Type
- Cloud service models
- Cloud deployment models
- Leveraged authorizations

✓ Section 13: Minimum Security Controls
  - Control Baselines
  - Control Classes
    - Technical Control Families

- Section 9: Review of Firewall types and IDS/IPS types

Firewalls are used to Implement Network Security Policy

- Firewalls support and enforce an organization's network security policy
- High-level directives on acceptable an unacceptable actions to protect critical assets
- Firewall security policy:
  - What services can be accessed
  - What IP addresses and ranges are restricted
  - What ports can be accessed

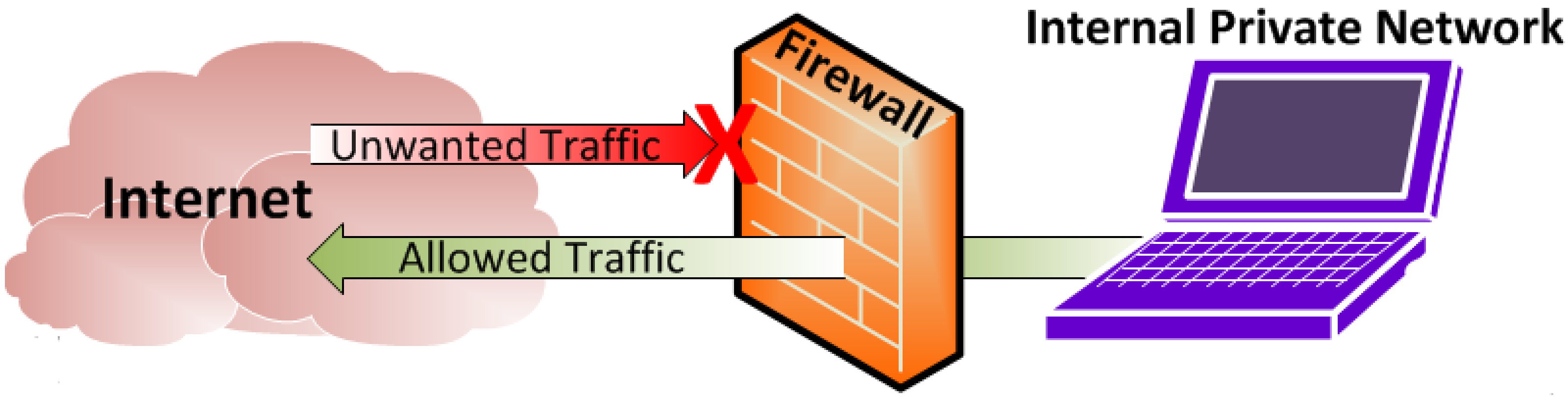


Firewalls are security architecture “choke points” in an IT network

- All communication should flow through and be inspected and restricted by firewalls
- Are used to restrict access to one network from another
  - Restrict access from the internet to access corporate networks
  - Restrict access between internal network segments
- Restrict access
  - Between origin and destination
  - Based on determination of acceptable traffic type(s)

Firewalls are used to Implement Network Security Policy

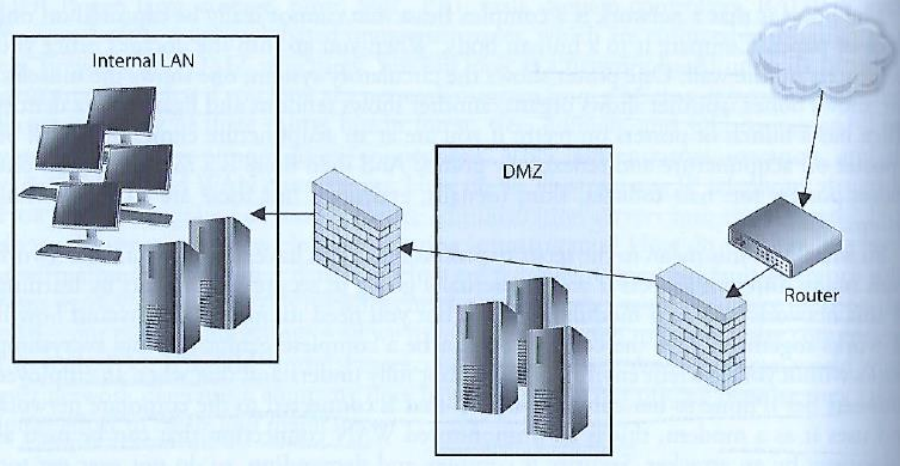
- Firewalls support and enforce an organization’s network security policy
- High-level directives on acceptable and unacceptable actions to protect critical assets
- Firewall security policy identifies:
  - What services can be accessed
  - What IP addresses and ranges are restricted
  - What ports can be accessed



Firewall Technology

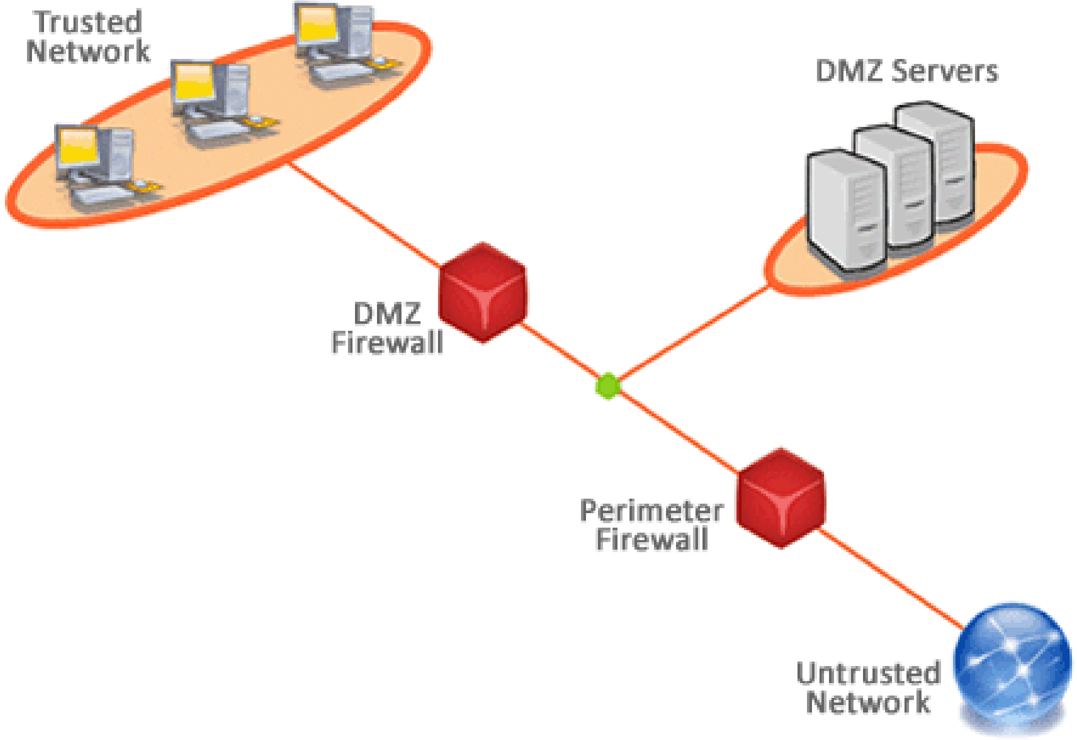
- May be implemented as a
  - Software product running on a server
  - Specialized hardware appliance
- Monitors data packets coming into and out of the network it is protecting
- Packets are filtered by:
  - Source and destination addresses and ports
  - Header information
  - Protocol type
  - Packet type
  - Service
  - Data content – i.e. application and file data content

Demilitarized Zone (DMZ)



Firewalls are installed to construct DMZ areas

- Network segments which are located between protected and unprotected networks
- Provides a buffer zone between the dangerous Internet and valuable assets the organization seeks to protect
- Usually 2 firewalls are installed to form a DMZ
  - May contain mail, file, and DNS (Domain Name System) servers
  - Usually contain an Intrusion Detection System sensor which listens for suspicious and malicious behavior
  - Servers in DMZ must be hardened to serve as the first line of protection against attacks coming from the internet

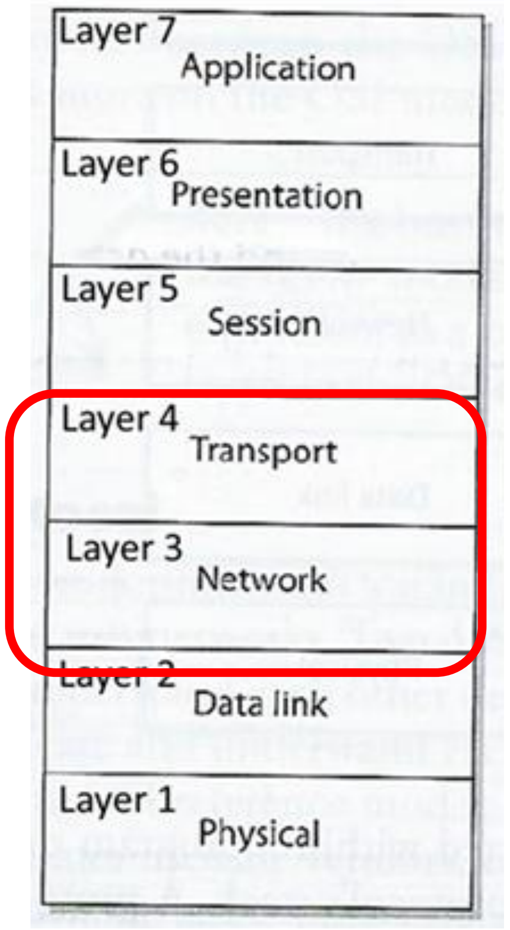


Types of Firewalls

1. Packet filtering
2. Dynamic packet filtering
3. Stateful inspection
4. Proxy Firewall
5. Kernal Proxy

Packet-filtering firewalls

- "First-generation" firewall technology – most basic and primitive
- Capabilities built into most firewalls and routers
- Configured with access control lists (ACLs) which dictate the type of traffic permitted into and out of the network
- Filters compare protocol header information from network and transport layers with ACLs

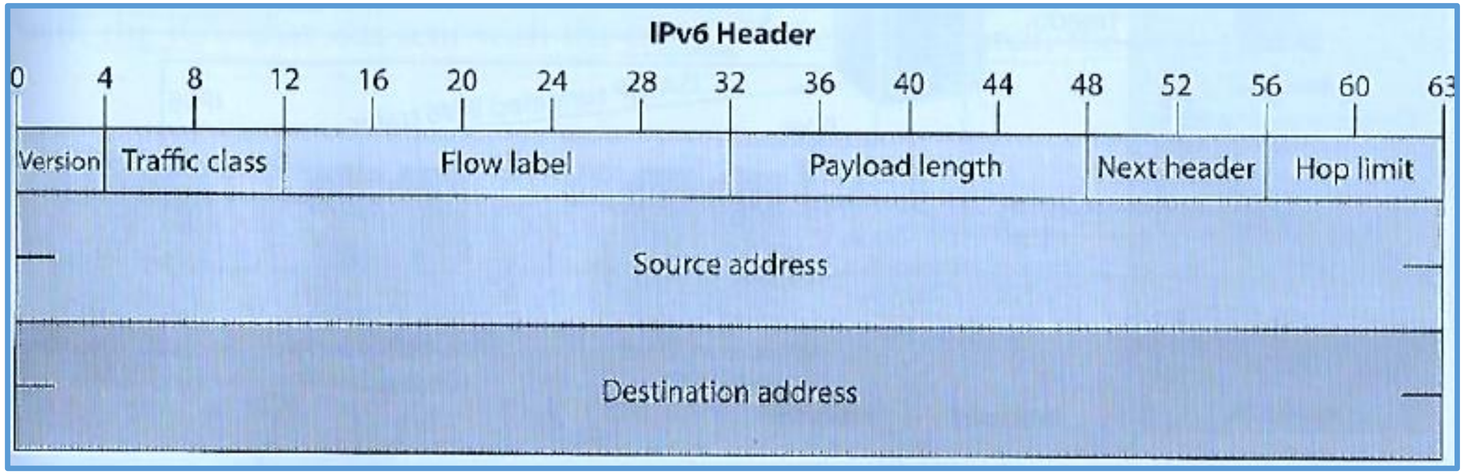


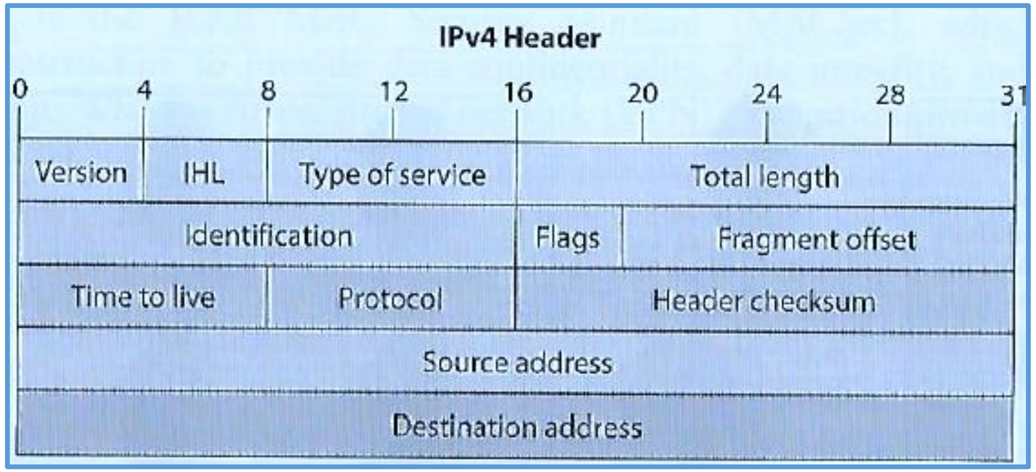
Packet-filtering Firewalls

Compares ACLS with network protocol header values to determine permit/deny network access based on:

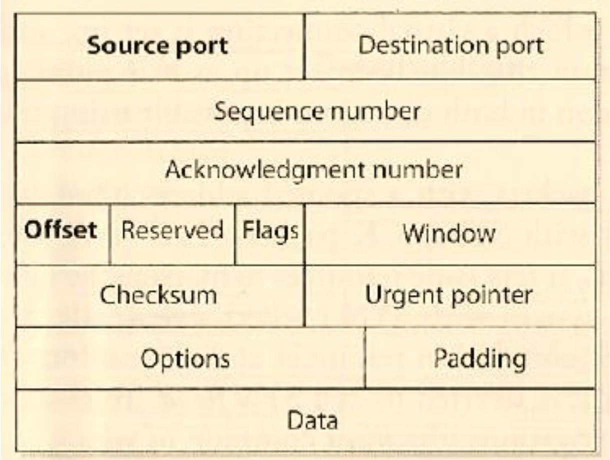
1. Source and destination IP addresses
2. Source and destination port numbers
3. Protocol types
4. Inbound and outbound traffic direction

Network Layer 3

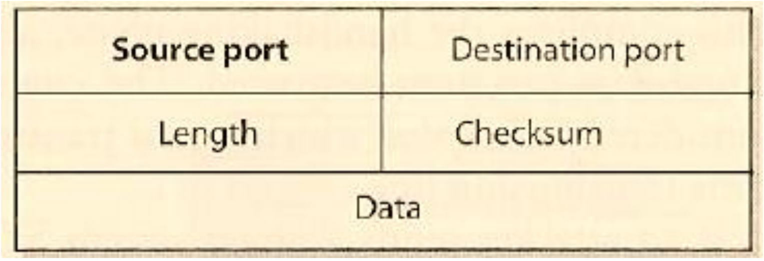




TCP format



UDP format



Transport Layer 4

TCP/IP Port numbers

Ports 0 to 1023 are Well-Known Ports

Ports 1024 to 49151 are Registered Ports – Often registered by a software developer to designate a particular port for their application

Ports 49152 to 65535 are Public Ports

Port # / Layer	Name	
1080	socks	SOCKS network application proxy services
1236	bvcontrol [rmtcfg]	Remote configuration server for Gracilis Packeten network switches[a]
1300	h323hostcallsc	H.323 telecommunication Host Call Secure
1433	ms-sql-s	Microsoft SQL Server
1434	ms-sql-m	Microsoft SQL Monitor
1494	ica	Citrix ICA Client
1512	wins	Microsoft Windows Internet Name Server
1524	ingreslock	Ingres Database Management System (DBMS) lock services
1525	prospero-np	Prospero non-privileged
1645	datametrics [old-radius]	Datametrics / old radius entry
1646	sa-msg-port [oldradacct]	sa-msg-port / old radacct entry
1649	kermit	Kermit file transfer and management service

Example ACL Rules

- Router configuration allowing SMTP (Simple Mail Transfer Protocol) traffic to travel from system 10.1.1.2 to system 172.16.1.1:

  permit tcp host 10.1.1.2 host 172.16.1.1 eq smtp

- Allow UDP traffic from 10.1.2 to 172.16.1.1:

  permit udp host 10.1.1.2 host 172.16.1.1

- Block all ICMP (Internet Control Message Protocol) i.e. router error messages and operational information traffic from entering through a certain interface:

  deny icmp any any

- Allow standard web traffic (to a web server listening on port 80) from system 1.1.1.1 to system 5.5.5.5:

  permit tcp host 1.1.1.1 host 5.5.5.5 eq www

Packet-filtering firewalls

Packet filtering firewalls: monitor traffic and provide “stateless inspection” of header attribute values (i.e. delivery information) of individual packets

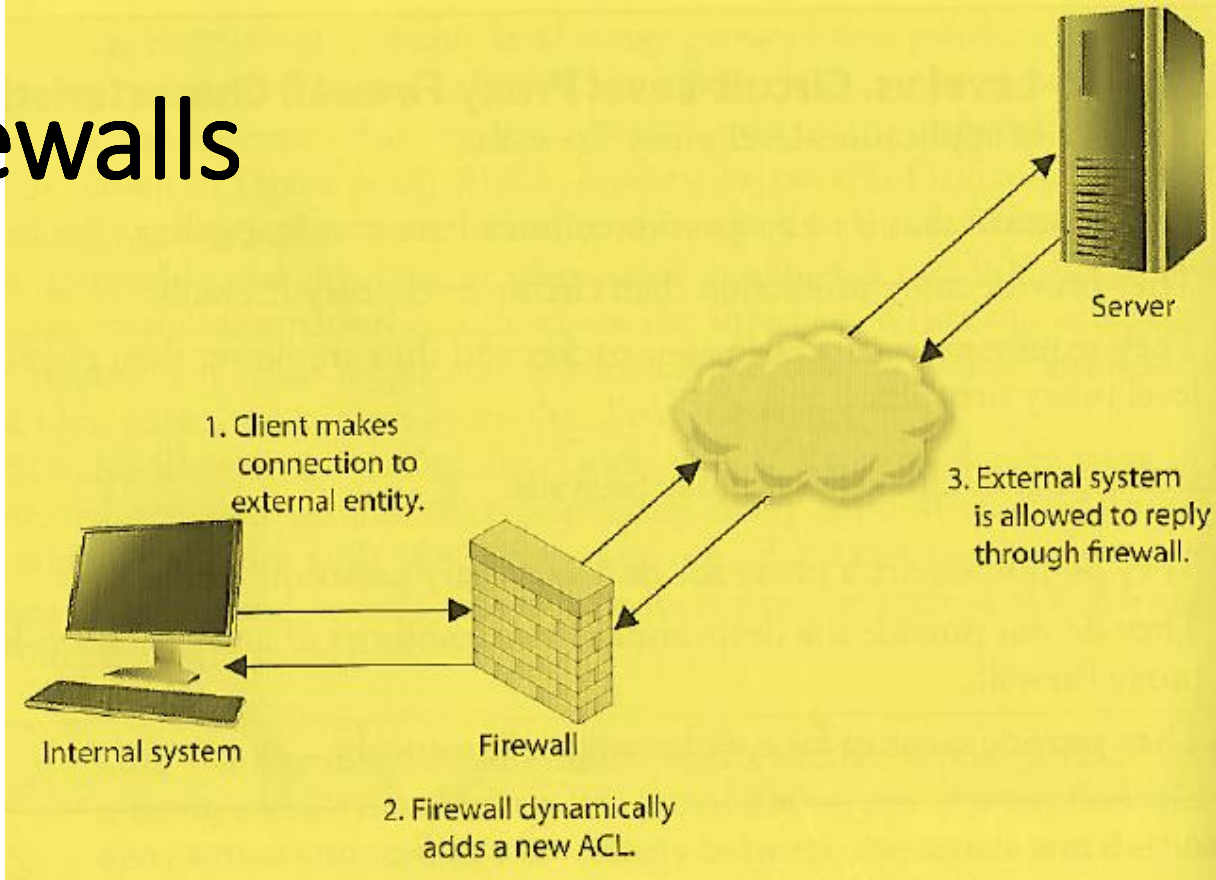
and after the decision to permit or deny access to the network is made the firewall *forgets* about the packets

- **Weakness:** No knowledge of data moving between applications communicating across the network
  - Cannot protect against packet content, e.g. probes for specific software with vulnerabilities and exploit a buffer overflow for example
  - Should not be used to protect an organization’s infrastructure and information assets
- **Strengths:** Useful at the edge of a network to quickly and efficiently strip out obvious “junk” traffic
  - High performance and highly scalable because they do not carry out extensive processing on the packets and are not application dependent
  - First line of defense to block all network traffic that is obviously malicious or unintended for a specific network
  - Typically complemented with more sophisticated firewalls able to identify non-obvious security risks

Dynamic Packet-Filtering Firewalls

When an internal system needs to communicate with a computer outside its trusted network it needs to choose an identify its source port so the receiving system knows how/where to reply

- Ports up to 1023 are reserved for specific server-side services and are known as "well-known ports"
- Sending system must choose a randomly identified port higher than 1023 to use to setup a connection with another computer



- The dynamic packet-filtering firewall creates an ACL that allows the external entity to communicate with the internal system via this high-numbered port
- The ACLs are dynamic in nature – once the connection is finished the ACL is removed
- The dynamic packet-filtering firewall offers the benefit of allowing any type of traffic outbound and permitting only response traffic inbound

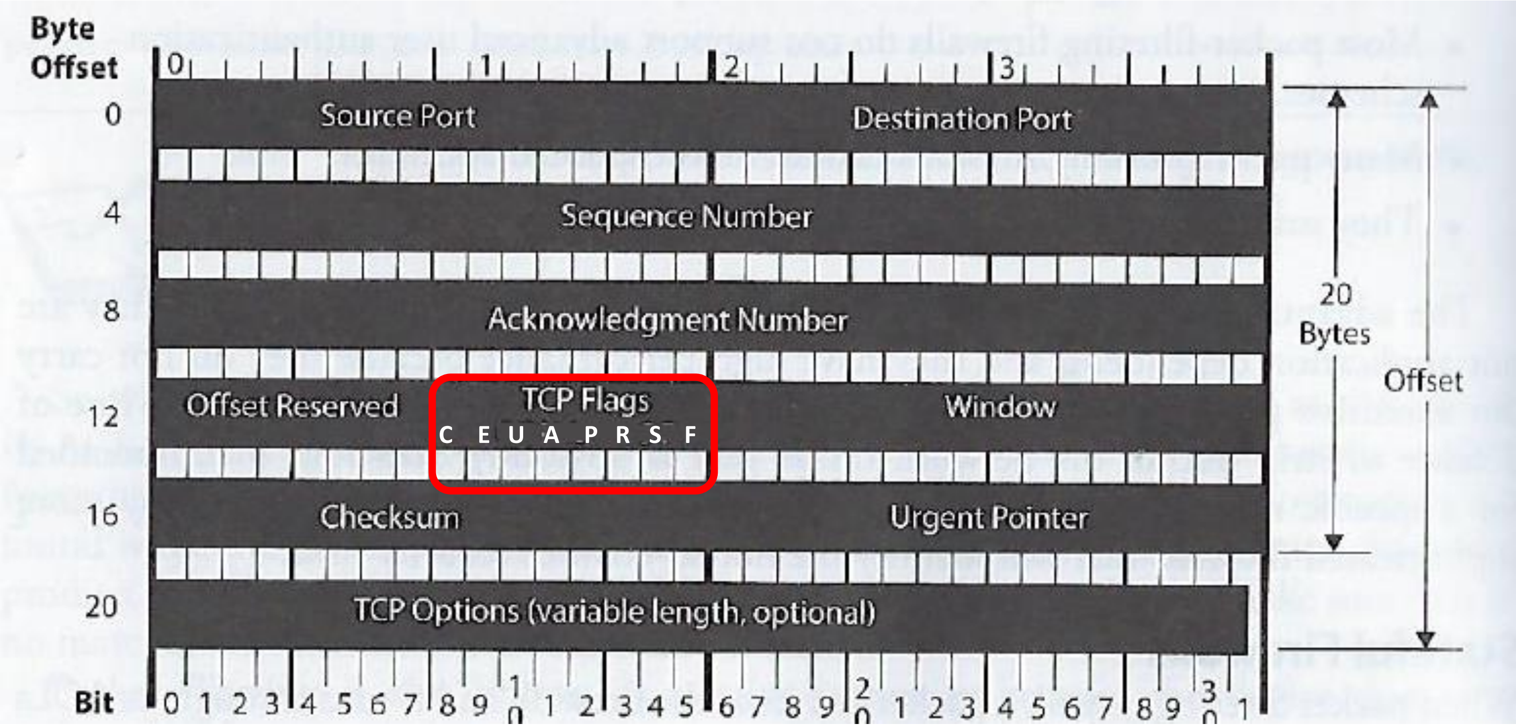
Stateful Inspection Firewall

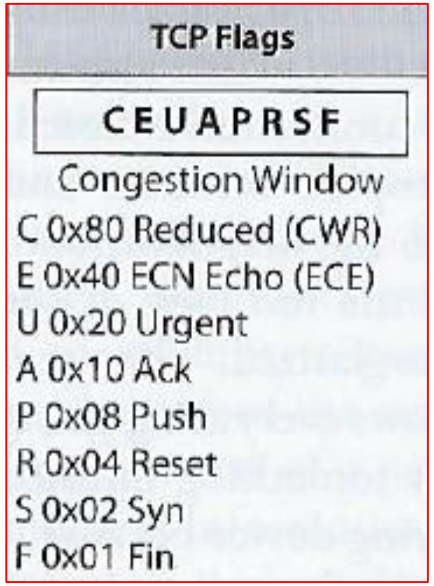
- Remembers and keeps track of what computers say to each other
  - Tracks where packets went until each particular connection between computers is closed
- Uses a "state table" which it updates to track the contents of packets each computer sent to each other
  - Makes sure the sequential process of packet message interchange involved in connection-oriented protocols (e.g. TCP – transmission control protocol) are properly synchronized and formatted
    - *If not an attack is detected and blocked*

Stateful Inspection example

Determine if all TCP Flags set to 1

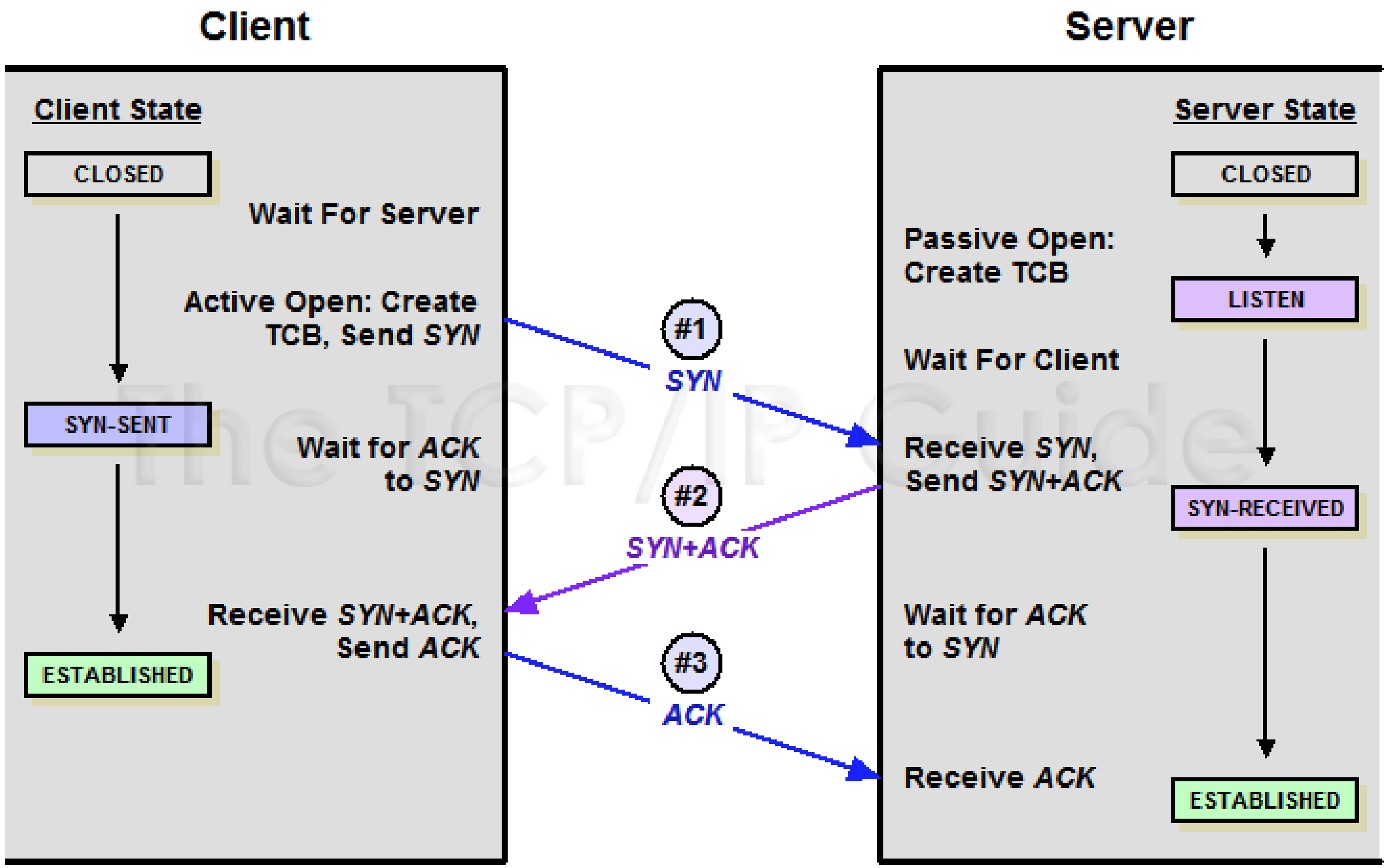
- Attackers send packets with all TCP flags set to 1 with hope that the firewall will not understand or check these values and forward them to the server
- Under no circumstances during legitimate TCP connections are all values turned to 1
- If detected connection is blocked





Stateful Inspection example

Stateful inspection firewall assures that TCP (connection-oriented protocol) proceeds through a series of states:



Stateful firewall keeps track of each of these states for each packet passing through, along with corresponding acknowledgement and sequence numbers

*Out of order acknowledgement and/or sequence numbers can imply a **replay attack** is underway and the firewall will protect internal systems from this activity*

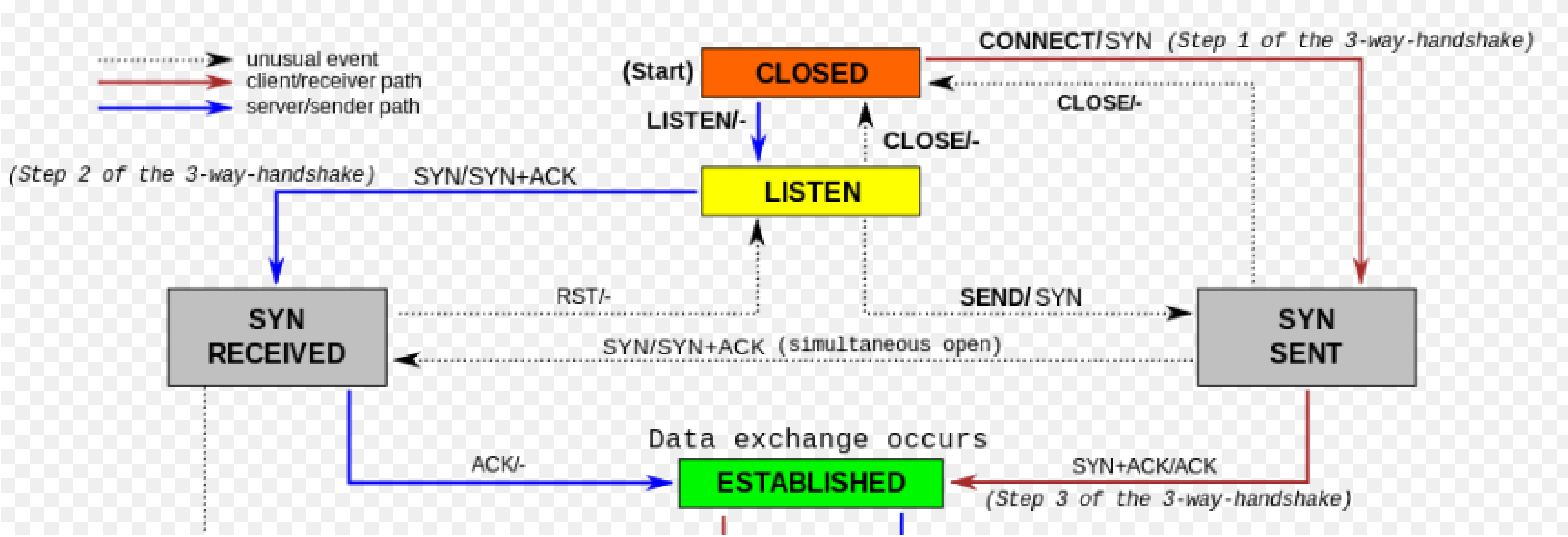
Stateful Inspection example

Stateful inspection firewall assures that TCP (connection-oriented protocol) proceeds through a series of states:

1. LISTEN
2. SYN-SENT
3. SYN-RECEIVED
4. ESTABLISHED

Stateful firewall keeps track of each of these states for each packet passing through, along with corresponding acknowledgement and sequence numbers

If a remote computer sends in a SYN/ACK packet without an internal computer first sending out a SYN packet, this is against protocol rules and the firewall will block the traffic



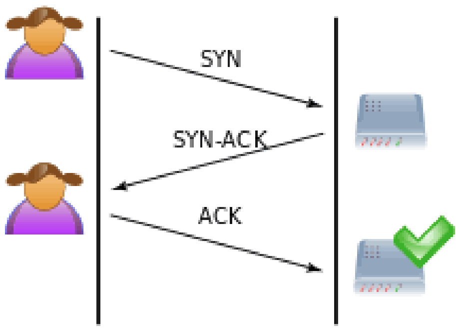
It knows how the protocols are supposed to work, and if something out of order (incorrect flag values, incorrect sequences, etc.) is detected the traffic is blocked

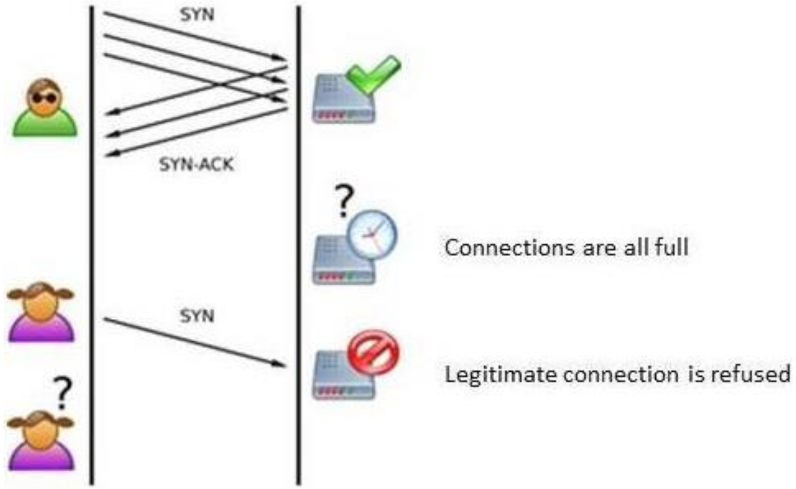
Stateful Inspection Firewalls

Strength: Maintains a state table that tracks each and every communication session to validate the session

- Provides high-degree of security, without introducing a huge performance hit
- Is scalable and transparent to users
- Tracks both connection-oriented protocols (e.g. TCP) and connectionless protocols (UDP and ICMP)

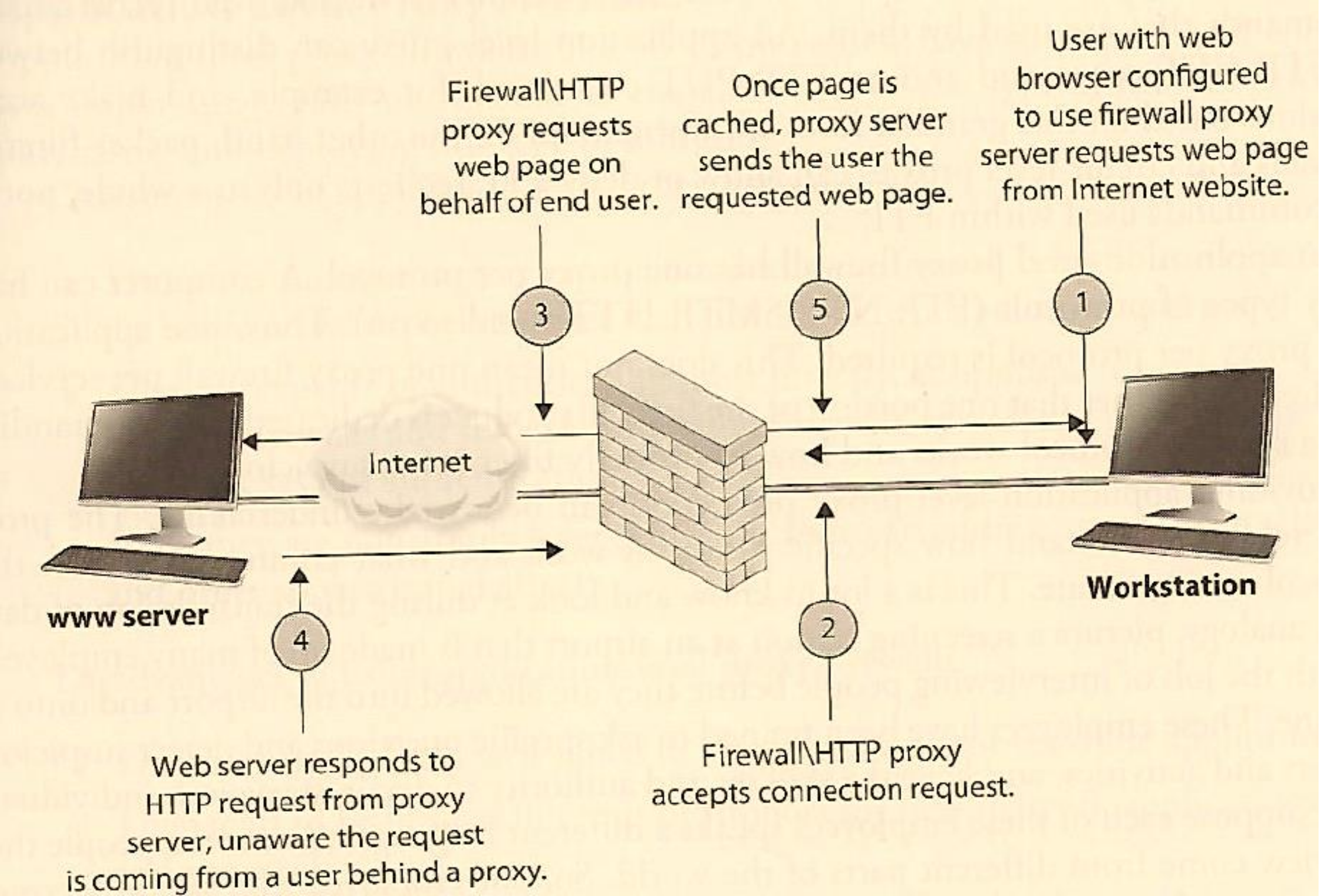
- **Weakness:** Succeptible to Denial of Service (DoS) attacks aided at flooding the state table with fake information
  - *Poorly designed stateful firewalls with state-tables filled with bogus information may freeze or reboot*





Proxy Firewall

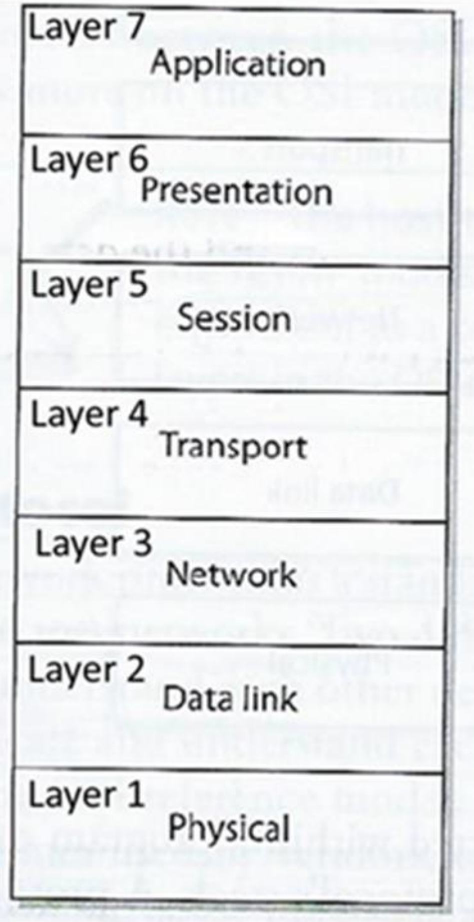
- Is a "middleman" standing between a trusted and untrusted networks, denying end to end connectivity between source and destination computers – puts itself between the pair in both directions intercepting and inspecting each message before delivering it to the intended recipient
- Applies ACL rules, and also…
  - *Ends the communication session, breaking the communication channel between source and destination, so there is no direct connection between two communicating computers*
  - *Inspects the traffic*
  - *When traffic is "approved" the proxy firewall starts a new session from itself to the receiving system*



Proxy Firewall – two types working at different levels in the OSI model

- **Circuit-level proxies** work at the lower levels of the OSI stack – up through the session layer
  - Creates a “circuit” connection between 2 computer systems
  - Cannot look into the contents of the packet to perform “deep inspection”, does not understand application-level protocols and cannot determine if the packets are safe or unsafe
  - Works similar to a packet filter looking at header information, making decisions based on address, port and protocol header values

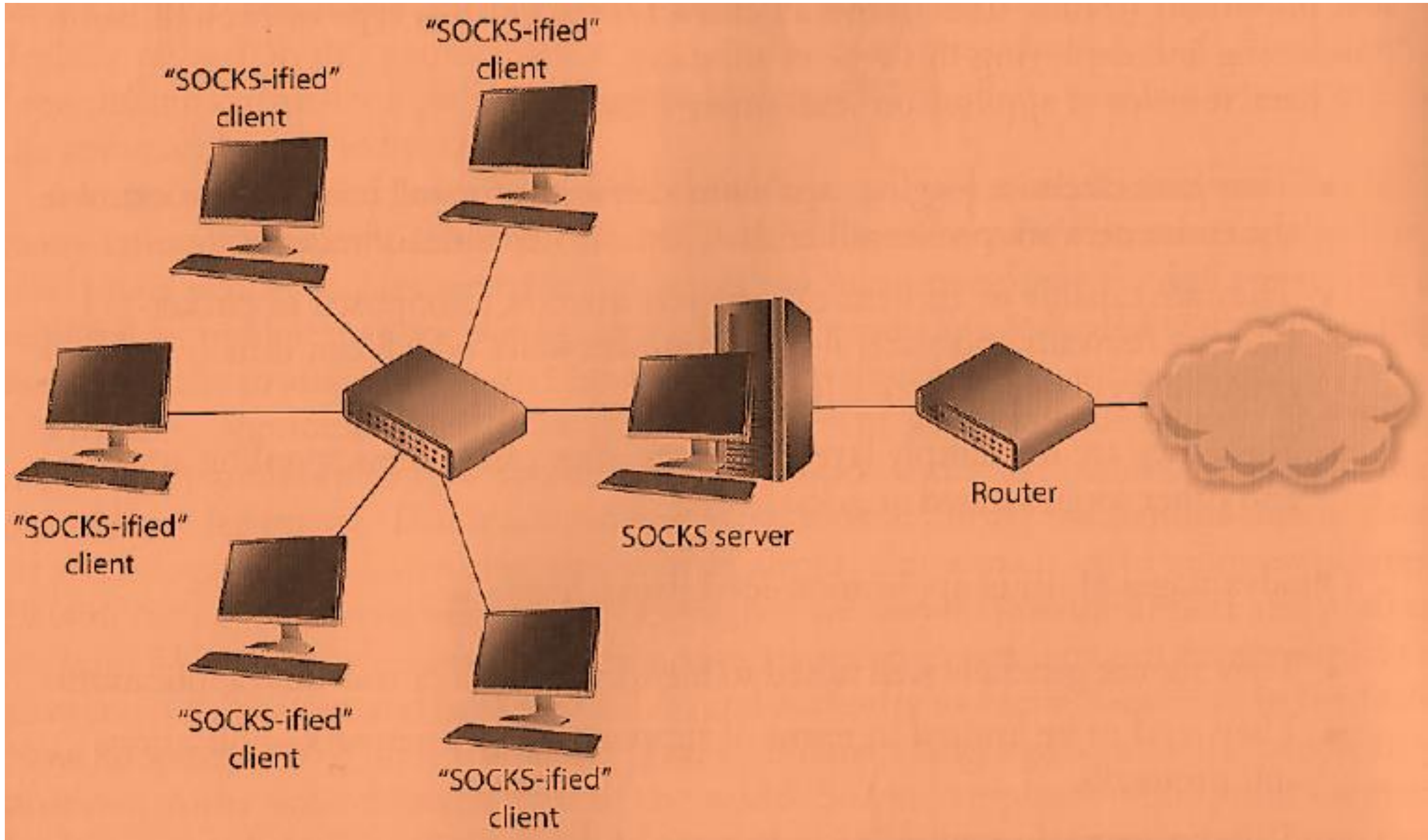
- **Application-level proxies** work up through the application layer
  - Understand entire contents of packets, making decisions based on API services, protocols and commands (e.g. FTP PUT and GET commands)
  - Each API protocol must have its own proxy able to understand the commands, how the protocol works, and how to detect suspicious data transmissions using the protocol
  - A Proxy Firewall will have a series of application-level proxies – one proxy per protocol (i.e. one for FTP, and different specific ones for NTP, SMTP, HTTP, …)



Circuit-level Proxy Firewalls

- Only examines network addresses and ports – similar to packet filtering firewalls, but provides proxy services insulating the internal identities and addresses of machines from external devices
- Can handle a much wider variety of protocols and services than an application proxy-level proxy firewall can

- Does not understand application-level protocols, and cannot provide more granular level control protecting from malicious transactions and content



Application-level Proxy Firewalls

Advantages

- Have extensive logging capabilities due to ability to examine contents of the entire network packet rather than just addresses and ports
- Capable of authenticating users directly
  - Packet-filtering and stateful-inspection firewalls only able to authenticate systems (not users)
- Functioning a higher levels in the OSI stack enable them to detect and address spoofing and other sophisticated attacks

Disadvantages

- May not be well suited for real-time or high-bandwidth applications
- Create performance issues due to processing needed to inspect and analyze “deep content” of packets
- Limited support for newer network applications and protocols

Application and Circuit Proxy Firewalls both

- Act as a proxy
- Deny actual end-to-end connectivity between the source and destination computers
- Clients attempting remote connection connects and communicates to the proxy; the proxy – in turn – establishes a connection to the destination system and makes requests to it on behalf of the client
- The proxy maintains 2 independent connections for every one network transmission, turning a 2-party session into a 4-party session – providing the middle processes emulating the 2 real systems

Application-level versus Circuit-level Proxy Firewalls

- **Application-level**
  - Need a unique proxy to monitor each API protocol
  - Provide more protection than circuit-level proxy firewalls
  - Require more processing per packet and are slower than circuit-level proxy firewalls
- **Circuit-level**
  - Provide security for a wider range of (lower level) protocols
  - Are more general purse as they function at lower levels in the OSI stack and do not require a proxy for each API protocol
  - Do not provide deep-inspection capabilities of an application-level proxy firewall

Kernal Proxy Firewalls

- Considered a “fifth generation” firewall
- Functions as a proxy – conducting network address translation so it function as a “middleman”
- Creates a dynamic, customized virtual network stacks for each packet that consists of only the protocol proxies needed to examine it
  - The packet is evaluated at every layer of the stack simultaneously
    - Data link header
    - Network header
    - Transport header
    - Session layer information
    - Application layer data
  - If anything is determined unsafe the packet is discarded
- Much faster than an application-level proxy because it is optimized to function at the lower level kernel level of the operating system

Next-Generation Firewalls (NGFW)

- Combines the best capabilities of the other firewalls
  - Ensures traffic is well-behaved and in accordance with applicable protocols
  - Breaks direct connection between internal and external systems (proxy)
  - Provides dynamic port assignment
- Also includes a signature-based Intrusion Detection System (IPS) engine
  - Able to look for specific indicators of attack even in traffic is well behaved
- Able to use centralized data sources
  - Able to be updated with new attack signatures from cloud aggregators
  - For consistent up to date whitelists, blacklists and policies
  - Can connect to Active Directory to provide URL to IP address translations
- Tend to be expensive – cost of ownership beyond small and medium sized organizations

Summary

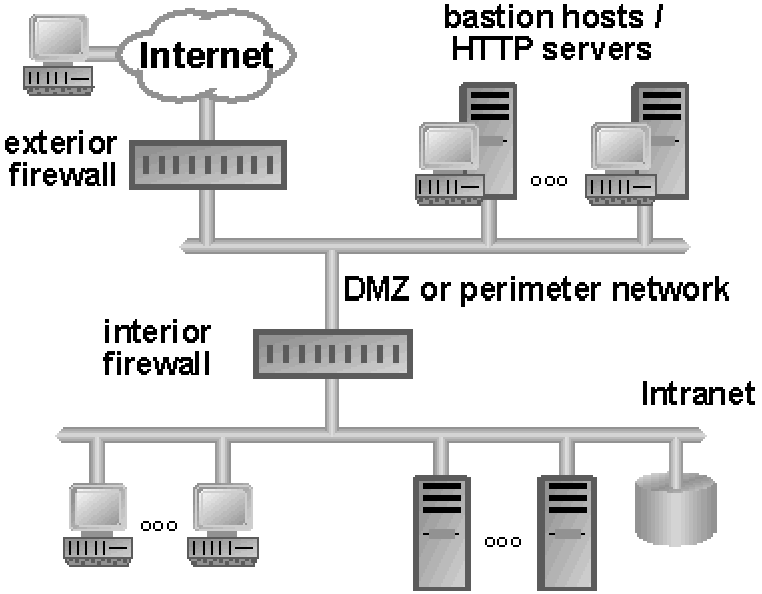
Firewall type	OSI Layer	Characteristics
Packet Filtering	Network Layer	Looks at destination and source addresses, ports, and services requested. Routers use ACLs monitor network traffic
Dynamic Packet Filtering	Network Layer	Allows any permitted type of traffic outbound and only response traffic inbound
Stateful	Network Layer	Looks at the state and context of packets. Keeps track of each conversation using state table
Circuit-level Proxy	Session Layer	Provides proxy services, but looks only at the header packet information (less detailed level of control that application-level proxy)
Application-level Proxy	Application Layer	Looks deep into packets and makes granular access control decisions, It requires one proxy per protocol
Kernal Proxy	Application Layer	Faster than application-level proxy because processing performed in operating system kernel. One network stack created for each packet
Next-generation	Multiple Layers	Very fast and supports high bandwidth. Built-in IPS, able to connect to external services like Active Directory

Firewall architectures…

1. Dual-homed Firewall
2. Screened host
3. Screened Subnet

Bastion Host

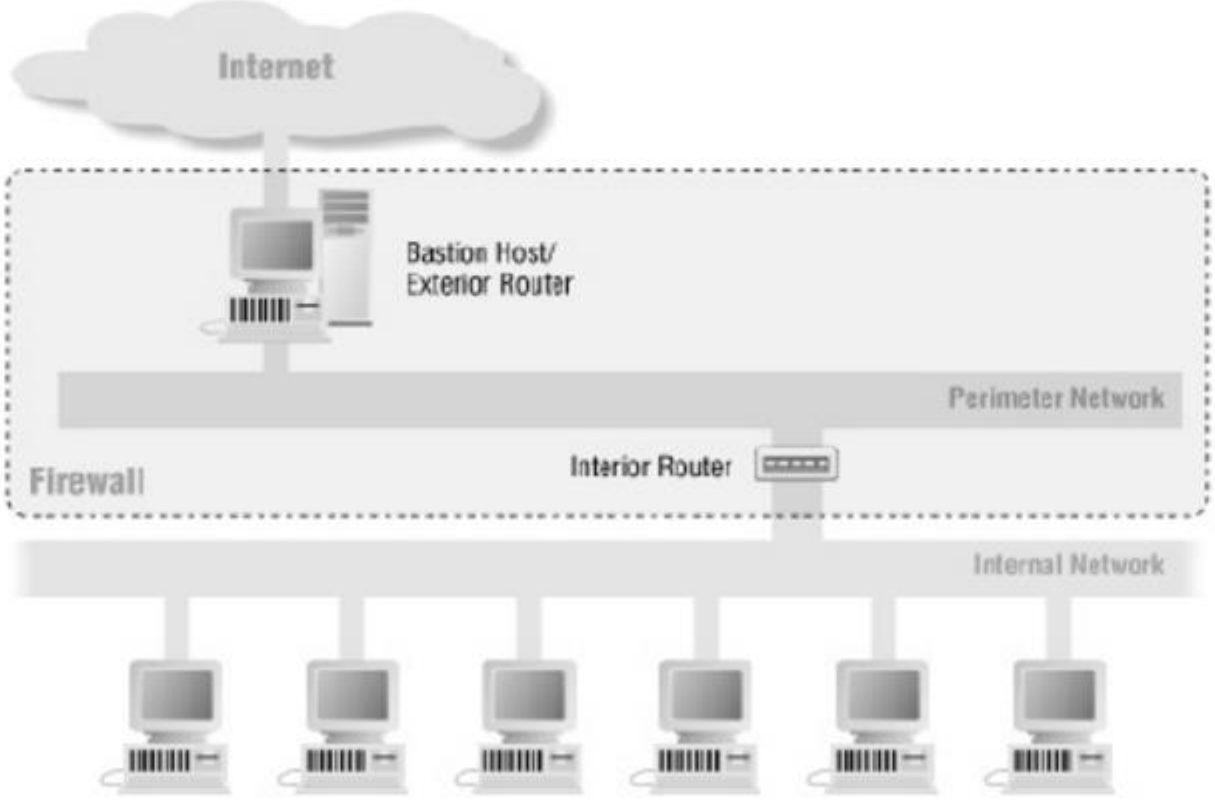
- Bastion host system is a highly exposed device closer than any other system to an untrusted network, that is most likely to be targeted by attacker
- Typically directly connected to an untrusted network, or placed on the public side of a DMZ
- Needs to be extremely locked down and hardened to reduce its attack surface (i.e. vulnerabilities reduced as much as possible):
  - All unnecessary:
    - Services disabled
    - Accounts removed
    - Applications removed
    - Subsystems and administrative tools removed



Dual-Homed Firewall Architecture

- A “dual-homed” device has two network interface cards (NICs)
  - Multi-homed devices have multiple NICs
- Firewall software running on a dual-homed device
  - Underlying operating system should have packet forwarding and routing turned off for security

- Packet comes to the external NIC from an untrusted network and is forwarded up through the firewall software and if not dropped forwarded to the internal NIC



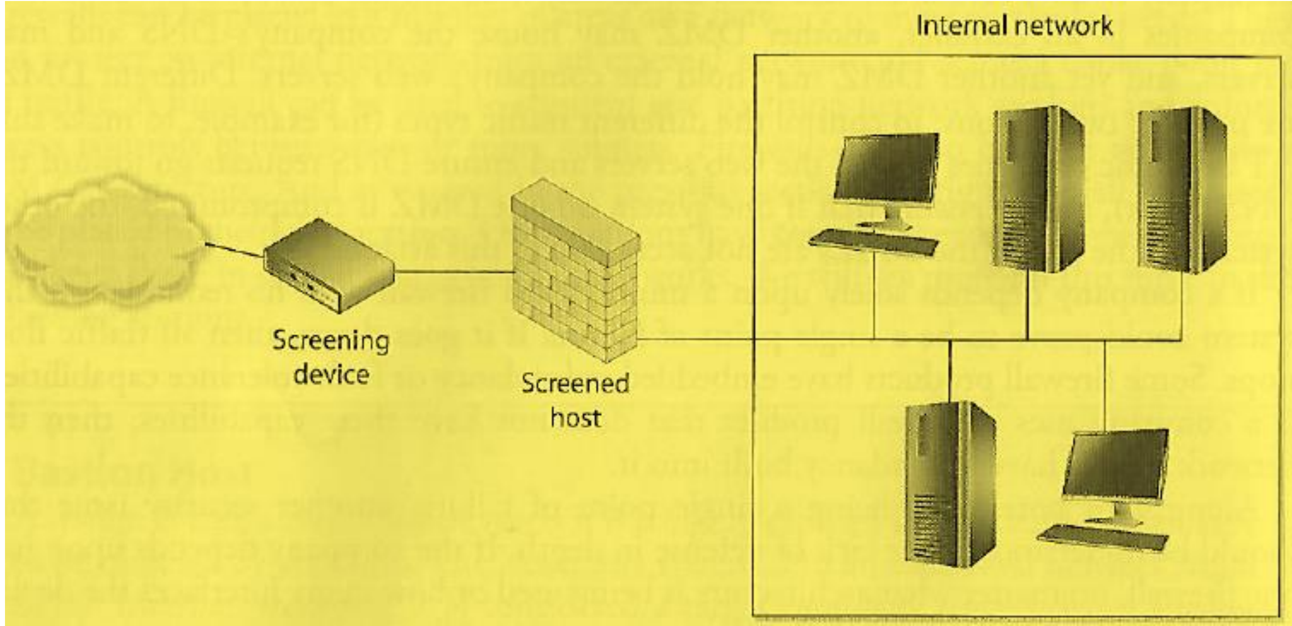
- Without redundancy, if this goes down the dual-homed firewall becomes a single point of failure
- On layer of protection lacks “defense in depth”

  If an attacker compromises one firewall they can gain direct access to the organizations network resources

Screened Host Firewall Architecture

- A firewall that communicates directly with a perimeter router and the internal network
    1. Traffic from the Internet first passes through a packet filtering router applying ACL rules which filters out (i.e. drops) junk packets
    2. Traffic that makes it past this phase is sent to the screen-host firewall which applies more rules to the traffic and drops the denied packets
    3. Remaining traffic moves to the internal network

"One-tier tiered configuration"



- Router provides network-level packet filtering
- Application-based firewall provides packet filtering at the application layer
- Security level is higher than a bastion dual-homed firewall because attacker would need to compromise 2 systems to achieve success

Screened Subnet Architecture

Adds another layer of depth to the security of the screened-host architecture

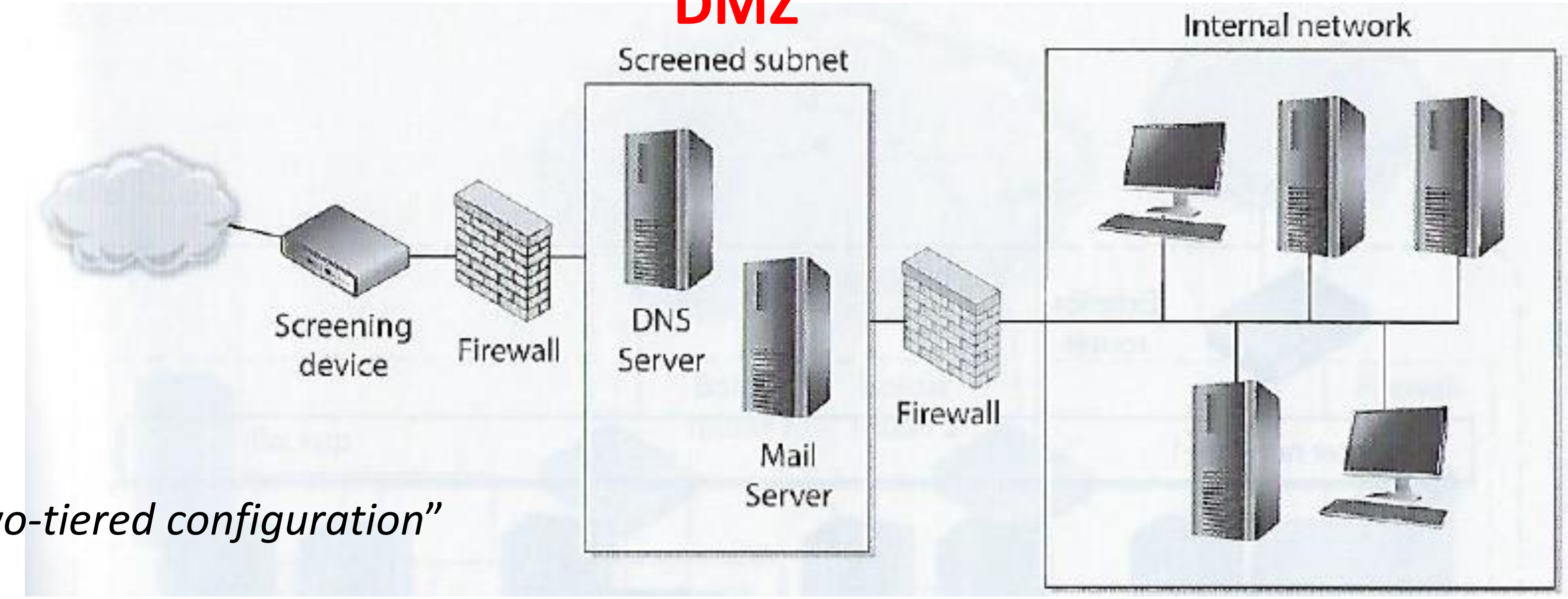
- The external firewall screens traffic entering the screened sub-network, instead of firewall redirecting traffic to the internal network
- The second interior firewall also filters the traffic – this creates a screened subnet (i.e. DMZ)

Creates a DMZ between 2 firewalls which functions as a small network isolated between trusted internal and untrusted external network

DMZ

3-devices working together provides more protection than a stand-alone firewall or a screened-host firewall

All 3 need to be compromised by an attacker to gain access to the internal network



“Two-tiered configuration”

Characteristics of Firewall Architecture

- **Dual-homed**
  - A single computer with separate NICs connected to internal and external network
  - Used to divide an external untrusted network from an internal trusted network
  - Must harden and disable computer's forwarding and routing functionality so the two networks communicate through the computer's firewall software and are truly segregated
- **Screened host**
  - A router filters and screens traffic applying its ACL to drop 'junk' traffic before it is passed to the firewall
- **Screened subnet**
  - An external router filters/screens traffic before it enters the subnet, sending remaining traffic through two firewalls before making its way to the internal network

Good firewall behavior…

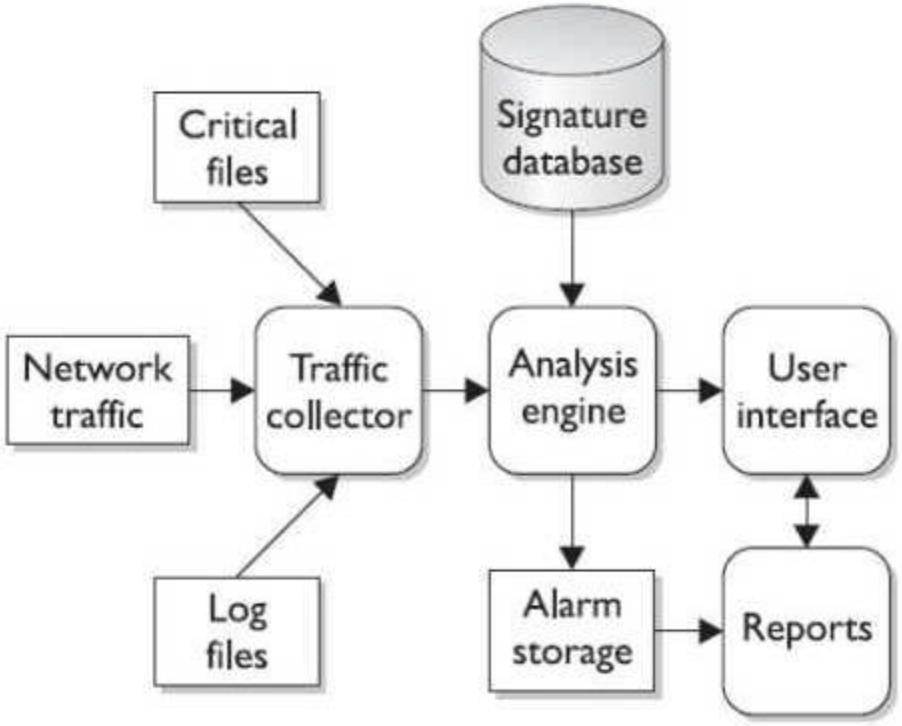
- The Firewall's ***default action is to deny*** any packets explicitly not allowed
  - If no rule in the ACL explicitly says the packet can come in, it is dropped
  - Any packet coming in from the Internet containing the source address of an internal host should be dropped
    - Spoofing or masquerading attack reflected in a modified packet header having the source address of a host inside the target network
  - No packet should be permitted to leave that does not contain a source address of an internal host – this is how DDoS zombies work
  - Many companies deny packets with source routing information in the headers which may circumnavigate internal routers and firewalls
- Firewalls ***not effective "out of the box"***
  - Need to understand internal default rules which may negate user provided rules
  - Can create bottlenecks
  - Need to effectively distribute them throughout the network to control network access points and provide appropriate "defense in depth"
  - Do not protect against malware, complex attack types, sniffers, rogue access points

Common firewall rules:

- Stealth rule
  - Disallow unauthorized systems from accessing to firewall software
- Silent rule
  - Identify and drop “noisy” traffic without logging it to reduce log sizes by not responding to unimportant packets
- Cleanup rule
  - Last rule in the rule base drops and logs remaining traffic that does not meet preceding rules
- Negate rule
  - Create tighter rules by specifying what system can be accessed and how (whitelisting), and do not use broad and permissive rules that default to any traffic (e.g. blacklisting)

Intrusion Detection Systems (IDSs)

- While firewalls and antivirus are preventive controls, IDSs are access control monitoring devices designed to
  1. Detect a security breach
  2. Aid in mitigating damage caused by hackers breaking into sensitive computer and network systems
- IDS' components
  1. Sensors
     - Collect and send traffic and user activity data to analyzers
  2. Analyzers
     - Look for suspicious activity and if found sends alert to administrator's interface
  3. Administrative interfaces



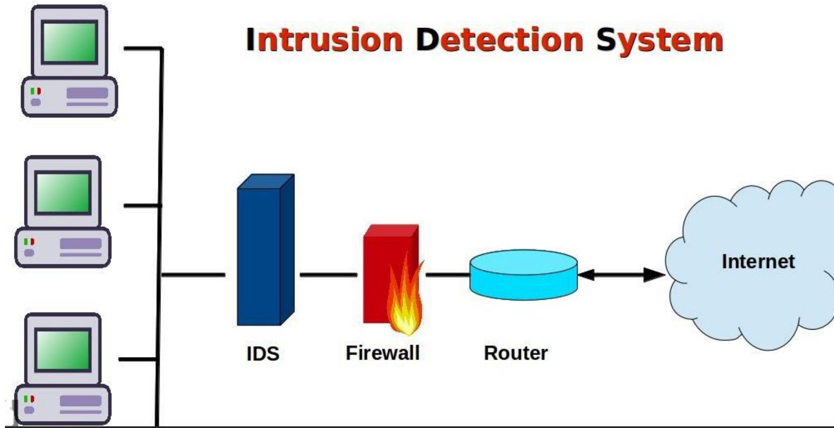
Intrusion Detection Systems (IDSs)

Two main types of IDS

1. **Host-based** for analyzing activity within a particular computer system
2. **Network-based** for monitoring network communications

IDS can be configured to:

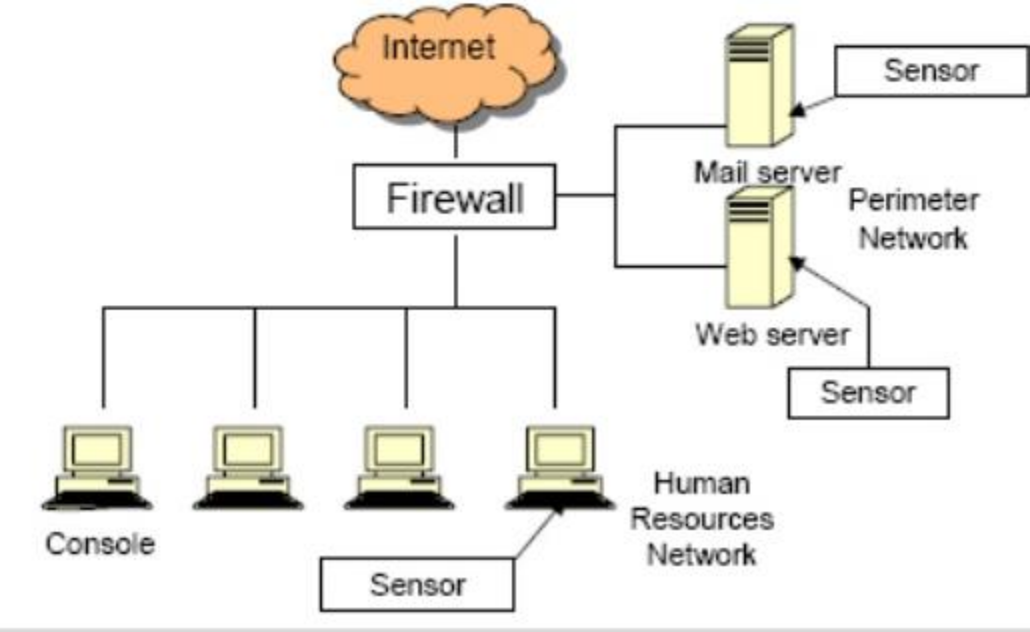
- Watch for attacks
- Parse audit logs
- Terminate a connection
- Alert administrator as attacks happen
- Expose a hacker and her/his techniques
- Illustrate which vulnerabilities need to be addressed



Intrusion Detection Systems (IDSs)

Host-based IDS (HIDS)

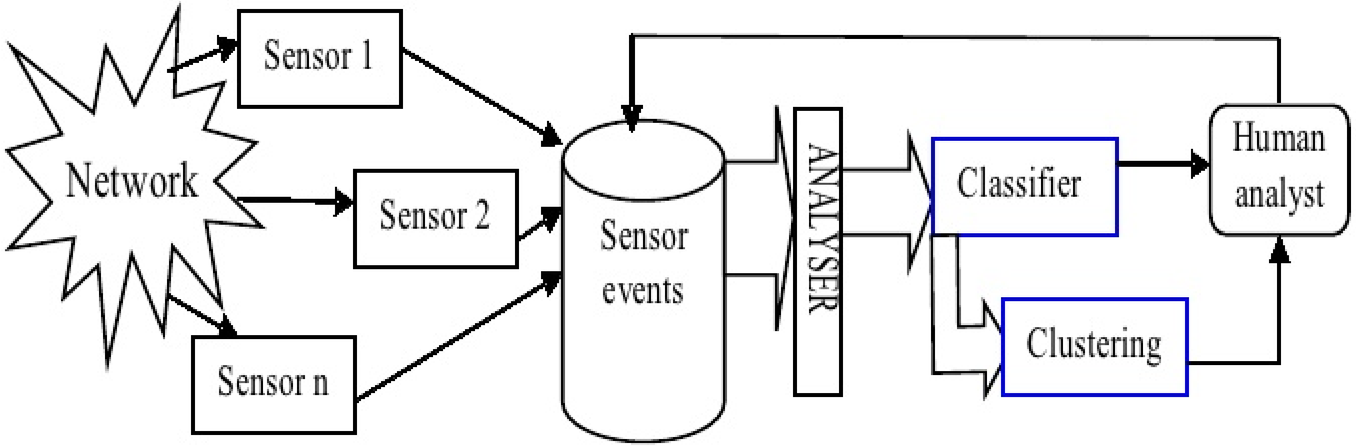
- Can be installed to look at the data packets within the higher levels of the OSI stack for anomalous or inappropriate activity on individual servers and/or workstations
- Usually installed on critical servers (too much administrative overhead to put them everywhere)
- Make sure users do not put the system at risk by activities such as deleting system files or reconfiguring important settings
- Does deeper inspection of the packets
- Does not understand network traffic



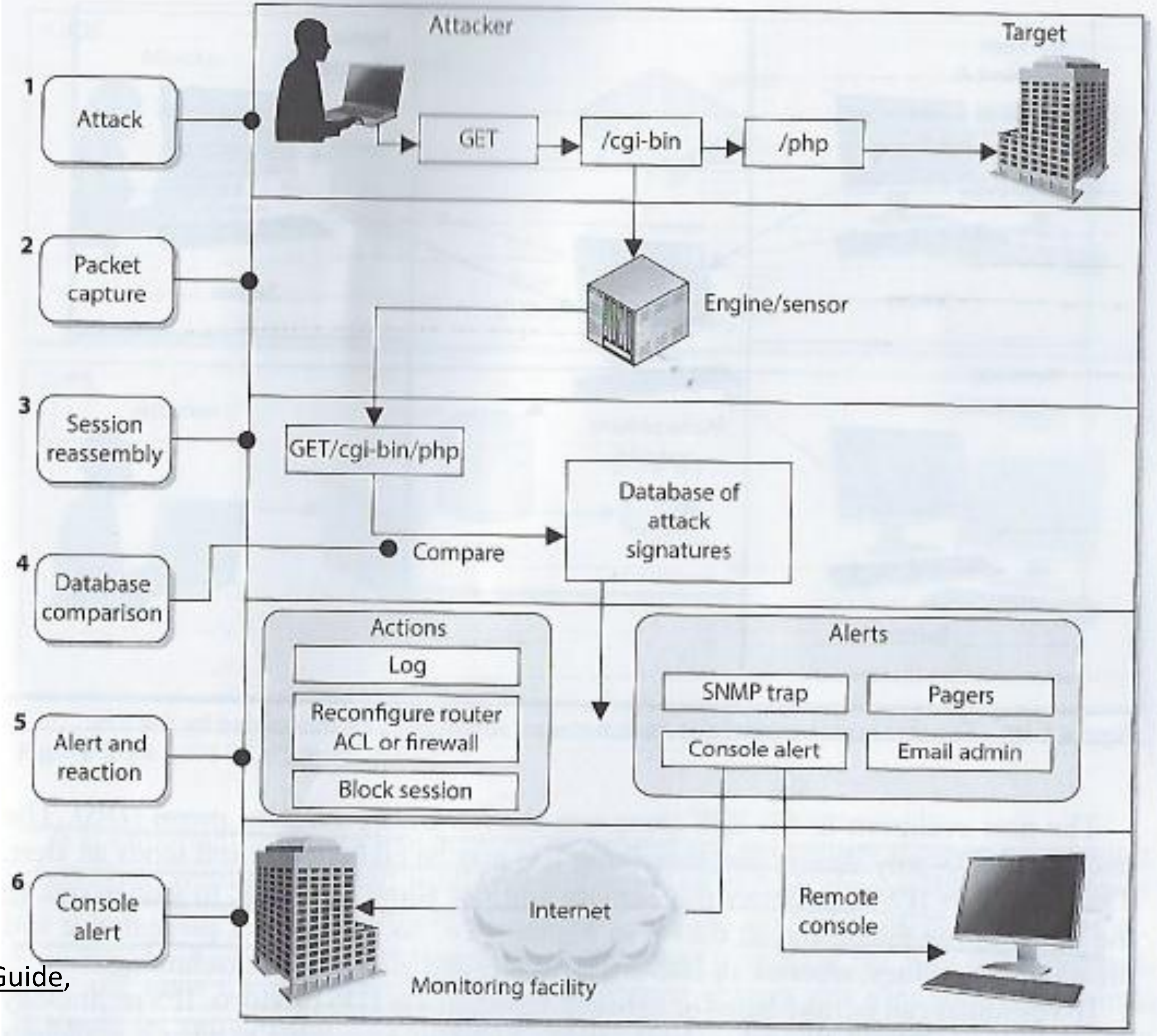
Intrusion Detection Systems (IDSs)

Network-based IDS (NIDS)

- Uses sensors which can be either host computers with specialized software installed or dedicated appliances
  - Each have a NIC (network interface card)
    - NIC is configured in promiscuous mode to capture all traffic (rather than packets addressed to the host computer
    - Copies packets – sending one copy up the TCP stack (for normal processing or possible analysis with a HIDS), and another copy to analyzer looking for specific patterns in the network traffic
- Monitors network traffic, cannot see the activity happening within the higher levels of the OSI stack (HIDS is used for this)



Basic architecture of a Network IDS

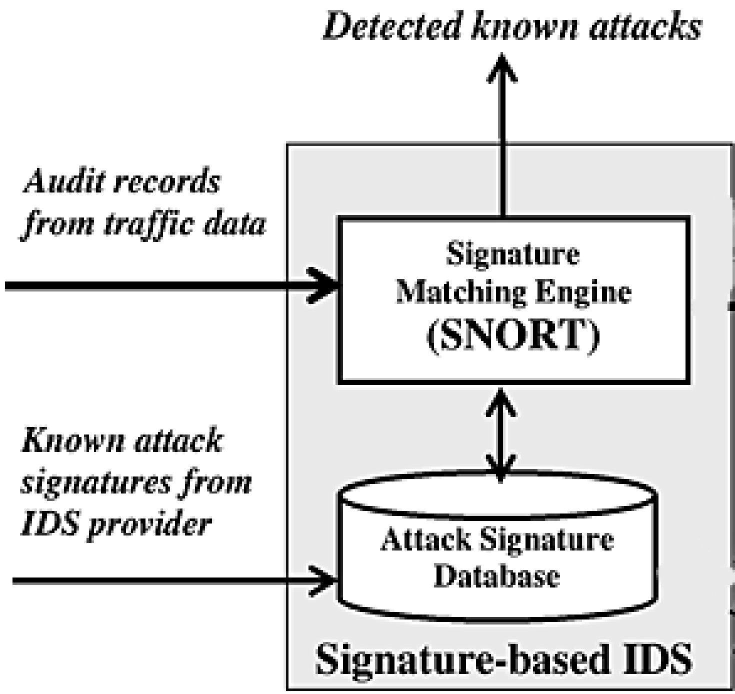


Harris, S. and Maymi, F. (2016) <u>All In One CISSSP Exam Guide</u>, Seventh Edition, McGraw-Hill Education

Intrusion Detection Systems (IDSs)

NIDS and HIDS can be one of the following types:

1. Signature-based:
   - Pattern matching, similar to antivirus software
   - Signatures must be continuously updated
   - Cannot identify new attacks
   - 2 types
     - Pattern matching: Compares individual packets to signatures
     - Stateful matching: Compares patterns among packets
2. Anomaly-based (a.k.a. Heuristic-based or Behavior-based):
   - Behavioral-based system able to learn from "normal activities"
   - Can detect new attacks
   - 3 Types:
     - Statistical anomaly-based – creates a normal profile used to compare sensed activities
     - Protocol anomaly-based – Identifies incorrect uses that violate protocols (e.g. TCP 3-way handshake)
     - Traffic anomaly-based – Identifies unusual activity in network traffic
3. Rule-based
   - Uses artificial intelligence expert systems that process rules in the form of "If *situation* then *action*" statements to identify combinations of activities within the data of the packets
     - *e.g. "IF a root user creates FileA AND FileB IN same directory and there is a call to Administrative ToolK THEN trigger alert"*
   - Cannot detect new attacks
   - The more complex the rules, the greater the need for processing power to support the software and hardware requirements so the IDS does not become a bottleneck and performance problem



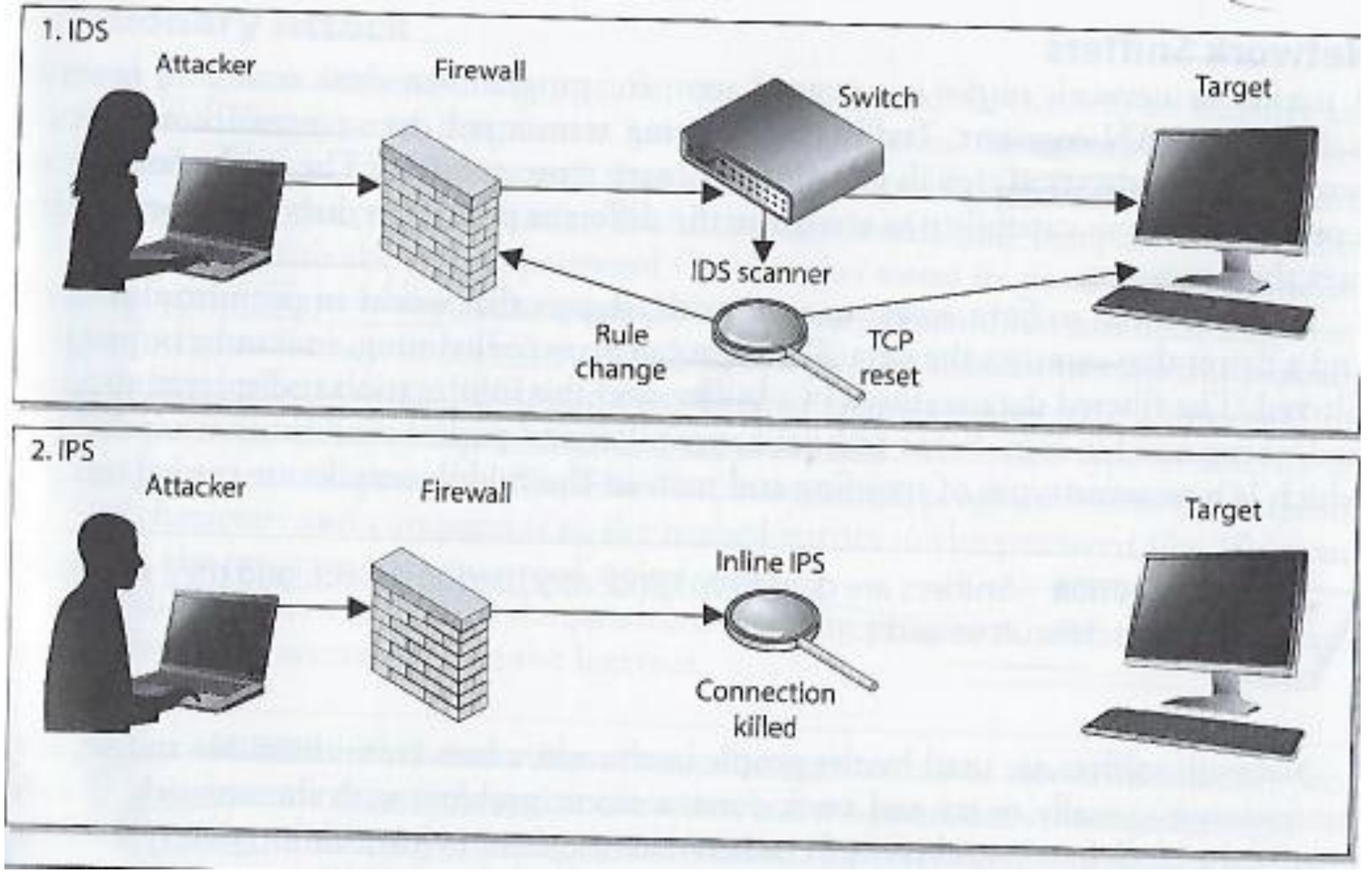
Intrusion Prevention System (IPS)

- IDS – Detect something bad may be taking place and send an alert
  - *Detective and "after the fact" response*
- IPS – Detect something bad may be taking place and block traffic from gaining access to target
  - *Preventive and proactive response*
  - *Host-based or Network-based (like IDS)*
  - *Can be content-based (looking deep into packets)*
    - *To conduct protocol analysis or signature matching*
  - *Also can use rate-based metrics to identify suspicious increases in volumes of traffic*
    - *E.g. DoS – flood attack*
    - *Traffic flow anomalies – "slow and low" stealth attack attempting to be undetected*

IDS versus IPS

Possible responses to a triggered event:

- Disconnect communications and block transmission of traffic
- Block a user from accessing a resource
- Send alerts of an event trigger to other hosts, IDS monitors and administrators



Agenda

- Team Project Presentation Schedule, Deliverables, Presentation timings
- Project Cloud System Security Plan
  - Section 2: Information System Categorization
    - E-Authentication Determination
  - Section 13: Minimum Security Controls
    - Control Baselines
    - Control Classes
      - Technical Control Families
        - Identity and Authentication Technical Control Family
- Section 8: Information System Type
  - Cloud service models
  - Cloud deployment models
  - Leveraged authorizations
- Section 13: Minimum Security Controls
    - Control Baselines
    - Control Classes
      - Technical Control Families
- Section 9: Review of Firewall types and IDS/IPS types

The importance of protecting audit logs generated by computers and network devices is highlighted by the fact that it is required by many of today's regulations. Which of the following does not explain why audit logs should be protected?

a. If not properly protected, these logs may not be admissible during a prosecution.
b. Audit logs contain sensitive data and should only be accessible to a certain subset of people.
c. Intruders may attempt to scrub (clean) the logs to hide their activities.
d. The format of the logs should be unknown and unavailable to the intruder.

The importance of protecting audit logs generated by computers and network devices is highlighted by the fact that it is required by many of today's regulations. Which of the following does not explain why audit logs should be protected?

a. If not properly protected, these logs may not be admissible during a prosecution.
b. Audit logs contain sensitive data and should only be accessible to a certain subset of people.
c. Intruders may attempt to scrub (clean) the logs to hide their activities.
d. The format of the logs should be unknown and unavailable to the intruder.

A system administrator configures a honeypot to track malicious user activity. The administrator installs the host in the DMZ without any patches and configures a web site and an SMTP server on it. The administrator has configured nothing else on the host. Identify a problem with this configuration.

a. The honeypot needs to be patched.
b. Honeypots should not run a web site.
c. Honeypot logs should be forwarded to another secured host.
d. Honeypots should not run SMTP services

A system administrator configures a honeypot to track malicious user activity. The administrator installs the host in the DMZ without any patches and configures a web site and an SMTP server on it. The administrator has configured nothing else on the host. Identify a problem with this configuration.

a. The honeypot needs to be patched.
b. Honeypots should not run a web site.
c. Honeypot logs should be forwarded to another secured host.
d. Honeypots should not run SMTP services

Harrison is evaluating access control products for his company. Which of the following is not a factor he needs to consider when choosing the products?

a. Classification level of data
b. Level of training that employees have received
c. Logical access controls provided by products
d. Legal and regulation issues

Harrison is evaluating access control products for his company. Which of the following is not a factor he needs to consider when choosing the products?

a. Classification level of data
b. Level of training that employees have received
c. Logical access controls provided by products
d. Legal and regulation issues

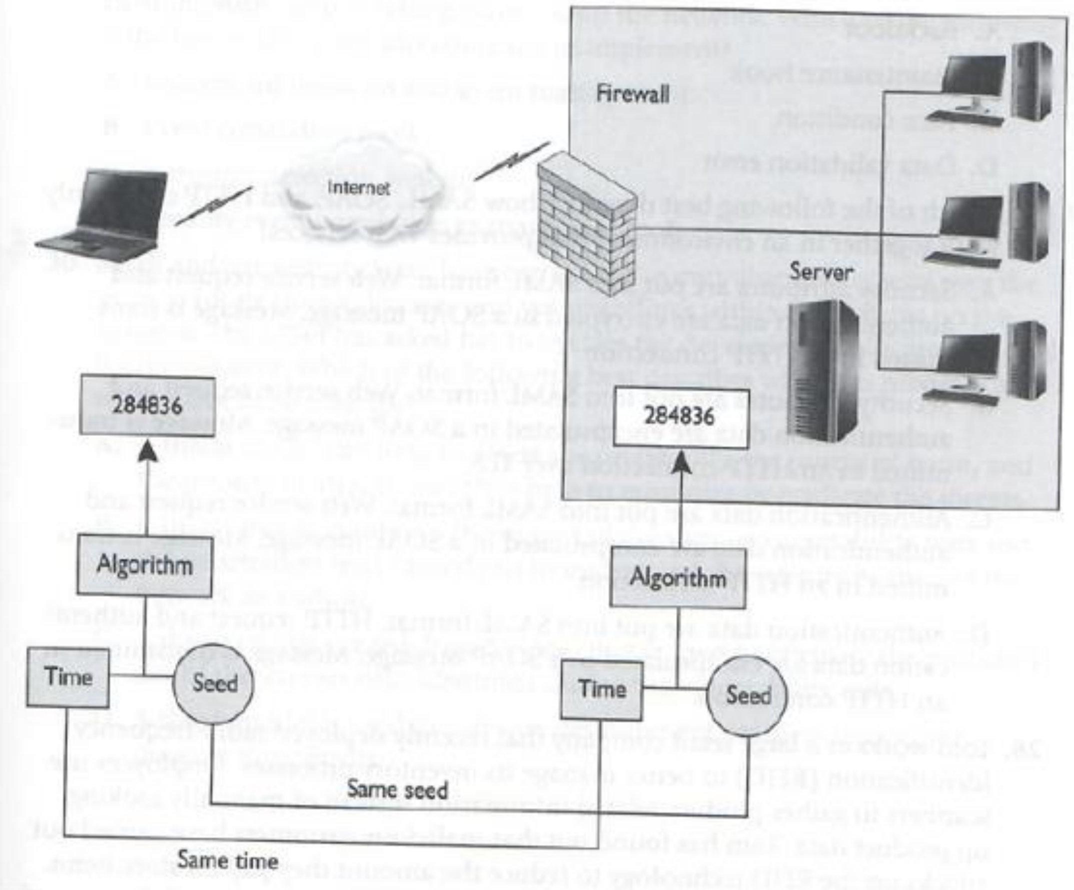
There are several types of intrusion detection systems (IDSs). What type of IDS builds a profile of an environment's normal activities and assigns an anomaly score to packets based on the profile?

a. State-based
b. Statistical anomaly-based
c. Misuse-detection system
d. Protocol signature-based

There are several types of intrusion detection systems (IDSs). What type of IDS builds a profile of an environment's normal activities and assigns an anomaly score to packets based on the profile?

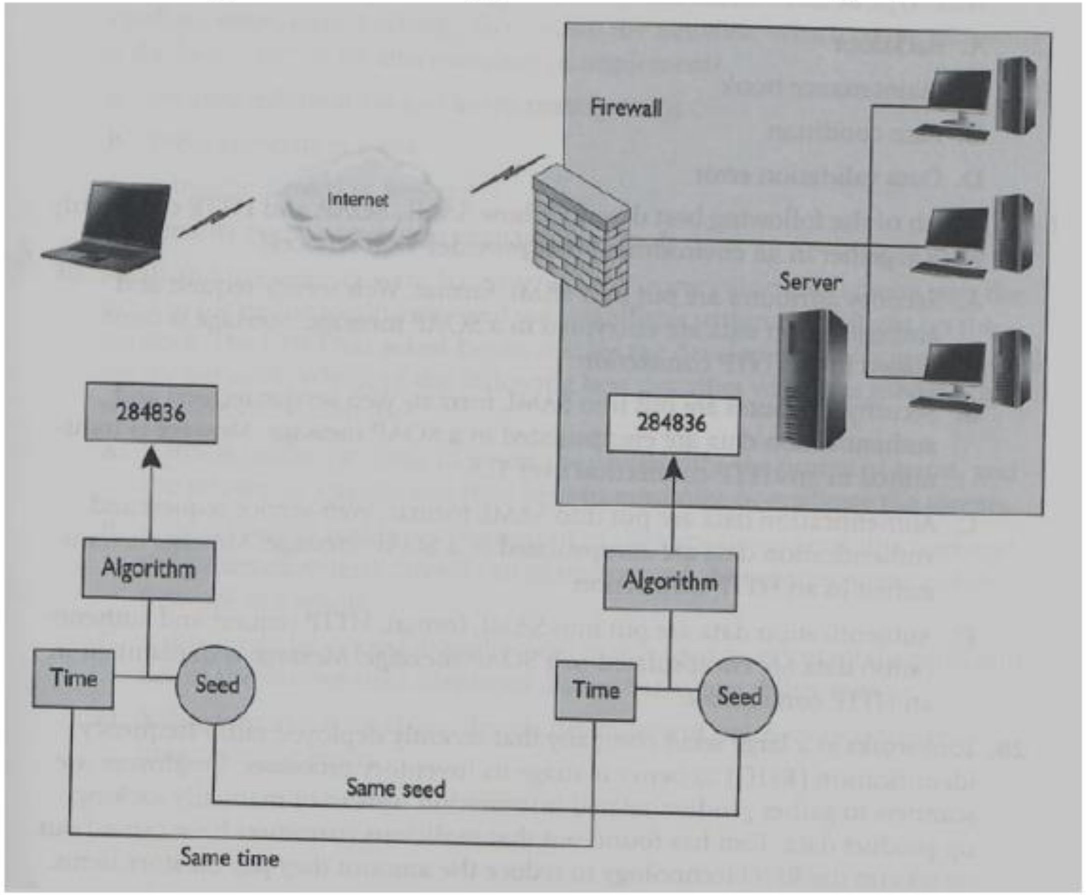
a. State-based
b. Statistical anomaly-based
c. Misuse-detection system
d. Protocol signature-based

There are different ways that specific technologies can create one-time passwords for authentication purposes. What type of technology is illustrated in the graphic that follows?



a. Counter synchronous token
b. Asynchronous token
c. Mandatory token
d. Synchronous token

There are different ways that specific technologies can create one-time passwords for authentication purposes. What type of technology is illustrated in the graphic that follows?



a. Counter synchronous token
b. Asynchronous token
c. Mandatory token
d. Synchronous token

MIS 5214

Weeks 11 & 12